acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

29 December, 2014

Developer Report

Generated by Acunetix WVS Reporter (v9.5 Build 20140602)

Scan of catalogo.minvu.cl

Scan details

Scan information	
Start time	19-12-2014 15:46:11
Finish time	19-12-2014 23:03:53
Scan time	7 hours, 17 minutes
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.4.7
Server OS	Unknown
Server technologies	

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	**79**
High	18
Medium	40
Low	6
Informational	15

Knowledge base

SSL server running [443]

A TLS1 server is running on TCP port 443.

-
SSL server information:
- Version: SSL2,SSL3,TLS1- Ciphers suported:
- TLS1_CK_RSA_WITH_RC4_128_SHA(OpenSSL ciphername: RC4-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: RC4(128), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_3DES_EDE_CBC_SHA(OpenSSL ciphername: DES-CBC3-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: 3DES(168), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_3DES_EDE_CBC_SHA(OpenSSL ciphername: EDH-RSA-DES-CBC3-SHA, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: 3DES(168), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_AES_128_CBC_SHA(OpenSSL ciphername: AES128-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: AES(128), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA(OpenSSL ciphername: DHE-RSA-AES128-SHA, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: AES(128), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_AES_256_CBC_SHA(OpenSSL ciphername: AES256-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: AES(256), Message authentication code: SHA1) - High strength

- TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA(OpenSSL ciphername: DHE-RSA-AES256-SHA, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: AES(256), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_CAMELLIA_128_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: Camellia(128), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: Camellia(128), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_CAMELLIA_256_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: Camellia(256), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: Camellia(256), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_SEED_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: SEED(128), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_SEED_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: SEED(128), Message authentication code: SHA1) - High strength
- TLS1_CK_ECDHE_RSA_WITH_RC4_128_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: ECDH, Autentication: RSA, Symmetric encryption method: RC4(128), Message authentication code: SHA1) - High strength
- TLS1_CK_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: ECDH, Autentication: RSA, Symmetric encryption method: 3DES(168), Message authentication code: SHA1) - High strength
- TLS1_CK_ECDHE_RSA_WITH_AES_128_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: ECDH, Autentication: RSA, Symmetric encryption method: AES(128), Message authentication code: SHA1) - High strength
- TLS1_CK_ECDHE_RSA_WITH_AES_256_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: ECDH, Autentication: RSA, Symmetric encryption method: AES(256), Message authentication code: SHA1) - High strength

- Certificate:

Issuer:
  Common Name: catalogo.minvu.cl
Recipient:
  Common Name: catalogo.minvu.cl

Certificate version: 2
Serial number: 009496046ee4d1491d
Finger print: 89ee9c88155028f612b589b3a892f42f
Algorithm ID: 1.2.840.113549.1.1.11
Valability start: Fri Nov 28 19:28:56 UTC-0300 2014
Valability end: Mon Nov 25 19:28:56 UTC-0300 2024
Expire in: 3629 days

List of file extensions

File extensions can provide information on what technologies are being used on this website.
List of file extensions detected:

- pl => 17 file(s)
- css => 5 file(s)
- js => 15 file(s)
- html => 1 file(s)

Top 10 response times

The files listed below had the slowest response times measured during the crawling process. The average response time for this site was 1596,85 ms. These files could be targetted in denial of service attacks.

1. /cgi-bin/koha/opac-search.pl, response time 2093 ms

GET /cgi-bin/koha/opac-search.pl HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache

Referer: https://catalogo.minvu.cl/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=ca76481c831b65f525433b9c1f5b4fe9
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
Accept: */*

2. /cgi-bin/koha/opac-detail.pl, response time 2031 ms

GET /cgi-bin/koha/opac-detail.pl?biblionumber=2533 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-topissues.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
Accept: */*

3. /cgi-bin/koha/opac-reserve.pl, response time 2000 ms

GET /cgi-bin/koha/opac-reserve.pl?biblionumbers= HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
Accept: */*

4. /cgi-bin/koha/opac-shelves.pl, response time 1906 ms

GET /cgi-bin/koha/opac-shelves.pl?direction=desc&sort=itemcallnumber&viewshelf=7 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
Accept: */*

5. /cgi-bin/koha/opac-MARCdetail.pl, response time 1875 ms

GET /cgi-bin/koha/opac-MARCdetail.pl?biblionumber=2533 HTTP/1.1
Pragma: no-cache

Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-detail.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=853c123ffe0ad8f6a7bbe104c10ae862
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
Accept: */*

6. /cgi-bin/koha/opac-ISBDdetail.pl, response time 1672 ms

GET /cgi-bin/koha/opac-ISBDdetail.pl?biblionumber=2532 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-detail.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c1418a5dcf13f8baa7256dfbc0c6c18e
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
Accept: */*

7. /cgi-bin/koha/opac-sendshelf.pl, response time 1594 ms

POST /cgi-bin/koha/opac-sendshelf.pl HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-sendshelf.pl
Content-Length: 75
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=66bdc53b945256d3fa420685ab41844d
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
Accept: */*

koha_login_context=opac&password=g00dPa%24%24w0rD&shelfid=7&userid=giulytce8. /, response time 1515 ms

GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Googlebot/2.1 (+http://www.googlebot.com/bot.html)
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
Accept: */*

9. /cgi-bin/koha/opac-ratings.pl, response time 1469 ms

POST /cgi-bin/koha/opac-ratings.pl HTTP/1.1

Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-ratings.pl
Content-Length: 182
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=e73ff7fca94e7d307af0f233e3b66ffc
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
Accept: */*

biblionumber=2533&borrowernumber=&koha_login_context=opac&password=g00dPa%24%24w0rD&rate_button=Val%c3%b3reme&rating=2&rating_avg_int=0.0&rating_total=0&rating_value=&userid=wxsjxdud10.
/opac-tmpl/lib/famfamfam/silk, response time 1422 ms

GET /opac-tmpl/lib/famfamfam/silk/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/opac-tmpl/lib/famfamfam/silk/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
Accept: */*

List of client scripts

These files contain Javascript code referenced from the website.

