REFERENCES

[Barbara2003] Barbara J. Page 3 – 4 of *Hidden Collections, Scholarly Barriers*, Association of Research Libraries Task Force on Special Collections, 2003 http://www.arl.org/bm~doc/hiddencollswhitepaperjun6.pdf

[Bradly et. al.]Bradly. K, Lei. J, Blackall C. Page 11 of *Memory of the World: Towards an Open source Repository and Preservation System,* United Nations Educational, Scientific and Cultural Organization (UNESCO), Paris, June 2007

[Bushey 2011] Bushey J. Page 02 *of International Council on Archives (ICA) "Access to Memory" (AtoM): Open-source software for archival description,* Archivi& Computer article for ICA-AtoM version 1.2, 2011

[Cenzic 2012]CenzicInc, Page 3-11 of *White Paper – Application Security Trends Report,* Cenzic Publication, California, USA, 2012

[Finkelstien et. al. 1990] Finkelstein A, Kramer J, Goedicke M. *Viewpoint Oriented Software Development* Proc. Of Third Int. Workshop on Software Engineering and its Applications, Toulouse, December 1990

[Fonseca 2007]Fonseca J, Pages 365-372 of the paper *Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on 17-19 December 2007,* Conference Publication, 2007

[Galbraith 1948] Galbraith V. H Page 03 of *Studies in the Public Records.*Thomas Nelson, London, 1949

[Gordon 2003] Gordon, M. Page 184 of *Optimization of Economic Analysis,* Rutledge Taylor and Francis Group Inc. 2003

[Harris 2010] Harris, Shon, Page 1000 of *All in one CISSP: Exam Guide – Fifth Edition,* Tata-McGrow Hill, New Delhi, 2010

[Hawryszkiewycz 1999a] Hawryszkiewycz I, Page 74 of *System Analysis and Design – Forth Edition,* Printice-Hall, Australia, 1999

[Hawryszkiewycz 1999b] Hawryszkiewycz I, *System Analysis and Design – Forth Edition,* Printice-Hall, Australia, 1999

[Hawryszkiewycz 1999c] Hawryszkiewycz I, Page 133 of *System Analysis and Design – Forth Edition,* Printice-Hall, Australia, 1999

[Helfert 2003] HelfertEric A. Page 257 of *Techniques of Financial Analysis: A Guide to value Creation,* Tata-McGrwHillInc, 2003

[ICA 2000] International Council on Archives, *International Standard for Archival Description (General), 2nd ed.*, Ottawa, 2000.

[ICA2 2000] International Council on Archives Page 07 of, *International Standard for ArchivalDescription (General), 2nd ed.*, Ottawa, 2000.

[ICA3 2000] International Council on Archives Page 08 of, *International Standard for ArchivalDescription (General), 2nd ed.*, Ottawa, 2000.

[Kerzner 2003] Kerzner, H. page 556 of *Project Management: A Systems Approach to Planning, Scheduling and Controlling.* John Wiley & Sons Inc. 2003

[Lavoie 2000] Lavoie B, Page 26-30 of *Meeting the challenges of digital preservation: The OAISreference model*, OCLC Newsletter, 2000

[McKemmish 1999] Sue McKemmish, et al, Page 08 of *Describing Records in Context in the Continuum:The Australian Recordkeeping Metadata Schema*, Archivaria, no. 48, Fall 1999

[Powers 1991] Powers, M. J, Castelino, M. G, Page 91 of *Inside the Financial Futures Market,* John Wiley & Sons, 1991

[Pressman 2001a] Pressman, Rodger S, Page 479 of *Software Engineering – A Practitioners Approach – Fifth Edition,* The McGraw-Hill Companies, Inc. 2001 ISBN:0-07-118458-9

[Pressman 2001b] Pressman, Rodger S, Page 465 of *Software Engineering – A Practitioners Approach – Fifth Edition,* The McGraw-Hill Companies, Inc. 2001 ISBN:0-07-118458

[RAD2008a] Page 15 of *Rules for Archival Description – Revised Version*, Canadian Committee of Archival Description: Bureau of Canadian Archivists, Ontario, 2008

[RAD2008b] Page xvii of *Rules for Archival Description – Revised Version*, Canadian Committee of Archival Description: Bureau of Canadian Archivists, Ontario, 2008

[RAD2008c] Page xxii of *Rules for Archival Description – Revised Version*, Canadian Committee of Archival Description: Bureau of Canadian Archivists, Ontario, 2008

[SA 1996] Standards Australia, *Records Management*, AS 4390, Homebush, 1996.

[Sibille and Fonseca 2011] Siblle C, da Fonseca V, Page 73/ 74 of *ICA-AtoM Software Presentation,* CITRA 2011 conference, Toledo, France, 2011

[Spiro1 1994] Spiro L, *Archival Management Software – A Report for the Council on Library and Information Resources. Council on* Library and Information, 2009

[Sommerville 2004a] Sommerville I, *Software Engineering – Seventh Edition,* Pearson Educations Ltd.

[Sommerville 2009] Sommerville I, Page 563 of *Software Engineering – Eighth Edition,* Pearson Educations Ltd.2009

[VanGarderen 2009a] VanGarderen . P. Page 16 of *The ICA-AtoM Project and Technology, Presentation at Association of Brazilian Archivists*, Third Meeting on Archival Information Databases, Rio De Janiero, Brazil. 16/17 March 2009

[VanGarderen 2009b] VanGarderen . P. Page 30 of *The ICA-AtoM Project and Technology, Presentation at Association of Brazilian Archivists*, Third Meeting on Archival Information Databases, Rio De Janiero, Brazil. 16/17 March 2009

[Wallace 2000] Wallace D, Page 253 – 269 of Archiving *Metadata Forum: Report from the Recordkeeping Metadata Working Meeting, June 2000*, Archival *Science*, vol. 1, no. 3, 2001

[Walch 1994] Walch V I*Standards for Archival Description – A Handbook.*The Society of American Archivists, 1994

[WWW1] Department of National Archives

http://www.archives.gov.lk/web/index.php?lang=en

[WWW2] Glossary of Library & Internet Terms, University of South Dakota Website
http://www.usd.edu/library/instruction/glossary.shtml

[WWW3] Wikipedia, the Free Encyclopedia – Archivist
http://en.wikipedia.org/wiki/Archivist

[WWW4] Wikipedia, the Free Encyclopedia – Archival Science
http://en.wikipedia.org/wiki/Archival_science

[WWW5] Wikipedia, the Free Encyclopedia – Archival Processing
http://en.wikipedia.org/wiki/Archival_processing

[WWW6] International Council for Archives
http://www.ica.org/

[WWW7] Wikipedia, the Free Encyclopedia – Respect des Fonds
http://en.wikipedia.org/wiki/Respect_des_fonds

[WWW8] Professional Exchange of Canada – Summary "Rules for Archival Description"
http://www.pro.rcip-chin.gc.ca/

[WWW9] Worldwide Web Consortium - Metadata
http://www.w3.org/Metadata/

[WWW10] National Archives of Australia - Glossary
http://www.naa.gov.au/records-management/publications/glossary.aspx

[WWW11] Dublin Core – Metadata Initiative
http://dublincore.org/

[WWW12] The ICA-AtoM – Documentation for release 1.3
https://www.ica-atom.org/doc/Release_1.3

[WWW13] Wikipedia, the Free Encyclopedia – Symfony
http://en.wikipedia.org/wiki/Symfony

[WWW14] Quebit – the Information Management Toolkit – Quebit, ICA-AtoM or DCB?
https://www.qubit-toolkit.org/wiki/Qubit,_ICA-AtoM_or_DCB%3F

[WWW15] The ICA-Atom – What is ICA-AtoM?
https://www.ica-atom.org/doc/What_is_ICA-AtoM%3F

[WWW16] The ICA-Atom – Technical Requirements
https://www.ica-atom.org/doc/Technical_requirements

[WWW17] The ICA-AtoM – Virtual Appliance
https://www.ica-atom.org/doc/ICA-AtoM_virtual_appliance

[WWW18] PC Magazine Website
http://www.pcmag.com/encyclopedia_term

[WWW19] Wikipedia, the Free Encyclopedia – Feasibility Study
http://en.wikipedia.org/wiki/Feasibility_study

[WWW20] O'Reilly Website
http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html

[WWW21] Department of Computer Science, University of Massachusetts Website
http://www.anw-cs.umass.edu/rlr/terms.htm

[WWW22] Allen Website – Project Planning and Feasibility Analysis
http://www.members.aol.com/AllenWeb/planning.htm

[WWW23] EC-Council – Citified Ethical Hacker
http://www.eccouncil.org/courses/certified_ethical_hacker.aspx

[WWW24] University of Salford, Observational Studies, Website
http://www.chssc.salford.ac.uk/healthSci/resmeth2000/resmeth/observat.htm

[WWW25] Communications Security Establishment of Canada, Website
www.cse-cst.gc.ca/documents/services/csg.../csg-cspc1011-eng.pdf

[WWW26] Wikipedia, the Free Encyclopedia - Reliability Engineering
http://en.wikipedia.org/wiki/Reliability_engineering#cite_note-1

[WWW27] Wikipedia, the Free Encyclopedia –Robustness
http://en.wikipedia.org/wiki/Robustness

[WWW28] OWASP – Open Web Application Security Project: SQL Injection
https://www.owasp.org/index.php/SQL_Injection

[WWW29] Tech Republic – 10 things you should do to secure Apache
http://www.techrepublic.com/blog/10things/10-things-you-should-do-to-secure-apache/477

[WWW30] OWASP – OWASP Top Ten Project
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[WWW31] Department of National Archives – The Overview
http://www.archives.gov.lk/web/

[WWW32] Department of National Archives – Services
http://www.archives.gov.lk/web/index.php?option=com_content&view=article&id=78&Itemid=87&lang=en

[WWW32] Process Renewal Group – Evolutionary Prototype for Client-Server Applications
http://www.processrenrewal.com/courses/sdpcs98.htm

[WWW33] Network World – Researches find security flaw in SHA-1 Algorithm
http://www.networkworld.com/news/2005/0216reseafind.html

[WWW34] OWASP – Guide Project
https://www.owasp.org/index.php/OWASP_Guide_Project

[WWW35] Wikipedia, the Free Encyclopedia – Phishing
http://en.wikipedia.org/wiki/Phishing

[WWW36] Marcus, R. Wiscom Technology. *Six things to consider before a major software implementation.* Websitehttp://www.westechnology.com/article.php?id=2749

[WWW37] Wikipedia, the Free Encyclopedia – Notepad ++
http://en.wikipedia.org/wiki/Notepad%2B%2B

[WWW38] Wikipedia, the Free Encyclopedia – NetBeans
http://en.wikipedia.org/wiki/NetBeans

[WWW39] NetBeans website - About
https://netbeans.org/about/index.html

[WWW40] Wikipedia, the Free Encyclopedia - phpMyAdmin
http://en.wikipedia.org/wiki/PhpMyAdmin

[WWW41] Purpose of CentOS – The CentOS website
http://www.centos.org/modules/tinycontent/index.php?id=3

[WWW42] Nmap Security Scanner
http://nmap.org/

[WWW43] Wikipedia, the Free Encyclopedia – Metasploit Project
http://en.wikipedia.org/wiki/Metasploit_Project

[WWW44] Wikipedia, the Free Encyclopedia – CentOS
http://en.wikipedia.org/wiki/CentOS

[WWW45] Oracle – Java SE Documentation - KeyTool
http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html

[WWW46] The Sunday Times – Online Edition – Cyber Attacks continue, state documents vulnerable
http://www.sundaytimes.lk/130210/news/cyber-attacks-continue-state-documents-vulnerable-32684.html

[WWW47] Lanka Journal Newspaper – Online Edition – Sri Lankan Government Websites hits in spite of attacks.
http://www.lankajournal.com/2013/01/sri-lanka-govt-web-sites-hit-in-spate-of-attacks/

[WWW48] E Hacking News – Online Journal
http://www.ehackingnews.com/2013/01/srilankan-ports-authority-site-breached.html

[WWW49] Wikipedia, the Free Encyclopedia – Vulnerability Scsnner
http://en.wikipedia.org/wiki/Vulnerability_scanner

[WWW50] Wikipedia, the Free Encyclopedia – DoS Arrack
https://en.wikipedia.org/wiki/Denial-of-service_attack

[WWW51] Open Web Application Security Project – OWASP Top 10
https://www.owasp.org/index.php/Top_10_2013-Top_10

APPENDIX A

SYSTEM DOCUMENTATION

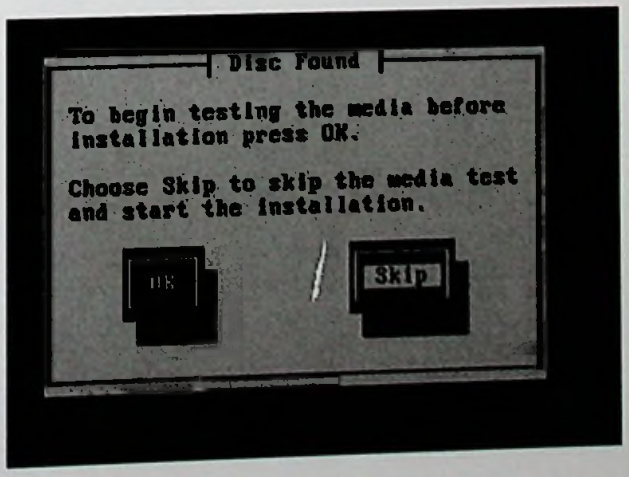
▪ INSTALLATION OF CENTOS

CentOS is the foundation to the Secured ICA-AtoM software and provide the 100% binary compatibility **[WWW44]** with the upstream source provider, Red Hat Enterprise Linux (RHEL). The following pictorial guidance helps to install and configure CentOS release 6.3 correctly.

- Boot the computer with CentOS 6.3 operating system installation DVD. On the boot up screen select '*Install or Upgrade an existing System*' from the menu as represented in Figure A-1.

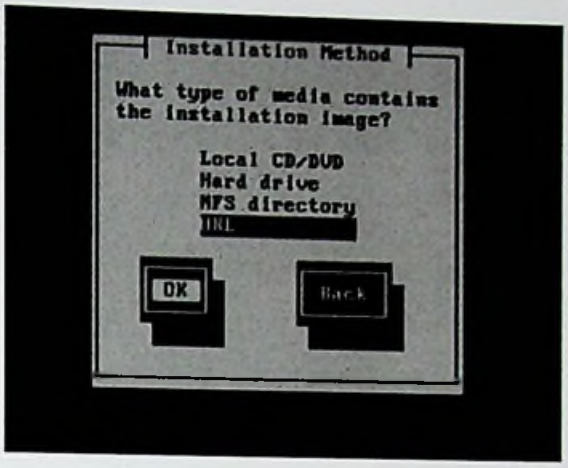
- Figure A-1 Boot up Screen of CentOS 6.3 -

- On the next screen – Select *Skip Media Test* as it may take long time to check media.



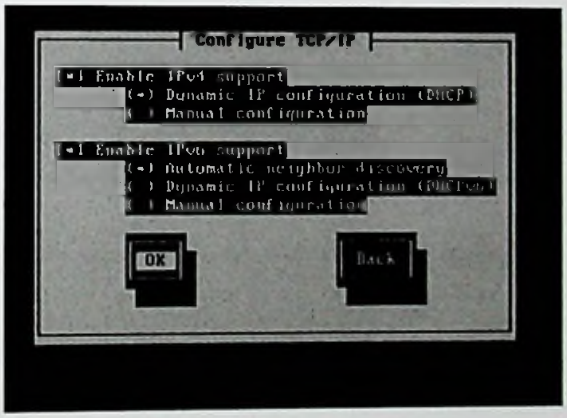
- Figure A-2 Skip Media Test -

- Select the installation method as Local CD/DVD. Shown in the Figure A-3.



- **Figure A-3 Select Installation Media** -

- Select *DHCP Configuration* on 'Enable IP v4 Support' from TCP/IP Configuration dialog box as shown in Figure A-4.

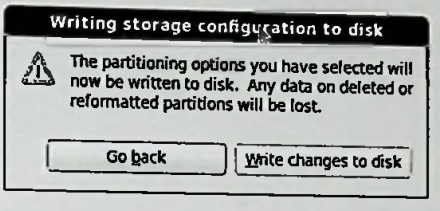


- **Figure A-4 Network Configuration** -

- Click Next, the GUI of the CentOS 6.3 installation will appear. This is illustrated in Figure A-5.

