

CONFIDENTIAL

Library
Web Application Penetration Test Report

The British Council



Author

Sergio Navarro
Consultant

Date
11th February 2014

Contents

| | |
|---|-----------|
| 1.0 PREFACE | 3 |
| 2.0 INTRODUCTION | 4 |
| 3.0 EXECUTIVE SUMMARY | 5 |
| 3.1 BUSINESS RISK..... | 5 |
| 3.2 STRATEGIC RECOMMENDATIONS..... | 6 |
| 4.0 CHANGE IN RISK OVER TIME..... | 7 |
| 4.1 EXECUTIVE SUMMARY | 7 |
| 4.2 ISSUE RESOLUTION | 7 |
| 5.0 PENETRATION TEST RESULTS..... | 9 |
| 5.1 TEST RESULTS SUMMARY..... | 9 |
| 5.2 VULNERABILITIES DETECTED | 10 |
| APPENDICES..... | 25 |
| APPENDIX A – RISK LEVEL CLASSIFICATION KEY | 25 |
| APPENDIX B – PORT SCAN RESULTS | 26 |
| APPENDIX C – PENETRATION TEST STEPS COMPLETED..... | 27 |
| APPENDIX D – ISSUE RESOLUTION ACTION PLAN | 28 |

1.0 Preface

Dionach Ltd personnel in preparation of this document:

FUNCTION

Consultant

NAME

Sergio Navarro

Customer distribution list:

FUNCTION

Head of Digital Performance and Governance

NAME

Javed Iqbal

CONTACT DETAILS

British Council
Global Security
Global Business Services
10 Spring Gardens
London
SW1A 2BN

Email: javed.iqbal@britishcouncil.org

Telephone: 0161 957 7314 (DDI)

CHANGE HISTORY

| Version | Date | Revision Description | Author |
|---------|------------|----------------------|----------------|
| 0.8 | 07/02/2014 | Initial Draft | Sergio Navarro |
| 0.9 | 10/02/2014 | Peer Review | Bil Bragg |
| 1.0 | 11/02/2014 | First Release | Sergio Navarro |

2.0 Introduction

This report provides the results of the penetration test that was undertaken from the 4th to 7th January 2014 by Dionach Limited for the British Council. The objectives of the test were to find and highlight any potential security threats and vulnerabilities relating to the British Council Library website from an external viewpoint.

Tests were performed on the British Council Library web application. The website address is as follows:

- <http://www.library.britishcouncil.org.in> (54.228.195.183)

Tests not performed were:

- Denial of Service
- Brute Force Password Cracking

Please note that test payment details were provided to use in the staging server at <http://lib.techletsolutions.com/>.

IMPORTANT LEGAL NOTE

Please note that it is impossible to 100% test an Internet connection for security vulnerabilities. This report does not form a guarantee that your site is secure from all threats. The tests performed and their resulting issues are from Dionach's point of view only. Dionach are unable to ensure or guarantee that the British Council websites and networks are completely safe from every form of attack. With the ever-changing environment of information technology, tests performed will exclude vulnerabilities in software or systems that are unknown at the time of the penetration test.

3.0 Executive Summary

3.1 Business Risk

The penetration test revealed two critical risk issues, two high risk issues and a number of lower risk issues. Overall, security of the website represents critical risk. The current security infrastructure is insufficient to prevent remote attackers from compromising the website and user personal information stored in the server.

The key issues found in the report are summarised as follows:

Koha Local File Inclusion; Critical Risk

The version of Koha library software installed is vulnerable to local file inclusion. This issue will allow anonymous attackers to read sensitive information from the web server, such as log files and configuration files which could reveal passwords in clear text.

Insufficient Access Control in the Registration Form; Critical Risk

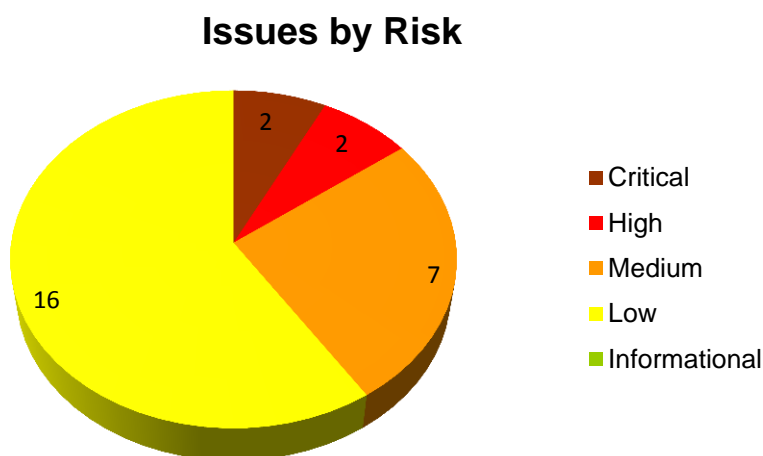
The library registration form does not properly enforce access control on the edit registration form. An anonymous attacker can gain access to registered users personal information. This has an impact on the British Council privacy and data protection compliance.

Add-ons Subscription Fee Tampering; High Risk

A vulnerability was found on the add-ons online subscription which allows users to modify the fee amount of the subscription. As a result a malicious user could exploit this issue in order to subscribe for 1 Rupee, for example. This could have reputational and financial implications for the British Council.

Dionach recommend that the website is retested following resolution or acceptance of the vulnerabilities identified in this report.

The following chart shows a summary of the associated risk levels for the issues discovered. These issues are listed in more technical detail in section 5.2.



