

Презентация по четвертому этапу индивидуального проекта

Сканер nikto

Вакутайпа М.

01 мая 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Вакутайпа Милдред
- НКАбд-02-23
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов
- 1032239009@rudn.ru
- <https://wakutaipa.github.io>

Цель работы

Научиться тестировать веб-приложений со сканером nikto.

Выполнение работы

По сколько буду сканировать веб-приложение DVWA запускаю его.



```
mwakutaipa@wakutaipa: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/mwakutaipa/.zsh_history  
(mwakutaipa@wakutaipa)-[~]  
$ sudo systemctl start mysql  
[sudo] password for mwakutaipa:  
(mwakutaipa@wakutaipa)-[~]  
$ sudo systemctl start apache2  
(mwakutaipa@wakutaipa)-[~]  
$
```

Рис. 1: запуск сервера

Изменение уровня безопасности

Далее изменяю уровня безопасности на среднее.

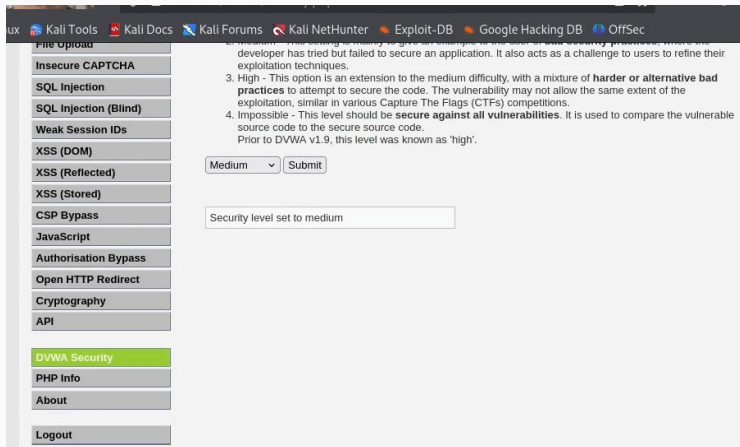


Рис. 2: Изменение уровня безопасности

Запускаю nikto используя #nikto и сканирую DVWA введя его полный URL без порта.

```
(mwakutaipa@wakutaipa)-[~]e/mwakutaipa/.zsh_history
$ #nikto
(mwakutaipa@wakutaipa)-[~]
$ nikto -h http://127.0.0.1/DVWA/
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2025-04-29 19:44:31 (GMT3)
```

Рис. 3: Сканирование 1 с nikto

Сканирование 2 с nikto

Сканирую второй раз введя полный URL DVWA с портом и заметила, что результаты не сильно отличаются.

```
(mwakutaipa@wakutaipa)-[~]  
$ nikto -h 127.0.0.1 -p 80  
- Nikto v2.5.0  
  
+ Target IP: 127.0.0.1  
+ Target Hostname: 127.0.0.1  
+ Target Port: 80  
+ Start Time: 2025-04-29 19:46:03 (GMT3)  
  
+ Server: Apache/2.4.62 (Debian)  
+ /: 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)  
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 62ea6484f649b, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
```

Рис. 4: Сканирование 2 с nikto

Выводы

Научилась тестировать веб-приложений со сканером nikto.