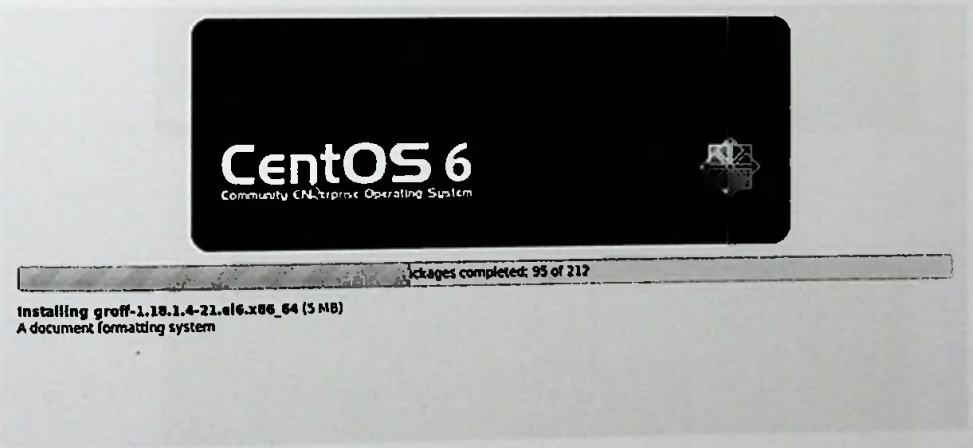
- **Figure A-5 Begin of GUI Installation Screens** -

- The rest of the installation process will take through the basic configuration of *Keyboard and Mouse, Language Selection, Storage Devices and partitioning, Host Name and root password.* Once the configuration is over, the installation asks for the confirmation of writing data to the Disk as depicted in Figure A-6. Select *Write Changes.*



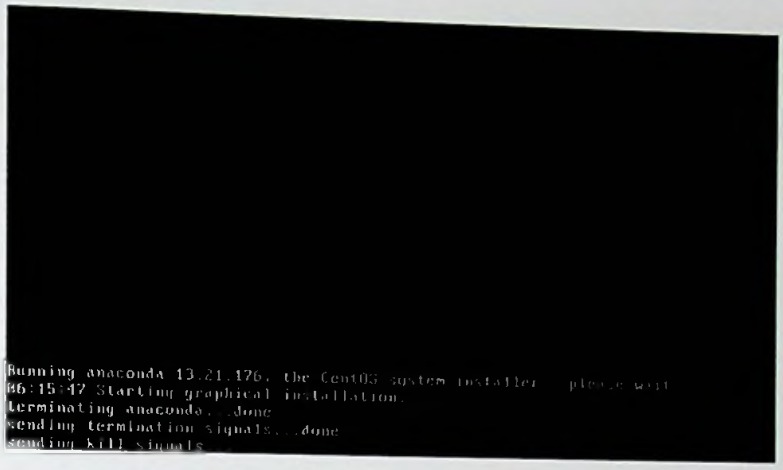
- **Figure A-6 Write Storage Configuration to disk** -

- The installation process of CentOS 6.3 will started. This process takes approximately 10 – 15 minutes. Figure A-7 depicts the installation progress and once the installation is complete, it will show the installation complete dialog box leading to *Reboot* as shown in Figure A-8.

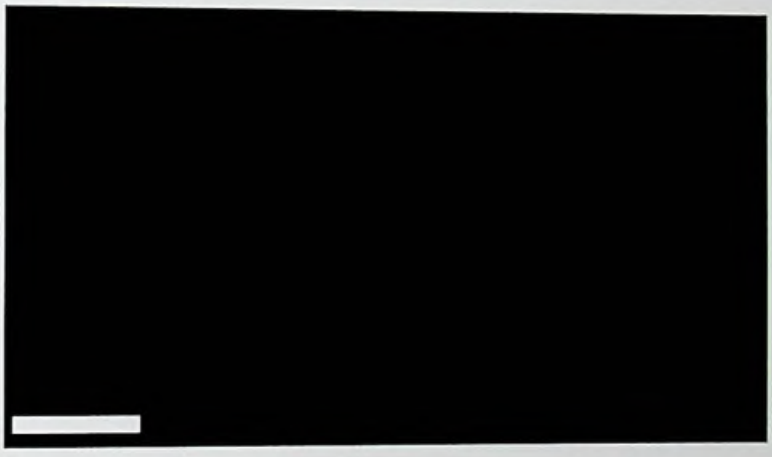


- **Figure A-7 Installation Progress** -

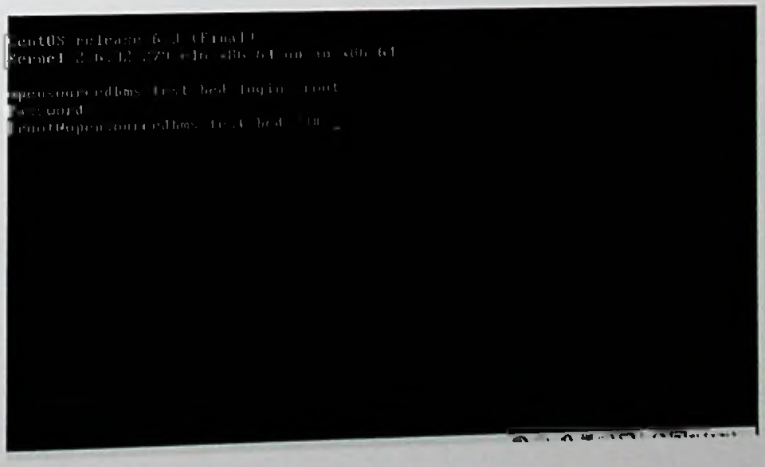
- Once the installation is complete, it will reboot. Once the system startup it will take to the log in console. This process illustrated in Figure A-9 to A-11.



- **Figure A-8 CentOS Rebooting Process** -



- **Figure A-9 CentOS Start-up** -



- **Figure A-10 CentOS Log in Prompt** -

As illustrated in Figure A-11, the root password is required to log in to the enable mode.

▪ INSTALLATION OF ICA-AtoM

ICA AtoM is a web based application which runs on designated server computer. Being the application is database driven and web based which is written in PHP, the system should assured to have Web Server, Database Server and PHP Programming language installed in the system before installing the binary files of ICA-AtoM.

Accordingly first few steps of ICA-AtoM installation process involves setting up th prerequisites such as installing Apache HTTP Server, PHP and MySQL.

▪ Install Apache httpd on CentOS

1. Install Apache httpd server
   `yum install httpd` ENTER

2. Set the Apachehttpd server to start on boot.
   `chkconfig --levels 235 httpd on` ENTER

3. Enable name based virtual hosting on port 80
   a. Open the httpd configuration file located at `etc/httpd/conf/httpd.conf`
   b. Un-comment the line containing the text **`NameVirtualHost *:80`**
   c. Save the File
   d. Restart the Apache httpd server daemon **`service httpd restart`** ENTER

▪ Install PHP on CentOS

1. Install PHP in Apache module

   `yum install php` ENTER

2. Restart the Apache
   `servicehttpd restart` ENTER

- **Install MySQL on CentOS**

1. Install MySQL using the following command
   yum install mysqlmysql-server ENTER

2. Create the system start-up links for MySQL (so that MySQL starts automatically whenever the system boots) and start the MySQL server.
   chkconfig --levels 235 mysqld on ENTER
   /etc/init.d/mysqld start ENTER

3. Set the password for MySQL root account.
   mysql_secure_installation ENTER
   ...
   Enter current password for root (enter for none):
   OK, successfully used password, moving on...

   Setting the root password ensures that nobody can log into the MySQLroot user without the proper authorisation.

   Set root password? [Y/n] ENTER
   New password: <-- yourrootsqlpassword ENTER
   Re-enter new password: <-- yourrootsqlpassword ENTER
   Password updated successfully!
   Reloading privilege tables..
   ... Success!

   ...
   Remove anonymous users? [Y/n] ENTER
   ... Success!
   Disallow root login remotely? [Y/n] ENTER
   ... Success!

   Remove test database and access to it? [Y/n] ENTER
   - Dropping test database...
   ... Success!

```
 - Removing privileges on test database...
 ... Success!

Reload privilege tables now? [Y/n] ENTER
 ... Success!

Cleaning up...
```

4. Create Database for ICA-AtoM Repository

```
mysql-p
mysql> create database icaatom; ENTER
exit;
```

- **Install ICA-AtoM**

1. Unload and Unpack ICA-AtoM software by downloading from the URL given below.

```
wget http://pear.qubit-toolkit.org/get/icaatom-1.3.0.tgz ENTER
```

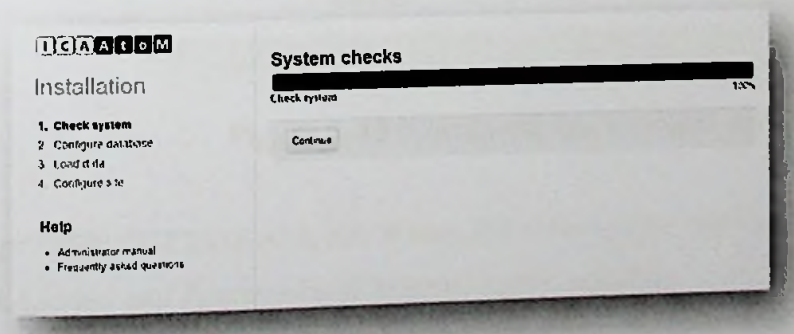
2. Move the ICA-AtoM installation directory.

```
tar-xvf icaatom-1.3.0.tgz ENTER
icaatom-1.3.0 cd && mv * / var / www / html ENTER
```

3. Change the SELINUX contexts.

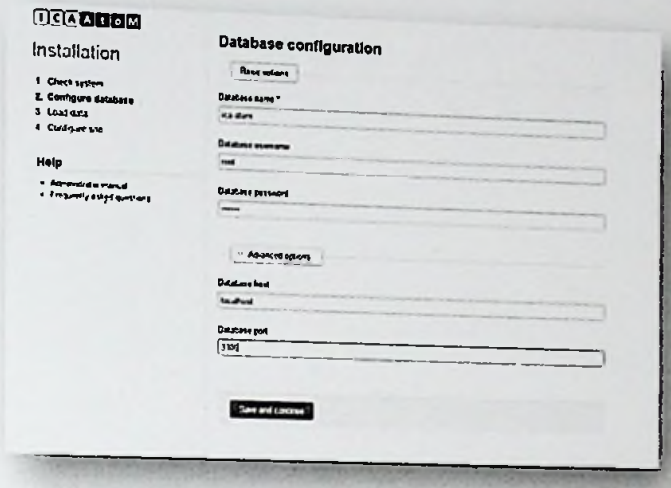
```
restorecon-R html /
chcon-u system_u html /-R
chownapache.apache html /-R ENTER
```

4. Begin installing ICA-AtoM via web console by accessing, `http://localhost`



- **Figure A-11 ICA-AtoM Web Installation start screen -**

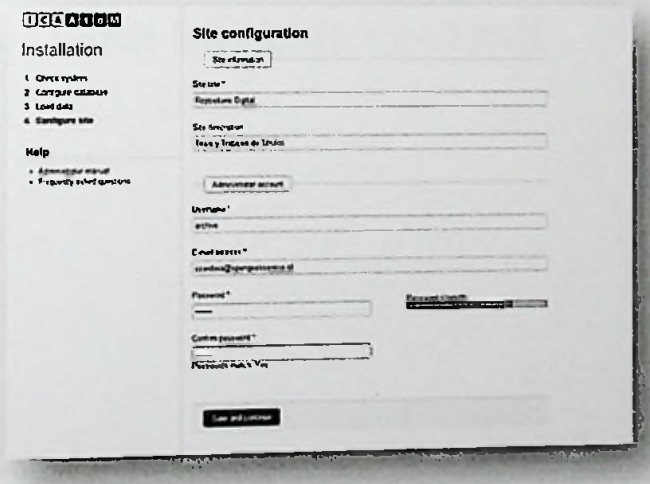
5. Configure the Database



- Figure A-12 ICA-AtoM Database Configuration -

As depicted in the Figure A12, *Database Name, Database username, Database Password, Host and Port* details will be given on this window.

6. Configure the ICA-AtoM Site.



- Figure A-13 ICA-AtoM Site Configuration -

As depicted in the Figure A13, *Site Name, Site Description, Administrator User Name, Email Address and Password* will be given on this window.

7. Once it set up the password, the ICA-AtoM is ready to launch. The particular site can be access via http://*ip_address*/ica/index.php.

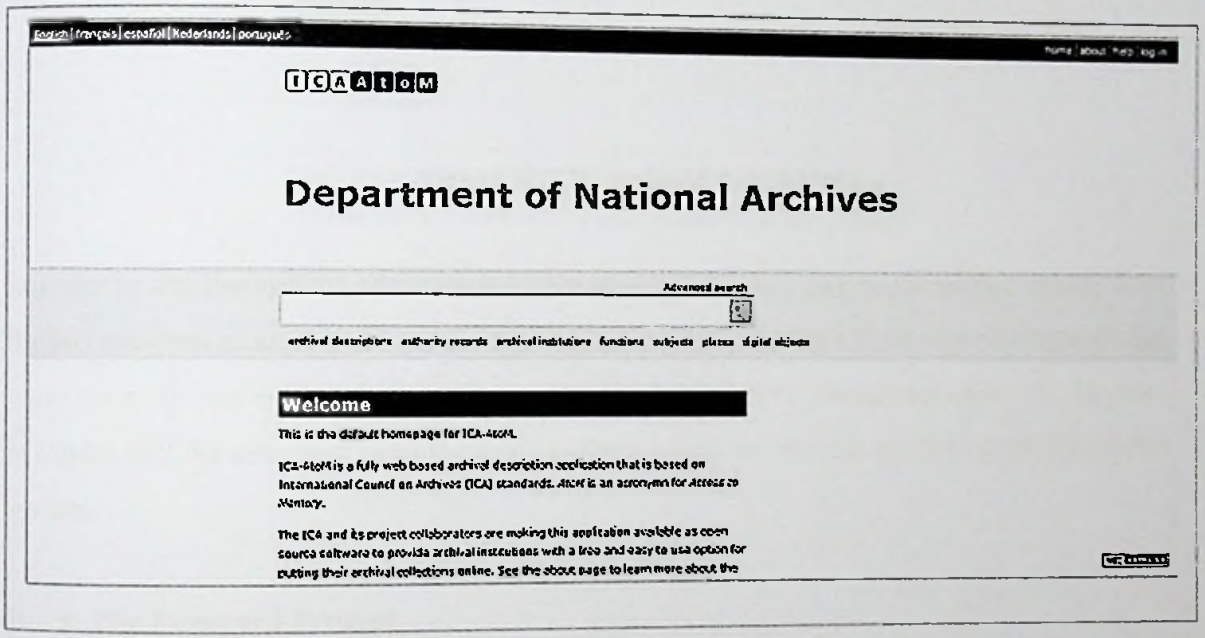
APPENDIX B

USER DOCUMENTATION

USER INTERFACE AND FUNCTIONALITY DOCUMENTATION FOR THE SECURED ICA-AtoM

The scope of the user documentation of Security Enhanced ICA-AtoM software is limited to the new functionality and security hardened modules of the system. This chapter is not intended to cover the overall functionality of ICA-AtoM which the software has specifically being built for. For the comprehensive user documentation can be accessed through the ICA-AtoM official web site fetching the URL *https://www.ica-atom.org/doc/User_manual*

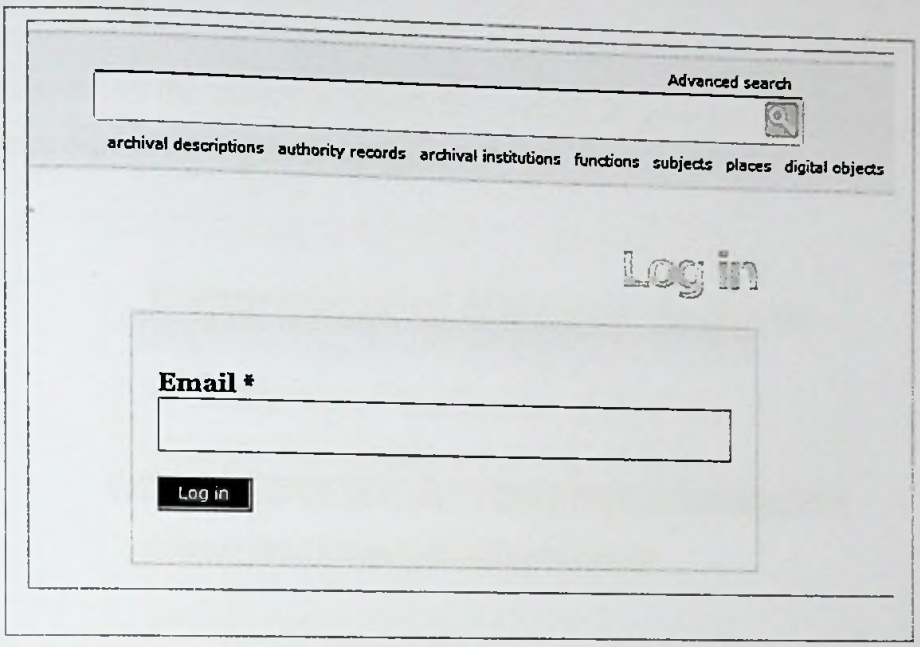
B – 1. The Index Page



- **Figure B-1 ICA-AtoM Index Page** -

The intended user or the administrator should access the system via the index page as illustrated in Figure B-1, above. In order to access the full functionality of the system the user should require to log in via the link provided top left corner of the index page.