3.2 Strategic Recommendations

The key issues identified in the report are shown below and split in three main areas:

Common Website Security Flaws

The British Council should ensure that website developers are aware of common website security flaws, particularly those which relate to access control, validation processes and password policies. Ensure that development procedures incorporate practices from the OWASP guide to secure web site development, which can be found at the following URLs:

http://www.owasp.org/index.php/Category:OWASP_Guide_Project
http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
https://www.owasp.org/index.php/Path_Traversal

Technical Vulnerability Management

Some instances identified in this report relate to insufficient patching of the web server. The British Council should review current server patch management processes, to ensure that security patches and updates are installed in a timely manner in order to protect against newly emerging threats.

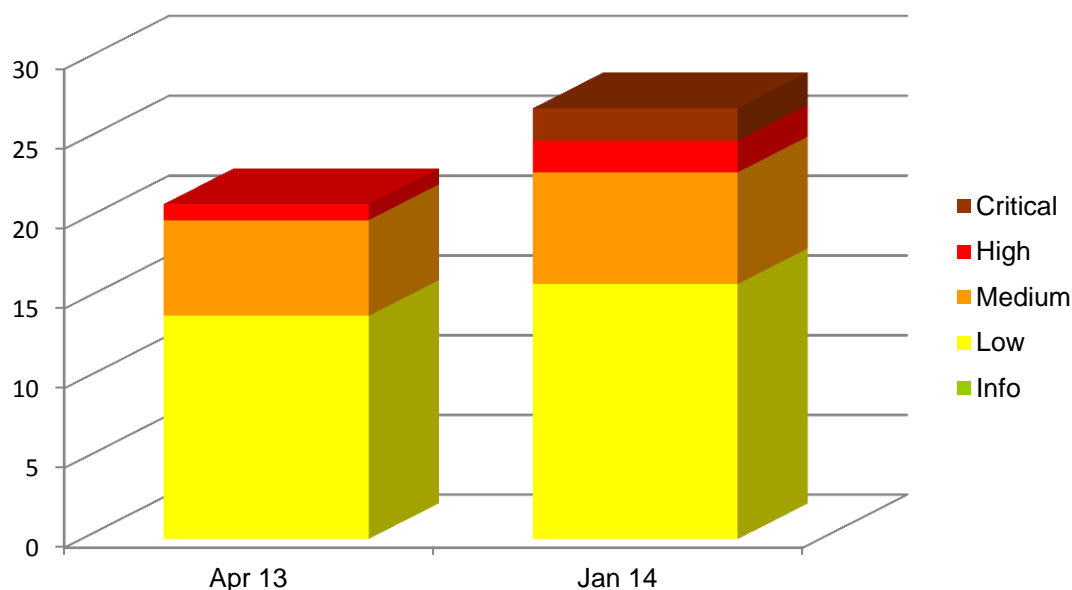
Password Management

The British Council should review their password policy with a view to enforcing strong, complex passwords in areas with administrative privileges. Also review current policy to ensure procedures are in place relating to the secure storage of passwords.

4.0 Change in Risk Over Time

4.1 Executive Summary

The penetration test reveals an increase in the overall level of risk from high to critical compared to the previous test. Whilst some of the issues identified in the previous report still appearing, a number of additional new risk issues have been identified. This is due in part to continual improvements in testing and detection methodologies, but also due to changes in the threat landscape.



4.2 Issue Resolution

The following table shows a list of the issues discovered in the previous penetration test carried out in April 2013 (reference number 500-212Q1).

| Previous Section | Description | Risk | Fixed | Comments |
|------------------|--|------|-------|--------------------|
| 4.2.1 | E-Journals Subscription Fee Tampering | High | No | See section 5.2.3 |
| 4.2.2 | Old Versions of Apache Web Server | Med | No | See section 5.2.5 |
| 4.2.3 | Cross-Site Request Forgery | Med | No | See section 5.2.6 |
| 4.2.4 | Website Clear Text Passwords and Personal Data | Med | No | See section 5.2.7 |
| 4.2.5 | Forms Vulnerable to Denial of Service | Med | No | See section 5.2.8 |
| 4.2.6 | Potential Spam Abuse | Med | No | See section 5.2.9 |
| 4.2.7 | No Account Lockout or Password Complexity | Med | No | See section 5.2.10 |

| Previous Section | Description | Risk | Fixed | Comments |
|------------------|--|------|---------|--|
| 4.2.8 | Login Page Allows Password Auto-Completion | Low | No | See section 5.2.13 |
| 4.2.9 | Session Cookie Not Marked Secure | Low | No | See section 5.2.14 |
| 4.2.10 | Website Supports Concurrent Sessions | Low | No | See section 5.2.17 |
| 4.2.11 | Sessions Not HTTP Only | Low | No | See section 5.2.18 |
| 4.2.12 | Website Vulnerable to Click Jacking | Low | No | See section 5.2.19 |
| 4.2.13 | No Robots File Detected | Low | No | See section 5.2.20 |
| 4.2.14 | Domain Expiring Soon | Low | No | The issue relates to the new expiration date. See section 5.2.21 |
| 4.2.15 | Old Version of OpenSSH | Low | Unknown | The service has been filtered. |
| 4.2.16 | Forgot Password Page Allows Library Card Number Harvesting | Low | No | See section 5.2.22 |
| 4.2.17 | Koha Reveals Version in Source Code | Low | No | See section 5.2.23 |
| 4.2.18 | Apache Header Shows Version | Low | No | See section 5.2.24 |
| 4.2.19 | Apache Web Server Manual | Low | No | See section 5.2.25 |
| 4.2.20 | Website Permits Directory Listing | Low | No | See section 5.2.26 |
| 4.2.21 | Closed TCP Ports | Low | No | See issue 5.2.27 |

5.0 Penetration Test Results

5.1 Test Results Summary

Test results are summarised in the table below in order of decreasing risk level. Full details for each of the issues, tactical recommendations, and links to vendor websites where relevant are presented in section 5.2. Please also refer to appendix A for a key to the risk level classification codes. Please see appendix B for the port scan results.