- /opac-tmpl/bootstrap/lib/jquery/jquery.js
- /opac-tmpl/bootstrap/lib/jquery/jquery-ui.js
- /opac-tmpl/bootstrap/lib/jquery/plugins/jquery.rating.js
- /opac-tmpl/bootstrap/lib/jquery/plugins/jquery.checkboxes.min.js
- /opac-tmpl/bootstrap/lib/jquery/plugins/jquery.highlight-3.js
- /opac-tmpl/bootstrap/lib/bootstrap/js/bootstrap.min.js
- /opac-tmpl/bootstrap/lib/modernizr.min.js
- /opac-tmpl/bootstrap/js/global.js
- /opac-tmpl/bootstrap/js/basket.js
- /opac-tmpl/bootstrap/js/tags.js
- /opac-tmpl/bootstrap/js/google-jackets.js
- /opac-tmpl/bootstrap/js/datatables.js
- /opac-tmpl/lib/jquery/plugins/jquery.dataTables.min.js

List of files with inputs

These files have at least one input (GET or POST).

- / - 3 inputs
- /cgi-bin/koha/opac-search.pl - 27 inputs
- /cgi-bin/koha/opac-user.pl - 1 inputs
- /cgi-bin/koha/opac-tags.pl - 1 inputs
- /cgi-bin/koha/opac-shelves.pl - 12 inputs
- /cgi-bin/koha/opac-topissues.pl - 2 inputs
- /cgi-bin/koha/opac-showreviews.pl - 1 inputs
- /cgi-bin/koha/opac-detail.pl - 3 inputs
- /cgi-bin/koha/svc/suggestion - 1 inputs
- /cgi-bin/koha/opac-search-history.pl - 2 inputs
- /cgi-bin/koha/opac-reserve.pl - 5 inputs

- /cgi-bin/koha/opac-ratings.pl - 3 inputs
- /cgi-bin/koha/opac-export.pl - 1 inputs
- /cgi-bin/koha/opac-MARCdetail.pl - 1 inputs
- /cgi-bin/koha/opac-ISBDdetail.pl - 1 inputs
- /cgi-bin/koha/opac-sendshelf.pl - 3 inputs
- /cgi-bin/koha/opac-downloadshelf.pl - 3 inputs
- /cgi-bin/koha/opac-showmarc.pl - 1 inputs

List of external hosts

These hosts were linked from this website but they were not scanned because they are not listed in the list of hosts allowed.(Settings->Scanners settings->Scanner->List of hosts allowed).

- portalsiac.minvu.cl
- twitter.com
- placehold.it
- www.gob.cl
- images.amazon.com
- ecx.images-amazon.com
- www.minvu.cl
- seccdn.libravatar.org
- www.delicious.com
- worldcat.org
- openlibrary.org
- www.bookfinder.com
- www.facebook.com
- www.linkedin.com
- www.scholar.google.com
- apis.google.com
- schema.org
- purl.org
- books.google.com

List of email addresses

List of all email addresses found on this host.

- cdocumentacion@minvu.cl
- soporte@opengeek.cl

Alerts summary

Cross site scripting (verified)

Classification	
CVSS	Base Score: 4.4 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-79

Affected items	Variation
/cgi-bin/koha/opac-downloadshelf.pl	4
/cgi-bin/koha/opac-shelves.pl	12
/cgi-bin/koha/opac-topissues.pl	1

Vulnerable Javascript library

Classification	
CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/opac-tmpl/bootstrap/lib/jquery/jquery-ui.js	1

Host header attack

Classification	
CVSS	Base Score: 2.6 - Access Vector: Local - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-20

Affected items	Variation
/cgi-bin/koha/opac-detail.pl	1
/cgi-bin/koha/opac-main.pl	1
/cgi-bin/koha/opac-search.pl	1
/cgi-bin/koha/opac-search-history.pl	1
/cgi-bin/koha/opac-shelves.pl	1
/cgi-bin/koha/opac-showreviews.pl	1
/cgi-bin/koha/opac-tags.pl	1
/cgi-bin/koha/opac-topissues.pl	1
/cgi-bin/koha/opac-user.pl	1
/cgi-bin/koha/svc/suggestion	1
/cgi-bin/koha/unapi	1
/opac-tmpl/bootstrap/css/jquery.rating.css	1
/opac-tmpl/bootstrap/css/opac.css	1
/opac-tmpl/bootstrap/css/print.css	1
/opac-tmpl/bootstrap/images/quienes-somos.html	1
/opac-tmpl/bootstrap/js/basket.js	1
/opac-tmpl/bootstrap/js/global.js	1
/opac-tmpl/bootstrap/js/google-jackets.js	1
/opac-tmpl/bootstrap/js/tags.js	1
/opac-tmpl/bootstrap/lib/bootstrap/css/bootstrap.min.css	1
/opac-tmpl/bootstrap/lib/bootstrap/js/bootstrap.min.js	1
/opac-tmpl/bootstrap/lib/jquery/jquery.js	1
/opac-tmpl/bootstrap/lib/jquery/jquery-ui.css	1
/opac-tmpl/bootstrap/lib/jquery/jquery-ui.js	1
/opac-tmpl/bootstrap/lib/modernizr.min.js	1

HTML form without CSRF protection

Classification	
CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
CWE	CWE-352

