Assignment 6.1

Course name: Password attacks and enumeration

Developers:

- Anders Carlsson
- Oleksii Baranovskyi

Performer:

- FB-01 Sakhnii Nazar

Table of Contents

Task 1. Enumeration

Purpose: understand how to detect and exploit enumeration

After the work the student must

- know: how execute enumeration

Tasks:

- analyze provided VM (192.168.56.9);
- detect credentials input;
- analyze the process.

Technical equipping of the workplace:

- OWASP Burp Suite
- OWASP Zend Attack Proxy
- Chrome developer tools
- Mozilla developer tools
- Brute forcers

Solution:

Launch VM. Open http://192.168.56.9 in browser. Analyze HTTP-parameters for GET/POST. Find credentialing. Exploit.

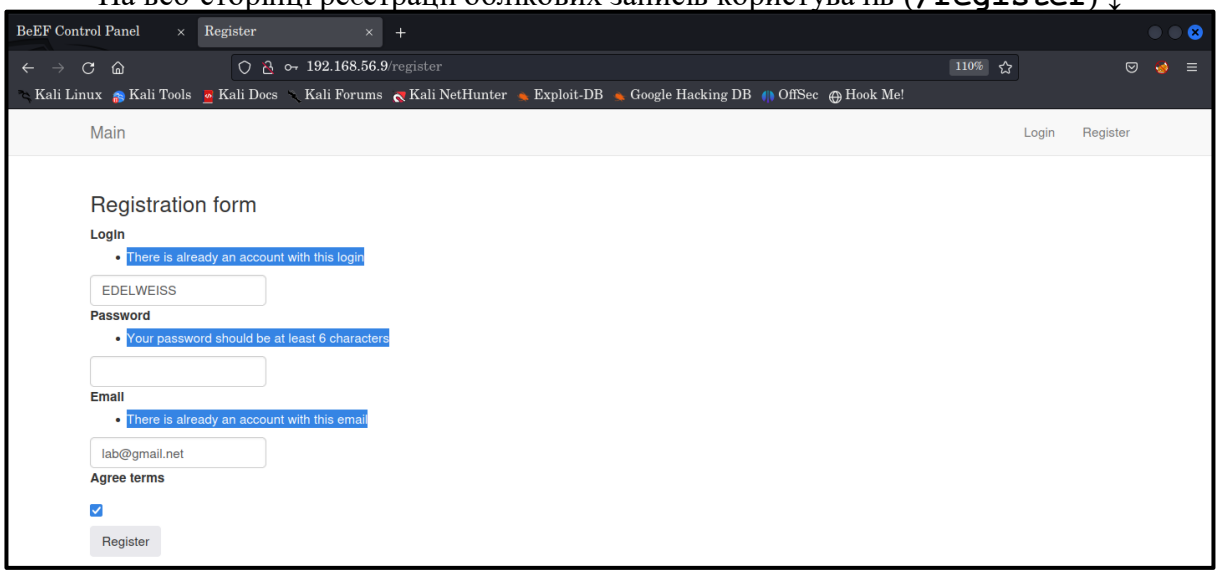
TASK 1

In how many places enumeration is possible? Prove it (screenshot).

