

Using Burp to Test for Components with Known Vulnerabilities

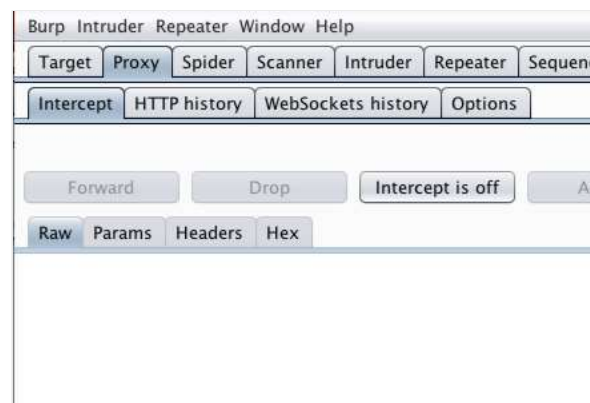
To determine whether your application is vulnerable it is important to keep abreast of the security status of the components that it uses. Vulnerabilities are reported to central clearing houses such as CVE and NVD.

Attackers are able to identify a weak component through scanning or manual analysis of a web application. You can simulate this process using Burp. In example we assess one potential vulnerability of a web server.

First, ensure that Burp is correctly **configured with your browser**.

Ensure Burp **Proxy** "Intercept is off".

Visit the web application you are testing in your browser.



Next, click the "**HTTP history**" tab.

In the HTTP history table select one of the captured request and response rows.

A screenshot of the Burp Suite application window showing the 'HTTP history' tab. The table displays a list of captured HTTP requests. The first row is highlighted.

#	Host	Method	URL
1	http://172.16.67.136	GET	/wordpress/
2	http://172.16.67.136	GET	/wordpress/wp-c
3	http://172.16.67.136	GET	/wordpress/wp-c
4	http://172.16.67.136	GET	/wordpress/wp-c
5	http://172.16.67.136	GET	/wordpress/wp-c
6	http://172.16.67.136	GET	/wordpress/wp-c
7	http://172.16.67.136	GET	/wordpress/wp-c
8	http://172.16.67.136	GET	/wordpress/
9	http://172.16.67.136	GET	/wordpress/wp-c
10	http://172.16.67.136	GET	/wordpress/wp-c

Click the "Response" tab.

Information regarding the web server used by the web application is provided in the response.

From either the "Raw" or "Headers" tab, make a note or copy the Server name and version number.

A screenshot of the Burp Suite application window showing the 'Response' tab. The table displays the response details for the selected request.

Name	Value
HTTP/1.1	200 OK
Date	Mon, 23 Feb 2015 15:59:55 GMT
Server	Apache/2.2.14 (Ubuntu) mod_mono/
X-Powered-By	PHP/5.3.2-1ubuntu4.5
X-Pingback	http://172.16.67.136/wordpress/xm
Status	200 OK
Vary	Accept-Encoding
Content-Length	8202
Keep-Alive	timeout=15, max=100
Connection	Keep-Alive
Content-Type	text/html; charset=UTF-8

With the server information at your disposal you can now use a search engine or one of the central clearing houses to check whether your web server has any known vulnerabilities.

Vulnerable components are usually fixed in a later version of the software. Upgrading or patching any components used by your web application is critical when securing your applications.

Additionally, it is possible to use the "Software Version Reporter" from the BApp store to **passively scan** for server software version numbers.

httpd.apache.org/security/vulnerabilities_22.html

Fixed in Apache httpd 2.2.15
important: mod_isapi module unload flaw

A flaw was found with within mod_isapi which mod_isapi, a remote attacker could send a n

Acknowledgements: We would like to thank

Reported to security team: 9th February 2010
Issue public: 2nd March 2010
Update Released: 5th March 2010
Affects: 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2

low: Subrequest handling of request header

Apache httpd 2.2 vulnerabilities

This page lists all security vulnerabilities fixed in released versions of Apache httpd the flaw is known to affect, and where a fla

Please note that if a vulnerability is shown below as being fixed in a '

This page is created from a database of vulnerabilities originally pop

Fixed in Apache httpd 2.2.29
important: mod_cgid denial of service CVE-2014-0231

A flaw was found in mod_cgid. If a server using mod_cgid hosted leading to denial of service.

Acknowledgements: This issue was reported by Rainer Jueng of th

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compare

Extensions BApp Store APIs Options

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to ex

Name	Installed	Rating	Detail
.NET Beautifier	<input type="checkbox"/>	★★★★★	
Active Scan++	<input type="checkbox"/>	★★★★★	Pro extension
Additional Scanne...	<input type="checkbox"/>	★★★★★	Pro extension
Authz	<input type="checkbox"/>	★★★★★	
Authorize	<input type="checkbox"/>	★★★★★	
Blazer	<input type="checkbox"/>	★★★★★	
Bradamsa	<input type="checkbox"/>	★★★★★	
Browser Repeater	<input type="checkbox"/>	★★★★★	
Buby	<input type="checkbox"/>	★★★★★	
Burp CSJ	<input type="checkbox"/>	★★★★★	
Bypass WAF	<input type="checkbox"/>	★★★★★	
Carbonator	<input type="checkbox"/>	★★★★★	Pro extension
CO2	<input type="checkbox"/>	★★★★★	
Cookie Attacker	<input type="checkbox"/>	★★★★★	Pro extension

Software Version
This extension can b
Often the server ver
examples are:
● "Apache Tomcat
● "Server: Apache/
● "X-AspNet-Vers
Author: August Det
Version: 1.1

Related articles:

- Getting started with Burp Proxy
- Getting started with Burp Scanner

Burp Suite

Web vulnerability scanner
Burp Suite Editions
Release Notes

Vulnerabilities

Cross-site scripting (XSS)
SQL injection
Cross-site request forgery
XML external entity injection
Directory traversal
Server-side request forgery

Customers

Organizations
Testers
Developers

Company

About
PortSwigger News
Careers
Contact
Legal
Privacy Notice

Insights

Web Security Academy
Blog
Research
The Daily Swig



Follow us

© 2020 PortSwigger Ltd