Affected items	Variation
/	1
/cgi-bin/koha/opac-search.pl	2
/cgi-bin/koha/opac-search.pl (4f2edc0d5164414c03ae99941efa0950)	1
/cgi-bin/koha/opac-search.pl (54c1af9f8946c385455a3698599c7ca9)	1
/cgi-bin/koha/opac-search.pl (770d980ffd9ef0bd2c222d69fbeb15c3)	1
/cgi-bin/koha/opac-shelves.pl (582e66bf7accc7010cfc550b47e6236e)	1
/cgi-bin/koha/opac-shelves.pl (6cb537b34db0fff1f16e3dd60c6b14a0)	1
/cgi-bin/koha/opac-shelves.pl (a0577af4fea5a6007b42dc44647e014b)	1
/cgi-bin/koha/opac-shelves.pl (bbd9059703ae68d495436a671ef009e6)	1
/cgi-bin/koha/opac-shelves.pl (dae2a959793b62a25028fa8f169820af)	1
/cgi-bin/koha/opac-shelves.pl (e0481242e83653532915c1a03da0fb21)	1
/cgi-bin/koha/opac-shelves.pl (fb23de97afb322476f2ccc3d6dce3775)	1
/cgi-bin/koha/opac-tags.pl	1
/cgi-bin/koha/opac-user.pl	1

Cookie without Secure flag set

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/	1

Login page password-guessing attack

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-307

Affected items	Variation
/cgi-bin/koha/opac-reserve.pl	3
/cgi-bin/koha/opac-sendshelf.pl	1
/cgi-bin/koha/opac-user.pl	1

Broken links

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/cgi-bin/koha/errors/404.pl	1
/cgi-bin/koha/opac-showreviews.pl&format=rss2	1
/opac-tmpl/bootstrap/images/estilos.css	1

Email address found

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/cgi-bin	1
/cgi-bin/koha	1
/cgi-bin/koha/errors/404.pl	1
/cgi-bin/koha/opac-showreviews.pl&format=rss2	1
/opac-tmpl/bootstrap/images/estilos.css	1
/opac-tmpl/bootstrap/images/quienes-somos.html	1
/opac-tmpl/img	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/	1
/cgi-bin/koha/opac-ratings.pl (132a3cea51a7d22cd3c58ac3e06b798a)	1
/cgi-bin/koha/opac-reserve.pl	1
/cgi-bin/koha/opac-sendshelf.pl (2c611560f31d18190a5f099697f162f5)	1

Possible server path disclosure (Unix)

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CWE	CWE-200

Affected items	Variation
/cgi-bin/koha/svc/suggestion	1

Alert details

Cross site scripting (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

- How To: Prevent Cross-Site Scripting in ASP.NET
- Acunetix Cross Site Scripting Attack
- VIDEO: How Cross-Site Scripting (XSS) Works
- The Cross Site Scripting Faq
- OWASP Cross Site Scripting
- XSS Annihilation
- XSS Filter Evasion Cheat Sheet
- Cross site scripting
- OWASP PHP Top 5

Affected items

/cgi-bin/koha/opac-downloadshelf.pl

Details

URL encoded GET input shelfid was set to 1"><script>prompt(954582)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-downloadshelf.pl?shelfid=1"><script>prompt(954582)</script>&showpriva
teshelves= HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-downloadshelf.pl

Details

URL encoded GET input shelfid was set to 1"><script>prompt(970124)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-downloadshelf.pl?shelfid=1"><script>prompt(970124)</script>&showpriva
teshelves= HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-downloadshelf.pl

Details

URL encoded GET input shelfid was set to 5"><script>prompt(966156)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-downloadshelf.pl?context=modal&shelfid=5"><script>prompt(966156)</scr
ipt>&showprivateshelves= HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-downloadshelf.pl

Details

URL encoded GET input shelfid was set to 5"><script>prompt(925918)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-downloadshelf.pl?context=modal&shelfid=5"><script>prompt(925918)</scr
ipt>&showprivateshelves= HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 7"><script>prompt(987898)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?viewshelf=7"><script>prompt(987898)</script> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 1"><script>prompt(919944)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-shelves.pl?sortfield=title&viewshelf=1"><script>prompt(919944)</scrip
t> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 7"><script>prompt(933264)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?viewshelf=7"><script>prompt(933264)</script> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 7"><script>prompt(991658)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?viewshelf=7"><script>prompt(991658)</script> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 7"><script>prompt(908472)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?viewshelf=7"><script>prompt(908472)</script> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 7"><script>prompt(976884)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-shelves.pl?direction=asc&sort=author&viewshelf=7"><script>prompt(9768
84)</script> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 7"><script>prompt(925556)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-shelves.pl?direction=asc&sort=author&viewshelf=7"><script>prompt(9255
56)</script> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 7"><script>prompt(905950)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-shelves.pl?direction=asc&sort=author&viewshelf=7"><script>prompt(9059
50)</script> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 7"><script>prompt(902859)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-shelves.pl?direction=asc&sort=author&viewshelf=7"><script>prompt(9028
59)</script> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 1"><script>prompt(984041)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-shelves.pl?sortfield=title&viewshelf=1"><script>prompt(984041)</scrip
t> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 1"><script>prompt(926527)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-shelves.pl?sortfield=title&viewshelf=1"><script>prompt(926527)</scrip
t> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-shelves.pl

Details

URL encoded GET input viewshelf was set to 1"><script>prompt(981409)</script>
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET
/cgi-bin/koha/opac-shelves.pl?sortfield=title&viewshelf=1"><script>prompt(981409)</scrip
t> HTTP/1.1
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

/cgi-bin/koha/opac-topissues.pl

Details

URL encoded GET input timeLimit was set to 3<script>prompt(924513)</script>
The input is reflected inside a text element.

Request headers

```
GET
/cgi-bin/koha/opac-topissues.pl?branch=BC&do_it=1&itemtype=MN&limit=10&timeLimit=3<scrip
t>prompt(924513)</script> HTTP/1.1
```

```
Referer: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
Host: catalogo.minvu.cl
```

Vulnerable Javascript library

Severity	**High**
Type	Configuration
Reported by module	Scripting (Javascript_Libraries_Audit.script)

Description

You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult Web References for more information.

Recommendation

Upgrade to the latest version.

