

Индивидуальный проект шаг 4

Генералов Даниил, 1032212280

2024 г.

Российский университет дружбы народов, Москва, Россия

Задание

В этом этапе индивидуального проекта требуется использовать сканер уязвимостей nikto, чтобы найти какие-то уязвимости в DVWA.

Выполнение

```

dmgeneralov@dmgeneralov-kali: ~
File Actions Edit View Help

+ 0 host(s) tested

(dmgeneralov@dmgeneralov-kali)-[~]
$ nikto -host localhost:4280 -followredirects
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 4280
+ Start Time: 2024-10-05 22:59:10 (GMT3)

+ Server: Apache/2.4.62 (Debian)
+ /: Cookie security created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved X-powered-by header: PHP/8.3.12.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /?PHPBB85F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /login.php: Admin login page/section found.
+ 7851 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time: 2024-10-05 22:59:28 (GMT3) (18 seconds)

+ 1 host(s) tested

WARNING!
XSS (Stored)
*****
Portions of the server's headers (Apache/2.4.62) are not in the Nikto 2.5.0 database or are newer than the known string. Would you like to send it to your hosting provider's public mailing list? It is recommended using a virtual machine. If you are a good machine, you

```

Рис. 1: nikto

```

dmgeneralov@dmgeneralov-kali: ~
File Actions Edit View Help

+ 0 host(s) tested

(dmgeneralov@dmgeneralov-kali)-[~]
$ nikto -host http://localhost:4280/vulnerabilities/sqli/
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 4280
+ Start Time: 2024-10-05 23:04:18 (GMT3)

+ Server: Apache/2.4.62 (Debian)
+ /vulnerabilities/sqli/: Cookie security created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /vulnerabilities/sqli/: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /vulnerabilities/sqli/: Retrieved x-powered-by header: PHP/8.3.12.
+ /vulnerabilities/sqli/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /vulnerabilities/sqli/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /vulnerabilities/sqli/test.php: Potential PHP MSSQL database connection string found.
+ /vulnerabilities/sqli/?PHPB885F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /vulnerabilities/sqli/test.php: This might be interesting.
+ 7851 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time: 2024-10-05 23:04:38 (GMT3) (20 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.62) are not in

```

Рис. 2: nikto

```

dmgeneralov@dmgeneralov-kali: ~
File Actions Edit View Help
(dmgeneralov@dmgeneralov-kali)-[~]
$ nikto -host http://localhost:4280/vulnerabilities/fi/?page=include.php
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 4280
+ Start Time: 2024-10-05 23:12:39 (GMT3)

+ Server: Apache/2.4.62 (Debian)
+ /vulnerabilities/fi/: Cookie security created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /vulnerabilities/fi/: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /vulnerabilities/fi/: Retrieved x-powered-by header: PHP/8.3.12.
+ /vulnerabilities/fi/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /vulnerabilities/fi/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /vulnerabilities/fi/index.php?page=../../../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on the host. (probably Rocket, but could be any index.php).
+ /vulnerabilities/fi/index.php: PHP include error may indicate local or remote file inclusion is possible.
+ /vulnerabilities/fi/include.php: PHP error reveals file system path.
+ /vulnerabilities/fi/index.php?module=PostWrap&page=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSNAKE's RFI list. See: https://gist.github.com/mubix/5d269c686584875015a2
+ /vulnerabilities/fi/index.php?page=http://blog.cirt.net/rfiinc.txt: Remote File Inclusion (RFI) from RSNAKE's RFI list. See: https://gist.github.com/mubix/5d269c686584875015a2
+ /vulnerabilities/fi/index.php?page=http://blog.cirt.net/rfiinc.txt?: Remote File Inclusion (RFI) from RSNAKE's RFI list. See: https://gist.github.com/mubix/5d269c686584875015a2
+ 7850 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2024-10-05 23:13:01 (GMT3) (22 seconds)

+ 1 host(s) tested
More Information

```

Рис. 3: nikto

Выводы

Мы успешно использовали Nikto, чтобы найти какие-то уязвимости в DVWA, определить их тип и получить ссылки на источники, где есть информация о том, как их можно исправить.