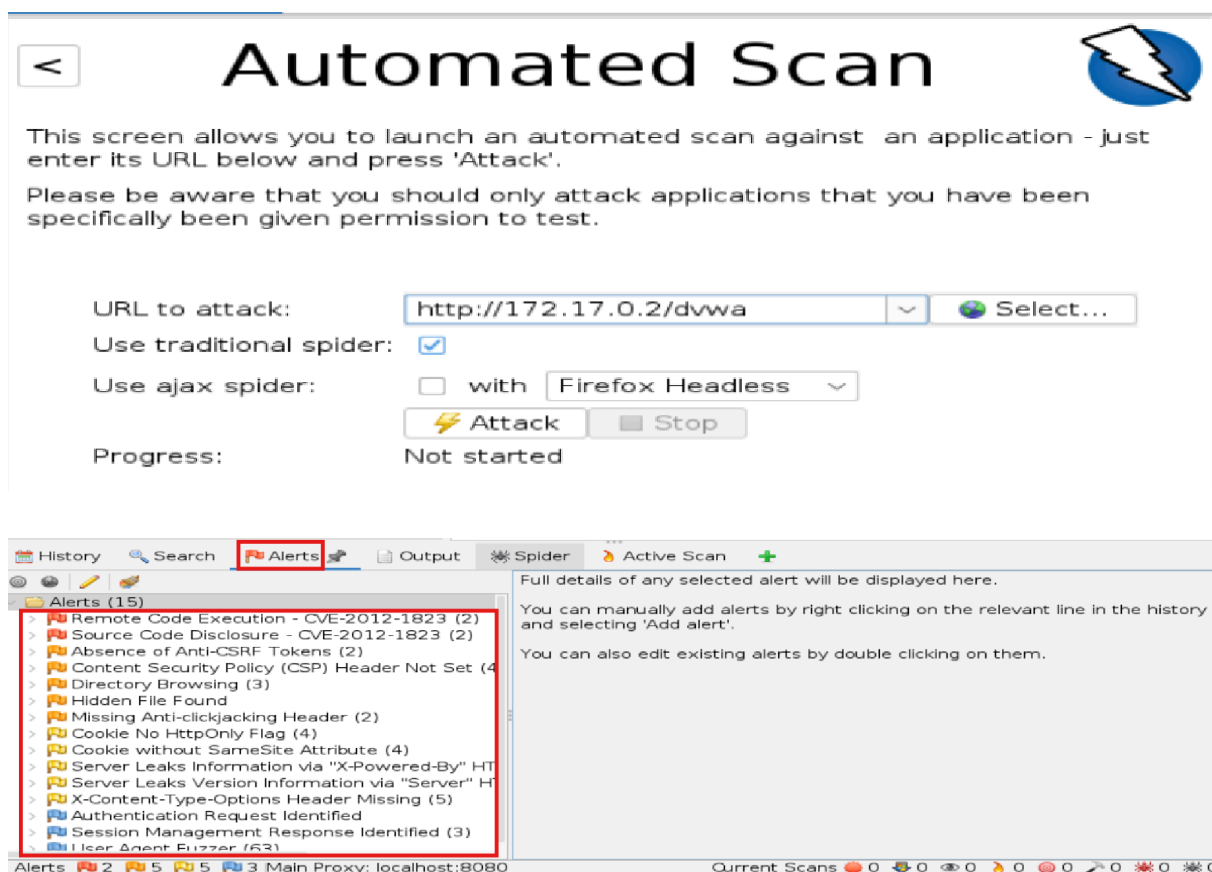


# Vulnerability Scan with OWASP ZAP

## 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.



**Remote Code Execution - CVE-2012-1823**

URL: `http://172.17.0.2/dvwa/?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input`

Risk: High

Confidence: Medium

Parameter:

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:

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

**Alert Tags**

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

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

## WSTG - v4.2

[Home](#) > [V4.2](#) > [4-Web Application Security Testing](#) > [07-Input Validation Testing](#)

### Testing for Command Injection

ID
WSTG-INPV-12

#### 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.