| Section | Description | Impact | L'hood | Risk | Page |
|---------|--|--------|--------|------|------|
| 5.2.1 | Koha Local File Inclusion | High | High | Crit | 10 |
| 5.2.2 | Insufficient Access Control in the Registration Form | High | High | Crit | 11 |
| 5.2.3 | Add-ons Subscription Fee Tampering | High | Med | High | 12 |
| 5.2.4 | Weak Passwords in Use | High | Med | High | 13 |
| 5.2.5 | Old Version of Apache Web Server | High | Low | Med | 14 |
| 5.2.6 | Cross-Site Request Forgery | High | Low | Med | 14 |
| 5.2.7 | Website Clear Text Passwords and Personal Data | High | Low | Med | 15 |
| 5.2.8 | Forms Vulnerable to Denial of Service | Med | Med | Med | 15 |
| 5.2.9 | Potential Spam Abuse | Med | Med | Med | 16 |
| 5.2.10 | No Account Lockout or Password Complexity | Med | Med | Med | 16 |
| 5.2.11 | Image Only CAPTCHA in use | Med | Med | Med | 17 |
| 5.2.12 | Predictable User Registration ID | Med | Low | Low | 17 |
| 5.2.13 | Login Page Allows Password Auto-Completion | Med | Low | Low | 17 |
| 5.2.14 | Session Cookie Not Marked Secure | Med | Low | Low | 18 |
| 5.2.15 | Very Weak CAPTCHA Mechanism | Med | Low | Low | 18 |
| 5.2.16 | Very Weak Mathematical Question Mechanism | Med | Low | Low | 19 |
| 5.2.17 | Website Supports Concurrent Sessions | Med | Low | Low | 19 |
| 5.2.18 | Session Not HTTP Only | Med | Low | Low | 20 |
| 5.2.19 | Website Vulnerable to Click Jacking | Med | Low | Low | 20 |
| 5.2.20 | No Robots File Detected | Med | Low | Low | 21 |
| 5.2.21 | Domain Expiring Soon | Med | Low | Low | 21 |
| 5.2.22 | Forgot Password Page Allows Library Card Number Harvesting | Low | Med | Low | 21 |
| 5.2.23 | Koha Library Software Reveals Version in Source Code | Low | Med | Low | 22 |
| 5.2.24 | Apache Header Shows Version | Low | Med | Low | 22 |
| 5.2.25 | Apache Web Server Manual | Low | Med | Low | 23 |
| 5.2.26 | Apache Web Server Icon Directories | Low | Med | Low | 23 |
| 5.2.27 | Closed TCP Ports | Low | Med | Low | 23 |

5.2 Vulnerabilities Detected

5.2.1 Koha Local File Inclusion

Risk: Critical

The website is using an old version of the open source Koha software (3.0.2) to manage the library system. There is a flaw in Koha that allow attacker to perform local file inclusion via the 'KohaOpacLanguage' cookie. This can be used by anonymous attackers to disclose the contents of internal files on the web server. Examples of sensitive information found in the web server through the exploitation of this vulnerability are shown below.

The following request shows how an anonymous user can read internal files of the web server, such as the '/etc/passwd' file which contains a list of the system's accounts.

Request

```
GET / HTTP/1.1
Host: www.library.britishcouncil.org.in
[...]
Cookie:KohaOpacLanguage=../../../../../../../../../../../../etc/passwd%00
```

Response

```
[...]
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
sshd:x:101:103:SSH daemon:/var/lib/sshd:/bin/false
statd:x:102:65534:NFS statd daemon:/var/lib/nfs:/sbin/nologin
nginx:x:103:104:user for nginx:/var/lib/nginx:/bin/false
webyast:x:104:105:User for WebYaST:/var/lib/webyast:/bin/false
mysql:x:60:106:MySQL database admin:/var/lib/mysql:/bin/false
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
vmmail:x:303:303:maildirs chef:/srv/maildirs:/bin/false
vacation:x:304:1000:Virtual
Vacation:/var/spool/vacation:/sbin/nologin
ntp:x:74:304:NTP daemon:/var/lib/ntp:/bin/false
[...]
```

The table below shows some of the information extracted from the webserver:

| Information | Username | Password |
|----------------|-----------|----------|
| MySQL Database | kohaadmin | *****a |
| Zebra Database | kohauser | z*****s |

Please note that vulnerabilities have been identified that relate to cross-site scripting in Koha versions prior to 3.4.1, although no examples of cross-site scripting were identified during the test.

Impact: High

Anonymous users can read sensitive files on the web server. This will include internal sensitive configuration files and logs files which could contain passwords in clear text.

Likelihood: High

This issue is straightforward to identify and exploit, and many configuration files have well-known, default names and paths.

Recommendation

Update to the latest Koha library version (3.14.0). More information can be found at the Koha community link:

<http://koha-community.org>

5.2.2 Insufficient Access Control in the Registration Form

Risk: Critical

The following registration pages for membership of the library web application do not enforce appropriate access controls, which allow anonymous users to see personal details of other British Council library registered users.

The registration form can be edited before making the payment. When users attempt to edit their details, a parameter called “reg_ID” is sent in the request, which use a predictable registration ID (see issue 5.2.12). Anonymous users can see the registration form personal details of other users. This can be achieved by changing the “reg_ID” parameter to another integer, when editing the registration form details.