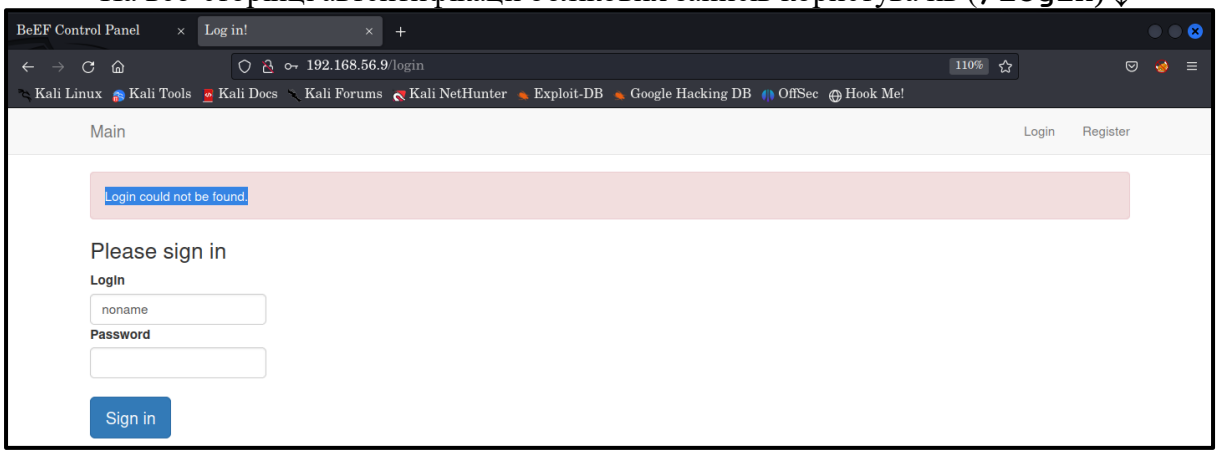
Answer:

Перерахунок логінів користувачів доступний у двох місцях на веб-сайті:

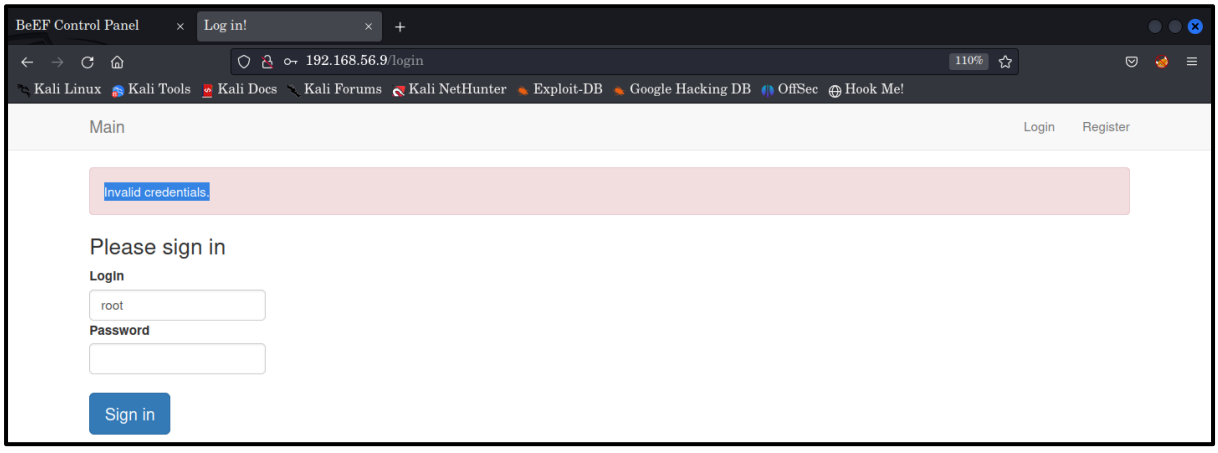
– На веб-сторінці реєстрації облікових записів користувачів (**`/register`**) ↓