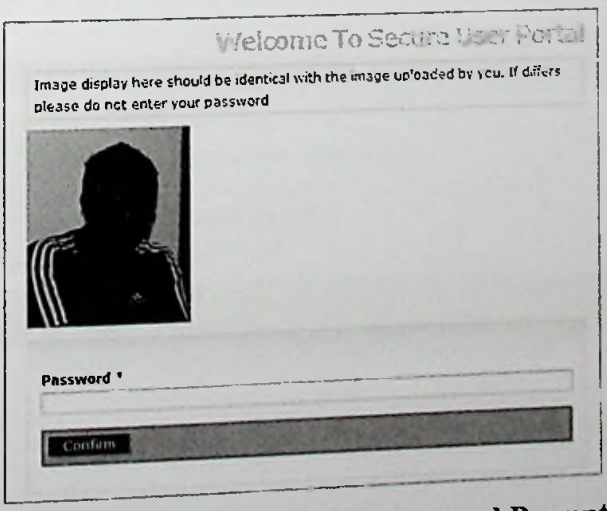
B – 2. The Login Page



- **Figure B-2 ICA-AtoM Login Page** -

In order to use the system, the intended user must provide his/ her email address within four limited attempts as each unsuccessful try, it gives an error message. Once the user exceeds the login tries, the session become expired and blocked the user for further attempts. As depicted in Figure B-2 the user must enter the email address which has already being registered with the system.

B – 3. The Password Prompt

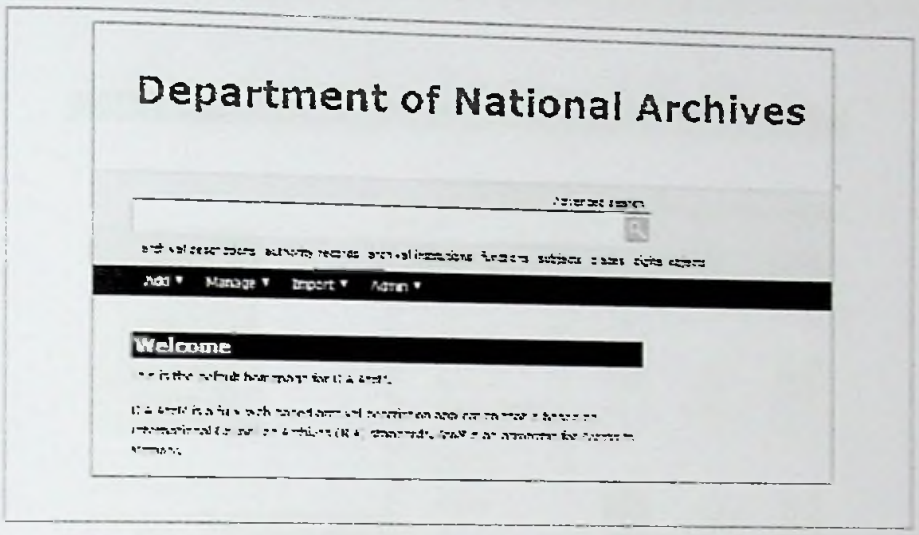


- **Figure B-3 ICA-AtoM Password Prompt** -

Once the user login with accepted email address he/ she will destined at the secure portal which prompts the secured image of the user. Accordingly the user gets the authority to check the

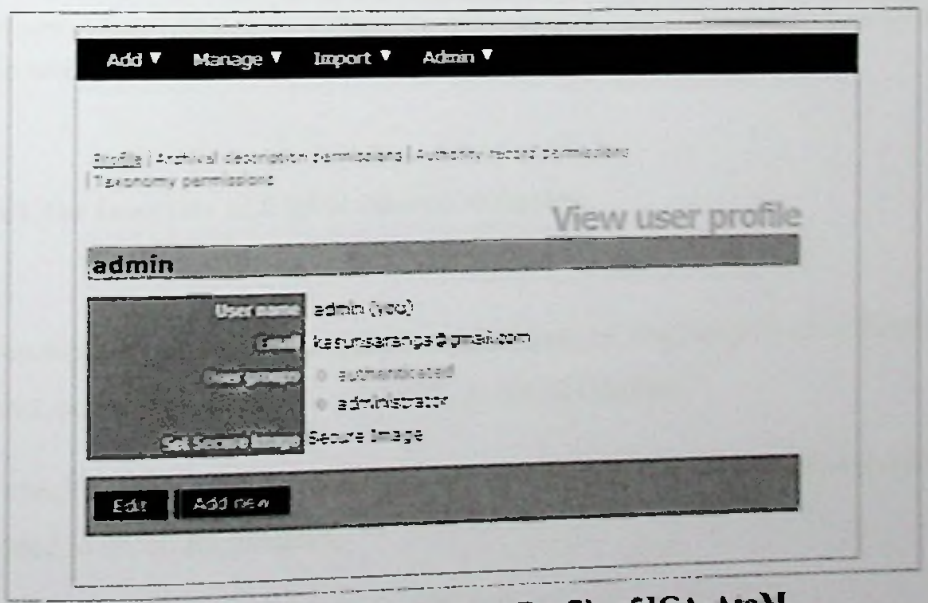
validity of the image which has been uploaded. If the image appears correctly, the user required to enter the password.

Once the user enters the correct password, the portal will direct the user to the ICA-AtoM Home Page as depicted in Figure B-4 below.



- Figure B-4 ICA-AtoM Home page -

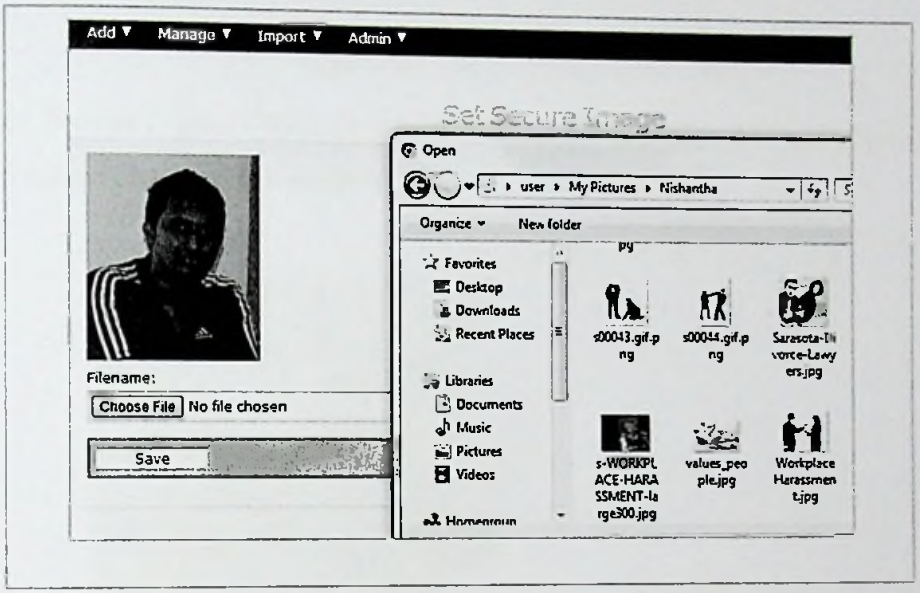
B – 4. Change Secured Image



- Figure B-5 View User Profile of ICA-AtoM -

In order to change the secured image, the user need to traverse *my profile* on the top left hand corner of the ICA-AtoM home page. It will open View User Profile Dialog Box with an option to 'Set the Secure Image'. This process illustrated in Figure (B-5) above.

Once the *Secure Image* URL clicks it will open up the uploaded secure image with an option to change the same. This process illustrated on the pictorial representation through Figure B-6.



- **Figure B-6 Change Secure Image** -

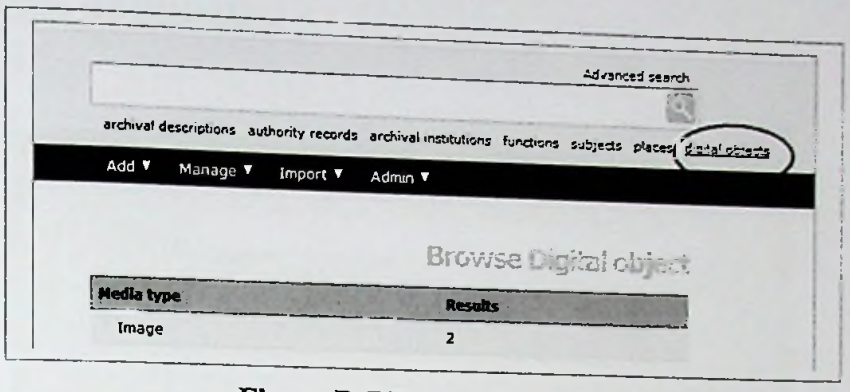
Once the secure image has been selected, the user needs to *'Save'* the image in order to activate it in next login.

B – 5. Check the Integrity of Digital Objects uploaded.

Archival Description can include an image or set of images. The integrity of such uploaded images cannot be evaluated through general ICA-AtoM interface.

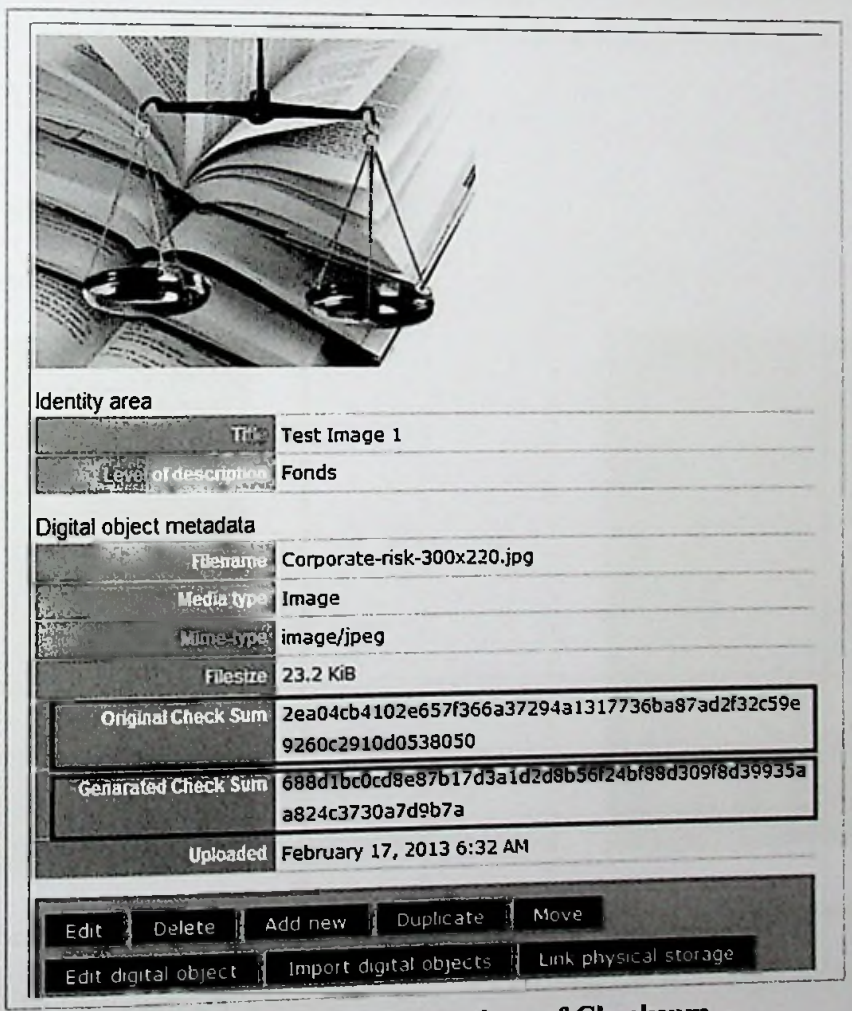
In order to check the image integrity, user needs to travers to *Digital Objects* and select the image intended to check for integrity.

This process has been illustrated in Figure B-7 below.



- **Figure B-7 Browse Digital Objects** -

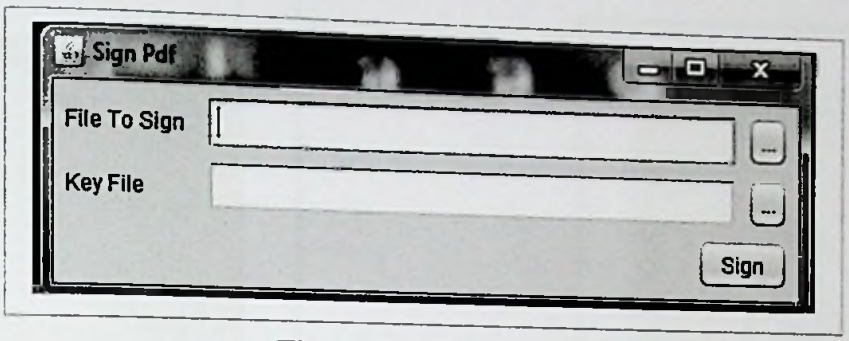
Once the user *Browse Digital Objects* it's required to click the image type and open the image that required checking for integrity.



- **Figure B-8 Comparison of Checksum** -

In order to check the integrity, user should compare the values given in *Original Check Sum* and *Generated Check Sum*. If the both values are not identical, then it can argue that the Original image has been tampered.

B – 6. Digitally Sign the Documents



- **Figure B-9 Sign PDF Toolkit** -

In order to Digitally sign the Document, the user required to browse and upload the file and the respective key file. Once the required files have been uploaded to the tool, press *Sign* Button.

