

Индивидуальный проект. Этап 4

Использование nikto

Парфенова Е. Е.

3 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Парфенова Елизавета Евгеньевна
- студент
- Российский университет дружбы народов
- 1032216437@pfur.ru
- <https://github.com/parfenovae>



Вводная часть

Важность наличия умения сканировать различные веб-приложения на уязвимости с целью их устранения

Цель: Использование веб-сканера Nikto для сканирования уязвимостей веб-приложений

Задачи: Использовать Nikto для сканирования DVWA

Теоретическое введение

Nikto – веб-сканер, проверяющий веб-серверы на самые частые ошибки, возникающие обычно из-за человеческого фактора. Проверяет целевой веб-сервер на наличие опасных файлов и исполняемых сценариев, инструментов администрирования базами данных, устаревшего программного обеспечения.

Он является бесплатным (open source) сканером. Утилита относится к классу blackbox сканеров. Программа может обнаруживать более 6700 потенциально опасных файлов и уязвимостей. Новые уязвимости добавляются в базу данных программы по мере их возникновения.

При сканировании сайта в логах сайта или в любой другой системе обнаружения вторжений, если Nikto используется, будет отображена информация о том, что сайт подвергается сканированию.

Среди функций Nikto можно выделить следующие:

- поддержка SSL
- поддержка HTTP прокси
- создание отчетов в текстовом формате, XML, HTML, NBE или CSV
- возможность сканирования портов
- поиск поддоменов
- поддержка плагинов для расширения функционала сканирования

Выполнение четвертого этапа проекта

Запуск веб-приложения DVWA

```
(eeparfenova@eeparfenova)-[~]  
$ sudo service apache2 start  
  
(eeparfenova@eeparfenova)-[~]  
$ service mariadb start  
  
(eeparfenova@eeparfenova)-[~]  
$ █
```

Рис. 1: Запуск веб-приложения DVWA

```
(eeparfenova@eeparfenova)-[~]  
$ perl -v  
  
This is perl 5, version 38, subversion 2 (v5.38.2) built for x86_64-linux-gnu-thread-multi  
(with 44 registered patches, see perl -V for more detail)  
  
Copyright 1987-2023, Larry Wall  
  
Perl may be copied only under the terms of either the Artistic License or the  
GNU General Public License, which may be found in the Perl 5 source kit.  
  
Complete documentation for Perl, including FAQ lists, should be found on  
this system using "man perl" or "perldoc perl". If you have access to the  
Internet, point your browser at https://www.perl.org/, the Perl Home Page.  
  
Home  
(eeparfenova@eeparfenova)-[~]  
$ nikto  
- Nikto v2.5.0
```

Рис. 2: Проверка наличия nikto

Сканирование DVWA. URL

```
(eeperfenova@eeperfenova)-[~]
$ nikto -h http://localhost/DVWA/ -output report.txt -Format text
- Nikto v2.5.8

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-10-01 20:07:14 (GMT3)

+ Server: Apache/2.4.62 (Ubuntu)
+ /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.netsec.org.uk/articles/missing-content-type-header/
+ Root page /DVWA redirects to: login.php
+ No CGI Directories Found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /DVWA/config/: Directory indexing found.
+ /DVWA/config/: Configuration information may be available remotely.
+ /DVWA/tests/: Directory indexing found.
+ /DVWA/tests/: This might be interesting.
+ /DVWA/database/: Directory indexing found.
+ /DVWA/database/: Database directory found.
+ /DVWA/docs/: Directory indexing found.
+ /DVWA/login.php: Admin login page/section found.
+ /DVWA/.git/index: Git Index file may contain directory listing information.
+ /DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /DVWA/.git/config: Git config file found. Infos about repo details may be present.
+ /DVWA/.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ 7850 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time: 2024-10-01 20:07:20 (GMT3) (6 seconds)

+ 1 host(s) tested
```

Рис. 3: Сканирование DVWA

Сканирование DVWA. URL

[illegible]

Рис. 4: Отчет в текстовом формате

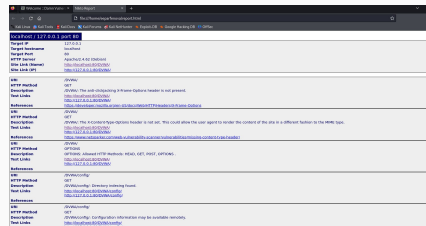


Рис. 5: Отчет в формате html

В результате сканирования было найдено 16 уязвимостей. В них входят:

- Отсутствие заголовка X-Frame-Options и X-Content-Type-Options
- Обнаружена индексация каталогов в /DVWA/config/, /DVWA/tests/, /DVWA/database/ и т.д.
- Найдены страницы для входа в административную панель и конфигурационные файлы Git (скрытая папка Git), которые могут содержать важную информацию о структуре проекта (сайта) и репозитории.

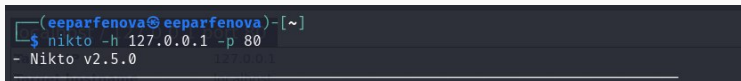

```
(esperfenova@esperfenova)-[~]
$ nikto -h 127.0.0.1
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    80
+ Start Time:     2024-10-01 20:14:37 (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: 622059c13b)c9, mtime: grip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ //etc/hosts: The server install allows loading of any system file by adding an extra '/' to the URL.
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /login.cgi?cli=xx32bak7cat20/etc/hosts: Some D-link router remote command execution.
+ /shell?cat=/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:      2024-10-01 20:14:44 (GMT3) (7 seconds)

+ 1 host(s) tested
```

Рис. 6: Сканирование с помощью IP

A terminal window with a dark background. The prompt is '(eeparfenova@eeparfenova)-[~]'. The command '\$ nikto -h 127.0.0.1 -p 80' has been entered. The output line shows '- Nikto v2.5.0' followed by '127.0.0.1' and a progress bar.

```
(eeparfenova@eeparfenova)-[~]  
$ nikto -h 127.0.0.1 -p 80  
- Nikto v2.5.0 127.0.0.1
```

Рис. 7: Команда сканирования с IP и портом

При таком сканировании было найдено 15 уязвимостей

- Утечка информации о файловой системе через ETags
- Уязвимость чтения системных файлов с помощью манипуляций с URL
- PHP Backdoor file manager был обнаружен в нескольких местах
- Уязвимость удаленного выполнения команд на роутерах D-Link.

Вывод

Мы использовали веб-сканера Nikto для сканирования уязвимостей веб-приложений, а конкретно для сканирования DVWA