– На веб-сторінці автентифікації облікових записів користувачів (**`/login`**) ↓



↑ або ↓



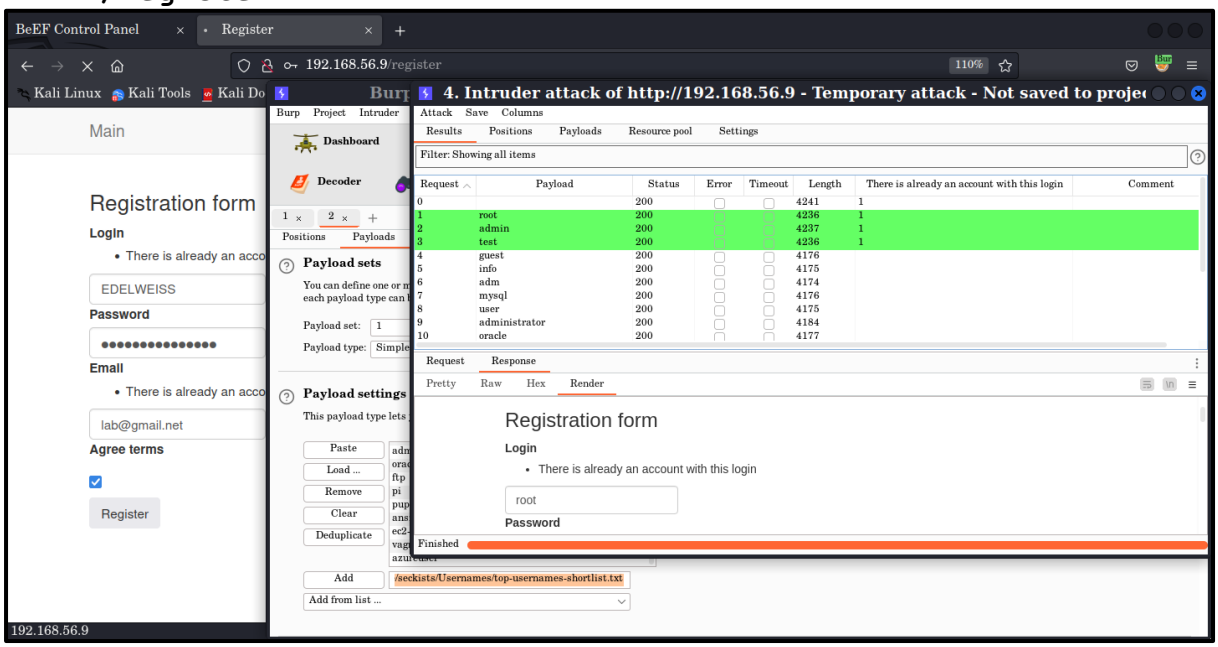
TASK 2

Which accounts you detect? Prove it (screenshot).

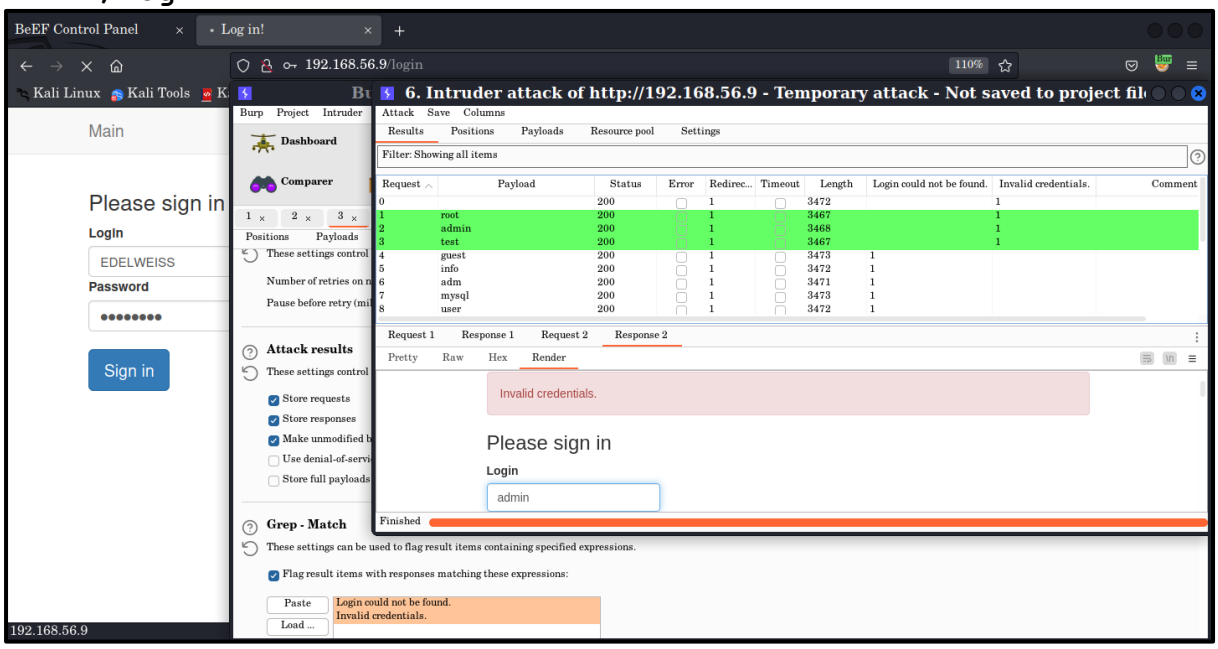
Answer:

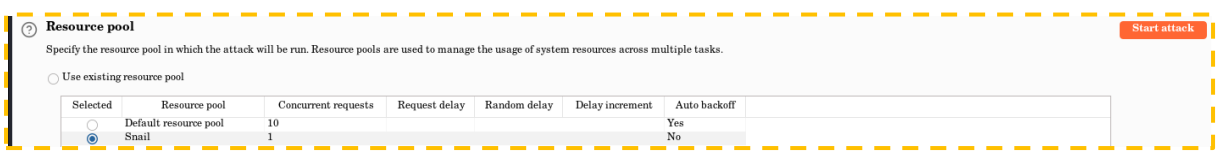
Добре, тоді спробуємо виконати сам процес перерахунку логінів користувачів на обох веб-сторінках, використовуючи при цьому інструмент **Burp Intruder**:

- **`/register`**



- **`/login`**





Task 2. Password attacks

Purpose: understand how to detect and exploit authentication vulnerabilities

After the work the student must

- know: how execute password attacks

Tasks:

- analyze provided VM (192.168.56.9);
- detect authentication input;
- analyze the process.

Technical equipping of the workplace:

- OWASP Burp Suite
- OWASP Zend Attack Proxy
- Chrome developer tools
- Mozilla developer tools
- Brute forcers

Solution:
Launch VM. Open http://192.168.56.9 in browser. Analyze HTTP-parameters for GET/POST. Find authentication. Exploit.

TASK 1
Is password attack possible? Prove it (screenshot).

Answer:
Оскільки на сервері відсутня функція моніторингу активності процесу автентифікації, а саме можливості відслідковувати кількість спроб введення даних з однієї IP-адреси, то маємо можливість здійснити атаку на паролі.

Для запобігання таким атакам, рекомендується впровадження додаткових заходів безпеки. Наприклад, можна реалізувати механізми блокування IP-адрес, які здійснюють надмірну кількість невдалих спроб входу, або вимагати складніші вимоги до паролів, такі як мінімальна довжина, використання різних типів символів і т.д.

У наступному завданні підтвердимо, що за допомогою такого потужного інструменту для виконання атак перебору паролів на веб-сайтах як **Burp Intruder**, ми досягнемо успіху та зможемо знайти істинний пароль для кожного знайденого раніше користувача.