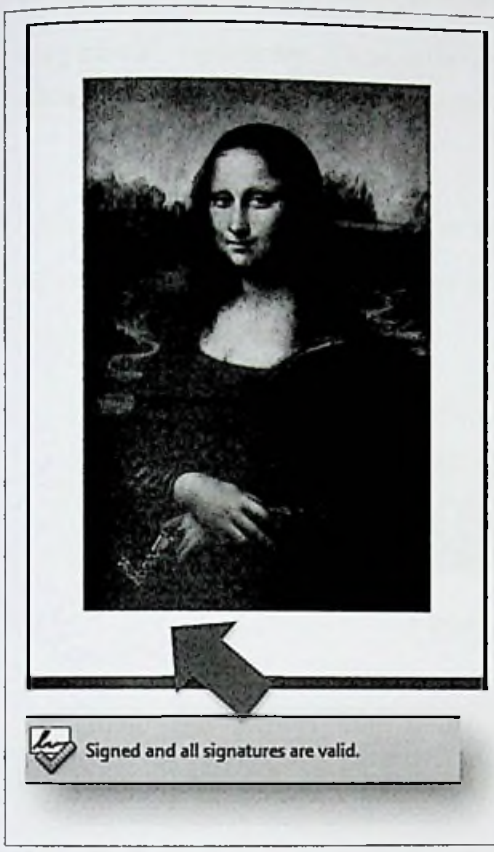
B – 7. Open Digitally Signed PDF documents

- **Figure B-10 Unsigned Document** -

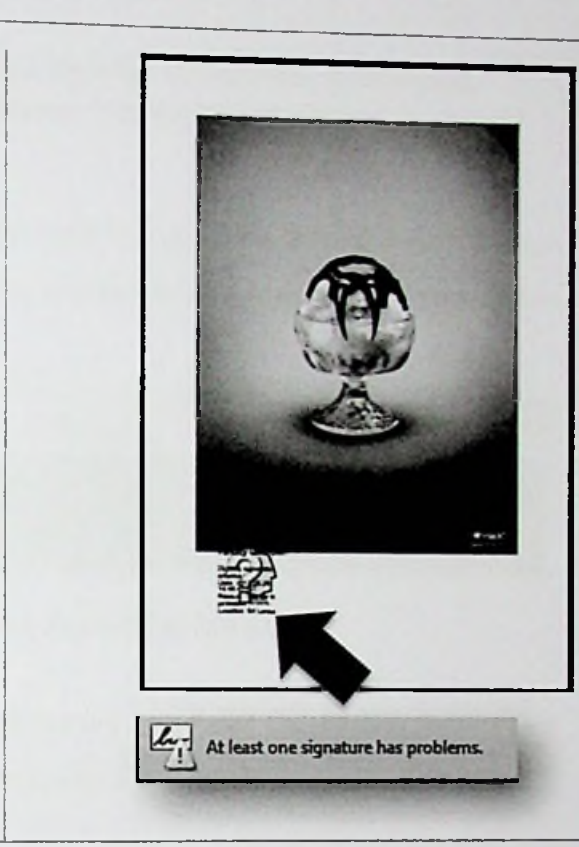
- **Figure B-11 Signed Document** -

The Signed *PDF* document can be viewed through any pdf viewer. As depicted in above two pictorial representation, the Figure (B-11) illustrate how the signed document successfully identified by the Adobe Reader.

B – 9. Checking the Adobe Reader Signature Panel Behavior.



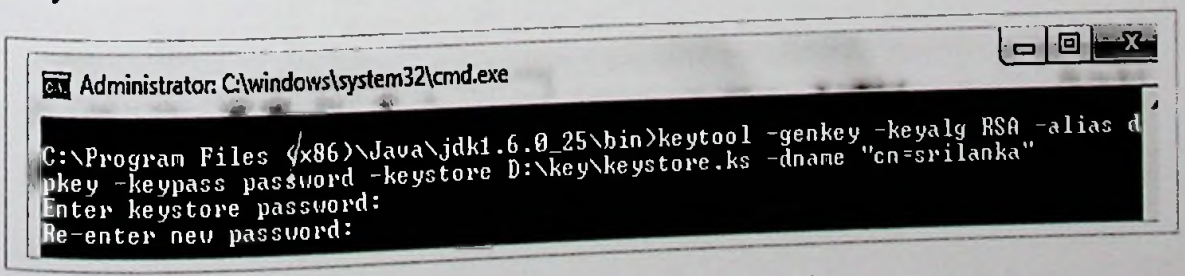
- **Figure B-12 Signed pdf with trusted signature panel** -



- **Figure B-13 Signed but unrecognized pdf with untrusted signature panel** -

B – 10. Create Signature Certificates

In order to generate key pare it is required to install Java SDK 6 in the local computer. The key pare will be generated using the *keytool – The Key and Certificate Management Tool* which is freely available with Java SDK 6 bundle.

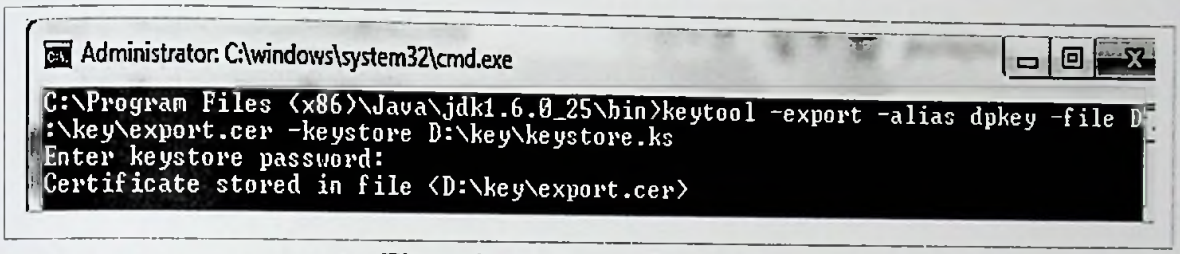


- **Figure B-14 Create a Key File** -

To create a *key file* type the following command in **C:\Program Files (x86)\Java\jdk1.6.0_25\bin>** prompt

```
keytool -genkey -keyalg RSA -alias dpkey -keypass password
-keystore D:\key\keystore.ks - dname "cn=srilanka"
```

This will generate a *keystore*file which can be used to sign the *pdf*document. However aexportcertificate (a Public Key) is required to generate based on the *private key* of the document sign authority.



- **Figure B-15 Create Export Certificate** -

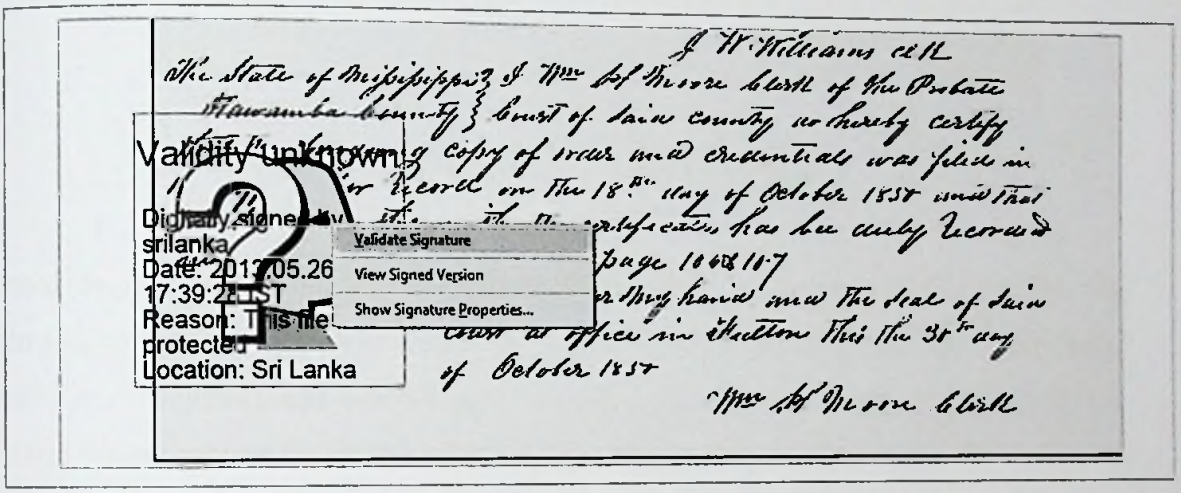
To create the *Export Certificate* type the following command in **C:\Program Files (x86)\Java\jdk1.6.0_25\bin>** prompt as illustrated in the Figure B-15.

```
keytool -export -alias dpkey -file D:\key\export.cer -keystore
D:\key\keystore.ks
Enter keystore password:
Certificate stored in file <D:\key\export.cer>
```

- **Figure B-16 Pair of Generated Keystore and Export Certificate** -

As illustrated in Figure B-16, the user requested to keep these two files handy and safely. The *Export.cer* is required to be emailed to the designated party in order to trust the identity in between. To trust the identity, the Acrobat or Reader is required to "trust" a signer's certificate. Hence it is required to configure a "trusted identity" by importing the signer's public key.

B – 11. Trust Identity in Adobe Reader

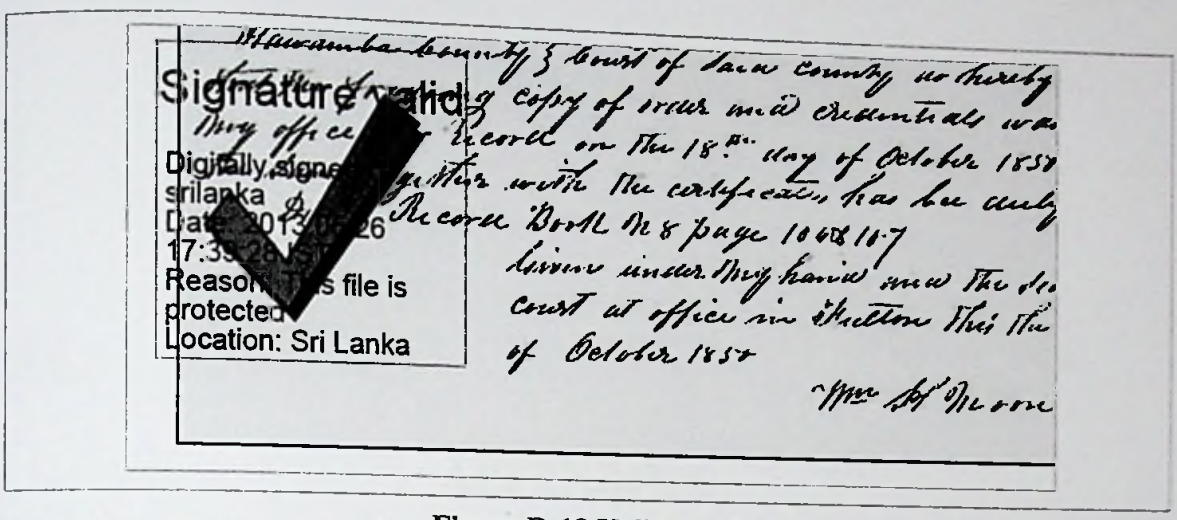


- **Figure B-17 Validating Untrusted Identity** -

To validate an untrusted identity as illustrated on Figure B-17, follow the following steps.

- Right click on the signed signature field
- Select "Validate Signature"
- Click "Signature Properties" button
- Select the "signer" tab (see screen shot)
- Click "Show Certificate" button
- Select the "Trust" tab
- Click the "Add to Trusted Identities" button
- Set the desired "trust" settings
- Click OK
- Right click on the signed signature field
- Select "Validate Signature" - you should now get the green check mark.

Once it follows the above steps, the untrusted document will become Trusted. This is illustrated on Figure (B-18) below.



- **Figure B-18 Validated Identity** -

Trusted identities in Acrobat\Reader are tied to the Windows account profile, this explains why when logged onto the system as *User1*, the signature shows a green check mark (the trusted identity is configured), and when logged onto the system as *User2*, the signature shows a different status, because the signers certificate has not been trusted under this profile. However when it checks the details about the signature (in the signatures pane) it will evidently prove that signature is trusted, but the signer is unknown (not trusted).

APPENDIX C

CODE LISTING

uploadImageAction.class.php

```
public function execute($request) {
      $this->resource = $this->getRoute()->resource;
      $this->form = new sfForm;
if (!$this->context->user->isAuthenticated()) {
         $this->redirect('@homepage');
      }
if ($request->isMethod('post')) {
         $allowedExts = array("jpg");
         $tmp = explode('.', $_FILES['file']['name']);
         $extension = end($tmp);
if ((($_FILES["file"]["type"] == "image/gif")
               || ($_FILES["file"]["type"] == "image/jpeg")
               || ($_FILES["file"]["type"] == "image/png")
               || ($_FILES["file"]["type"] == "image/pjpeg"))

&&in_array($extension, $allowedExts)) {
if ($_FILES["file"]["error"] > 0) {
               $this->form->getErrorSchema()->addError(new sfValidatorError(new
sfValidatorPass, $_FILES["file"]["error"]));
               ;
            } else {
echo $this->context->user->getUserID();
move_uploaded_file($_FILES["file"]["tmp_name"], "/var/www/html/ica/userimage/" . $this-
>context->user->getUserID() . ".jpg");


            }
         } else {
            $this->form->getErrorSchema()->addError(new sfValidatorError(new
sfValidatorPass, 'Invalid File')); }...
```

[Ref:uploadImageAction.class.php of /var/www/html/ica/apps/qubit/modules/user/actions]

uploadImageSuccess.php

```
.
.
.
<form action="uploadImage" method="post"
enctype="multipart/form-data">
.
.
.
<imgsrc=<?php echo "/ica/userimage/" . $this->context->user->getUserID() . ".jpg" ?>
title='Current' alt='You have not upload your secure Image' /><br>
<label for="file">Filename:</label>
<input type="file" name="file" id="file">
<div class="actions section">
<h2 class="element-invisible">
<?php echo __('Actions') ?></h2>
```

[Ref: uploadImageSuccess.php of /var/www/html/ica/apps/qubit/modules/user/templates]

Above code is mainly responsible of uploading the secured image and throw it to the *uploadImageAction.class.php* to do further validation of the uploaded image and store the same against the User ID.

loginNewAction.class.php

```
public function execute($request) {
      $this->form = new sfForm;
      $this->form->getValidatorSchema()->setOption('allow_extra_fields', true);

      // Redirect to @homepage if the user is already authenticated
if ($this->context->user->isAuthenticated()) {
         $this->redirect('@homepage');
      }

      $this->form->setDefault('next', '/ica/index.php/;user/login?email=' . $request-
>getParameter('email'));
      $this->form->setValidator('next', new sfValidatorString);
      $this->form->setWidget('next', new sfWidgetFormInputHidden);

      $this->form->setDefault('email', $request->getParameter('email'));
      $this->form->setValidator('email', new sfValidatorString);
      $this->form->setWidget('email', new sfWidgetFormInputHidden);

      $this->form->setValidator('password', new sfValidatorString(array('required' => true),
array(
            'required' => $this->context->i18n->__('You must enter your password'))));
      $this->form->setWidget('password', new sfWidgetFormInputPassword);

if ($request->isMethod('post')) {

         $this->form->bind($request->getPostParameters());
```

[Ref: loginNewAction.class.php of /var/www/html/ica/apps/qubit/modules/user/actions]

loginNewSuccess.php

.

.

.

```
<?php if ('user' != $sf_request->module || 'login' != $sf_request->action): ?>
<div class="messages status">
<?php echo __('Image display here should be identical with the image uploaded by you. If
differs please do not enter your password') ?>
</div>
<imgsrc=<?php echo "/ica/userimage/" . $this->context->user->getUserID() . ".jpg" ?>
title='Current' alt='You have not upload your secure Image. Please upload after login' />

<?phpendif; ?>
<?php echo $form->renderGlobalErrors() ?>
<?php echo $form->renderFormTag(url_for(array('module' => 'user', 'action' => 'loginnew')))
?>
<?php echo $form->renderHiddenFields() ?>
<fieldset>
<?php //echo $form->email->renderRow() ?>
<?php echo $form->password->renderRow() ?>
```

.

.

.

[Ref: loginNewSuccess.php of /var/www/html/ica/apps/qubit/modules/user/templates]

Above code is mainly responsible of uploading the secured image and throw it to the *loginNewAction.class.php* to validate the uploaded image against the email address provided to login to the Secured ICA-AtoM system.

loginAction.class.php

```
$this->form->setValidator('email', new sfValidatorEmail(array('required' => true), array(
    'required' => $this->context->i18n->__('You must enter your email address'),
    'invalid' => $this->context->i18n->__('This isn\'t a valid email address'))));
  $this->form->setWidget('email', new sfWidgetFormInput);

if ($request->isMethod('post'))
  {
    $this->form->bind($request->getPostParameters());

if ($this->form->isValid())
    {

// Password validation logic changed- Calling preauthenticate method instead of
authenticate

if ($this->context->user->preauthenticate($this->form->getValue('email')))
     {

if (null !== $next = $this->form->getValue('next'))
      {
       $this->redirect('/ica/index.php/;user/loginnew?email='.$this->form-
>getValue('email'));
      }

      //$this->redirect('@homepage');
}else{
       $this->form->getErrorSchema()->addError(new sfValidatorError(new
sfValidatorPass, 'Sorry, unknown  email addresss')); ...
```

[Ref: line no:34 of loginAction.class.php of /var/www/html/ica/apps/qubit/modules/user/actions]

loginSuccess.php

.
.
.

```
<?php if ('user' != $sf_request->module || 'login' != $sf_request->action): ?>
<div class="messages status">
<?php echo __('Please log in to access that page') ?>
</div> ...
```

.
.
.

```
<?php echo $form->email->renderRow() ?>
<?php//echo $form->password->renderRow() ?>
```

[Ref: line no:19 of loginSuccess.php of /var/www/html/ica/apps/qubit/modules/user/templates]

The password field of the login page has been removed as stated in the above code. This is to implement *two-factor-authentication* to the Secured ICA-AtoM software.

