Индивидуальный проект шаг 4

Генералов Даниил, 1032212280

2024 г.

Российский университет дружбы народов, Москва, Россия

Задание

Задание

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

Выполнение

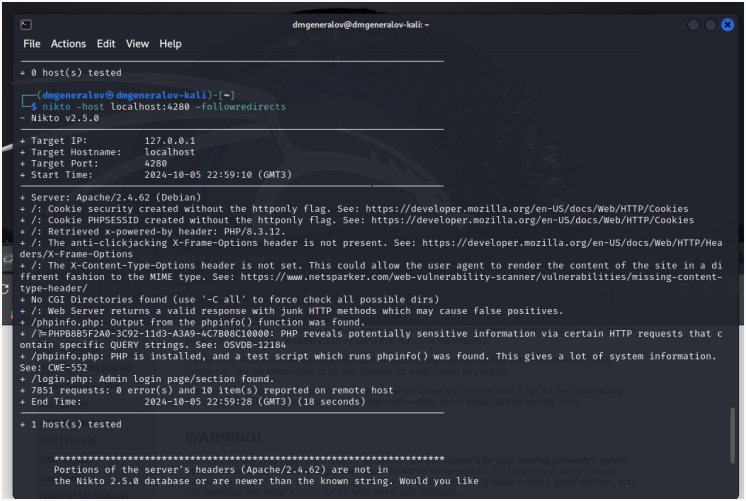
dmgeneralov@dmgeneralov-kali: ~
File Actions Edit View Help
+ 0 host(s) tested
(dmgeneralov㉿dmgeneralov-kali)-[~]
$ nikto -host localhost:4280 -followredirects
- Nikto v2.5.0
+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 4280
+ Start Time: 2024-10-05 22:59:10 (GMT3)
+ Server: Apache/2.4.62 (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.
+ /?=PHPB8B5F2A0-3C92-11d3-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
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

Рис. 1: nikto

Nikto

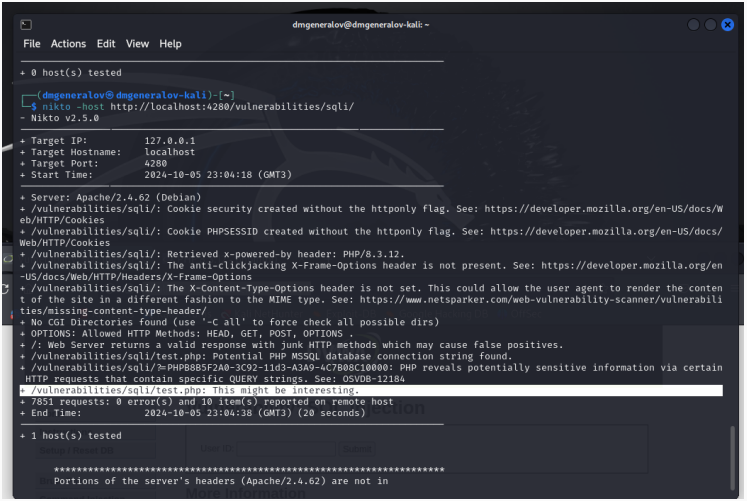

Рис. 2: nikto

Nikto

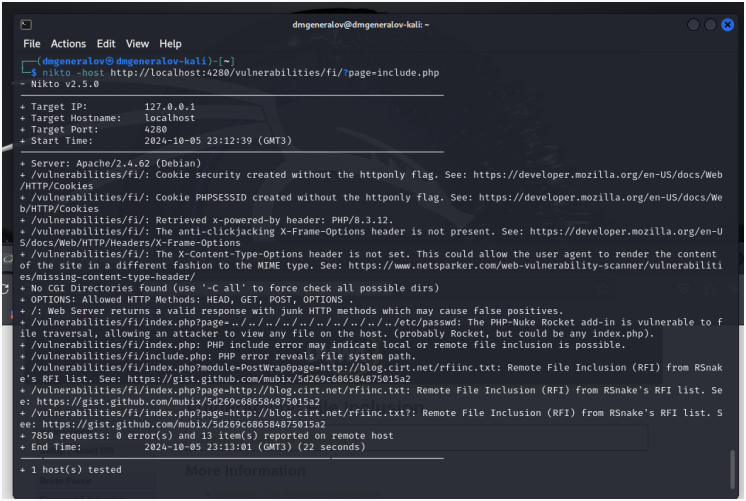

Рис. 3: nikto

Выводы

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.