References

http://bugs.jqueryui.com/ticket/8859

Affected items

/opac-tmpl/bootstrap/lib/jquery/jquery-ui.js

Details

Detected Javascript library jquery-ui-autocomplete version 1.9.2.
The version was detected from file content.

Request headers

```
GET /opac-tmpl/bootstrap/lib/jquery/jquery-ui.js HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=a8bf673427802c899f044a769e38ad1e
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Host header attack

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (Host_Header_Attack.script)

Description

In many cases, developers are trusting the HTTP Host header value and using it to generate links, import scripts and even generate password resets links with its value. This is a very bad idea, because the HTTP Host header can be controlled by an attacker. This can be exploited using web-cache poisoning and by abusing alternative channels like password reset emails.

Impact

An attacker can manipulate the Host header as seen by the web application and cause the application to behave in unexpected ways.

Recommendation

The web application should use the SERVER_NAME instead of the Host header. It should also create a dummy vhost that catches all requests with unrecognized Host headers. This can also be done under Nginx by specifying a non-wildcard SERVER_NAME, and under Apache by using a non-wildcard serverName and turning the UseCanonicalName directive on. Consult references for detailed information.

References

Practical HTTP Host header attacks
Apache
nginx

Affected items

/cgi-bin/koha/opac-detail.pl

Details

Host header evilhostHoC5djMF.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/opac-detail.pl HTTP/1.1
Host: evilhostHoC5djMF.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-main.pl

Details

Host header evilhostdYewguto.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/opac-main.pl HTTP/1.1
Host: evilhostdYewguto.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-search.pl

Details

Host header evilhostKTPcsAQi.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/opac-search.pl HTTP/1.1
Host: evilhostKTPcsAQi.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-search-history.pl

Details

Host header evilhostrXMG9veT.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/opac-search-history.pl HTTP/1.1
Host: evilhostrXMG9veT.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-shelves.pl

Details

Host header evilhostsMcoV7Nr.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl HTTP/1.1
Host: evilhostsMcoV7Nr.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-showreviews.pl

Details

Host header evilhostE6kmeUPq.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/opac-showreviews.pl HTTP/1.1
Host: evilhostE6kmeUPq.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-tags.pl

Details

Host header evilhostH5IkUo7u.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/opac-tags.pl HTTP/1.1
Host: evilhostH5IkUo7u.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-topissues.pl

Details

Host header evilhostxS9eti3G.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/opac-topissues.pl HTTP/1.1
Host: evilhostxS9eti3G.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-user.pl

Details

Host header evilhostyF5nEpcO.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/opac-user.pl HTTP/1.1
Host: evilhostyF5nEpcO.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/svc/suggestion

Details

Host header evilhostYZ8AfV1F.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/svc/suggestion HTTP/1.1
Host: evilhostYZ8AfV1F.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/unapi

Details

Host header evilhostZ4X00uZL.com was reflected inside a A tag (href attribute).

Request headers

```
GET /cgi-bin/koha/unapi HTTP/1.1
Host: evilhostZ4X00uZL.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/css/jquery.rating.css

Details

Host header evilhostIHfJbEX5.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/css/jquery.rating.css HTTP/1.1
Host: evilhostIHfJbEX5.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/css/opac.css

Details

Host header evilhostsgwGzbu9.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/css/opac.css HTTP/1.1
Host: evilhostsgwGzbu9.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/css/print.css

Details

Host header evilhostGe6IwACq.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/css/print.css HTTP/1.1
Host: evilhostGe6IwACq.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/images/quienes-somos.html

Details

Host header evilhostxOmlv5Ts.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/images/quienes-somos.html HTTP/1.1
Host: evilhostxOmlv5Ts.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/js/basket.js

Details

Host header evilhost7p2L8JaX.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/js/basket.js HTTP/1.1
Host: evilhost7p2L8JaX.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/js/global.js

Details

Host header evilhostfqhzBmQ6.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/js/global.js HTTP/1.1
Host: evilhostfqhzBmQ6.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/js/google-jackets.js

Details

Host header evilhostCh7GYkRP.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/js/google-jackets.js HTTP/1.1
Host: evilhostCh7GYkRP.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/js/tags.js

Details

Host header evilhostm0zoS8dT.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/js/tags.js HTTP/1.1
Host: evilhostm0zoS8dT.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/lib/bootstrap/css/bootstrap.min.css

Details

Host header evilhostkf975NYO.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/lib/bootstrap/css/bootstrap.min.css HTTP/1.1
Host: evilhostkf975NYO.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/lib/bootstrap/js/bootstrap.min.js

Details

Host header evilhostJqaWKjFn.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/lib/bootstrap/js/bootstrap.min.js HTTP/1.1
Host: evilhostJqaWKjFn.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/lib/jquery/jquery.js

Details

Host header evilhostL1tXJFPa.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/lib/jquery/jquery.js HTTP/1.1
Host: evilhostL1tXJFPa.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/lib/jquery/jquery-ui.css

Details

Host header evilhostlirpKtcy.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/lib/jquery/jquery-ui.css HTTP/1.1
Host: evilhostlirpKtcy.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/lib/jquery/jquery-ui.js

Details

Host header evilhostjANrnG6g.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/lib/jquery/jquery-ui.js HTTP/1.1
Host: evilhostjANrnG6g.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/lib/modernizr.min.js

Details

Host header evilhostVY6WOkFT.com was reflected inside a A tag (href attribute).