QubitUser.php

.
.
.

```
public function setPassword($password) {
    $salt = md5(rand(100000, 999999) . $this->getEmail());
    $this->setSalt($salt);
// Implemented SHA 512
    $this->setSha1Password(hash('sha512', $salt . $password));
```

.
.
.

[Ref: line no:84 of QubitUser.php of /var/www/html/ica/lib/model]

```
.
.
.
public static function checkCredentials($username, $password, &$error) {
      $validCreds = false;
      $error = null;
      // anonymous is not a real user
if ($username == 'anonymous') {
         $error = 'invalid username';
return null;
      } ...
// above code will check the credentials
```

[Ref: line no:179 of QubitUser.php of /var/www/html/ica/lib/model]

```
.
.
.
public static function checkUser($username, &$error) {

      $validCreds = false;
      $error = null;
      // anonymous is not a real user
if ($username == 'anonymous') {
         $error = 'invalid username';

return null;
      }

      $criteria = new Criteria;
      $criteria->add(QubitUser::EMAIL, $username);
      $user = QubitUser::getOne($criteria);
.
.
.
```

```
.
.
.
    // user account exists?
if ($user !== null) {

      // Stop if user is not active
if (!$user->active) {

          $error = 'inactive user';

return null;
        }

        // password is OK?
if (hash('sha512',$user->getSalt() . $password) == $user->getSha1Password()) {
          $validCreds = true;
        } else {
          $error = 'invalid password';
        }
    } else {
        $error = 'invalid username';
    }...
```

[Ref: line no:139 of QubitUser.php of /var/www/html/ica/lib/model]

myUser.class.php

.
.
.

```
public function presignIn($user)
 {
     $this->user = $user;
       //   foreach ($user->getAclGroups() as $group)
       //   {
       //     $this->addCredential($group->getName(array('culture' => 'en')));
       //   }

   $this->setAttribute('user_id', $user->id);
   $this->setAttribute('user_slug', $user->slug);
   $this->setAttribute('user_name', $user->username);
 }...
```

[Ref: line no:83 of myUser.class.php of /var/www/html/ica/lib]

Above code explicitly creates the *presignIn* function to be called on loginAction.class.php

.
.
.

```
public function preauthenticate($username)
 {
   $authenticated = false;
   // anonymous is not a real user
if ($username == 'anonymous')
   {
return false;
   }...
```

[Ref: line no:128 of myUser.class.php of /var/www/html/ica/lib]

Above code explicitly creates the *preAuthenticate*function to be called on loginAction.class.php

_metadata.php

.

.

.

```
<?php if (check_field_visibility('app_element_visibility_digital_object_checksum')): ?>
<?php echo render_show(__('Original Check Sum'), $resource->checksum) ?>
<?phpendif; ?>

<?php if (check_field_visibility('app_element_visibility_digital_object_path')): ?>
<?php echo render_show(__('Genarated Check Sum'),  hash_file($resource->checksumType,
'/var/www/html/ica'.$resource->path . $resource->name) ) ?>
<?phpendif; ?>
```

.

.

.

[Ref: line no:35 of _metadata.php of /var/www/html/ica/apps/qubit/modules/digitalobject/templates]

APPENDIX D

SECURING APACHE

SECURING APACHE FROM BRUTE FORCE AND DOS ATTACKS

In this chapter two great security modules which protect Apache server from brute force attacks and DOS attacks will be discussed. Further moving in to the installation guide, *Mod_Security* and *Mod_evasive*and its importancy will be discussed.

MOD_SECURITY

mod_Security is an open source web application firewall (WAF) and intrusion detection and prevention system for web applications. It is used to protect and monitor real time HTTP traffic and web applications from brute force attacks.

MOD_EVASIVE

mod_evasive is an open source evasive manoeuvres system for Apache server to provide evasive action in the event of an HTTP Brute Force, DOS or DDOS attack. It was designed to use as a network traffic detection and network management tool and can be easily configured and integrated into firewalls, ipchains, routers etc. Presently, it sends misuses reports via email and syslog facilities.

INSTALL MOD_SECURITY ON CENT OS 6.3

Step 1 – Installing Dependancies for mod_security

```
# yum install gcc make
# yum install libxml2 libxml2-devel httpd-develpcre-devel curl-devel
```

Step 2 – Installing mod_security

```
# cd /usr/src
# wget http://www.modsecurity.org/download/modsecurity-apache_2.6.6.tar.gz
# tar xzf modsecurity-apache_2.6.6.tar.gz
# cd modsecurity-apache_2.6.6
# ./configure
# make install
# cpmodsecurity.conf-recommended /etc/httpd/conf.d/modsecurity.conf
```

The above code need to be run as *root.*

Step 3 – Downloading OWASP mod_security Core Rule Set

For base configuration, Mod_Security requires Open Web Application Security Project core rules. to protect from unknown vulnerabilities which often found on web applications, these rules are essentially used. In order to download and install rule set for mod_security. Run the following commands.

```
# cd /etc/httpd/
# wget http://downloads.sourceforge.net/project/mod-security/modsecurity-crs/0-CURRENT/modsecurity-crs_2.2.5.tar.gz
# tar xzf modsecurity-crs_2.2.5.tar.gz
# mv modsecurity-crs_2.2.5 modsecurity-crs
# cdmodsecurity-crs
# cp modsecurity_crs_10_setup.conf.example modsecurity_crs_10_config.conf
```

Step 4 – Configuring mod_security

- Apache configuration files are required to modify in order to load the mod_security module. Hence the httpd.conf file is required to be edited.

  ```
  # vi /etc/httpd/conf/httpd.conf
  ```

- Search for the line *LoadModule* in the httpd.conf and below line should add at the bottom.

  ```
  LoadModule security2_module modules/mod_security2.so
  ```

- To set the basic rule set in the httpd.conf file. Following lines of code should add at the end of the file.

  ```
  <IfModule security2_module>
    Include modsecurity-crs/modsecurity_crs_10_config.conf
    Include modsecurity-crs/base_rules/*.conf
  </IfModule>
  ```

Next, restart the Apache service to enable mod_security module and their rules.

/etc/init.d/httpd restart

More information of *mod_security*can be obtained through accessing following links.
http://www.modsecurity.org/
https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project#tab=Installation

INSTALL MOD_EVASIVE ON CENT OS 6.3

Step 1 – Installing mod_evasive

cd /usr/src
wget http://www.zdziarski.com/blog/wp-content/uploads/2010/02/mod_evasive_1.10.1.tar.gz
tarxzf mod_evasive_1.10.1.tar.gz
cdmod_evasive
apxs -cia mod_evasive20.c

Step 2 – Configuring mod_evasive

- By default installation adds the following line of mod_evasive configuration to Apache configuration file. But this is essentially required to verify that the code is present. Otherwise the below line of code should add to the httpd.conf file.

  LoadModule evasive20_module /usr/lib/httpd/modules/mod_evasive20.so

- Add the mod_evasive configuration parameters to Apache configuration at the end. Replace given *email address* with security administrator's Email Id to get email alerts.

```
<IfModule mod_evasive20.c>
DOSHashTableSize    3097
DOSPageCount        2
DOSSiteCount        50
DOSPageInterval     1
DOSSiteInterval     1
DOSBlockingPeriod   60
DOSEmailNotifykasunsaranga@gmail.com
</IfModule>
```

- Next, restart the Apache service to enable mod_security module and their rules.

  # /etc/init.d/httpd restart

More information of *mod_evasive*can be obtained through accessing following link.

http://www.zdziarski.com/blog/?page_id=442

APPENDIX E

INTERNATIONAL STANDARD FOR ARCHIVAL DESCRIPTION (GENERAL)

International Standard for Archival Description (General)

ISAD (G) is the International Standard for Archival Description (General). It was developed by a Committee of the International Council on Archives. The Committee based its work where possible on existing national standards for archival description. The first edition came out in 1996 and it was revised in 2000.

ISAD defines the concept of hierarchical structure and states which data elements should be included at each level. But ISAD represents traditional values of approach rather than a detailed cataloguing standard. ISAD (G) is a rather general standard and it states that it should be used in conjunction with existing national standards or as a basis to develop them.

Four Principals of ISAD (G)

- Description proceed from General to Specific
- Information should be relevant to the description
- Description should be linked with levels
- Non-repetition of information

For International exchange of descriptive information, it has been identified six core elements **[ICA3 2000]**. Such that;

1. Reference Code
2. Title
3. Creator
4. Date
5. Extent of the unit of description
6. Level of Description

The complete 26 levels of data elements used by the ISAD (G) is as follows.

1. **Identity Statement Area**
   1.1. Reference code
   1.2. Title
   1.3. Date
   1.4. Level of Description

1.5. Extent and medium of level of description

2. **Context Area**
   2.1. Name of creator
   2.2. Administrative History
   2.3. Archival History
   2.4. Immediate source of acquisition or transfer
3. **Content and structure area**
   3.1. Scope and content
   3.2. Appraisal, destruction and scheduling information
   3.3. Accruals
   3.4. System of Arrangement
4. **Conditions of Accruals and Used Area**
   4.1. Condition of governing access
   4.2. Conditions governing reproduction
   4.3. Language/ scripts of material
   4.4. Physical characteristics and technical requirements
   4.5. Finding Aids
5. **Allied Material Area**
   5.1. Existence of Locations and Origins
   5.2. Existence of Location and Copies
   5.3. Related Units of Description
   5.4. Publication Notes
6. **Notes Area**
   6.1. Note
7. **Description Control Area**
   7.1. Archivist's Note
   7.2. Rules or Conventions
   7.3. Date of Description

APPENDIX F

TECHNICAL REQUIREMENTS OF ICA-ATOM

Technical Requirements of ICA-AtoM

The Browser

ICA-AtoM is platform independent software tool. In the development document, it has been described as "ICA-AtoM has been designed with minimal assumptions about the technology available to users and contributors. All that is required is access to the internet and a web browser. Any web browser will do." **[WWW16]**

However the software is much relies on JavaScript on the client side, it is much essential to use a browser which supports JavaScript. Supported web browsers are can be depicted as; Safari 4.0+, Firefox 3.5+, Google Chrome and Internet Explorer 8+. However the upcoming release of AtoM has announced that it's no longer supporting IE version 8 and earlier.

The Development Platform

Since the ICA-AtoM is a database driven, web based application and written in PHP the instructions assume that there should be a web server, database server and PHP programming language installed on the system. However the ICA-AtoM has tested and recommends having following configuration on the system for the smooth functioning of ICA-AtoM

Webserver	-	Apache HTTPD version 2.0 or 2.2
MySQL Database	-	MySQL version 5.0, 5.1 or 5.5
PHP	-	PHP version 5.3 or better

The Installation Platform

As we discussed above, the ICA-AtoM is platform independent software, its supports all Windows, Linux and Mac OS X versions. The ICA-AtoM recommends installing the software on Linux, specially on Ubuntu distro as it backed by large community support. However it's equally supports other major Linux distributions. Further it recommends installing WAMP

server on Windows environment and MAMP server on Mac OS X before installing the ICA-AtoM.

The official website provides two download versions such that;

- ICA-AtoM software along with the installer (12MB)
  Download URL - http://pear.qubit-toolkit.org/get/icaatom-1.3.0.tgz

- ICA-AtoM Virtual Appliance (214 MB)
  Download URL - http://qubit-toolkit.org/VEbuild/ica-atom-vmserver-1.2.0.tgz

In order to install ICA-AtoM on virtual platform, following hardware configurations has recommended **[WWW17]**.

- Processor: Pentium IV or higher
- RAM: 256B unallocated memory
- Hard Drive space: a minimum of 1GB to test the system on a small scale

APPENDIX G

HARDENING CentOS

Reaping idle users

echo "Idle users will be removed after 15 minutes"
echo "readonly TMOUT=900" >> /etc/profile.d/os-security.sh
echo "readonly HISTFILE" >> /etc/profile.d/os-security.sh
chmod +x /etc/profile.d/os-security.sh

Kernel Network Security

Since we're looking at server security, wireless shouldn't really be an issue. If you need a wireless network, you can skip this step, because we're about to disable all the wireless drivers. You could go through the contents of */lib/modules* for your current kernel and remove all the wireless drivers. This will certainly disable wireless; however it's not a permanent solution. The next time you upgrade the kernel, they'll be right back, and you'll be doing this all over again. Instead, a simple loop can be used to disable them via a blacklist file in */etc/modprobe.d*

for i in $(find /lib/modules/`uname -r`/kernel/drivers/net/wireless -name ".ko" -type f) ; do*
echo blacklist $i >> /etc/modprobe.d/blacklist-wireless ; done

Using TCP Wrappers

TCP wrappers can provide a quick and easy method for controlling access to applications linked to them. Examples of TCP Wrapper aware applications are sshd, and portmap. A restrictive example is below. This example blocks everything but ssh.

echo "ALL:ALL" >> /etc/hosts.deny
echo "sshd:ALL" >> /etc/hosts.allow

Restricting Root

echo "tty1" > /etc/securetty
chmod 700 /root

Block Shell and Login Access for Non-Root System Accounts

Using /etc/passwd, obtain a listing of all users, their UIDs, and their shells, for instance by running.

awk -F: '{print $1 ":" $3 ":" $7}' /etc/passwd

Identify the system accounts from this listing. These will primarily be the accounts with UID numbers less than 500, other than root. For each identified system account SYSACCT , lock the account. *usermod -L SYSACCT* and disable its shell. *usermod -s /sbin/nologin SYSACCT*

Verify that No Accounts Have Empty Password Fields

awk -F: '($2 == "") {print}' /etc/shadow

If this produces any output, fix the problem by locking each account

Verify that All Account Password Hashes are Shadowed

awk -F: '($2 != "x") {print}' /etc/passwd

The hashes for all user account passwords which is readable by all users.

Verify that No Non-Root Accounts Have UID 0

awk -F: '($3 == "0") {print}' /etc/passwd

This should print only one line, for the user root. If any other lines appear, ensure UID-0 accounts are authorized, and that there is a good reason for them to exist.

Set Boot Loader Password

The default RHEL boot loader for x86 systems is called GRUB. To protect its configuration:

1. Select a password and then generate a hash from it by running.
   grub-md5-crypt
2. Insert the following line into /etc/grub.conf immediately after the header comments. (Use the output from grub-md5-crypt as the value of password-hash).

password --md5 password-hash

3. Verify the permissions on /etc/grub.conf (which is a symlinkto ../boot/grub/grub.conf).

chownroot:root /etc/grub.conf

chmod 600 /etc/grub.conf

Disable Interactive Boot

Edit the file */etc/sysconfig/init.* Add or correct the setting:
PROMPT=no

Configure GUI Screen Locking

In the default GNOME desktop, the screen can be locked by choosing Lock Screen from the System menu. The gconftool-2 program can be used to enforce mandatory screen locking settings for the default GNOME environment. Run the following commands to enforce idle activation of the screen saver, screen locking, ablank-screen screensaver, and 15-minute idle activation time.

*gconftool-2 --direct *
*--config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory *
*--type bool *
--set /apps/gnome-screensaver/idle_activation_enabled true
*gconftool-2 --direct *
*--config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory *
*--type bool *
--set /apps/gnome-screensaver/lock_enabled true
*gconftool-2 --direct *
*--config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory *
*--type string *
--set /apps/gnome-screensaver/mode blank-only
*gconftool-2 --direct *
*--config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory *

*--type int *

--set /apps/gnome-screensaver/idle_delay 15

Enable SELinux

Edit the file */etc/selinux/config*. Add or correct the following lines.

SELINUX=enforcing

SELINUXTYPE=targeted

Edit the file */etc/grub.conf*. Ensure that the following arguments DO NOT appear on any kernel command line in the file.

selinux=0

enforcing=0

Ensure SELinux is Properly Enabled

Run the command.

$ /usr/sbin/sestatus

If the system is properly configured, the output should indicate.

SELinux status: enabled

Current mode: enforcing

Mode from config file: enforcing

Policy from config file: targeted

Check for Unconfined Daemons

To check for unconfined daemons, run the following command.

ps -eZ | egrep "initrc" | egrep -vw "tr|ps|egrep|bash|awk" | tr ':' ' ' | awk '{ print SNF }'

It should produce no output in a well-configured system.