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-registration.pl>

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-group-registration.pl>

POST <http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-registration.pl>

```
[...]
reg_id=18106
[...]
```

An example of the information gathered of the user registration ID 18105, is shown below:

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-registration.pl>

| | |
|---|-----------------------------|
| Address * | City * |
| 4-N-102, AWHO GURJINDER VIHAR, SECTOR - CHI-1 | GREATER NOIDA |
| Please enter Address. | Please enter your City. |
| Pin Code * | State * |
| 20 | UTTAR PRADESH |
| Please enter Pin Code. | Please enter your State. |
| Country * | Email Address * |
| INDIA | @yahoo.com |
| Please enter your Country. | Please enter Email Address. |
| Telephone No | Mobile * |
| | 880 |

Impact: High

Sensitive and personal information about library users is displayed anonymously. The information gathered such as username, email address and telephone number can be used by attackers for identity theft or social engineering attacks. This could impact the reputation of the British Council if a user had confidential data exposed as a result of this vulnerability.

Likelihood: High

This information can be accessed by an anonymous attacker. This issue is straightforward to identify as the registration form uses a sequential integer for the "reg_ID" field.

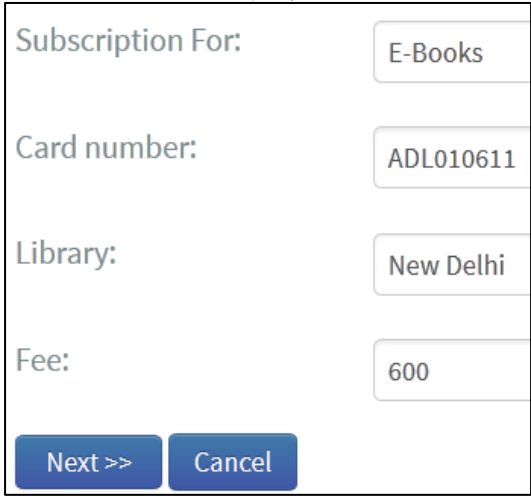
Recommendation

Implement access control checks so that the current user can only see their own registration form details. Also consider using a random ID such as a GUID (Globally Unique Identifier).

5.2.3 Add-ons Subscription Fee Tampering**Risk: High**

Diamond membership plan users can use the British Council Library web application to subscribe to electronic journals or books (e-journals or e-books). The online subscription process relies on client-side parameters to determine the subscription fee, which can be changed to suit the website user. As a result it is possible to reduce the price of a subscription.

The screenshot displays the real cost of the subscription fee amount:



| | |
|---------------------------------|-----------|
| Subscription For: | E-Books |
| Card number: | ADL010611 |
| Library: | New Delhi |
| Fee: | 600 |
| <div>Next >> Cancel</div> | |

The following proof of concept shows how, by modifying the hidden "event_fee" parameter, it was possible to reduce the subscription fee amount from 600 INR to 1 INR as the lowest amount allows by the application:

POST <http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-sub.pl>

event_fee=1

As a result a malicious user is able to reduce the subscription fee amount:

Card Number : ADL010611

Subscription : E-Books

Library : New Delhi

Fee : 1.00

Procced to PaymentCancel

Please note that this issue was only tested by using the Diamond membership plan provided by the British Council. Other plans with the same add-ons subscription structure may be vulnerable.

Impact: High

Attackers could exploit this issue in order to subscribe without the correct fee amount. This could have reputational and financial implications for the British Council.

Likelihood: Medium

Exploiting this flaw would be straightforward, using a simple web browser add-on such as Tamper Data for Firefox or a local web proxy such as Burp.

Recommendation

Implement server-side validation of the online subscription process, in particular ensure that only product IDs are posted to the customer's web browser and that the product's price is stored or calculated using server-side parameters only. Additionally, implement both integrity checking on the price and a final validation check once the customer confirms their purchase.

5.2.4 Weak Passwords in Use

Risk: High

Database administrator credentials were found at the web server by exploiting the local file inclusion vulnerability (see issue 5.2.1). These were seen to have a very weak password.

Impact: High

Anyone guessing this password or obtaining it through the local file inclusion issue (see issue 5.2.1) could gain access to sensitive information or systems.

Likelihood: Medium

These passwords would be quickly guessed, particularly by someone with knowledge of internal systems or procedures.

Recommendation

Rename the administrative accounts to a less obvious username and use a password that is not based on the software in use. Enforce complex passwords with a minimum length of eight characters and requiring at least one digit and one non alphanumeric character. Additionally, review policy and procedures to ensure that there are no other systems with similarly weak credentials.

5.2.5 Old Version of Apache Web Server

Risk: Medium

The web server at <https://www.library.britishcouncil.org.in/> may be running an outdated version of the Apache web server. The version reported by the server banner is Apache 2.2.22 and the latest Apache stable versions are 2.2.26 and 2.4.7.

Further information relating to the potential security vulnerabilities associated with older versions of Apache can be found at the following link:

http://httpd.apache.org/security/vulnerabilities_22.html

This may be a false positive as this issue is based upon version information exposed by the web server's response headers (see issue 5.2.24).

Impact: High

An attacker could potentially exploit these vulnerabilities to steal other users' sessions and so get access to the system or perform a denial of service attack on the server.

Likelihood: Low

A small number of security vulnerabilities are documented for this version of Apache, however, they are primarily related to indirect attacks that could potentially allow users' sessions to be hijacked.

Recommendation

Check the version of Apache web server to ensure that the latest secure version is installed. Further information can be found from the Apache HTTP server project website:

<http://httpd.apache.org>

5.2.6 Cross-Site Request Forgery

Risk: Medium

The website is vulnerable to cross-site request forgery (CSRF) on all pages that cause actions such as updates and deletes. A CSRF attack forces a logged-on victim's browser to send a request to a vulnerable web application, which then performs the chosen action on behalf of the victim. Example is the following link, which is for updating a user's password:

POST <http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-passwd.pl>

| |
|--|
| Oldkey=hello123&Newkey=hello123&Confirm=hello123 |
|--|

Please see the following OWASP reference for more information:

http://www.owasp.org/index.php/Cross-Site_Request_Forgery

Impact: High

The integrity of information may be affected.