Request headers

```
GET /opac-tmpl/bootstrap/lib/modernizr.min.js HTTP/1.1
Host: evilhostVY6WOkFT.com
X-Forwarded-Host: catalogo.minvu.cl
Cookie: CGISESSID=eea1c20f4689e096bb3cf4f7808217a5
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

HTML form without CSRF protection

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker''s choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/

Details

Form name: searchform
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl
Form method: GET

Form inputs:

- idx [Select]
- q [Text]
- branch_group_limit [Select]

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://catalogo.minvu.cl/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=ca76481c831b65f525433b9c1f5b4fe9
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-search.pl

Details

Form name: <empty>
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl
Form method: GET

Form inputs:

- idx [Select]
- q [Text]
- idx [Select]
- q [Text]
- idx [Select]
- q [Text]
- do [Submit]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
[... (line truncated)

Request headers

```
GET /cgi-bin/koha/opac-search.pl HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=ca76481c831b65f525433b9c1f5b4fe9
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-search.pl

Details

Form name: <empty>
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl
Form method: GET

Form inputs:

- idx [Select]
- q [Text]
- idx [Select]
- q [Text]
- idx [Select]
- q [Text]
- do [Submit]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
[... (line truncated)

Request headers

```
GET /cgi-bin/koha/opac-search.pl HTTP/1.1
Pragma: no-cache
```

```
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=ca76481c831b65f525433b9c1f5b4fe9
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-search.pl (4f2edc0d5164414c03ae99941efa0950)

Details

Form name: searchform
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl
Form method: GET

Form inputs:

- idx [Select]
- q [Text]
- branch_group_limit [Select]

Request headers

```
GET /cgi-bin/koha/opac-search.pl?branch_group_limit=branch:BN&idx=nb&q=1 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=ca76481c831b65f525433b9c1f5b4fe9
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-search.pl (54c1af9f8946c385455a3698599c7ca9)

Details

Form name: hold_form
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-reserve.pl
Form method: GET

Form inputs:

- biblionumbers [Hidden]

Request headers

```
GET /cgi-bin/koha/opac-search.pl?do=Buscar&idx=ti&limit-yr=1&q=1&sort_by=relevance
HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-search.pl (770d980ffd9ef0bd2c222d69fbeb15c3)

Details

Form name: <empty>
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl
Form method: GET

Form inputs:

- idx [Select]
- q [Text]
- op [Select]
- idx [Select]
- q [Text]
- op [Select]
- idx [Select]
- q [Text]
- do [Submit]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [Checkbox]
- limit [... (line truncated)

Request headers

```
GET /cgi-bin/koha/opac-search.pl?expanded_options=1 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-shelves.pl (582e66bf7accc7010cfc550b47e6236e)

Details

Form name: myform
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Form method: POST

Form inputs:

- REM-1411 [Checkbox]

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?sortfield=title&viewshelf=7 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-shelves.pl (6cb537b34db0fff1f16e3dd60c6b14a0)

Details

Form name: myform
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Form method: POST

Form inputs:

- REM-2001 [Checkbox]
- REM-1986 [Checkbox]
- REM-1811 [Checkbox]
- REM-1809 [Checkbox]
- REM-1807 [Checkbox]

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?direction=asc&sort=author&viewshelf=5 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-shelves.pl (a0577af4fea5a6007b42dc44647e014b)

Details

Form name: myform
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Form method: POST

Form inputs:

- REM-1811 [Checkbox]
- REM-2001 [Checkbox]
- REM-1809 [Checkbox]
- REM-1807 [Checkbox]
- REM-1986 [Checkbox]

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?direction=desc&sort=title&viewshelf=5 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-shelves.pl (bbd9059703ae68d495436a671ef009e6)

Details

Form name: myform
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Form method: POST

Form inputs:

- REM-1986 [Checkbox]
- REM-1807 [Checkbox]
- REM-1809 [Checkbox]
- REM-2001 [Checkbox]
- REM-1811 [Checkbox]

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?viewshelf=5 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl?sortfield=&viewshelf=5
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-shelves.pl (dae2a959793b62a25028fa8f169820af)

Details

Form name: myform
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Form method: POST

Form inputs:

- REM-1925 [Checkbox]
- REM-1949 [Checkbox]
- REM-1908 [Checkbox]
- REM-1939 [Checkbox]
- REM-1924 [Checkbox]

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?viewshelf=3 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl?sortfield=&viewshelf=3
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-shelves.pl (e0481242e83653532915c1a03da0fb21)

Details

Form name: myform
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Form method: POST

Form inputs:

- REM-244 [Checkbox]

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?sortfield=title&viewshelf=1 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-shelves.pl (fb23de97afb322476f2ccc3d6dce3775)

Details

Form name: myform
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Form method: POST

Form inputs:

- REM-1807 [Checkbox]
- REM-2001 [Checkbox]
- REM-1986 [Checkbox]
- REM-1811 [Checkbox]
- REM-1809 [Checkbox]

Request headers

```
GET /cgi-bin/koha/opac-shelves.pl?direction=desc&sort=author&viewshelf=5 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-tags.pl

Details

Form name: <empty>
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-tags.pl
Form method: GET

Form inputs:

- limit [Text]

Request headers

```
GET /cgi-bin/koha/opac-tags.pl HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=ca76481c831b65f525433b9c1f5b4fe9
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-user.pl

Details

Form name: searchform
Form action: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl
Form method: GET

Form inputs:

- idx [Select]
- q [Text]
- branch_group_limit [Select]

Request headers

```
GET /cgi-bin/koha/opac-user.pl HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=ca76481c831b65f525433b9c1f5b4fe9
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Cookie without Secure flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

/

Details

Cookie name: "CGISESSID"
Cookie domain: "catalogo.minvu.cl"

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://catalogo.minvu.cl/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=ca76481c831b65f525433b9c1f5b4fe9
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Login page password-guessing attack

Severity	**Low**
Type	Validation
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks

Affected items

/cgi-bin/koha/opac-reserve.pl

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /cgi-bin/koha/opac-reserve.pl HTTP/1.1
Content-Length: 61
Content-Type: application/x-www-form-urlencoded
Referer: catalogo.minvu.cl
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

koha_login_context=AwuxhSh3&password=k05ZD6e7&userid=bfaqemly
```