Network Parameters for Hosts Only

Is this system going to be used as a firewall or gateway to pass IP traffic between different networks? If not, edit the file */etc/sysctl.conf* and add or correct the following lines.

net.ipv4.ip forward = 0

net.ipv4.conf.all.send redirects = 0

net.ipv4.conf.default.send redirects = 0

These settings disable hosts from performing network functionality which is only appropriate for routers.

Ensure System is Not Acting as a Network Sniffer

The system should not be acting as a network sniffer, which can capture all traffic on the network to which it is connected. The output of /proc/net/packet should display exactly one header line, with entries similar to.

skRefCnt Type Proto Iface R Rmem User Inode

If numbers appear in a row below this header, then a sniffing process (such as tcpdump or wireshark) is using the interface and this should be investigated.

Determine which Services are Enabled at Boot

Run the command:

chkconfig --list | grep :on

The first column of this output is the name of a service which is currently enabled at boot. Review each listed service to determine whether it can be disabled. If it is appropriate to disable some service srvname , do so using the command.

chkconfigsrvname off

Inetd and Xinetd

Is there an operational need to run the deprecated inetd or xinetd software packages? If not, ensure that they are removed from the system.
yum erase inetdxinetd

Telnet

Is there a mission-critical reason for users to access the system via the insecure telnet protocol, rather than the more secure SSH protocol? If not, ensure that the telnet server is removed from the system.
yum erase telnet-server

Remove Telnet Clients

In order to prevent users from casually attempting to use a telnet server, and thus exposing their credentials over the network, remove the telnet package, which contains a telnet client program.
yum erase telnet
If Kerberos is not used, remove the krb5-workstation package, which also includes a telnet client.
yum erase krb5-workstation

Remove the Rsh Server Commands from the System

Since there is no a mission-critical reason at ICA-AtoM for users to access the system via the insecure rlogin, rsh, or rcp commands rather than the more secure ssh and scp ensure that the rsh server is removed from the system.
yum erase rsh-server

Remove the Rsh Client Commands from the System

In order to prevent users from casually attempting to make use of an rsh server and thus exposing their credentials over the network, remove the rsh package, which contains client programs for many of r-commands described above.

yum erase rsh

TFTP Server

Is there an operational need to run the deprecated TFTP server software? If not, ensure that it is removed from the system.

yum erase tftp-server

Talk

To remove the talk daemons from the system, run the following command.

yum erase talk-server

Remove talk Package

yum erase talk

Kdump Kernel Crash Analyzer (kdump)

chkconfigkdump off

Software RAID Monitor (mdmonitor)

chkconfigmdmonitor off

Disable HAL Daemon

chkconfighaldaemon off

Disable anacron

yum erase anacron

Disable at

chkconfigatd off

Disable X Windows at System Boot

Edit the file */etc/inittab*, and correct the line *id:5:initdefault*: to.
id:3:initdefault.

Disable netfs

mount -t nfs,nfs4,smbfs,cifs,ncpfs

Disable RPC Portmapper

chkconfigportmap off

IPTables

Configure IP tables /Firewall as required.

Limit su Access to the Root Account

1. Ensure that the group wheel exists, and that the usernames of all administrators who should be allowed to execute commands as root are members of that group.
   grep ^wheel /etc/group
2. Edit the file */etc/pam.d/su*. Add, uncomment, or correct the line:auth required pam_wheel.so use_uid.

Limit Users' SSH Access

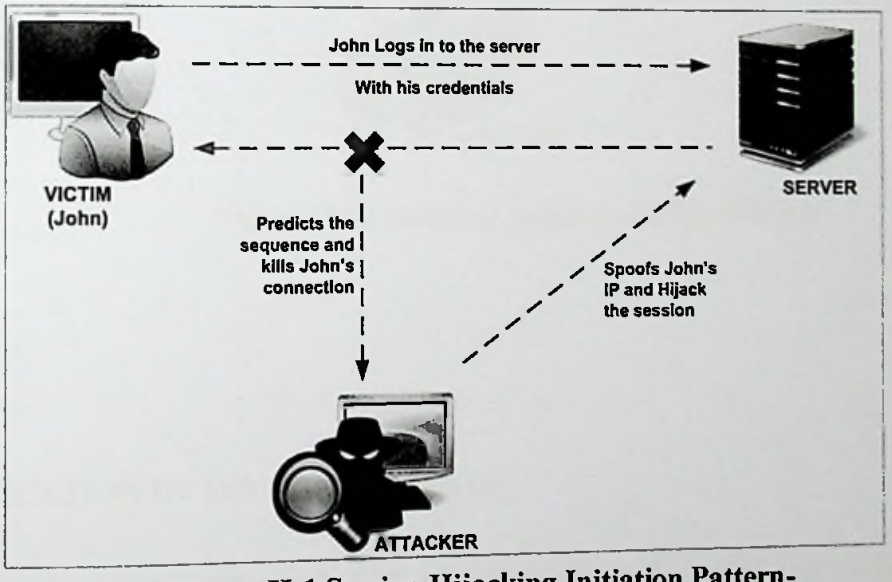
By default, the SSH configuration allows any user to access the system. In order to allow all users to login
via SSH but deny only a few users, add or correct the following line.
DenyUsers USER1 USER2

APPENDIX H

SESSION HIJACKING

WHAT IS SESSION HIJACKING

Session Hijacking refers to an attack by which a hacker exploits a valid computer session and gains access to a client's session identifier. Since HTTP is a stateless protocol, when a user logs into a website, a session is created on that Web Server for that user, this session contains all this user's information being used by the server so the username and password is not needed at every page request. The server uses a unique identifier (Session Identifier) to authenticate this user to this session; this session identifier is passed between the web server and the user's computer at every request. Session Hijacking is an attack by which the hacker steals this user's session identifier and then sends this session identifier as their own to the server and tricks the server into thinking they are that user. The pictorial representation below illustrates the communication path of a typical Session Hijacking.

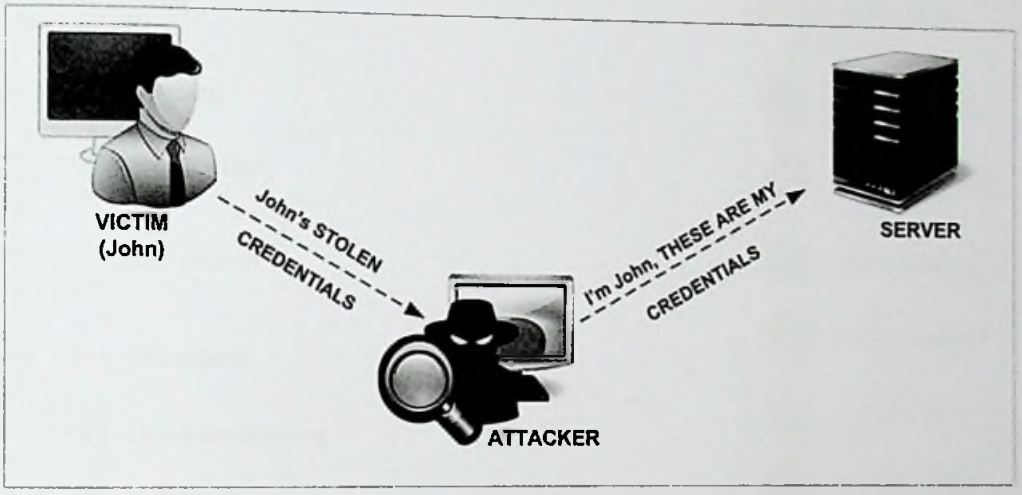


- **Figure H-1 Session Hijacking Initiation Pattern-**

After gaining access to a client's session identifier for a website, the hacker then injects the client's session identifier into his/her browser. From then on, when that attacker connects to that website, since his session identifier is the same as the authentic user, he will be logged in as that user and will have access to all of that user's information and privileges on that website. Note - attackers cannot get a user's password using session hijacking.

Spoofing *vs*Hijacking

Session Hijacking is a process of taking over an existing active session. On this scenario, attacker relies on the legitimate user to make a connection and authenticate. On the other hand, the spoofing attack, attacker pretends to be another user or machine to gain access. However attacker does not take over an existing active session. Instead he initiates a new session using victim's stolen credentials. The Figure H-02 illustrates the Spoofing attack.



- **Figure H-02 Spoofing Attack Initiation Pattern -**

CLASSIFICATION OF SESSION HIJACKING

Session Hijacking can be classified under two main groups. Such that; Active and Passive. Active Session Hijacking process involves finding an active session and takes over it. With passive attack, attacker hijacks the session, but sits back and watches the traffic that is being sent forth.

With reference to the ICA AtoM and its architecture, the Session Hijacking is OSI Model is worthwhile to discuss. The below pictorial representation discussed the two main types of the session hijacking found on OSI model which are Network and Application Level Hijacking and their methods.

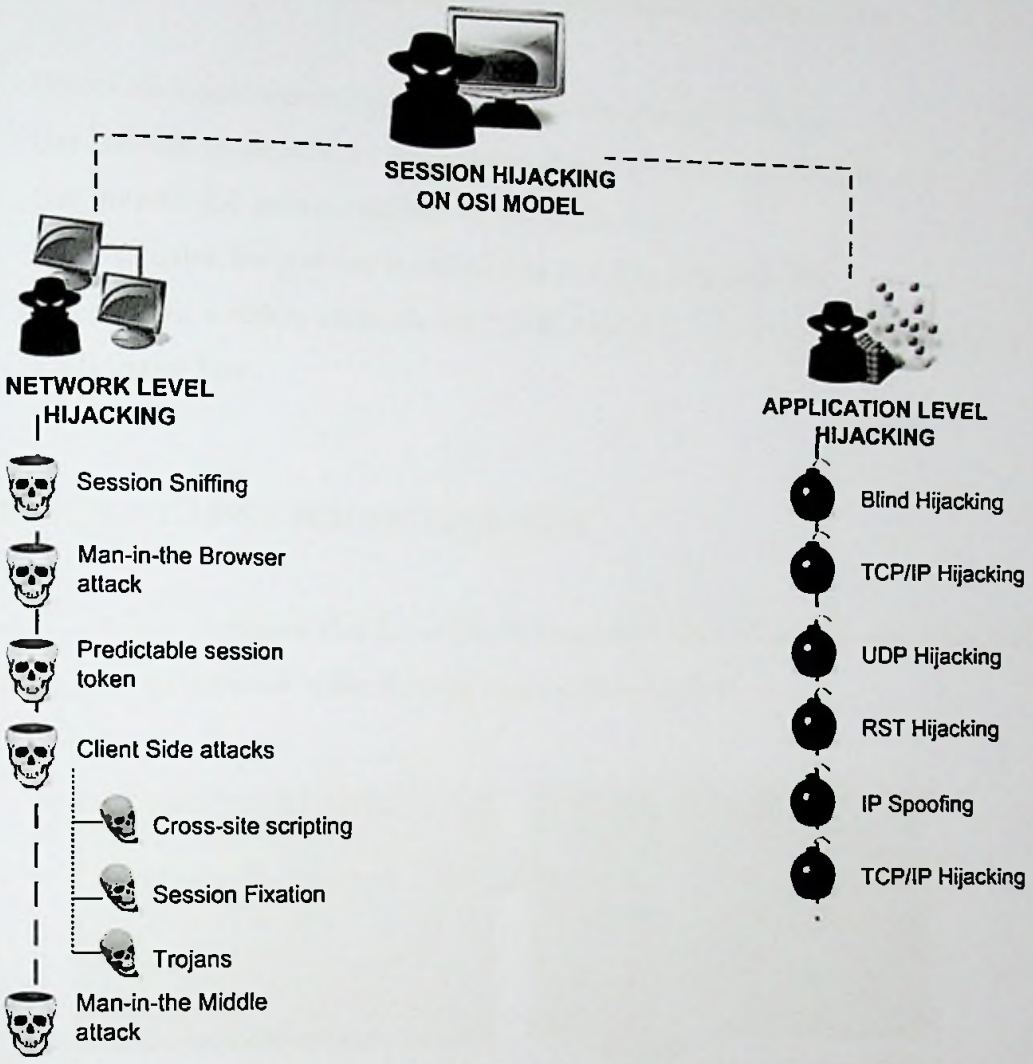


Figure H-03 Session Hijacking on OSI Model-

PROTECTING AGAINST SESSION HIJACKING

Session Hijacking can be prevented. The following methods of steps can be highlighted in the perspective of Web Developers and Web Users.

Methods to Prevent Session Hijacking – To be followed by the Web Developer

- Reduce the life-span of a session cookie
- Expire the session as soon as the user logs out
- Prevent eavesdropping within the network
- Regenerate the session ID after a successful login, to prevent session fixation attack.

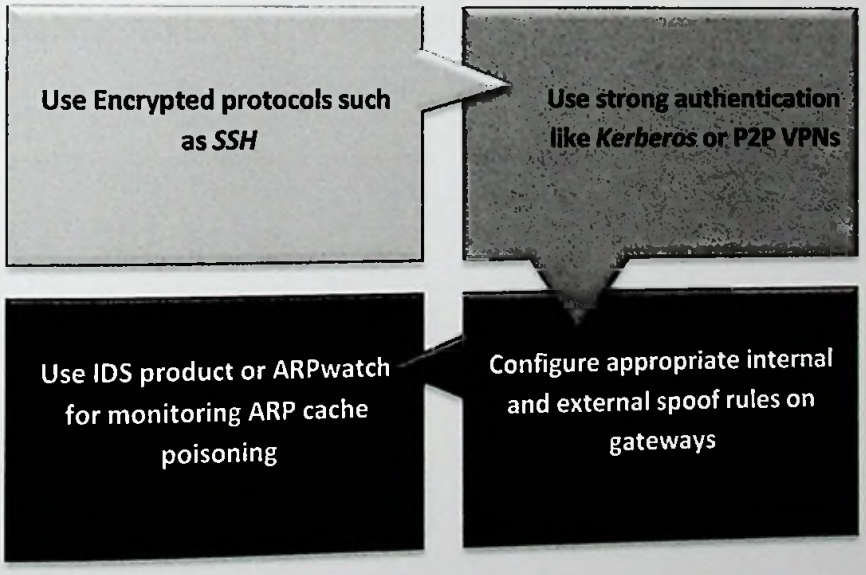
- Encrypt the data and session key transferred between the user and the web server.

Methods to Prevent Session Hijacking – To be followed by the Web User

- Do not click on the links that are received through mails or IM's
- Use firewalls to prevent the malicious content from entering the network.
- Use firewall and browser settings to restrict cookies
- Make sure that the web site is certified by the certifying authority
- Prefer *https*, a secure transmission rather than *http*, when transmitting sensitive and confidential data.

DEFENDING AGAINST SESSION HIJACKING

When the user has identified that he or she become the victim of session hijacking, use the following methods depicted in the pictorial representation below.



