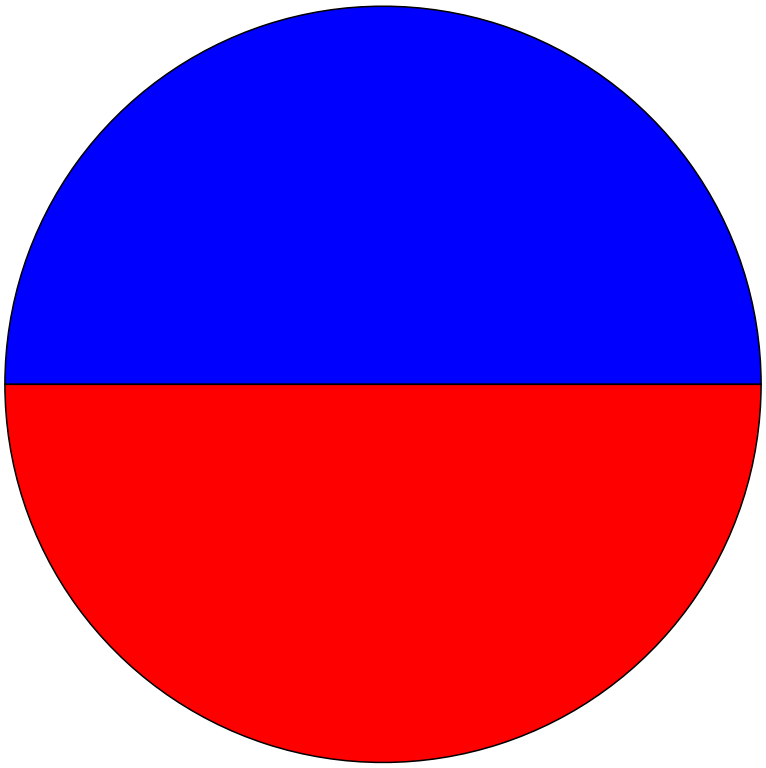
WebVulScan Detailed Report

Summary

Target Site:	http://127.0.0.1/DVWA/
Start Date/Time:	Wednesday 27th April 2016 08:46:09 AM
Finish Date/Time:	Wednesday 27th April 2016 08:51:08 AM
Duration:	4 minutes and 59 seconds
Report Generated on:	Wednesday 27th April 2016 08:51:08 AM
No. URLs Found:	2
No. Vulnerabilites Found:	4
No. HTTP Requests Sent:	245

Vulnerability Distribution

- 2 high risk
- 2 medium risk
- 0 low risk



Vulnerabilities Found

Directory Listing Enabled

Priority:

High

Description:

The contents of one or more directories can be viewed by web users. Therefore, when a user requests a directory such as http://www.example.com/directoryname/ using their browser, a list of all files and directories contained in the requested directory will be displayed to the user.

This could possibly expose sensitive information such as executables, text files, documentation, and installation and configuration files. An attacker could use these to map out the server's directory structure and identify potentially vulnerable files or applications.

Recommendations:

This can be a high risk vulnerability. This is typically enabled in the server's configuration file but can sometimes arise from a vulnerability in particular applications. You can eliminate this vulnerability by disabling directory listing in the server's configuration file and restart the server. The location and name of this file differs depending on what web server you are using.

Instances Found:

URL: http://127.0.0.1/DVWA/dvwa/css/
Method: GET
URL Requested: http://127.0.0.1/DVWA/dvwa/css/

URL: http://127.0.0.1/DVWA/dvwa/images/
Method: GET
URL Requested: http://127.0.0.1/DVWA/dvwa/images/

HTTP Banner Disclosure

Priority:

Medium

Description:

The application discloses information about the technologies used such as the web server, operating system, cryptography tools, or programming languages. An attacker could identify vulnerabilities in these technologies and use them to exploit the server, therefore, potentially exploiting the application.

Recommendations:

You can disable the server from disclosing this information to users. This is typically done by editing the configuration files of the various technologies and then restarting the system.

Instances Found:

URL: http://127.0.0.1/DVWA/
Method: GET
Information Exposed: Apache/2.4.10 (Win32) OpenSSL/0.9.8zb PHP/5.3.29

URL: http://127.0.0.1/DVWA/
Method: GET
Information Exposed: PHP/5.3.29

Thank you for scanning with WebVulScan!