

MediaWiki open source project

Static analysis tools used:

- **RIPS** (Re-Inforce PHP Security)
- **RATS** (Rough Auditing Tool for Security)

Case studied and analysis methodology

- **OWASP ASVS v9**, Data Protection
 - Guarantee and enforce Confidentiality, Integrity, and Availability (CIA).
- Brute method, tune tools (RATS) for highest level of warning scan on whole source code and analyze results
- Manual detection and inspection of project's modules code to ensure compliance or not to security standard policies described by ASVS.

Result

Command Execution:	2
Protocol Injection:	1
File Disclosure:	11
File Inclusion:	31
File Manipulation:	14
SQL Injection:	1
Cross-Site Scripting:	41
HTTP Response Splitting:	1
Session Fixation:	1
Possible Flow Control:	3
Reflection Injection:	2
Sum:	108

Scanned files:	3726
Include success:	4131/4612 (90%)
Considered sinks:	298
User-defined functions:	36623
Unique sources:	157
Sensitive sinks:	77541



RIPS

Number of warnings reasonable to code extension.

Some false positive detected

- **Command injection** related to maintenance scripts.
- **SQL injection** warning due to an external library which runs a query without prepared statements, parameters are still sufficiently sanitised.

RATS

- Tons of verbose false warnings related to undistinguished comments-related characters.
- Most interesting warnings related to insecure function with related output hints on how to handle them more safely.

```
includes//GlobalFunctions.php:2421: High: popen
includes//GlobalFunctions.php:2433: High: popen
includes//GlobalFunctions.php:2497: High: popen
Argument 1 to this function call should be checked to ensure that it does not
come from an untrusted source without first verifying that it contains nothing
dangerous.

includes//cache/FileCacheBase.php:146: High: gzopen
Argument 1 to this function call should be checked to ensure that it does not
come from an untrusted source without first verifying that it contains nothing
dangerous.

includes//mail/UserMailer.php:411: High: mail
Arguments 1, 2, 4 and 5 of this function may be passed to an external
program. (Usually sendmail). Under Windows, they will be passed to a
remote email server. If these values are derived from user input, make
```

9.4 — Anti caching headers to prevent personal information to get saved on disk cache by most common browsers

```
# In general, the absence of a last modified header should be enough to prevent
# the client from using its cache. We send a few other things just to make sure.
$response->header( 'Expires:' . gmdate( 'D, d M Y H:i:s', 0 ) . ' GMT' );
$response->header( 'Cache-Control: no-cache, no-store, max-age=0, must-revalidate' );
$response->header( 'Pragma: no-cache' );
```

- Expires: date(...) -> HTTP 1.0 proxies & eventually HTTP 1.1
- Cache control (...) -> HTTP 1.1 browser agents & proxies
- Pragma: no-cache -> Prehistoric clients (e.g. IE6, HTTP 1.0 browsers agents < 1997)

For HTTP 1.1 *Cache-control* takes control over *Expires*, omitting it if the server auto-includes a valid date header, then you could theoretically rely on Expires only, but that may fail if e.g. end user manipulates the operating system date and the client software is relying on it. Parameter *max-age* alone will make resource (URL) "stale" and require browsers to check with the server if there's a newer version

Header	Cookie	Parametri	Risposta	Tempi	Analisi dello stack
URL richiesta: http://localhost/mediawiki/mw-config/index.php?css=1					
Metodo di richiesta: GET					
Status code: 200 OK ⓘ Modifica e reinvia Header non elaborati (raw)					
Versione: HTTP/1.1					
⌵ Filtra header					
▼ Header risposta (0 B)					
ⓘ Cache-Control: no-store, no-cache, must-revalidate					
ⓘ Content-type: text/css;charset=UTF-8					
ⓘ Date: Tue, 22 May 2018 08:25:01 GMT					
ⓘ Expires: Thu, 19 Nov 1981 08:52:00 GMT					
ⓘ Pragma: no-cache					
ⓘ Server: lighttpd/1.4.35					
ⓘ Transfer-Encoding: chunked					
ⓘ X-Content-Type-Options: nosniff					
▼ Header richiesta (0 B)					
ⓘ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8					
ⓘ Accept-Encoding: gzip, deflate					
ⓘ Accept-Language: en-GB,en;q=0.5					
ⓘ Connection: keep-alive					
ⓘ Cookie: mw_installer_session=cqju156afj6qj8rd6a0ll7v0v5					
ⓘ Host: localhost					
ⓘ User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu...) Gecko/20100101 Firefox/60.0					