Likelihood: Low

The victim needs to be logged in and the attacker needs to have knowledge of the website.

Recommendation

Restrict actions to POST methods and add a hidden key field to forms that validate requests. The hidden key should be unique to the page request and validated on post back. Please see the above OWASP link for more information.

5.2.7 Website Clear Text Passwords and Personal Data**Risk: Medium**

The website at <http://www.library.britishcouncil.org.in/> uses plain text HTTP for communication between the web browser and the web server. This means that all usernames, passwords, sensitive information and user sessions are transmitted over the network in clear text.

Impact: High

An attacker can sniff sensitive information off the local network.

Likelihood: Low

An attacker will need to be on the same local network as someone using the website to sniff the personal information. This is a straightforward attack on an open or shared wireless network.

Recommendation

Enforce encryption over HTTPS with a digital certificate signed by a trusted Certificate Authority.

5.2.8 Forms Vulnerable to Denial of Service**Risk: Medium**

The forms below allows an attacker to make multiple, scripted submissions. An attacker can write a script that will send large number of requests or messages which could overwhelm the web application and cause a denial of service. Please note that some registration forms include a math question but this mechanism can be bypassed by users before submitting the form (see issue 5.2.16).

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-registration.pl>
<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-group-registration.pl>
<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-corp-registration.pl>
<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-suggestions.pl>

Impact: Medium

Internal mail, database and web servers could be overwhelmed by inbound messages. The department processing these requests may receive thousands of emails, and not be able to identify and respond to legitimate ones.

Likelihood: Medium

A simple script or pre-built tool could be used to perform this attack; however, an attacker would need to be motivated to attack the British Council in this manner.

Recommendation

Consider using an effective CAPTCHA mechanism on these and other forms. One possible solution is Google's reCAPTCHA software, available at the following URL:

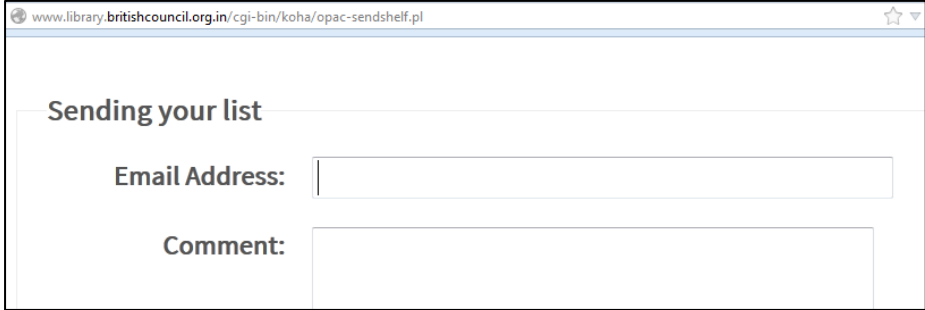
<http://www.google.com/recaptcha>

5.2.9 Potential Spam Abuse

Risk: Medium

The online catalogue website has a page that allows anonymous emails to be sent through the website. This type of functionality is commonly found to be vulnerable to abuse by spammers. The page is shown below.

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-sendshelf.pl>



The screenshot shows a web browser window with the URL www.library.britishcouncil.org.in/cgi-bin/koha/opac-sendshelf.pl. The page content is titled "Sending your list". Below the title, there are two input fields. The first is labeled "Email Address:" and the second is labeled "Comment:". Both fields are empty and have a light blue border.

Impact: Medium

This would impact the reputation of the British Council. The mail server may be blacklisted by organisations that use services such as the Spamhaus block list. This would prevent emails being successfully delivered that use this mail server, which could be many other websites.

Likelihood: Medium

Spammers continually look for forms that send automated emails to see if they can be abused. This attack is relatively straightforward to implement.

Recommendation

Consider adding a CAPTCHA to the send list form.

5.2.10 No Account Lockout or Password Complexity

Risk: Medium

There is no account lockout following multiple login failures. Password complexity is not enforced beyond a minimum of 7 characters, it was possible to enter a password of '1234567'. This leaves the web application susceptible to brute force attacks.

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-user.pl>

Impact: Medium

A successful brute force attack will lead to the exposure of personal details.

Likelihood: Medium

An attacker will require knowledge of user names. Users will also need to use fairly weak passwords such as dictionary words or common names.

Recommendation

Lockout accounts for a short period of time, say 5 minutes, if the account has multiple login failures, such as 5 in a row. Alternatively, use CAPTCHA after a certain number of login failures. Assign a failure count to the user record rather than the user's session. Password complexity can be difficult to enforce for the general public, therefore awareness tools such as a password strength meter can help to provide user guidance on selecting strong passwords.

5.2.11 Image Only CAPTCHA in use

Risk: Medium

The CAPTCHAs on the Library website are image based, and does not provide an alternate option for people who are visually impaired. This fact may dissuade some visitors from accessing the website and could affect the reputation of the British Council.

Impact: Medium

Some people with visual disabilities may find the website difficult to use. If there is a law about discrimination in this issue, the British Council reputation may be affected.

Likelihood: Medium

This could exclude visually impaired users from using the website.

Recommendation

Provide an alternate CAPTCHA system such as an audio message. Google's reCAPTCHA software provides both options to the user. Please visit the following link for further information:

<http://www.google.com/recaptcha>

5.2.12 Predictable User Registration ID

Risk: Low

The website at the following URLs, which are used to register users for the library application, generate sequential IDs. An attacker can therefore guess a series of valid registration user IDs, and use them to gather users registration information (see issue 5.2.2).

