

Отчет к 4 этапу индивидуального проекта

Common information

discipline: Основы информационной безопасности

group: НПМбд-02-21

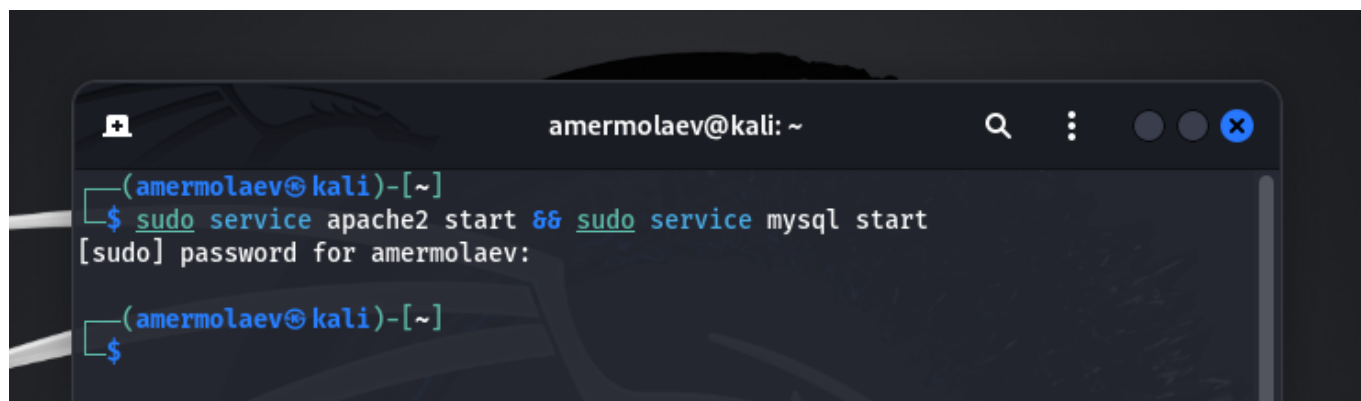
author: Ермолаев А.М.

Цель работы

Приобретение практических навыков по использованию инструмента nikto - базового сканера безопасности веб-сервера.

Выполнение работы

Для работы приложения запустим сервисы Apache2 и MySQL:



```
amermolaev@kali: ~  
(amermolaev@kali)-[~]  
$ sudo service apache2 start && sudo service mysql start  
[sudo] password for amermolaev:  
(amermolaev@kali)-[~]  
$
```

Теперь откроем в браузере приложение DVWA, перейдем в раздел

DVWA Security

и выберем опцию "Low":

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

DVWA Security

Security Level

Security level is currently: low.

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

Теперь воспользуемся утилитой nikto. Базовые опции таковы:

```
nikto -h <host or ip>
```

```
(amermolaev@kali)-[~]
└─$ nikto -h http://localhost/DVWA/
Nikto v2.5.0
-----
+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-09-30 17:48:07 (GMT3)
-----
+ Server: Apache/2.4.62 (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/
+ Root page /DVWA redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /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: 2024-09-30 17:48:17 (GMT3) (10 seconds)
-----
+ 1 host(s) tested
```

Теперь для эксперимента изменим настройку защиты на "Impossible" из запустим утилиту повторно:

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

Authentication Bypass

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'.

Impossible

Submit

Security level set to impossible

```
amercolaev@kali: ~
$ nikto -h http://localhost/DVWA/
Nikto v2.5.0
-----
+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-09-30 17:50:32 (GMT3)
-----
+ Server: Apache/2.4.62 (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/
+ Root page /DVWA redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /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: 2024-09-30 17:50:41 (GMT3) (9 seconds)
-----
+ 1 host(s) tested
```

Как видно, вывод утилиты не изменился.

Проведем анализ вывода:

- **Server: Apache/2.4.62 (Debian)**
- **/DVWA/: The anti-clickjacking X-Frame-Options header is not present.**

Отсутствие заголовка X-Frame-Options означает, что сайт может быть подвержен атаке clickjacking.

Кликджекинг (clickjacking) — обманная технология, основанная на размещении вызывающих какие-то действия невидимых элементов на сайте поверх видимых активных (кнопки, воспроизведение видео и т. д.).

- **/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.**

Если заголовок X-Content-Type-Options не установлен, это может привести к тому, что старые версии Internet Explorer и Chrome будут выполнять MIME-анализ тела ответа. Это может привести к тому, что тело ответа будет интерпретировано и отображено как тип контента, отличный от объявленного.

- **Root page /DVWA redirects to: login.php**

Иллюстрация имени авторизационного скрипта.

- **OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD.**

Эндпоинт имеет несколько методов.

- **/DVWA/config/: Directory indexing found.**

Найдена индексация каталогов.

- **/DVWA/config/: Configuration information may be available remotely.**

Найден эндпоинт, по которому может содержаться информация о конфигурации

- **/DVWA/tests/: Directory indexing found.**

Найдена индексация каталогов.

- **/DVWA/tests/: This might be interesting.**

Найдена папка с тестами.

- **/DVWA/database/: Directory indexing found.**

Найдена индексация каталогов.

- **/DVWA/database/: Database directory found.**

Найдена директория, содержащая информацию о БД

- **/DVWA/docs/: Directory indexing found.**

Найдена индексация каталогов.

- **/DVWA/login.php: Admin login page/section found.**

Найден эндпоинт для входа в админ-панель

- **/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.**

Найдена информацию о системе контроля версий.

- **/DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.**

Файл .dockerignore содержит список файлов и папок, которые быть исключены при сборки образов Docker для развертывания в контейнерах.

Вывод

В рамках выполнения работы я приобрел практический навык по использованию инструмента nikto - базового сканера безопасности веб-сервера.

Список литературы

- <https://github.com/digininja/DVWA?tab=readme-ov-file>
- <https://www.kali.org/>
- <https://www.kali.org/tools/nikto/>
- <https://habr.com/ru/companies/otus/articles/492546/>