/cgi-bin/koha/opac-reserve.pl

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /cgi-bin/koha/opac-reserve.pl HTTP/1.1
Content-Length: 76
Content-Type: application/x-www-form-urlencoded
Referer: catalogo.minvu.cl
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

biblionumbers=&koha_login_context=pdD2rtZ9&password=irqqyBjj&userid=fpdatbky
```

/cgi-bin/koha/opac-reserve.pl

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /cgi-bin/koha/opac-reserve.pl HTTP/1.1
Content-Length: 79
Content-Type: application/x-www-form-urlencoded
Referer: catalogo.minvu.cl
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

biblionumber=2532&koha_login_context=XTaz8sNN&password=BUWoGGhV&userid=hsmelkqo
```

/cgi-bin/koha/opac-sendshelf.pl

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /cgi-bin/koha/opac-sendshelf.pl HTTP/1.1
Content-Length: 71
Content-Type: application/x-www-form-urlencoded
Referer: catalogo.minvu.cl
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

koha_login_context=m5WkAZgt&password=V8KB8wj6&shelfid=1&userid=guvaqeef
```

/cgi-bin/koha/opac-user.pl

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
POST /cgi-bin/koha/opac-user.pl HTTP/1.1
Content-Length: 61
Content-Type: application/x-www-form-urlencoded
Referer: catalogo.minvu.cl
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

koha_login_context=2tQioenL&password=63hPK2MN&userid=rbxcpmqc
```

Broken links

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

/cgi-bin/koha/errors/404.pl

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /cgi-bin/koha/errors/404.pl HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-detail.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-showreviews.pl&format=rss2

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /cgi-bin/koha/opac-showreviews.pl&format=rss2 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-showreviews.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=efd8161dc331bf6810981c18fc56e328
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/images/estilos.css

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /opac-tmpl/bootstrap/images/estilos.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/opac-tmpl/bootstrap/images/quienes-somos.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Email address found

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_Dir.script)

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Email Address Disclosed on Website Can be Used for Spam

Affected items

/cgi-bin

Details

Pattern found: soporte@opengeek.cl

Request headers

```
GET /cgi-bin HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://catalogo.minvu.cl/cgi-bin
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha

Details

Pattern found: soporte@opengeek.cl

Request headers

```
GET /cgi-bin/koha HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://catalogo.minvu.cl/cgi-bin/koha
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/errors/404.pl

Details

Pattern found: soporte@opengeek.cl

Request headers

```
GET /cgi-bin/koha/errors/404.pl HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-detail.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-showreviews.pl&format=rss2

Details

Pattern found: soporte@opengeek.cl

Request headers

```
GET /cgi-bin/koha/opac-showreviews.pl&format=rss2 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-showreviews.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=efd8161dc331bf6810981c18fc56e328
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/images/estilos.css

Details

Pattern found: soporte@opengeek.cl

Request headers

```
GET /opac-tmpl/bootstrap/images/estilos.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/opac-tmpl/bootstrap/images/quienes-somos.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/bootstrap/images/quienes-somos.html

Details

Pattern found: cdocumentacion@minvu.cl

Request headers

```
GET /opac-tmpl/bootstrap/images/quienes-somos.html HTTP/1.1
Pragma: no-cache
```

```
Cache-Control: no-cache
Referer: http://catalogo.minvu.cl/opac-tmpl/bootstrap/images/quienes-somos.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/opac-tmpl/img

Details

Pattern found: soporte@opengeek.cl

Request headers

```
GET /opac-tmpl/img HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://catalogo.minvu.cl/opac-tmpl/img
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Password type input with auto-complete enabled

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:
<INPUT TYPE="password" AUTOCOMPLETE="off">

Affected items

/

Details

Password type input named password from form named auth with action /cgi-bin/koha/opac-user.pl has autocomplete enabled.

Request headers

```
GET / HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://catalogo.minvu.cl/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=ca76481c831b65f525433b9c1f5b4fe9
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-ratings.pl (132a3cea51a7d22cd3c58ac3e06b798a)

Details

Password type input named password from form named auth with action /cgi-bin/koha/opac-ratings.pl has autocomplete enabled.

Request headers

```
POST /cgi-bin/koha/opac-ratings.pl HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-detail.pl
Content-Length: 113
Content-Type: application/x-www-form-urlencoded
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

biblionumber=1&borrowernumber=&rate_button=Val%c3%b3reme&rating=1&rating_avg_int=5.0&rat
ing_total=1&rating_value=
```

/cgi-bin/koha/opac-reserve.pl

Details

Password type input named password from form named auth with action /cgi-bin/koha/opac-reserve.pl has autocomplete enabled.

Request headers

```
GET /cgi-bin/koha/opac-reserve.pl HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-topissues.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/cgi-bin/koha/opac-sendshelf.pl (2c611560f31d18190a5f099697f162f5)

Details

Password type input named password from form named auth with action /cgi-bin/koha/opac-sendshelf.pl has autocomplete enabled.

Request headers

```
GET /cgi-bin/koha/opac-sendshelf.pl?shelfid=7 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Possible server path disclosure (Unix)

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

One or more fully qualified path names were found on this page. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