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-registration.pl>

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-group-registration.pl>

Impact: Medium

An attacker can extract multiple user registration IDs, and then use them to read form user information against the library registration form.

Likelihood: Low

This issue is quickly identifiable by simple inspection of the generated user registration IDs.

Recommendation

Consider using a random, non-sequential value for the user registration IDs such as a GUID (Globally Unique Identifier).

5.2.13 Login Page Allows Password Auto-Completion

Risk: Low

The website has a login page that allows password auto-completion.

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-user.pl>

password

Impact: Medium

A user who can automatically login to this website is more vulnerable to exploitation through cross-site scripting or if they leave their computer unattended.

Likelihood: Low

An attacker can only exploit this through another vulnerability such as cross-site scripting or physical access to the user's PC.

Recommendation

Add an attribute named "autocomplete" to the password field on the login page that is set to "off".

5.2.14 Session Cookie Not Marked Secure
Risk: Low

The session cookie for the tested website is not marked as secure. The relevant cookie name is below. Unmarked cookies will be sent by the web browser as part of a regular HTTP request as well as with the more secure HTTPS request. If a logged in user clicks on a link such as <http://www.library.britishcouncil.org.in/>, then the session cookie will be sent over the network in clear text.

| |
|-----------|
| CGISESSID |
|-----------|

Impact: Medium

A local attacker can intercept a session cookie and hijack a user's session. This will give the attacker access to confidential information depending on the role of the victim user.

Likelihood: Low

An attacker will need to be on the same network as the victim to sniff the session cookie and use an element of social engineering to get the victim to navigate to an HTTP link, for example sent in an email.

Recommendation

Mark the session cookie as secure. Please note that website is currently only available over HTTP, so setting a secure session cookie over HTTP will prevent session management functioning. To avoid that issue enforce encryption over HTTPS (see issue 5.2.7) with a digital certificate which matches the URL, and is signed by a trusted certification authority.

5.2.15 Very Weak CAPTCHA Mechanism
Risk: Low

The images used for the implemented CAPTCHA mechanism will not prevent more advanced automated OCR techniques. There are commercial tools available for breaking CAPTCHA images. Example images are as follows:

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-detail.pl?biblionumber=<<ID>>>



Moreover the MD5 hash of the CAPTCHA solution is displayed in the source code of the page. An attacker can write an automated script to retrieve and brute force the CAPTCHA hash from the source code prior to sending the request. As the CAPTCHA code is only 3 characters, it is quick to brute force.

An example of MD5 hash in the source code is shown below:

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-detail.pl?biblionumber=<<ID>>>

mdhash=718a056e741edc84150411c119fd9ebf

Impact: Medium

An attacker will be able to carry out denial of service attacks and send spam by sending multiple emails through the website.

Likelihood: Low

It would require an attacker to spend resources on this website. Additionally, it is unlikely that an attacker would target the British Council in this manner.

Recommendation

Consider implementing a stronger CAPTCHA mechanism. A popular solution is Google's reCAPTCHA. The following article from OWASP discusses CAPTCHA in more detail:

[http://www.owasp.org/index.php/Testing_for_Captcha_\(OWASP-AT-008\)](http://www.owasp.org/index.php/Testing_for_Captcha_(OWASP-AT-008))

5.2.16 Very Weak Mathematical Question Mechanism

Risk: Low

The registration pages of the website found at the following URLs include the same math question in each request. Additionally, the value entered for this is not checked and so any text can be entered and is considered correct.

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-group-registration.pl>

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-registration.pl>

Please answer this simple math question. $9 + 3 =$

Impact: Medium

This allows an attacker to write an automated script to attempt against the registration form, although a new membership will be valid from the date of online payment.

Likelihood: Low

It would require an attacker to build a custom script to exploit this vulnerability. They would need to be motivated to target the site in this way.

Recommendation

Consider using an effective CAPTCHA mechanism on these and other forms (see issue 5.2.8). Also ensure that it is implemented correctly, and cannot be bypassed in this manner.

5.2.17 Website Supports Concurrent Sessions

Risk: Low

The website at <https://www.library.britishcouncil.org.in/> allows multiple simultaneous logins, using the same valid credentials, each being granted a separate session.

Impact: Medium

There is little accountability if logins are shared, as audited actions cannot be tied to an individual person. As there is no alerting or prevention of concurrent sessions then users may be unaware if their account has been compromised.

Likelihood: Low

Valid credentials would be required to generate a valid session.

Recommendation

Institute server side controls to prevent concurrent sessions.

5.2.18 Session Not HTTP Only**Risk: Low**

The website does not set the "HttpOnly" flag on the session cookie ("CGISESSID"). This means that an attacker could exploit any cross-site scripting vulnerabilities and hijack cookies using JavaScript. See the following OWASP link for more information.

<https://www.owasp.org/index.php/HttpOnly>

Impact: Medium

An attacker successfully exploiting any cross-site scripting issues may be able to hijack an administrator's cookies and be logged in as an administrator.

Likelihood: Low

The website needs to be vulnerable to cross-site scripting, and the attacker needs to exploit this indirect attack.

Recommendation

Set the session cookie to "HttpOnly".

5.2.19 Website Vulnerable to Click Jacking**Risk: Low**

The website at the following URL render correctly when embedded in an IFRAME element:

<http://1dn.eu/iframe.asp?url=www.library.britishcouncil.org.in>

As a result, an attacker could socially engineer a situation where a victim is directed to a website under an attacker's control and manipulated into unknowingly performing actions on the target website. This is possible even with cross-site request forgery protection in place.

Impact: Medium

A user may be manipulated into performing an unintended action on the website, which could potentially lead to sensitive data being exposed, or impact on the accountability of actions performed on the website.

Likelihood: Low

An attacker would need technical knowledge, and would need to devote time and resource to targeting the website. Additionally, a victim would need to be logged into the website, and some social engineering would be required to successfully exploit this vulnerability.

