Индивидуальный проект.

Этап 4. Использование nikto

Стариков Данила Андреевич

19 апреля 2024

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Цели и задачи

Цели и задачи

- Познакомиться с утилитой nikto для поиска уязвимостей веб-серверов
- Проверить ее работу на ранее установленном сервере DVWA

Результаты

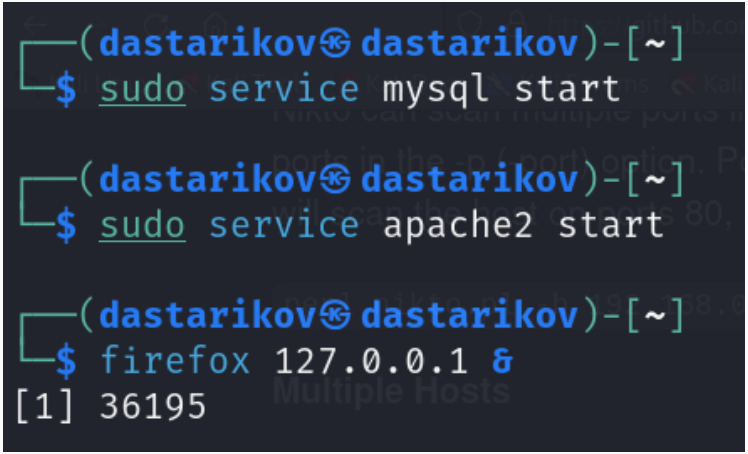


Рис. 1: Запус веб-сервера DVWA.

Результаты

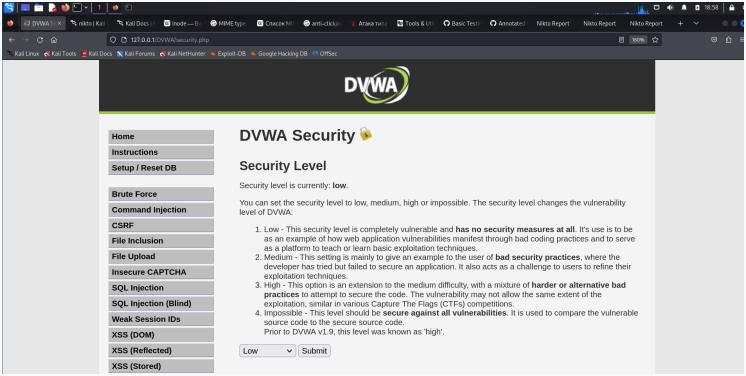


Рис. 2: Проверка работы сервера.

Результаты

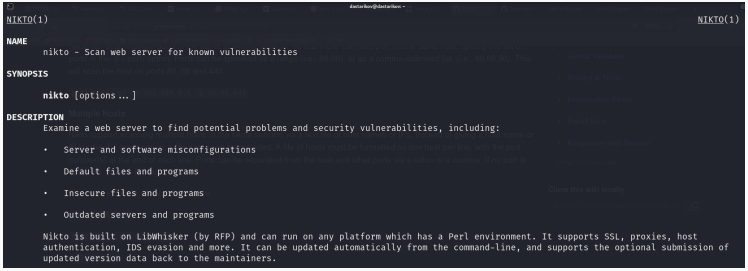


Рис. 3: Man-page nikto.

Результаты

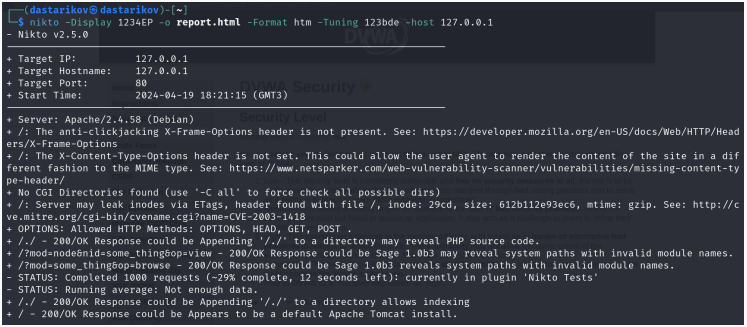
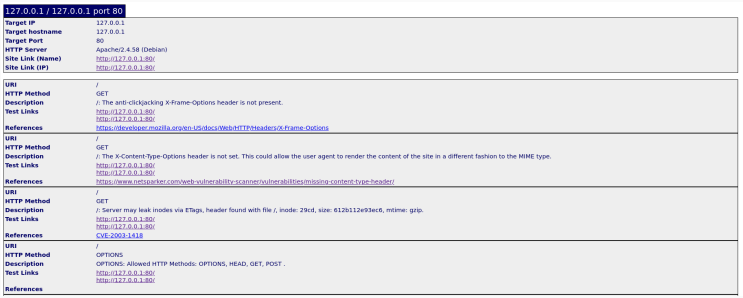


Рис. 4: Консольный вывод программы во время работы.

Результаты



127.0.0.1 / 127.0.0.1 port 80	
Target IP	127.0.0.1
Target hostname	127.0.0.1
Target Port	80
HTTP Server	Apache/2.4.58 (Debian)
Site Link (Name)	http://127.0.0.1:80/
Site Link (IP)	http://127.0.0.1:80/

URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/
HTTP Method	GET
Description	/: 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.
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/
HTTP Method	GET
Description	/: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 612b112e93ec6, mtime: gzip.
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	CVE-2003-1418
URI	/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	

Рис. 5: Пример найденной уязвимости веб-сервера.

Результаты

Host Summary

Start Time	2024-04-19 18:37:42
End Time	2024-04-19 18:38:01
Elapsed Time	19 seconds
Statistics	4300 requests, 0 errors, 5 findings

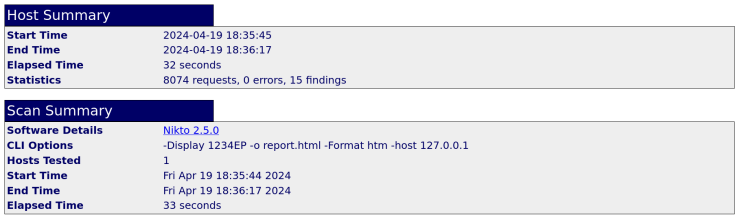
Scan Summary

Software Details	Nikto 2.5.0
CLI Options	-Display 1234EP -o report0.html -Format htm -Tuning 123bde -host 127.0.0.1
Hosts Tested	1
Start Time	Fri Apr 19 18:37:41 2024
End Time	Fri Apr 19 18:38:01 2024
Elapsed Time	20 seconds

© 2008 Chris Sullo

Рис. 6: Итоговый отчет по тестированию веб-сервера.

Результаты



Host Summary

Start Time	2024-04-19 18:35:45
End Time	2024-04-19 18:36:17
Elapsed Time	32 seconds
Statistics	8074 requests, 0 errors, 15 findings

Scan Summary

Software Details	Nikto 2.5.0
CLI Options	-Display 1234EP -o report.html -Format htm -host 127.0.0.1
Hosts Tested	1
Start Time	Fri Apr 19 18:35:44 2024
End Time	Fri Apr 19 18:36:17 2024
Elapsed Time	33 seconds

Рис. 7: Итоговый отчет по тестированию веб-сервера с большим числом тестов.

Итог

Итог

- В результате работы познакомились с утилитой `nikto` и проверили уязвимости веб-сервера DVWA с разными параметрами теста.