

Индивидуальный проект - этап 4

Мохаммади Мохаммад Хафиз¹

2 октября, 2024, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Целью данной работы является изучение сканера уязвимостей nikto.

Процесс выполнения лабораторной работы

Nikto — это популярный сканер веб-серверов с открытым исходным кодом, который проверяет веб-серверы на наличие уязвимостей, неправильных настроек, устаревших версий ПО и прочих проблем безопасности.

Nikto написан на Perl, и для его работы необходимо наличие Perl на системе.

Сканирование веб-сервера

```
perl nikto.pl -h <URL>
```

Nikto может использоваться для пассивного сканирования DVWA, выявления базовых уязвимостей и проверок на неправильную конфигурацию.

Когда DVWA запущено, мы можем использовать Nikto для сканирования. Основной командой для сканирования будет:

```
perl nikto.pl -h http://localhost/dvwa/
```

Сканирование localhost

```
[user@webmaster] ~  
$ nikt0 -h localhost  
- Nikto v2.3.0  
  
+ Target IP: 127.0.0.1  
+ Target Hostname: localhost  
+ Target Port: 80  
+ Start Time: 2024-10-05 12:05:51 (GMT3)  
  
+ Server: Apache/2.4.59 (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: 29d, size: 6210543cc327, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD  
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-56  
+ 7850 requests: 0 error(s) and 5 item(s) reported on remote host  
+ End Time: 2024-10-05 12:06:13 (GMT3) (22 seconds)  
  
+ 1 host(s) tested
```

Figure 1: Тестирование localhost

Сканирование localhost/dvwa/

```
(user@mhhammadil): ~  
$ nikto -h localhost -root /dvwa  
- Nikto v2.5.0  
  
+-----+  
+ Target IP:      127.0.0.1  
+ Target Hostname: localhost  
+ Target Port:    80  
+ Target Path:    /dvwa  
+ Start Time:     2024-10-05 12:06:33 (GMT+3)  
+-----+  
  
+ Server: Apache/2.4.59 (Debian)  
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /dvwa/: 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: GET, POST, OPTIONS, HEAD  
+ 2549 requests: 0 error(s) and 3 item(s) reported on remote host  
+ End Time:      2024-10-05 12:06:53 (GMT+3) (20 seconds)  
+-----+  
  
+ 1 host(s) tested
```

Figure 2: Тестирование localhost/dvwa/

Выводы по проделанной работе

Мы изучили возможности сканера nikto.