Recommendation

Set the "X-Frame-Options" HTTP header to "SAMEORIGIN" to prevent third party websites from including the web page in IFRAME tags. Note that some older browsers may not support this HTTP header.

For Apache add the following line to the website's configuration files:

```
Header always append X-Frame-Options SAMEORIGIN
```

5.2.20 No Robots File Detected

Risk: Low

The website does not make use of a robots.txt file to prevent automated website indexing by search engines such as Google and Bing.

Impact: Medium

Website content which may not be appropriate for search engine indexing may be made available in search engine results. This could lead to a subsequent impact on confidentiality.

Likelihood: Low

Provided appropriate access control and change management procedures are in place, it is unlikely that inappropriate content will be exposed in this manner.

Recommendation

Consider including a robots.txt file in the website that lists specific paths which are appropriate for search engine indexing. Note that using disallow rules can reveal potentially sensitive or inappropriate website folders to attackers which might otherwise have been undetected. Note also that while some search engines honour robots.txt files, not all do, and the use of robots.txt file will not prevent the use of an automated "spider" on the website.

More information about robots.txt files can be found here: <http://www.robotstxt.org/>

5.2.21 Domain Expiring Soon

Risk: Low

Ownership of the domain "BRITISHCOUNCIL.ORG.IN" will expire in less than 3 months, on 30th April 2014.

Impact: Medium

If the ownership of the domain is not renewed, then it could be bought by a third party, who would then have complete control over it. This would result in unavailability of any websites using the domain, and could also lead to extra expense of having to buy the domain from the third party; or legal costs for trying to reclaim it.

Likelihood: Low

Most registrars will notify domain owners when their domain is up for renewal, and some will auto-renew domains without manual intervention. It is unlikely that an attacker would target the British Council in this manner.

Recommendation

Ensure that the domains are renewed prior to the expiry date.

5.2.22 Forgot Password Page Allows Library Card Number Harvesting

Risk: Low

The forgot password page displays whether library card numbers exist or have already been registered. An attacker can therefore guess or brute force a series of library card numbers to find out what accounts exist.

<http://www.library.britishcouncil.org.in/cgi-bin/koha/opac-forgotpassword.pl>

Invalid card number: This membership card number does not exist. Please try again or contact your Library for assistance.

Impact: Low

An anonymous attacker could potentially enumerate library card numbers.

Likelihood: Medium

An attacker can use an automated attack tool to run a brute-force or dictionary attack against this page to find valid library card numbers.

Recommendation

For the forgot password page use a message such as “if the library card number entered is correct, you will receive further instructions via email”. The use of CAPTCHA can also hinder automated attacks.

5.2.23 Koha Library Software Reveals Version in Source Code**Risk: Low**

The website reveals the version of Koha installed in the HTML source code of the web page as shown in the example below:

<http://www.library.britishcouncil.org.in/>

```
<meta name="generator" content="Koha 3.0203067">
```

Impact: Low

The version information can be useful information to an attacker when searching for vulnerabilities. Unnecessary system information is exposed.

Likelihood: Medium

This information is present in the HTML source code of the web page, so is straightforward to identify.

Recommendation

Remove this information from the HTML source code of the web page.

5.2.24 Apache Header Shows Version**Risk: Low**

The Apache web server at <http://www.library.britishcouncil.org.in/> shows the version of Apache installed.

```
Server: Apache/2.2.22 (Linux/SUSE)
```

Impact: Low

The version information can be useful information to an attacker when searching for vulnerabilities. Unnecessary system information is exposed.

Likelihood: Medium

This information is presented in HTTP headers so a simple scan or banner grab would obtain this information.

Recommendation

Amending the following directive setting in the Apache “httpd.conf” configuration file will ensure that only the basic header “Apache” will be returned.

```
ServerTokens      Prod
ServerSignature   Off
```

“ServerSignature Off” tells Apache not to display the server version on error pages, or other pages it generates. “ServerTokens Prod” tells Apache to only return “Apache” in the Server header.

5.2.25 Apache Web Server Manual

Risk: Low

The website has the Apache web server manual available in the manual directory. This shows information on the version of Apache and how to use it. The link below shows the location:

<http://www.library.britishcouncil.org.in/manual/>

Impact: Low

The manual exposes the major version of Apache running.

Likelihood: Medium

The default location for the manual is in the manual directory.

Recommendation

The manual is unnecessary for a production web server and should be removed. Review your web server hardening procedures.

5.2.26 Apache Web Server Icon Directories

Risk: Low

The Apache web server displays the default icons directory at the following URL:

<http://www.library.britishcouncil.org.in/icons/>

```
/icons/
```

Impact: Low

This indicates that the web server has not been hardened.

Likelihood: Medium

This is disclosed by navigating to the icons directory on the web server.

Recommendation

Many Linux distributions create an alias to the icons directory in the Apache "httpd.conf" configuration file. Remove the following line from the "httpd.conf" file to disable the icons directory on the web server. Note that the exact location of the icons directory will vary between distributions.

```
Alias /icons/ "/usr/share/apache2/icons/"
```

5.2.27 Closed TCP Ports

Risk: Low

The TCP port 8080 was found to be in state 'closed' rather than 'filtered'. This often indicates that traffic is permitted through the firewall, but that there is no service listening on the port. Such port can potentially be used by an attacker to bind a shell daemon or remote access Trojan to, which can then be accessed remotely.

The port observed to be closed is shown in the port scan in appendix B.

Impact: Low

This issue relies on an attacker being able to exploit a remote command execution vulnerability.

Likelihood: Medium

Closed ports are easily detected through well-known port scanning techniques.