Affected items

/cgi-bin/koha/svc/suggestion

Details

Pattern found: /usr/share/perl5/JSON.pm

Request headers

```
GET /cgi-bin/koha/svc/suggestion HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: CGISESSID=c14ce406794e5360246c7c529405803b
Host: catalogo.minvu.cl
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Scanned items (coverage report)

Scanned 69 URLs. Found 18 vulnerable.

URL: https://catalogo.minvu.cl/

Vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
/cgi-bin/koha/svc/	Path Fragment

Input scheme 2	
Input name	Input type
/opac-tmpl/bootstrap/images/	Path Fragment (suffix .html)

Input scheme 3	
Input name	Input type
Host	HTTP Header

URL: https://catalogo.minvu.cl/cgi-bin

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/cgi-bin/koha

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-search.pl

Vulnerabilities has been identified for this URL

151 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
branch_group_limit	URL encoded GET
idx	URL encoded GET
q	URL encoded GET

Input scheme 2	
Input name	Input type
do	URL encoded GET
idx	URL encoded GET
limit	URL encoded GET
limit-yr	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET

Input scheme 3	
Input name	Input type
do	URL encoded GET

Input scheme 4	
Input name	Input type
expanded_options	URL encoded GET

Input scheme 5	
Input name	Input type
format	URL encoded GET
idx	URL encoded GET

limit	URL encoded GET
q	URL encoded GET

Input scheme 6	
Input name	Input type
	URL encoded GET
count	URL encoded GET
format	URL encoded GET
sort_by	URL encoded GET

Input scheme 7	
Input name	Input type
q	URL encoded GET
tag	URL encoded GET

Input scheme 8	
Input name	Input type
q	URL encoded GET

Input scheme 9	
Input name	Input type
biblionumber	URL encoded GET
idx	URL encoded GET
loggedinuser	URL encoded GET
q	URL encoded GET
rating-1	URL encoded GET
rating-2	URL encoded GET
rating-3	URL encoded GET
rating-4	URL encoded GET
rating-8	URL encoded GET
sort_by	URL encoded GET

Input scheme 10	
Input name	Input type
idx	URL encoded GET
limit	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET

Input scheme 11	
Input name	Input type
expand	URL encoded GET
idx	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET

Input scheme 12	
Input name	Input type
idx	URL encoded GET
offset	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET

Input scheme 13	
Input name	Input type
count	URL encoded GET
format	URL encoded GET
idx	URL encoded GET
q	URL encoded GET

sort_by	URL encoded GET

Input scheme 14	
Input name	Input type
biblionumber	URL encoded GET
idx	URL encoded GET
loggedinuser	URL encoded GET
q	URL encoded GET
rating-1	URL encoded GET
rating-2	URL encoded GET
rating-3	URL encoded GET
rating-4	URL encoded GET
rating-5	URL encoded GET
sort_by	URL encoded GET

Input scheme 15	
Input name	Input type
format	URL encoded GET
idx	URL encoded GET
q	URL encoded GET

Input scheme 16	
Input name	Input type
biblionumber	URL encoded GET
idx	URL encoded GET
loggedinuser	URL encoded GET
q	URL encoded GET
rating-2001	URL encoded GET
rating-2532	URL encoded GET
sort_by	URL encoded GET

Input scheme 17	
Input name	Input type
biblionumber	URL encoded GET
idx	URL encoded GET
loggedinuser	URL encoded GET
q	URL encoded GET
rating-35	URL encoded GET
rating-36	URL encoded GET
rating-37	URL encoded GET
rating-38	URL encoded GET
rating-39	URL encoded GET
sort_by	URL encoded GET

Input scheme 18	
Input name	Input type
biblionumber	URL encoded GET
idx	URL encoded GET
limit	URL encoded GET
loggedinuser	URL encoded GET
q	URL encoded GET
rating-1978	URL encoded GET
rating-2532	URL encoded GET
sort_by	URL encoded GET

Input scheme 19	
Input name	Input type
idx	URL encoded GET

limit	URL encoded GET
limit	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET

Input scheme 20	
Input name	Input type
expand	URL encoded GET
idx	URL encoded GET
limit	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET

Input scheme 21	
Input name	Input type
count	URL encoded GET
format	URL encoded GET
idx	URL encoded GET
limit	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET

Input scheme 22	
Input name	Input type
do	URL encoded GET
idx	URL encoded GET
limit-yr	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET

Input scheme 23	
Input name	Input type
count	URL encoded GET
do	URL encoded GET
format	URL encoded GET
idx	URL encoded GET
limit	URL encoded GET
limit-yr	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET
sort_by	URL encoded GET

Input scheme 24	
Input name	Input type
count	URL encoded GET
do	URL encoded GET
format	URL encoded GET
idx	URL encoded GET
limit-yr	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET
sort_by	URL encoded GET

Input scheme 25	
Input name	Input type
do	URL encoded GET
idx	URL encoded GET
limit	URL encoded GET

limit-yr	URL encoded GET
op	URL encoded GET
q	URL encoded GET
sort_by	URL encoded GET

Input scheme 26	
Input name	Input type
addto	URL encoded GET
biblionumber	URL encoded GET
idx	URL encoded GET
loggedinuser	URL encoded GET
q	URL encoded GET
rating-1	URL encoded GET
rating-2	URL encoded GET
rating-3	URL encoded GET
rating-4	URL encoded GET
rating-8	URL encoded GET
sort_by	URL encoded GET

Input scheme 27	
Input name	Input type
addto	URL encoded GET
biblionumber	URL encoded GET
idx	URL encoded GET
loggedinuser	URL encoded GET
q	URL encoded GET
rating-2001	URL encoded GET
rating-2532	URL encoded GET
sort_by	URL encoded GET

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-user.pl

Vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
koha_login_context	URL encoded POST
password	URL encoded POST
userid	URL encoded POST

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-tags.pl

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
limit	URL encoded GET

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-shelves.pl

Vulnerabilities has been identified for this URL

31 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
sortfield	URL encoded GET
viewshelf	URL encoded GET

Input scheme 2	
Input name	Input type
display	URL encoded GET

Input scheme 3	
Input name	Input type
viewshelf	URL encoded GET

Input scheme 4	
Input name	Input type
shelfoff	URL encoded GET

Input scheme 5	
Input name	Input type
display	URL encoded GET
shelfoff	URL encoded GET

Input scheme 6	
Input name	Input type
direction	URL encoded GET
sort	URL encoded GET
viewshelf	URL encoded GET

Input scheme 7	
Input name	Input type
REM-1411	URL encoded POST

Input scheme 8	
Input name	Input type
shelves	URL encoded GET

Input scheme 9	
Input name	Input type
REM-1807	URL encoded POST
REM-1809	URL encoded POST
REM-1811	URL encoded POST
REM-1986	URL encoded POST
REM-2001	URL encoded POST

Input scheme 10	
Input name	Input type
REM-244	URL encoded POST

Input scheme 11	
Input name	Input type
REM-1908	URL encoded POST
REM-1924	URL encoded POST
REM-1925	URL encoded POST
REM-1939	URL encoded POST
REM-1949	URL encoded POST

Input scheme 12	
Input name	Input type
addshelf	URL encoded POST
allow_add	URL encoded POST
allow_delete_other	URL encoded POST
allow_delete_own	URL encoded POST
category	URL encoded POST
owner	URL encoded POST
shelves	URL encoded POST

sortfield	URL encoded POST

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-main.pl

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-topissues.pl

Vulnerabilities has been identified for this URL

10 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
branch	URL encoded GET
do_it	URL encoded GET
itemtype	URL encoded GET
limit	URL encoded GET
timeLimit	URL encoded GET

Input scheme 2	