V 9.1 — Sensitive data does not get cached

- No client-side caching (Cache-Control and Pragma headers)
- HTML forms auto-complete disabled
- What can happen:
 - sensitive data disclosure
- What if auto-complete + XSS vulnerability?
 - user interaction not needed (BlackHat USA conference 2010 & others)
- From MediaWiki official documentation:

Caching is only done for pages which:

- are not special pages.
- are not redirects.
- are being viewed in current version, plain view, no url parameters

V 9.1 — Sensitive data does not get cached

 <about:cache?storage=disk&context=> 

Information about the Network Cache Storage Service

☐ Private ☐ Anonymous AppID ☐ In Browser Element [Back to overview](#)

disk

Number of entries: 37
Maximum storage size: 358400 KiB
Storage in use: 1084 KiB
Storage disk location: /Users/lorenzo/Library/Caches/Firefox/Profiles/x8boeqso.default/cache2

Key	Data size	Fetch count	Last Modified	Expires	Pinning
http://192.168.1.111/mediawiki-1.30.0/load.php?debug=false&lang=en&modules=jquery.accessKeyLabel%2CcheckboxShiftClick%2Cclient%2CgetAttrs%2ChighlightText%2Cmw-jump%2Csuggestions%2CtabIndex%2Cthrottle-debounce%7Cmediawiki.RegExp%2Capi%2Cnotify%2CsearchSuggest%2Cstorage%2Cuser%2Cutil%7Cmediawiki.api.user%7Cmediawiki.page.ready%2Cstartup%7Cskins.vector.js%7Cuser.defaults&skin=vector&version=1bh3k65	54417 bytes	1	2018-05-21 16:10:32	2018-05-21 16:15:32	
http://192.168.1.111/mediawiki-1.30.0/load.php?debug=false&lang=en&modules=jquery%2Cmediawiki&only=scripts&skin=vector&version=0uv9445	176438 bytes	3	2018-05-21 16:10:09	2018-06-20 16:10:08	
http://192.168.1.111/mediawiki-1.30.0/load.php?debug=false&lang=en&modules=startup&only=scripts&skin=vector	17362 bytes	3	2018-05-21 16:10:07	2018-05-21 16:15:07	
http://192.168.1.111/mediawiki-1.30.0/index.php?title=Special:CreateAccount&returnto=Main+Page	<u>0 bytes</u>	0	No last modified time	No expiration time	

8

V 9.3 — Sensitive data does not get sent in the URL

- Data sent through GET requests will be accessible:
 - in the browser history
 - into server application's log files
 - by any intermediary (i.e. proxies) if unencrypted
- We've ensured every HTML form containing sensitive data had the *method* attribute set as POST, thus no such data is sent as URL parameter

V 9.9 — Client side storage does not contain secrets

- HTML5 Local Storage
- Cookies
- Secrets could be disclosed without the proper authorisation:
 - XSS
 - client vulnerabilities (i.e. SMB on Windows)
 - physical access

V 9.9 — Client side storage does not contain secrets

moz-extension://dedd2cd7-6c40-4775-83b9-c2fb39b2e22b - Cookie Quick Manager - Mozilla Firefox

Domains	Cookies	Details											
192.168.1.111 6	<table><tbody><tr><td>my_wiki_session=j3cu62988a7v3k8bmm8b7q4krecub14m</td></tr><tr><td>my_wikiUserID=6</td></tr><tr><td>my_wikiUserName=Atestuser</td></tr><tr><td>UseDC=master</td></tr><tr><td>UseCDNCache=false</td></tr><tr><td>cpPosTime=1525882369.9011</td></tr></tbody></table>	my_wiki_session=j3cu62988a7v3k8bmm8b7q4krecub14m	my_wikiUserID=6	my_wikiUserName=Atestuser	UseDC=master	UseCDNCache=false	cpPosTime=1525882369.9011	<table><tbody><tr><td>Domain</td></tr><tr><td>Name</td></tr><tr><td>Value</td></tr><tr><td>URL</td></tr><tr><td>B64</td></tr></tbody></table>	Domain	Name	Value	URL	B64
my_wiki_session=j3cu62988a7v3k8bmm8b7q4krecub14m													
my_wikiUserID=6													
my_wikiUserName=Atestuser													
UseDC=master													
UseCDNCache=false													
cpPosTime=1525882369.9011													
Domain													
Name													
Value													
URL													
B64													
		<table><tbody><tr><td>Path</td></tr><tr><td>Store</td></tr><tr><td>httpOnly</td></tr><tr><td>isSecure</td></tr><tr><td>isSession</td></tr></tbody></table>	Path	Store	httpOnly	isSecure	isSession						
Path													
Store													
httpOnly													
isSecure													
isSession													

168.1.111 ☐ Sub-domains

Thank you for your attention!

Any questions??