Recommendation

Investigate the configuration of the devices located on IP addresses listed in the port scan. Drop traffic to all ports that do not have services listening on them.

Appendices

Appendix A – Risk Level Classification Key

Dionach technical consultants assess risk scores by using a risk assessment system based upon the OWASP risk rating methodology. Estimations are made for both impact and likelihood of a detected vulnerability.

Impact

The estimation of impact is based upon the following factors:

Technical Impact:

- Loss of Confidentiality
- Loss of Integrity
- Loss of Availability
- Loss of Accountability

Business Impact:

- Financial damage
- Reputation damage
- Non-compliance
- Privacy violation

Examples:

| | |
|----------------|---|
| High Impact: | <ul style="list-style-type: none"> • A vulnerability that, if exploited, would give access to personally identifiable or financial information. • Loss of availability of an essential business system. |
| Medium Impact: | <ul style="list-style-type: none"> • Loss of availability of a business system. • Information disclosure that, although not confidential, may lead to reputational damage. |
| Low Impact: | <ul style="list-style-type: none"> • Unnecessary disclosure of non-confidential information that may be useful to an attacker, such as versions or patch levels. • Loss of availability of a non-essential service. |

Likelihood

The estimation of likelihood is based upon the following factors:

Threat Agent Factors:

- Skill Level of potential attackers
- Motivation for attackers
- Ease of opportunity
- Size of the group of potential hackers

Vulnerability Factors:

- Ease of discovery
- Ease of exploit
- Awareness
- Intrusion detection

Examples:

| | |
|--------------------|--|
| High Likelihood: | <ul style="list-style-type: none"> • An easy to exploit vulnerability leading to unauthorised access to systems or networks. |
| Medium Likelihood: | <ul style="list-style-type: none"> • A configuration without a defence in depth approach that might otherwise prevent a system or network compromise. |
| Low Likelihood: | <ul style="list-style-type: none"> • Obscure, unpublished or very difficult to exploit vulnerability that may lead to unauthorised access to systems or networks. |

Risk

The estimation of impact and likelihood combine to produce the overall risk severity:

| Overall Risk Severity | | | | |
|-----------------------|--------|---------------|--------|----------|
| Impact | High | Medium | High | Critical |
| | Medium | Low | Medium | High |
| | Low | Informational | Low | Medium |
| | | Low | Medium | High |
| Likelihood | | | | |

Appendix B – Port Scan Results

A full TCP port scan and a common UDP port scan were run on the IP addresses in the supplied range. All ports are TCP unless otherwise indicated. The echo symbol (↵) signifies that the IP address responded to an ICMP ping.

| | | |
|-----------------------|------------|---|
| 54.228.195.183 | | ec2-54-228-195-183.eu-west-1.compute.amazonaws.com www.library.britishcouncil.org.in |
| 80 | HTTP | Apache/2.2.22 (Linux/SUSE) |
| 8080 | HTTP-PROXY | CLOSED |

Appendix C – Penetration Test Steps Completed

The following checks were completed as part of this penetration test. Any issues that were found during these checks are identified in the penetration test results section 5.0.

- Information gathering, including organisation websites, business social networking and technical websites checked for sensitive information relating to the organisation and employees.
- DNS zone transfer.
- TCP and UDP port scans.
- Network vulnerability scanning.
- Manual tests for network vulnerabilities.
- Web application vulnerability scanning.
- OWASP: Manual tests on sample input fields, parameters, cookies for injection attacks, cross-site scripting, cross-site request forgery, insecure direct object reference, cryptographic issues, malicious file execution, information leakage, and improper error handling.
- OWASP: Manual tests on sample pages and links for broken authentication, broken session management, failure to restrict URL access, privilege escalation.
- OWASP: Insecure communications.
- Click-jacking.
- Default and organisation specific credentials for any network and application logins discovered.
- CAPTCHA bypass.

Appendix D – Issue Resolution Action Plan

Below is an action plan for tracking resolution of the issues identified in this report. It allows owners to be assigned to each issue with a proposed resolution date. Note that some issues, especially some low risk issues, may have a cost higher than the benefit of removing the risk, so a resolution may not be required.

| Section | Description | Risk | Owner | Date | Fixed |
|---------|--|------|-------|------|-------|
| 5.2.1 | Koha Local File Inclusion | Crit | | | |
| 5.2.2 | Insufficient Access Control in the Registration Form | Crit | | | |
| 5.2.3 | Add-ons Subscription Fee Tampering | High | | | |
| 5.2.4 | Weak Passwords in Use | High | | | |
| 5.2.5 | Old Version of Apache Web Server | Med | | | |
| 5.2.6 | Cross-Site Request Forgery | Med | | | |
| 5.2.7 | Website Clear Text Passwords and Personal Data | Med | | | |
| 5.2.8 | Forms Vulnerable to Denial of Service | Med | | | |
| 5.2.9 | Potential Spam Abuse | Med | | | |
| 5.2.10 | No Account Lockout or Password Complexity | Med | | | |
| 5.2.11 | Image Only CAPTCHA in use | Med | | | |
| 5.2.12 | Predictable User Registration ID | Low | | | |
| 5.2.13 | Login Page Allows Password Auto-Completion | Low | | | |
| 5.2.14 | Session Cookie Not Marked Secure | Low | | | |
| 5.2.15 | Very Weak CAPTCHA Mechanism | Low | | | |
| 5.2.16 | Very Weak Mathematical Question Mechanism | Low | | | |
| 5.2.17 | Website Supports Concurrent Sessions | Low | | | |
| 5.2.18 | Session Not HTTP Only | Low | | | |
| 5.2.19 | Website Vulnerable to Click Jacking | Low | | | |
| 5.2.20 | No Robots File Detected | Low | | | |
| 5.2.21 | Domain Expiring Soon | Low | | | |