- **Figure H-04 Defend Against Session Hijacking-**

APPENDIX I

SCANNING AND VULNERABILITY ASSESSMENT RESULTS

SCANNING PROCESS

Vulnerability assessment has been mainly '*Nessus Vulnerability Scanner*'. The actual reports given below will give the comparison of both **General ICA-AtoM vs. the Security Enhanced ICA-AtoM.**

'*NESSUS*' SCANNING RESULTS OF GENERAL ICA-ATOM SOFTWARE

Executive Summary

Critical	High	Medium	Low	Info	Total
1	1	13	3	44	62

Details of the Vulnerabilities Found

Severity	Plugin ID	Name
Critical (10.0)	60086	PHP 5.4.x < 5.4.5 _php_stream_scandir Overflow
High (7.5)	10481	MySQL Unpassworded Account Check
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	10677	Apache mod_status /server-status Information Disclosure
Medium (5.0)	10678	Apache mod_info /server-info Information Disclosure
Medium (5.0)	11411	Backup Files Disclosure
Medium (5.0)	46803	PHP expose_php Information Disclosure
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	31705	SSL Anonymous Cipher Suites Supported

Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	53491	SSL / TLS Renegotiation DoS
Medium (4.3)	61644	Apache 2.4 < 2.4.3 Multiple Vulnerabilities
Low (2.6)	26194	Web Server Uses Plain Text Authentication Forms
Low (2.6)	34850	Web Server Uses Basic Authentication Without HTTPS
Low	47830	CGI Generic Injectable Parameter

'NESSUS' SCANNING RESULTS OF SECURED ICA-ATOM SOFTWARE

Executive Summary

Critical	High	Medium	Low	Info	Total
0	**0**	**6**	**0**	**35**	**41**

Details of the Vulnerabilities Found

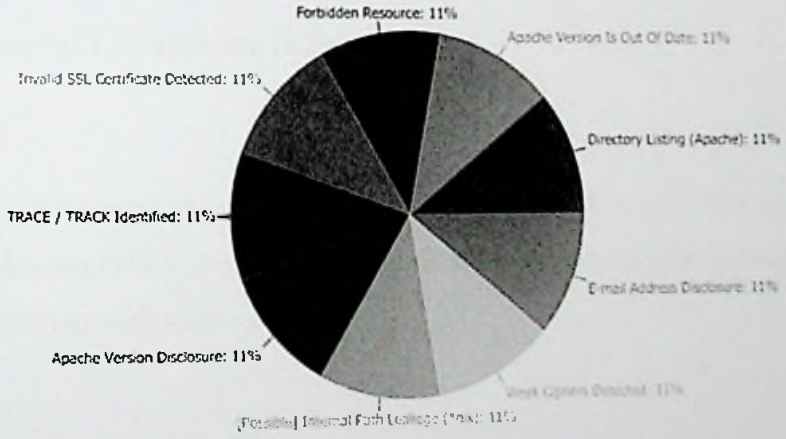
Severity	Plugin ID	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	46803	PHP expose_php Information Disclosure
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported

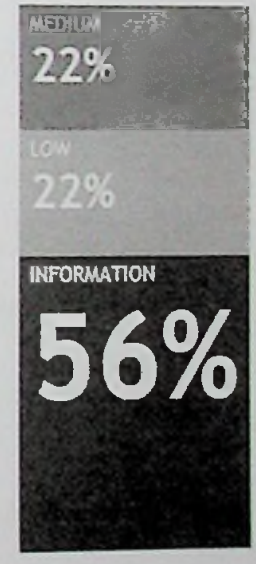
For the completion of the Vulnerability Assessment, the developed system has further being scanned through a different vulnerability scanner which is Netsparker. The report given below has been extracted from Netsparker VA Software.

Complete Executive Summary of *Nessus* scanning results of both General and Secured ICA-AtoM is annexed herewith.

'NETSPARKER' SCANNING RESULTS OF SECURED ICA-ATOM SOFTWARE

VULNERABILITIES





Executive Summary

Critical	High	Medium	Low	Info	Total
0	0	2	2	5	9

Details of the Vulnerabilities Found

Severity	Name
Medium	Invalid SSL Certificate Detected
Medium	Weak Ciphers Detected

Severity	Name
Low	Trace/ Track Identified
Low	Apache Version Disclosure

Justification of Netsparker© Scanning Results.

1. Invalid SSL Certificate Detected

Synopsis

Netsparker© detected the web server is configured to allow using weak ciphers during secure communication (SSL). It should allow only strong ciphers on the web server to protect secure communication with visitors.

Impact

Attackers can mount brute-force attacks to decrypt your secure communication between your server and the visitors.

Remedy

Configure the webserver to disallow using weak ciphers.
For Apache, it should modify the SSLCipherSuite directive in the httpd.conf.
SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

Action Taken by the Developer/ Justification

Configure the Apache Server. Vulnerability hence rectified.

2. Weak Ciphers Detected

Synopsis

Netsparker©detected that, the web server uses an invalid SSL certificate. An SSL certificate can be created and signed by anyone. It should have a valid SSL certificate to make visitors sure about the secure communication between the particular website and them.

Impact

Attackers can perform Man In the Middle attacks and observe the encryption traffic between the web server and the visitor.

Remedy

Fix the problem with SSL certificate to provide secure communication between the website and its visitors.

Action Taken by the Developer/ Justification

This alarm can be treated as False Positive! The SSL certificate that the Secured ICA-AtoM used is newly developed and unique. Moreover the same has not been verified by any certificate signing authorities, hence remain unknown to the browsers.

3. Track/ Trace Identifies

Synopsis

Netsparker© identified that the TRACE/TRACK method is allowed. It is possible to bypass Http-Only cookie limitation and read the cookies in an XSS attack by using TRACE/TRACK method within an XmlHttpRequest. This is not possible with modern browsers so the vulnerability can only be used when targeting users with unpatched & old browsers.

Impact

Attackers can perform Man In the Middle attacks and observe the encryption traffic between the web server and the visitor.

Remedy

Disable this method in all production systems. Even though the application is not vulnerable to Cross-site Scripting a debugging feature such as TRACE/TRACK should not be required in a production system and therefore should be disabled.

Action Taken by the Developer/ Justification

This alarm can be treated as False Positive!End users accessing the system through latest browsers.

4. Apache Version Disclosure

Synopsis

Netsparker©dentified that the target web server is disclosing the Apache version in its HTTP response. This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Remedy

Configure the web server to prevent information leakage from the SERVER header of its HTTP response.

Action Taken by the Developer/ Justification

Configure the Apache Server. Vulnerability hence rectified.

Complete *Netsparker*scanning results of General ICA-AtoM is annexed herewith.

Nessus Report

Nessus Scan Report

06/Jan/2013:21:07:04

HomeFeed: Commercial use of the report is prohibited

Table Of Contents

Hosts Summary (Executive)

localhost

Summary

Critical	High	Medium	Low	Info	Total
1	1	13	3	44	62

Details

Severity	Plugin Id	Name
Critical (10.0)	60086	PHP 5.4.x < 5.4.5 _php_stream_scandir Overflow
High (7.5)	10481	MySQL Unpassworded Account Check
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	10677	Apache mod_status /server-status Information Disclosure
Medium (5.0)	10678	Apache mod_info /server-info Information Disclosure
Medium (5.0)	11411	Backup Files Disclosure
Medium (5.0)	46803	PHP expose_php Information Disclosure
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	31705	SSL Anonymous Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	53491	SSL / TLS Renegotiation DoS
Medium (4.3)	61644	Apache 2.4 < 2.4.3 Multiple Vulnerabilities
Low (2.6)	26194	Web Server Uses Plain Text Authentication Forms
Low (2.6)	34850	Web Server Uses Basic Authentication Without HTTPS
Low	47830	CGI Generic Injectable Parameter
Info	10107	HTTP Server Type and Version
Info	10147	Nessus Server Detection
Info	10394	Microsoft Windows SMB Log In Possible
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10662	Web mirroring
Info	10719	MySQL Server Detection
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Info	10863	SSL Certificate Information
Info	11011	Microsoft Windows SMB Service Detection
Info	11032	Web Server Directory Enumeration
Info	11153	Service Detection (HELP Request)
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	12634	Authenticated Check: OS Name and Installed Package Enumeration
Info	14272	netstat portscanner (SSH)
Info	17219	phpMyAdmin Detection
Info	17975	Service Detection (GET request)
Info	19506	Nessus Scan Information
Info	20108	Web Server / Application favicon.ico Vendor Fingerprinting
Info	20301	VMware ESX/GSX Server detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	29700	iSCSI Target Detection
Info	33817	CGI Generic Tests Load Estimation (all tests)
Info	39463	HTTP Server Cookies Set
Info	39470	CGI Generic Tests Timeout
Info	40665	Protected Web Page Detection
Info	40773	Web Application Potentially Sensitive CGI Parameter Detection
Info	42057	Web Server Allows Password Auto-Completion
Info	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45590	Common Platform Enumeration (CPE)
Info	49704	External URLs
Info	50345	HTTP X-Frame-Options Response Header Usage
Info	51080	Web Server Uses Basic Authentication over HTTPS
Info	54615	Device Type

Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	57323	OpenSSL Version Detection
Info	58651	Netstat Active Connections
Info	62563	SSL Compression Methods Supported

Nessus Report

Nessus Scan Report

19/Feb/2013:20:41:40

HomeFeed: Commercial use of the report is prohibited

Any time Nessus is used in a commercial environment you MUST maintain an active subscription to the ProfessionalFeed in order to be compliant with our license agreement: http://www.nessus.org/products/nessus-professionalfeed

Table Of Contents

Hosts Summary (Executive)

192.168.233.135

Summary

Critical	High	Medium	Low	Info	Total
0	0	6	0	35	41

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	46803	PHP expose_php Information Disclosure
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	62565	TLS CRIME Vulnerability
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	10662	Web mirroring
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	17219	phpMyAdmin Detection
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection

Info	39463	HTTP Server Cookies Set
Info	39520	Backported Security Patch Detection (SSH)
Info	39521	Backported Security Patch Detection (WWW)
Info	40984	Browsable Web Directories
Info	42057	Web Server Allows Password Auto-Completion
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	49704	External URLs
Info	50344	HTTP X-Content-Security-Policy Response Header Usage
Info	50345	HTTP X-Frame-Options Response Header Usage
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported

NETSPARKER SCAN REPORT SUMMARY

TARGET URL	http://localhost/icaatom-1.2.1/
SCAN DATE	14/1/2013 3:50:05 PM
REPORT DATE	27/8/2013 11:21:47 PM
SCAN DURATION	02:37:18

Total Requests 27530

Average Speed 2.92 req/sec.

12 identified

3 confirmed

0 critical

8 informational

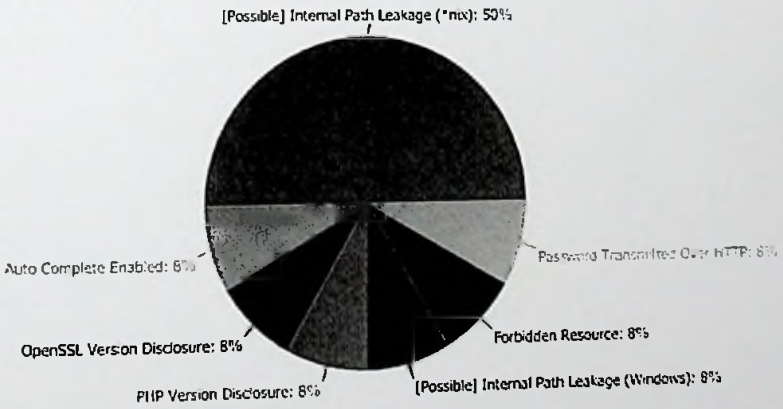
Authentication

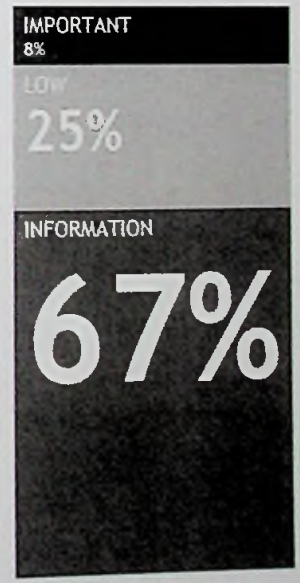
Scheduled

SCAN SETTINGS

ENABLED ENGINES: Static Tests, Find Backup Files, SQL Injection, Boolean SQL Injection, Blind SQL Injection, Cross-site Scripting, Command Injection, Blind Command Injection, Local File Inclusion, Remote File Inclusion, Remote Code Evaluation, HTTP Header Injection, Open Redirection, Expression Language Injection

VULNERABILITIES





VULNERABILITY SUMMARY

URL	Parameter	Method	Vulnerability	Confirmed
/icaatom-1.2.1/			PHP Version Disclosure	No
/icaatom-1.2.1//%22ns=%22netsparker(0x00000D)			OpenSSL Version Disclosure	No
/icaatom-1.2.1/index.php/;user/login			Forbidden Resource	Yes
			Password Transmitted Over HTTP	Yes
			Auto Complete Enabled	Yes
/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/install.php			[Possible] Internal Path Leakage (Windows)	No
/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/admin.css			[Possible] Internal Path Leakage (*nix)	No
/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system.css			[Possible] Internal Path Leakage (*nix)	No
/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-behavior.css			[Possible] Internal Path Leakage (*nix)	No
/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-menus.css			[Possible] Internal Path Leakage (*nix)	No
/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/garland/style.css			[Possible] Internal Path Leakage (*nix)	No
/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/seven/style.css			[Possible] Internal Path Leakage (*nix)	No

1. Password Transmitted Over HTTP

Netsparker identified that password data is sent over HTTP.

1 TOTAL
IMPORTANT
CONFIRMED
1

Impact

If an attacker can intercept network traffic he/she can steal users credentials.

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

Remedy

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input starting from the login process should only be served over HTTPS.

Classification

OWASP A9 PCI v1.2-6.5.9 PCI v2.0-6.5.4 CWE-319 CAPEC-65 WASC-04

1.1. /icaatom-1.2.1/index.php/;user/login CONFIRMED

http://localhost/icaatom-1.2.1/index.php/;user/login

Form target action

/icaatom-1.2.1/index.php/;user/login

Request

```
GET /icaatom-1.2.1/index.php/;user/login HTTP/1.1
Referer: http://localhost/icaatom-1.2.1/
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Cookie: symfony=ob116012ckagqgp867opf6c8u6
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 14 Jan 2013 10:21:26 GMT
Server: Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4
X-Powered-By: PHP/5.4.4
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="pt"> <head> <meta
http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="title" content="National Archives" /><meta name="description" content="Open archival description system" />
<title>National Archives</title> <link rel="shortcut icon" href="/favicon.ico"/> <link media="all" href="/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system.css"
rel="stylesheet" type="text/css" /><link media="all" href="/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-behavior.css" rel="stylesheet" type="text/css" /><link
media="all" href="/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-menus.css" rel="stylesheet" type="text/css" /><link media="all" href="/icaatom-
1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/garland/style.css" rel="stylesheet" type="text/css" /><link media="print" href="/icaatom-
1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/garland/print.css" rel="stylesheet" type="text/css" /><link href="/icaatom-1.2.1/vendor/yui/button/assets/skins/sam/button.css" media="screen"
rel="stylesheet" type="text/css" /><link href="/icaatom-1.2.1/vendor/yui/menu/assets/skins/sam/menu.css" media="screen" rel="stylesheet" type="text/css" /><link href="/icaatom-
1.2.1/plugins/sfTranslatePlugin/css/l10n_client.css" media="screen" rel="stylesheet" type="text/css" /><link href="/icaatom-1.2.1/css/form.css" media="screen" rel="stylesheet" type="text/css" />
<link href="/icaatom-1.2.1/css/graphic.css" media="screen" rel="stylesheet" type="text/css" /><link href="/icaatom-1.2.1/css/main.css" medi
-
```

2. Auto Complete Enabled

1 TOTAL
LOW
CONFIRMED
1

"Auto Complete" was enabled in one or more of the form fields. These were either "password" fields or important fields such as "Credit Card".

Impact

Data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers such as cyber cafes or airport terminals.

Remedy

Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields.

Actions to Take

1. See the remedy for the solution.
2. Find all instances of inputs which store private data and disable autocomplete. Fields which contain data such as "Credit Card" or "CCV" type data should not be cached. You can allow the application to cache usernames and remember passwords, however, in most cases this is not recommended.
3. Re-scan the application after addressing the identified issues to ensure that all of the fixes have been applied properly.

Required Skills for Successful Exploitation

Dumping all data from a browser can be fairly easy and there exist a number of automated tools to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the auto-complete feature to see previously entered values.