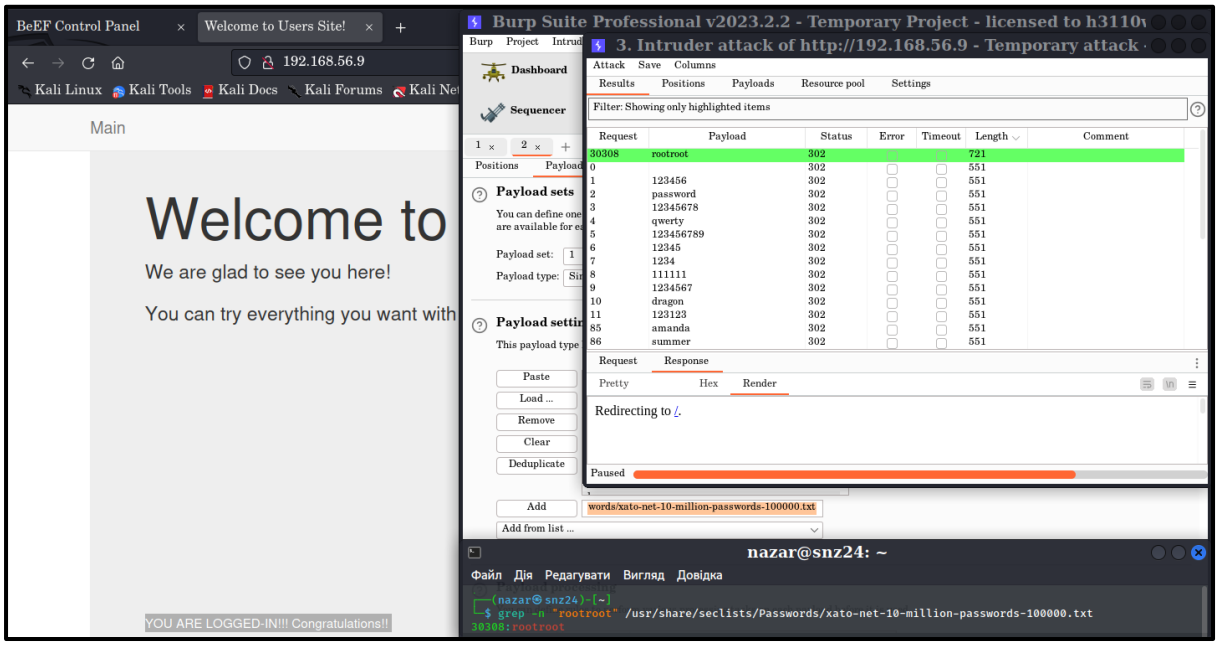
TASK 2

Which accounts were cracked? Prove it (screenshot).

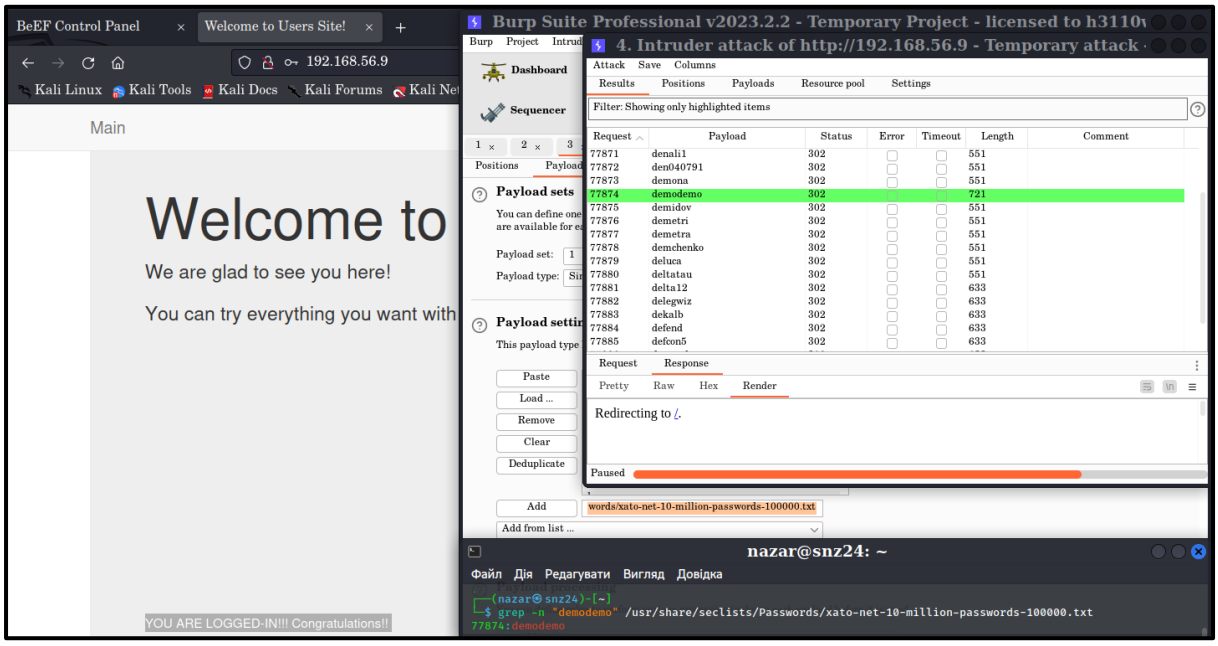
Answer:

