

Индивидуальный проект Этап №4

Использование nikto

Чванова Ангелина Дмитриевна

2024 год

Российский университет дружбы народов, Москва, Россия

Докладчик

- Чванова Ангелина Дмитриевна
- студент
- Российский университет дружбы народов
- angelinachdm@gmail.com
- <https://adchvanova-new.github.io/ru/>



Цель работы

Изучение сканера nikto и методов тестирования веб-приложений с помощью сканера nikto

Задание

Использование nikto.

Теоретическое введение

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. Поскольку *nikto* построен исключительно на LibWhisker2, он сразу после установки поддерживает кросс-платформенное развертывание, SSL (криптографический протокол, который подразумевает более безопасную связь), методы аутентификации хоста (NTLM/Basic), прокси и несколько методов уклонения от идентификаторов. Он также поддерживает перечисление поддоменов, проверку безопасности приложений (XSS, SQL-инъекции и т. д.) и способен с помощью атаки паролей на основе словаря угадывать учетные данные авторизации.

Выполнение лабораторной работы

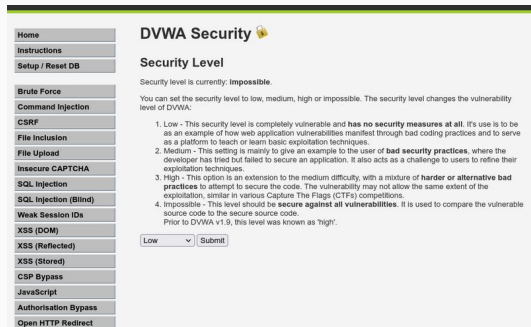
Для того чтобы работать с nikto, нужно подготовить веб-приложение, которое будем сканировать. В нашем случае было выбрано DVWA, для этого запускаем apache2

```
(kali㉿kali)-[~/Downloads]
$ sudo systemctl start mysql
[sudo] password for kali:
(kali㉿kali)-[~/Downloads]
$ sudo systemctl start apache2
```

Рис. 1: Запуск apache2

Выполнение лабораторной работы

В адресной строке браузера вводим адрес DVWA, переходим в режим выбора уровня безопасности, ставим минимальный (nikto при обычном сканировании для режима impossible и low выдаст одинаковые потенциальные уязвимости, так как все уязвимости остаются, но изменяется сложность, с которой их можно использовать)



The screenshot shows the DVWA Security configuration page. On the left is a sidebar with navigation links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, Authorisation Bypass, and Open HTTP Redirect. The main content area is titled 'DVWA Security' with a padlock icon. Below the title is the 'Security Level' section, which states 'Security level is currently: impossible.' and explains that the level can be set to low, medium, high, or impossible. A list of four levels is provided: 1. Low (completely vulnerable), 2. Medium (bad security practices), 3. High (extension of medium difficulty), and 4. Impossible (secure against all vulnerabilities). At the bottom, there is a dropdown menu currently set to 'Low' and a 'Submit' button.

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect

DVWA Security

Security Level

Security level is currently: impossible.


You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and has **no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low ▼ Submit

Выполнение лабораторной работы

Запускаем nikto

A terminal window with a dark background. The prompt is '(kali@kali)-[~/Downloads]' in blue and white. Below it, the command '\$ #nikto' is entered in blue, followed by a white cursor. There is some faint, illegible text in the background of the terminal window.

```
(kali@kali)-[~/Downloads]  
$ #nikto
```

Рис. 3: Запуск nikto

Выполнение лабораторной работы

Проверяем веб-приложение, введя его полный URL и не вводя порт

```
$ 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: 2024-04-27 17:34:23 (GMT3)

+ Server: Apache/2.4.58 (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
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/
+ Root page /DVWA redirects to: login.php
+ No GET Directories found (use '-c all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /DVWA///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /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.
["[B]"["[B]"["[B]"["[B]"["[B]"["[B]"["[B]"["[B]"+ /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/wp-content/themes/twentyeleven/images/headers/server-phpfilesrc-/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/wp-content/themes/twentyeleven/images/headers/server-phpfilesrc-/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-wordpress/wp-includes/Requests/Utility/content-post.php?filesrc-/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/js/tinymce/themes/MODERN/Meuihu.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-wordpress/wp-includes/js/tinymce/themes/MODERN/Meuihu.php?filesrc-/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /DVWA/login.cgi?cll=aa%20aa%2Cat%20/etc/hosts: Some D-link router remote command execution.
+ /DVWA/shell.txt:/etc/hosts: A backdoor was identified.
+ /DVWA/dockergenerator_dockergenerator file found. It may be possible to grasp the directory structure and learn more about the site.
8874 requests: 0 error(s) and 26 item(s) reported on remote host
End Time: 2024-04-27 17:35:22 (GMT3) (59 seconds)
```

Рис. 4: Проверка веб-приложения

Выполнение лабораторной работы

Затем сканируем, введя адрес хоста и адрес порта, результаты отличаются незначительно

[illegible]

Рис. 5: Сканирование

Анализ результатов сканирования

Кроме адреса хоста и порта веб-приложения, никто выводит информацию о различных уязвимостях приложения:

Сервер: Apache/2.4.58 (Debian) + /DVWA/: Заголовок X-Frame-Options, защищающий от перехвата кликов, отсутствует. Смотрите:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

- /DVWA/: Заголовок X-Content-Type-Options не задан. Это может позволить пользовательскому агенту отображать содержимое сайта способом, отличным от MIME-типа. Смотрите:
<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>

Анализ результатов сканирования

- /DVWA/config/: Информация о конфигурации может быть доступна удаленно.
- /DVWA/tests/: Найдена индексация каталога.
- /DVWA/tests/: Это может быть интересно.
- /DVWA/database/: Найдена индексация каталога.
- /DVWA/база данных/: Найден каталог базы данных.
- /DVWA/документы/: Найдена индексация каталога.
- /DVWA/login.php: Найдена страница входа администратора/раздел.

Анализ результатов сканирования

- /DVWA/.git/index: Индексный файл Git может содержать информацию о списке каталогов.
- /DVWA/.git/HEAD: Найден файл Git HEAD. Может содержаться полная информация о репозитории.
- /DVWA/.git/config: Найден конфигурационный файл Git. Может содержаться информация о деталях репозитория.
- /DVWA/.gitignore: найден файл .gitignore. Можно разобраться в структуре каталогов.
- /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts:
Обнаружен файловый менеджер с бэкдором на PHP.

Анализ результатов сканирования

Бэкдор, тайный вход (от англ. back door — «чёрный ход», «лазейка», буквально «задняя дверь») — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным. Также в результатах nikto отображает код OSVDB 561 и дает ссылку на CVE-2003-1418. OSVDB — это аббревиатура базы данных уязвимостей с открытым исходным кодом.

- Заголовок ETag, который раскрывает номер vode.
- Многочастную границу MIME, которая раскрывает идентификаторы дочерних процессов (PID).

В рамках выполнения этапа индивидуального проекта был изучен и использован сканер nikto для тестирования веб-приложений

Список литературы

[1] Документация по Virtual Box:

<https://www.virtualbox.org/wiki/Documentation>