Input name	Input type
branch	URL encoded POST
do_it	URL encoded POST
itemtype	URL encoded POST
limit	URL encoded POST
timeLimit	URL encoded POST

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-showreviews.pl

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
format	URL encoded GET

URL: https://catalogo.minvu.cl/cgi-bin/koha/unapi

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-detail.pl

No vulnerabilities has been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
biblionumber	URL encoded GET

Input scheme 2	
Input name	Input type
biblionumber	URL encoded GET
shelfbrowse_itemnumber	URL encoded GET

Input scheme 3	
Input name	Input type
biblionumber	URL encoded GET
query_desc	URL encoded GET

URL: https://catalogo.minvu.cl/cgi-bin/koha/svc/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/cgi-bin/koha/svc/suggestion

Vulnerabilities has been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
q	URL encoded GET
render	URL encoded GET

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-search-history.pl

No vulnerabilities has been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
action	URL encoded GET

Input scheme 2	
Input name	Input type
action	URL encoded GET
previous	URL encoded GET
type	URL encoded GET

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-reserve.pl

Vulnerabilities has been identified for this URL

13 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
biblionumber	URL encoded GET

Input scheme 2	
Input name	Input type
biblionumbers	URL encoded GET

Input scheme 3	
Input name	Input type
koha_login_context	URL encoded POST
password	URL encoded POST
userid	URL encoded POST

Input scheme 4	
Input name	Input type
biblionumber	URL encoded POST
koha_login_context	URL encoded POST
password	URL encoded POST
userid	URL encoded POST

Input scheme 5	
Input name	Input type
biblionumbers	URL encoded POST
koha_login_context	URL encoded POST
password	URL encoded POST

userid	URL encoded POST

URL: https://catalogo.minvu.cl/cgi-bin/koha/errors/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/cgi-bin/koha/errors/404.pl

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-ratings.pl

No vulnerabilities has been identified for this URL

20 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
biblionumber	URL encoded POST
borrowernumber	URL encoded POST
rate_button	URL encoded POST
rating	URL encoded POST
rating_avg_int	URL encoded POST
rating_total	URL encoded POST
rating_value	URL encoded POST

Input scheme 2

Input name	Input type
biblionumber	URL encoded POST
borrowernumber	URL encoded POST
koha_login_context	URL encoded POST
password	URL encoded POST
rate_button	URL encoded POST
rating	URL encoded POST
rating_avg_int	URL encoded POST
rating_total	URL encoded POST
rating_value	URL encoded POST
userid	URL encoded POST

Input scheme 3

Input name	Input type
koha_login_context	URL encoded POST
password	URL encoded POST
userid	URL encoded POST

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-export.pl

No vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
bib	URL encoded GET
format	URL encoded GET
op	URL encoded GET

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-MARCdetail.pl

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
biblionumber	URL encoded GET

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-ISBDdetail.pl

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
biblionumber	URL encoded GET

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-sendshelf.pl

Vulnerabilities has been identified for this URL

8 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
shelfid	URL encoded GET

Input scheme 2	
Input name	Input type
koha_login_context	URL encoded POST
password	URL encoded POST
shelfid	URL encoded POST
userid	URL encoded POST

Input scheme 3	
Input name	Input type
koha_login_context	URL encoded POST
password	URL encoded POST
userid	URL encoded POST

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-downloadshelf.pl

Vulnerabilities has been identified for this URL

8 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
shelfid	URL encoded GET
showprivateshelves	URL encoded GET

Input scheme 2	
Input name	Input type
format	URL encoded POST
save	URL encoded POST
shelfid	URL encoded POST

Input scheme 3	
Input name	Input type
context	URL encoded GET
shelfid	URL encoded GET
showprivateshelves	URL encoded GET

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-showreviews.pl&format=rss2

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/cgi-bin/koha/opac-showmarc.pl

No vulnerabilities has been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET
viewas	URL encoded GET

URL: https://catalogo.minvu.cl/opac-tmpl/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/css/opac.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/css/print.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/css/jquery.rating.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/jquery/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/jquery/jquery-ui.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/jquery/jquery.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/jquery/jquery-ui.js

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/jquery/plugins/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/jquery/plugins/jquery.rating.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/jquery/plugins/jquery.checkboxes.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/jquery/plugins/jquery.highlight-3.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/jquery/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/bootstrap/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/bootstrap/css/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/bootstrap/css/bootstrap.min.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/bootstrap/js/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/bootstrap/js/bootstrap.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/bootstrap/img/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/modernizr.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/lib/enquire.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/images/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/images/quienes-somos.html

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/images/estilos.css

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/js/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/js/global.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/js/basket.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/js/tags.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/js/google-jackets.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/js/datatables.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/js/script.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/itemtypeimg/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/bootstrap/itemtypeimg/bridge/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/lib/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/lib/jquery/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/lib/jquery/plugins/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/lib/jquery/plugins/jquery.dataTables.min.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/lib/famfamfam/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/lib/famfamfam/silk/

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: https://catalogo.minvu.cl/opac-tmpl/img

Vulnerabilities has been identified for this URL

No input(s) found for this URL