

Vulnerability Scan with OWASP ZAP

Scan a Website and Investigate Vulnerability References

In this part of the lab, you will conduct a vulnerability scan using the Zed Attack Proxy (ZAP). Your target is an intentionally vulnerable website that is available on your VM. You will then use WSTG (Web Security Testing Guide) to learn more about a vulnerability that you discovered.

The screenshot shows the OWASP ZAP interface. At the top, it says "Automated Scan". Below that, there's a note: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'." It also includes a warning: "Please be aware that you should only attack applications that you have been specifically been given permission to test." The main configuration area has fields for "URL to attack" (set to "http://172.17.0.2/dvwa"), "Use traditional spider" (checked), and "Use ajax spider" (unchecked). There are "Attack" and "Stop" buttons. The "Progress" status is "Not started". Below this, the "Alerts" tab is selected, showing a list of 15 detected vulnerabilities. These include "Remote Code Execution - CVE-2012-1823" (2), "Source Code Disclosure - CVE-2012-1823" (2), "Absence of Anti-CSRF Tokens" (2), "Content Security Policy (CSP) Header Not Set" (4), "Directory Browsing" (3), "Hidden File Found" (1), "Missing Anti-clickjacking Header" (2), "Cookie No HttpOnly Flag" (4), "Cookie without SameSite Attribute" (4), "Server Leaks Information via "X-Powered-By" Header" (1), "Server Leaks Version Information via "Server" Header" (1), "X-Content-Type-Options Header Missing" (5), "Authentication Request Identified" (1), "Session Management Response Identified" (3), and "User Agent Fuzzer (R2)" (1).

The screenshot shows the OWASP ZAP interface with the 'Alerts' tab selected. A specific alert for 'Remote Code Execution - CVE-2012-1823' is highlighted with a red box. The alert details are as follows:

- URL:** http://172.17.0.2/dvwa/?d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input
- Risk:** High
- Confidence:** Medium
- Parameter:** (empty)
- Attack:** <?php exec('echo Samboviz6tj4gsyj5869';\$colm);echo join(" ,,\$colm);die();?>
- Evidence:** Samboviz6tj4gsyj5869
- CWE ID:** 20
- WASC ID:** 20
- Source:** Active (20018 - Remote Code Execution - CVE-2012-1823)
- Input Vector:** (empty)
- Description:** Some PHP versions, when configured to run using CGI, do not correctly handle query strings that lack an unescaped "=" character, enabling arbitrary code execution. In this case, an operating system command was

The screenshot shows the OWASP ZAP interface with the 'Alerts' tab selected. The same alert for 'Remote Code Execution - CVE-2012-1823' is highlighted. Below the alert details, there is a 'Solution' section with instructions to upgrade PHP or use Apache's mod_rewrite module. There is also a 'Reference' section with links to the project's website and the CVE definition. At the bottom, the 'Alert Tags' section is shown in a table:

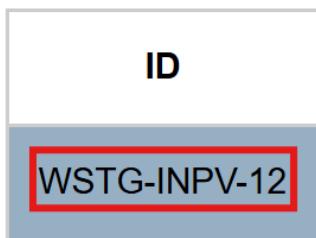
Key	Value
WSTG-v42-INPV-12	https://owasp.org/www-project-web-security...
OWASP_2021_A06	https://owasp.org/Top10/A06_2021-Vulnera...
OWASP_2017_A09	https://owasp.org/www-project-top-ten/201...
CVE-2012-1823	https://nvd.nist.gov/vuln/detail/CVE-2012-1823

Scroll down to the Alert Tags section of the vulnerability. Note the WSTG key and value.

WSTG - v4.2

[Home](#) > [V42](#) > [4-Web Application Security Testing](#) > [07-Input Validation Testing](#)

Testing for Command Injection



Summary

This article describes how to test an application for OS command injection.

Navigate to the WSTG site and read about the vulnerability and methods of testing for it. Review this information about the vulnerability to understand what WSTG offers to the penetration tester.