Front matter

lang: ru-RU title: "personal project#4" subtitle: "Дисциплина: Основы информационной безопасности" author: "Георгес Гедеон"

Formatting

toc-title: "Содержание" toc: true # Table of contents toc_depth: 2 lof: true # Список рисунков lot: true # Список таблиц fontsize: 12pt linestretch: 1.5 papersize: a4paper documentclass: scrreprt polyglossia-lang: russian polyglossia-otherlangs: english mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase indent: true pdf-engine: lualatex header-includes:

- \linepenalty=10 # the penalty added to the badness of each line within a paragraph (no associated penalty node) Increasing the value makes tex try to have fewer lines in the paragraph.
- \interlinepenalty=0 # value of the penalty (node) added after each line of a paragraph.
- \hyphenpenalty=50 # the penalty for line breaking at an automatically inserted hyphen
- \exhyphenpenalty=50 # the penalty for line breaking at an explicit hyphen
- \binoppenalty=700 # the penalty for breaking a line at a binary operator
- \relpenalty=500 # the penalty for breaking a line at a relation
- \clubpenalty=150 # extra penalty for breaking after first line of a paragraph
- \widowpenalty=150 # extra penalty for breaking before last line of a paragraph
- \displaywidowpenalty=50 # extra penalty for breaking before last line before a display math
- \brokenpenalty=100 # extra penalty for page breaking after a hyphenated line
- \predisplaypenalty=10000 # penalty for breaking before a display
- \postdisplaypenalty=0 # penalty for breaking after a display

- \floatingpenalty = 20000 # penalty for splitting an insertion (can only be split footnote in standard LaTeX)
- \raggedbottom # or \flushbottom
- \usepackage{float} # keep figures where there are in the text
- \floatplacement{figure}{H} # keep figures where there are in the text

---

Цель работы

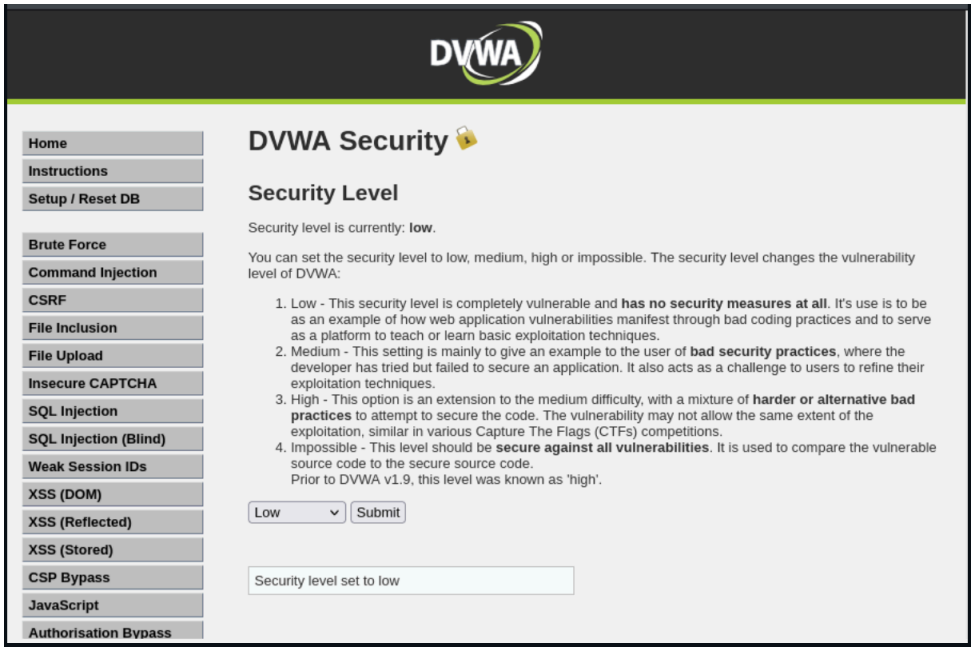
Приобретение практических навыков по использованию nikto - базового сканера безопасности веб-сервера.

Выполнение работы

Для работы приложения запустим сервесы Apache2 и MySQL:

```
┌──$ sudo service apache2 start && sudo service mysql start
```

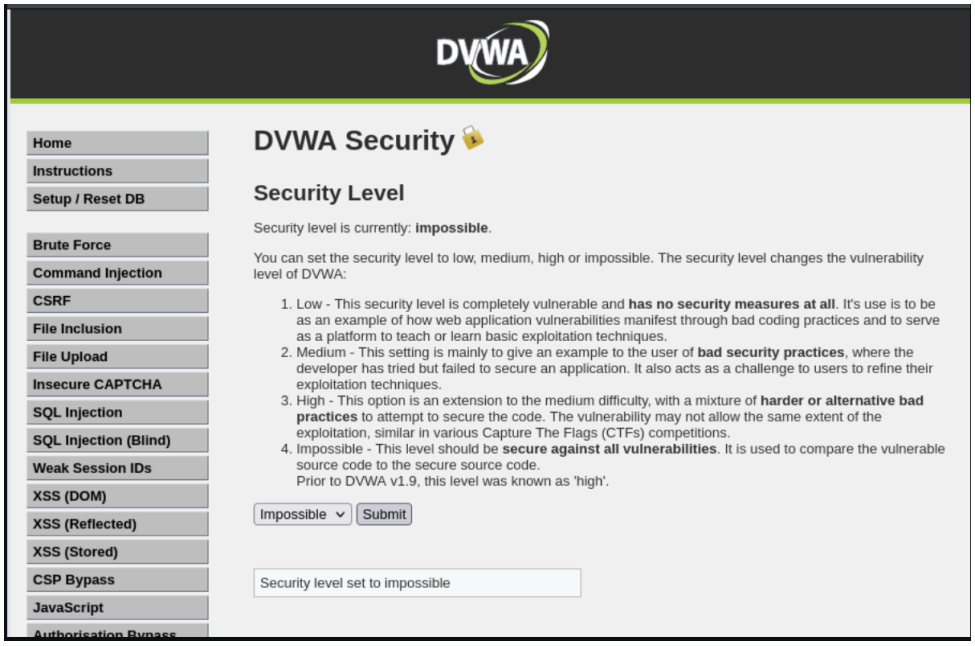
Теперь в браузере откроем приложение DVWA, перейдем в раздел "DVWA Security" и выберем опцию "Low":



Далее воспользуемся утилитой nikto. Базовые опции таковы: "nikto -h < host or ip>":

```
└─$ nikto -h http://localhost/DVWA/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2024-10-01 22:21:44 (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/vulnerabiliti
es/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 a
bout the site.
+ 7850 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:           2024-10-01 22:22:10 (GMT3) (26 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Теперь для эксперименты изменим настройку защиты на "Impossible" и запустим утилиту повторно:



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 данной лабораторной работы я приобрела практический навык по использованию nikto - базового сканера безопасности веб-сервера.