Отже, усі акаунти було скомпрометовано, так як для кожного було знайдено пароль:

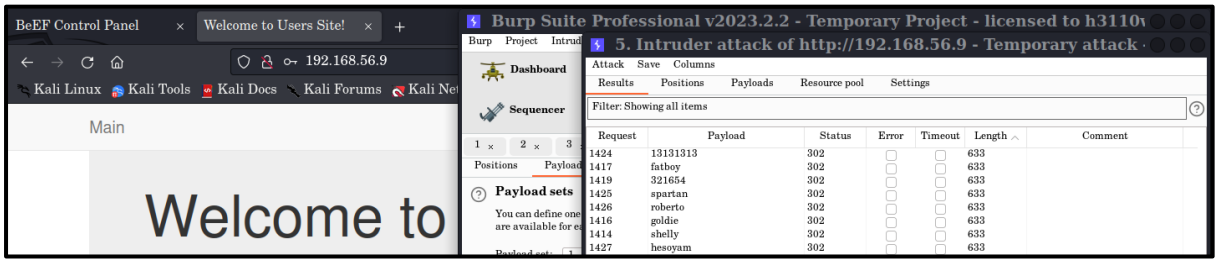
- `root:rootroot`

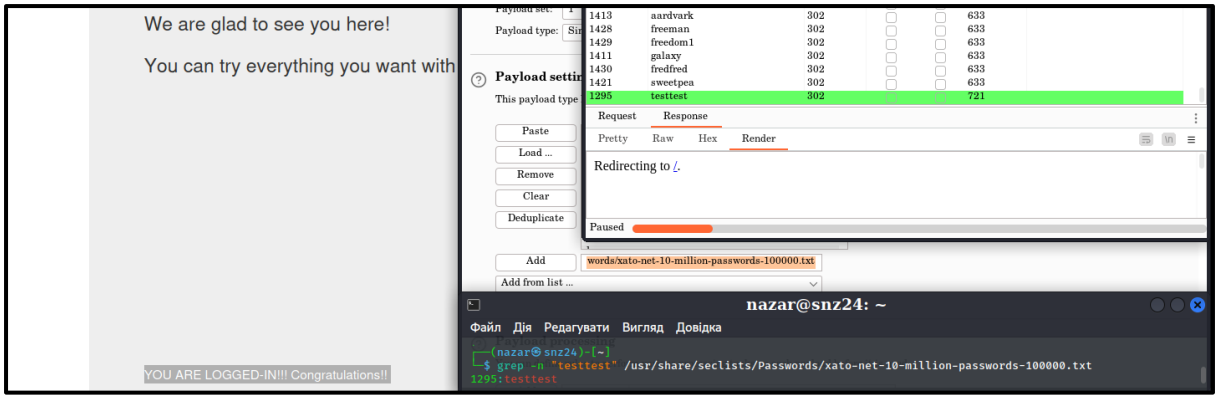


- `admin:demodemo`



- `test:testtest`




We are glad to see you here!
You can try everything you want with
YOU ARE LOGGED-IN!!! Congratulations!!
Payload type:
Payload setti
This payload type
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ...
words/xato-net-10-million-passwords-100000.txt
1413 aardvark 302 633
1428 freeman 302 633
1429 freedom1 302 633
1411 galaxy 302 633
1430 fredfred 302 633
1421 sweetpea 302 633
1295 testtest 302 721
Request
Response
Pretty
Raw
Hex
Render
Redirecting to /.
Paused
nazar@snz24: ~
Файл Дія Редагувати Вигляд Довідка
(nazar㉿snz24)-[~]
$ grep -n "testtest" /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt
1295:testtest