External References

- Using AutoComplete in HTML Forms

Classification

CWE-16 WASC-15

2.1. /icaatom-1.2.1/index.php/;user/login CONFIRMED

http://localhost/icaatom-1.2.1/index.php/;user/login

Identified Field Name

password

Request

```
GET /icaatom-1.2.1/index.php/;user/login HTTP/1.1
Referer: http://localhost/icaatom-1.2.1/
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Cookie: symfony=ob116012ckogqgp867opf6c8u6
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 14 Jan 2013 10:21:26 GMT
Server: Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4
X-Powered-By: PHP/5.4.4
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="pt"> <head> <meta
http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="title" content="National Archives" /><meta name="description" content="Open archival description system" />
<title>National Archives</title> <link rel="shortcut icon" href="/favicon.ico"/> <link media="all" href="/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-behavior.css" rel="stylesheet" type="text/css" /><link
rel="stylesheet" type="text/css" /><link media="all" href="/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-menus.css" rel="stylesheet" type="text/css" /><link media="all" href="/icaatom-
1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system.css" rel="stylesheet" type="text/css" /><link media="print" href="/icaatom-
1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/garland/style.css" rel="stylesheet" type="text/css" /><link media="all" href="/icaatom-1.2.1/vendor/yui/button/assets/skins/sam/button.css" media="screen"
rel="stylesheet" type="text/css" /><link href="/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/garland/print.css" rel="stylesheet" type="text/css" /><link href="/icaatom-
1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/garland/menu.css" media="screen" rel="stylesheet" type="text/css" /><link href="/icaatom-1.2.1/vendor/yui/menu/assets/skins/sam/menu.css" media="screen"
rel="stylesheet" type="text/css" /><link href="/icaatom-1.2.1/css/form.css" media="screen" rel="stylesheet" type="text/css" /><link href="/icaatom-1.2.1/plugins/sfTranslatePlugin/css/l10n_client.css" media="screen" rel="stylesheet" type="text/css" /><link href="/icaatom-1.2.1/css/main.css" medi
<link href="/icaatom-1.2.1/css/graphic.css" media="screen" rel="stylesheet" type="text/css" /><link href="/icaatom-1.2.1/css/main.css" medi
-
```

3. PHP Version Disclosure

1 TOTAL
LOW

Netsparker identified that the target web server is disclosing the PHP version in its HTTP response. This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of PHP.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

Classification

OWASP A6 PCI v1.2-6.5.6 CWE-16 CAPEC-170 WASC-45

3.1. /icaatom-1.2.1/

http://localhost/icaatom-1.2.1/

Extracted Version

5.4.4

Certainty

Request

```
GET /icaatom-1.2.1/ HTTP/1.1
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 14 Jan 2013 10:20:07 GMT
Server: Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4
X-Powered-By: PHP/5.4.4
Set-Cookie: symfony=ah49a46d8b3hgu8imclbn2qvg2; path=/icaatom-1.2.1
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8


<!DOCTYPE html PUBLIC "-//W3C//DT
-
```

4. OpenSSL Version Disclosure

1 TOTAL

LOW

Netsparker identified that the target web server is disclosing the OpenSSL version in its HTTP response. This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of OpenSSL.

Impact

An attacker can look for specific security vulnerabilities for the identified version. Also the attacker can use this information in conjunction with the other vulnerabilities in the application or the web server.

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

Classification

OWASP A6 PCI v1.2-6.5.6 CWE-200 CAPEC-170

4.1. /icaatom-1.2.1/

http://localhost/icaatom-1.2.1/

Extracted Version

1.0.1c

Certainty

Request

```
GET /icaatom-1.2.1/ HTTP/1.1
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 14 Jan 2013 10:20:07 GMT
Server: Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4
X-Powered-By: PHP/5.4.4
Set-Cookie: symfony=ah49a46d8b3hgu8imc1bn2qvg2; path=/icaatom-1.2.1
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8


<!DOCTYPE html PUBLIC "-//W3C//DT
-
```

5. Forbidden Resource

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for information purposes.

1 TOTAL

INFORMATION
CONFIRMED
1

Impact

There is no impact resulting from this issue.

5.1. /icaatom-1.2.1//%22ns=%22netsparker(0x00000D) CONFIRMED

http://localhost/icaatom-1.2.1//%22ns=%22netsparker(0x00000D)

Parameters

Parameter	Type	Value
URI-BASED	Full URL	/"ns="netsparker(0x00000D)

Request

```
GET /icaatom-1.2.1//%22ns=%22netsparker(0x00000D) HTTP/1.1
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Cookie: symfony=ob116012ckogqgp867opf6c8u6
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 403 Forbidden
Date: Mon, 14 Jan 2013 10:20:33 GMT
Server: Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Content-Language: en


<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>Access forbidden!</title>
<link rev="made" href="mailto:postmaster@localhost" />
<style type="text/css"><!--/*--><![CDATA[/*><!--*/
body { color: #000000; background-color: #FFFFFF; }
a:link { color: #0000CC; }
p, address {margin-left: 3em;}
span {font-size: smaller;}
/*]]>*/--></style>
</head>

<body>
<h1>Access forbidden!</h1>
<p>



You don't have permission to access the requested object.
It is either read-protected or not readable by the server.


</p>
<p>
If you think this is a server error, please contact
the <a href="mailto:postmaster@localhost">webmaster</a>.

</p>

<h2>Error 403</h2>
<address>
<a href="/">localhost</a><br />
<span>Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4</span>
</address>
</body>
</html>
```

6. [Possible] Internal Path Leakage (*nix)

Netsparker identified an internal path in the document.

6 TOTAL
INFORMATION

Impact

There is no direct impact however this information can help an attacker either to identify other vulnerabilities or during the exploitation of other identified vulnerabilities.

Remedy

First ensure that this is not a false positive. Due to the nature of the issue. Netsparker could not confirm that this file path was actually the real file path of the target web server.

- Error messages should be disabled.
- Remove this kind of sensitive data from the output.

External References

- OWASP - Full Path Disclosure

Classification

PCI v1.2-6.5.6 CWE-200 CAPEC-118 WASC-13

6.1. /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/seven/style.css

http://localhost/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/seven/style.css?0

Identified Internal Path(s)

- /misc/menu-collapsed.png
- /misc/menu-expanded.png

Certainty

Request

```
GET /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/seven/style.css?0 HTTP/1.1
Referer: http://localhost/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/install.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Cookie: symfony=ob116012ckogqgp867opf6c8u6
Accept-Encoding: gzip, deflate
```

Response

```
-
st-style-image: none;}ul.menu li { margin: 0;}ol { list-style-type: decimal; margin: 0.25em 0 0.25em 2em;}.item-list ul li.collapsed, ul.menu li.collapsed { list-style-image:url(../../misc/menu-
collapsed.png); list-style-type:disc;}.item-list ul li.expanded, ul.menu li.expanded { list-style-image:url(../../misc/menu-expanded.png); list-style-type:circle;}quote, code { margin: .5em
0;}code, pre, kbd { font-size: 1.25em;}/** * Skip link. */#skip-link { margin-top: 0; position: absolute; left: 50%; mar
-
```

6.2. /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/admin.css

http://localhost/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/admin.css?0

Identified Internal Path(s)

- /misc/watchdog-error.png
- /misc/watchdog-warning.png
- /misc/watchdog-ok.png

Certainty

Request

```
GET /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/admin.css?0 HTTP/1.1
Referer: http://localhost/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/install.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Cookie: symfony=ob116012ckogqgp867opf6c8u6
Accept-Encoding: gzip, deflate
```

Response

```
-
eport th { background-repeat: no-repeat; background-position: 5px 50%; /* LTR */ padding-top: 6px; padding-bottom: 6px;}table.system-status-report tr.error th { background-image:
url(../../misc/watchdog-error.png);}table.system-status-report tr.warning th { background-image: url(../../misc/watchdog-warning.png);}table.system-status-report tr.ok th { background-image:
url(../../misc/watchdog-ok.png);}/** * Formatting for theme configuration */.theme-settings-left { float: left; width: 49%;}.theme-settings-right { float: right; width: 49%;}.theme-settings-
bottom { clear: both
-
```

6.3. /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/garland/style.css

http://localhost/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/garland/style.css

Identified Internal Path(s)

- /misc/watchdog-ok.png

Certainty

Request

```
GET /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/themes/garland/style.css HTTP/1.1
Referer: http://localhost/icaatom-1.2.1/
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Cookie: symfony=ob1l6012ckogqgp867opf6c8u6
Accept-Encoding: gzip, deflate
```

Response

```
…
m 2em; /* LTR */}ol.task-list li.active { background: transparent url(images/task-list.png) no-repeat 3px 50%; /* LTR */}ol.task-list li.done { color: #353; background: transparent
url(../../misc/watchdog-ok.png) no-repeat 0px 50%; /* LTR */}ol.task-list li.active { margin-right: 1em; /* LTR */}fieldset ul.clearfix li { margin: 0; padding: 0; background-image: none;}dl {
margin: 0.5em 0 1em
…
```

6.4. /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-menus.css

http://localhost/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-menus.css

Identified Internal Path(s)

- /misc/menu-expanded.png
- /misc/menu-collapsed.png
- /misc/menu-leaf.png

Certainty

Request

```
GET /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-menus.css HTTP/1.1
Referer: http://localhost/icaatom-1.2.1/
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Cookie: symfony=ob1l6012ckogqgp867opf6c8u6
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 14 Jan 2013 10:20:26 GMT
Server: Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4
Last-Modified: Sun, 15 Jul 2012 13:32:24 GMT
ETag: "3a7-4c4de57fe3bd8"
Accept-Ranges: bytes
Content-Length: 935
Content-Type: text/css


/* $Id: system-menus.css,v 1.1 2007/10/05 14:50:25 goba Exp $ */ul.menu { list-style: none; border: none; text-align:left; /* LTR */}ul.menu li { margin: 0 0 0 0.5em; /* LTR */}li.expanded {
list-style-type: circle; list-style-image: url(../../misc/menu-expanded.png); padding: 0.2em 0.5em 0 0; /* LTR */ margin: 0;}li.collapsed { list-style-type: disc; list-style-image:
url(../../misc/menu-collapsed.png); /* LTR */ padding: 0.2em 0.5em 0 0; /* LTR */ margin: 0;}li.leaf { list-style-type: square; list-style-image: url(../../misc/menu-leaf.png); padding: 0.2em
0.5em 0 0; /* LTR */ margin: 0;}li a.active { color: #000;}td.menu-disabled { background: #ccc;}ul.links { margin: 0; padding: 0;}ul.links.inline { display: inline;}ul.links li { display: inline;
list-style-type: none; padding: 0 0.5em;}.block ul { margin: 0; padding: 0 0 0.25em 1em; /* LTR */}
```

6.5. /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-behavior.css

http://localhost/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-behavior.css

Identified Internal Path(s)

- /misc/throbber.gif
- /misc/menu-expanded.png
- /misc/menu-collapsed.png
- /misc/grippie.png
- /misc/draggable.png
- /misc/tree.png
- /misc/tree-bottom.png
- /misc/progress.gif

Certainty

Request

```
GET /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system-behavior.css HTTP/1.1
Referer: http://localhost/icaatom-1.2.1/
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Cookie: symfony=ob1l60l2ckogqgp867opf6c8u6
Accept-Encoding: gzip, deflate
```

Response

```
…
00; white-space: pre; cursor: default;}#autocomplete li.selected { background: #0072b9; color: #fff;}/* Animated throbber */html.js input.form-autocomplete { background-image:
url(../../misc/throbber.gif); background-repeat: no-repeat; background-position: 100% 2px; /* LTR */}html.js input.throbbing { background-position: 100% -18px; /* LTR */}/** * Collapsing
fieldsets */html.js fields
…
t.collapsed legend a span.element-invisible { display: block; overflow: hidden;}html.js fieldset.collapsible legend a { display: inline; padding-left: 15px; /* LTR */ background:
url(../../misc/menu-expanded.png) 5px 75% no-repeat; /* LTR */}html.js fieldset.collapsible legend span.summary { display: inline; font-size: 0.9em; color: #999; margin-left: 0.5em;}*html.js
fieldset.collapsed legend a { background-image: url(../../misc/menu-collapsed.png); /* LTR */ background-position: 5px 50%; /* LTR */}/* Note: IE-only fix due to '* html' (breaks Konq.eror
otherwise). */* html.js fieldset.collapsed legend,* html.js fieldset.collapsed legend
…
ldset-wrapper { overflow: auto;}/** * Resizable textareas */.resizable-textarea { width: 95%;}.resizable-textarea .grippie { height: 9px; overflow: hidden; background: #eee
url(../../misc/grippie.png) no-repeat center 2px; border: 1px solid #ddd; border-top-width: 0; cursor: s-resize;}html.js .resizable-textarea textarea { margin-bottom: 0; width: 100%; display:
block;}/** * Tab
…
0.5em; /* LTR */ text-decoration: none;}a.tabledrag-handle:hover { text-decoration: none;}a.tabledrag-handle .handle { margin-top: 4px; height: 13px; width: 13px; background:
url(../../misc/draggable.png) no-repeat 0 0;}a.tabledrag-handle-hover .handle { background-position: 0 -20px;}div.indentation { width: 20px; height: 1.7em; margin: -0.4em 0.2em -0.4em -0.4em; /*
LTR */ padding: 0.42em 0 0.42em 0.6em; /* LTR */ float: left; /* LTR */}div.tree-child { background: url(../../misc/tree.png) no-repeat 11px center; /* LTR */}div.tree-child-last { background:
url(../../misc/tree-bottom.png) no-repeat 11px center; /* LTR */}div.tree-child-horizontal { background: url(../../misc/tree.png) no-repeat -11px center;}/** * Progress bar */.progress { font-
weight: bold;}.progress .bar { border-radius: 3px; -moz-border-radius: 3px; -webkit-border-radius: 3px; background: #ccc; border: 1px solid #666; margin: 0 0.2em;}.progress .filled { background:
#0072b9 url(../../misc/progress.gif); height: 1.5em; width: 5px;}.progress .percentage { float: right; /* LTR */}.progress-disabled { float: left; /* LTR */}.ajax-progress { float: left; /* LTR
*/}.ajax-progress .throbber { width: 15px; height: 15px; margin: 2px; background: transparent url(../../misc/throbber.gif) no-repeat 0px -18px; float: left; /* LTR */}tr .ajax-progress .throbber
{ margin: 0 2px;}.ajax-progress-bar { width: 16em;}/** * Multiselect form */dl.multiselect dd, dl.multiselect
…
```

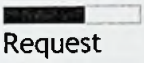
6.6. /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system.css

http://localhost/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system.css

Identified Internal Path(s)

- /misc/help.png
- /misc/permissions.png
- /misc/configure.png

Certainty



Request

```
GET /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/modules/system/system.css HTTP/1.1
Referer: http://localhost/icaatom-1.2.1/
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Cookie: symfony=ob1l60l2ckogqgp867opf6c8u6
Accept-Encoding: gzip, deflate
```

Response

```
…
/}.more-help-link a, a.module-link { padding: 1px 0 1px 20px; /* LTR */}a.module-link { display: block; white-space: nowrap;}.more-help-link a, a.module-link-help { background:
url(../../misc/help.png) 0 50% no-repeat; /* LTR */}a.module-link-permissions { background: url(../../misc/permissions.png) 0 50% no-repeat; /* LTR */}a.module-link-configure { background:
url(../../misc/configure.png) 0 50% no-repeat; /* LTR */}.more-link { text-align: right; /* LTR */}.module-help { margin-left: 1em; /* LTR */ float: right; /* LTR */}.item-list .pager { clear:
both; text-align: c
…
```

7. [Possible] Internal Path Leakage (Windows)

1 TOTAL
INFORMATION

Netsparker identified an internal path in the document.

Impact

There is no direct impact however this information can help an attacker either to identify other vulnerabilities or during the exploitation of other identified vulnerabilities.

Remedy

First ensure that this is not a false positive. Due to the nature of the issue. Netsparker could not confirm that this file path was actually the real file path of the target web server.

- Error messages should be disabled.
- Remove this kind of sensitive data from the output.

External References

- OWASP - Full Path Disclosure

Classification

PCI v1.2-6.5.6 CWE-200 CAPEC-118 WASC-13

7.1. /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/install.php

http://localhost/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/install.php?profile=standard

Identified Internal Path(s)

[] C:\xampp\htdocs\icaatom-1.2.1\plugins\sfDrupalPlugin\vendor\drupal\install.php

Certainty

Request

```
GET /icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/install.php?profile=standard HTTP/1.1
Referer: http://localhost/icaatom-1.2.1/plugins/sfDrupalPlugin/vendor/drupal/install.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; Netsparker)
Cache-Control: no-cache
Accept-Language: en-us,en;q=0.5
Host: localhost
Cookie: symfony=ob1l60l2ckogqgp867opf6c8u6
Accept-Encoding: gzip, deflate
```

Response

```
-
=0
ETag: "1358159197"
X-Generator: Drupal 7 (http://drupal.org)
Content-Length: 3660
Content-Type: text/html; charset=utf-8

Strict Standards: Only variables should be passed by reference in C:\xampp\htdocs\icaatom-1.2.1\plugins\sfDrupalPlugin\vendor\drupal\install.php on line 1204<!DOCTYPE html PUBLIC "-//W3C//DTD
XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="lt
-
```