

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.....	1
Task 2. Password attacks.....	4

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 Zed 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.

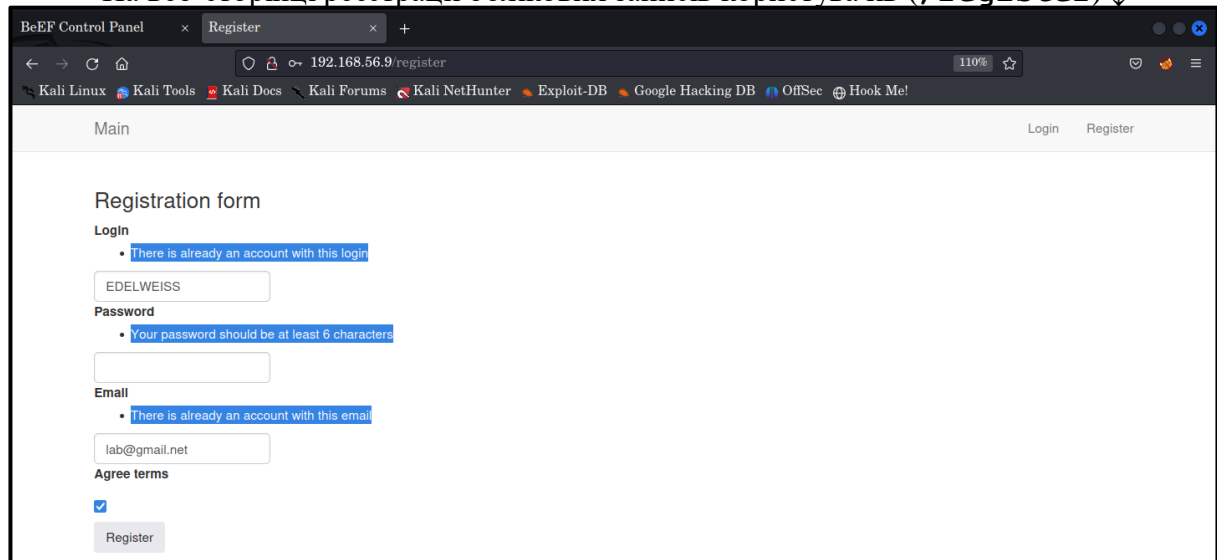
TASK 1

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

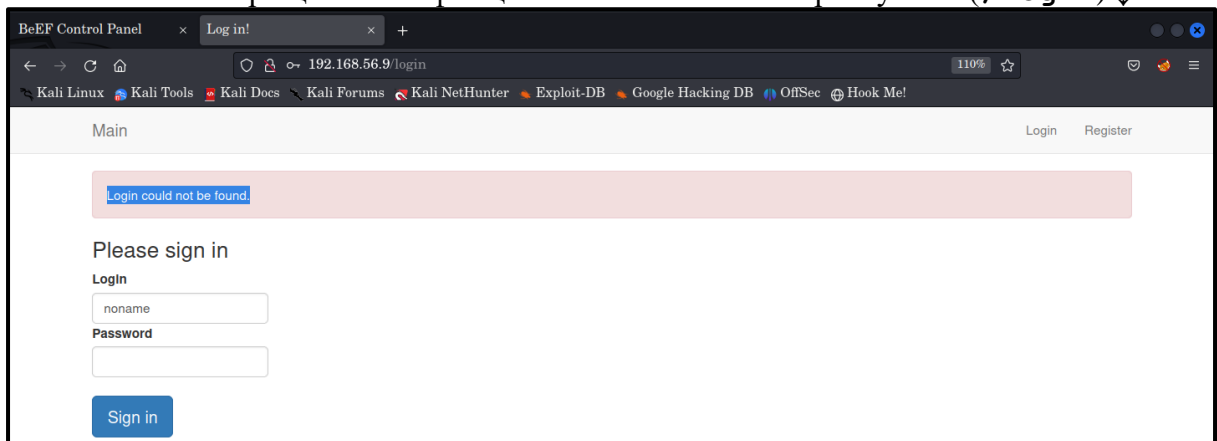
Answer:

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

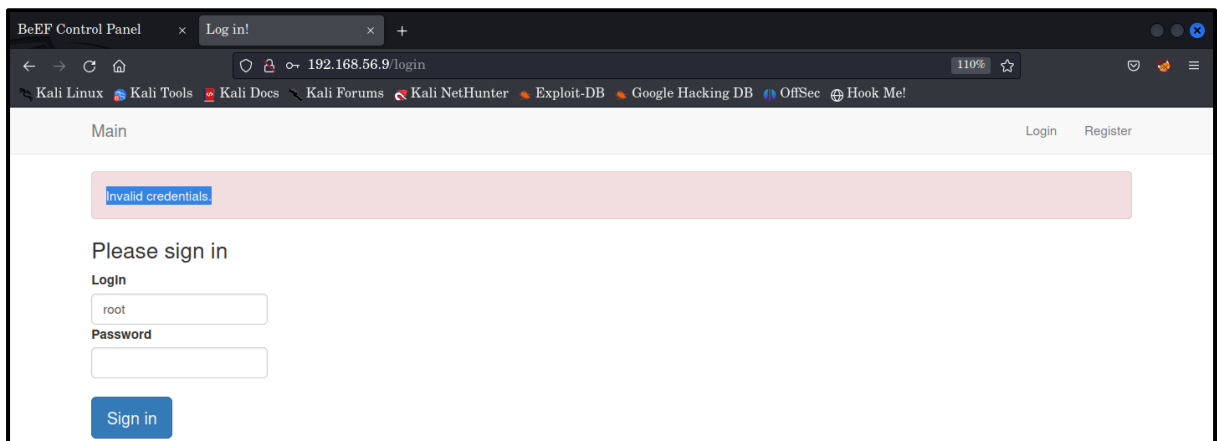
- На веб-сторінці реєстрації облікових записів користувачів (**/register**) ↓



- 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**

The screenshot shows the Burp Suite interface with the BeEF Control Panel on the left and the main workspace on the right. The workspace displays a registration form with fields for Login, Password, and Email. The main workspace is titled "4. Intruder attack of http://192.168.56.9 - Temporary attack - Not saved to project". The "Results" tab is active, showing a table of attack results. The table has columns: Request, Payload, Status, Error, Timeout, Length, and Comment. The results show that the attack was successful for the payloads "root", "admin", and "test".

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			4241	1
1	root	200			4236	1
2	admin	200			4237	1
3	test	200			4236	1
4	guest	200			4176	
5	info	200			4175	
6	adm	200			4174	
7	mysql	200			4176	
8	user	200			4175	
9	administrator	200			4184	
10	oracle	200			4177	

➤ **/login**

The screenshot shows the Burp Suite interface with the BeEF Control Panel on the left and the main workspace on the right. The workspace displays a login form with fields for Login and Password. The main workspace is titled "6. Intruder attack of http://192.168.56.9 - Temporary attack - Not saved to project file". The "Results" tab is active, showing a table of attack results. The table has columns: Request, Payload, Status, Error, Redirec..., Timeout, Length, Login could not be found, Invalid credentials, and Comment. The results show that the attack was successful for the payloads "root", "admin", and "test".

Request	Payload	Status	Error	Redirec...	Timeout	Length	Login could not be found	Invalid credentials	Comment
0		200		1		3472		1	
1	root	200		1		3467		1	
2	admin	200		1		3468		1	
3	test	200		1		3467		1	
4	guest	200		1		3473			
5	info	200		1		3472			
6	adm	200		1		3471			
7	mysql	200		1		3473			
8	user	200		1		3472			

The screenshot shows the Burp Suite settings for Redirections and Resource pool. The Redirections section is highlighted with a dashed yellow border. The Resource pool section is also highlighted with a dashed yellow border. The Resource pool section includes a table with columns: Selected, Resource pool, Concurrent requests, Request delay, Random delay, Delay increment, and Auto backoff.

Selected	Resource pool	Concurrent requests	Request delay	Random delay	Delay increment	Auto backoff
<input type="radio"/>	Default resource pool	10				Yes
<input checked="" type="radio"/>	Snail	1				No

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 Zed 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**

The screenshot shows the Burp Suite interface during an intruder attack. The 'Sequencer' tab is active, displaying a list of requests. The first request, with ID 30308, is highlighted in green, indicating a successful attack. The payload for this request is 'rootroot'. The status is '302', and the length is 721. The response is shown in the 'Response' tab, indicating a redirect to the login page. Below the Burp Suite window, a terminal window shows the command being executed: `grep -n "rootroot" /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt`, which returns the result: `30308:rootroot`.

❖ **admin:demodemo**

The screenshot shows the Burp Suite interface during an intruder attack. The 'Sequencer' tab is active, displaying a list of requests. The request with ID 77874 is highlighted in green, indicating a successful attack. The payload for this request is 'demodemo'. The status is '302', and the length is 721. The response is shown in the 'Response' tab, indicating a redirect to the login page. Below the Burp Suite window, a terminal window shows the command being executed: `grep -n "demodemo" /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt`, which returns the result: `77874:demodemo`.

❖ **test:testtest**

The screenshot shows the Burp Suite interface during an intruder attack. The 'Sequencer' tab is active, displaying a list of requests. The request with ID 1417 is highlighted in green, indicating a successful attack. The payload for this request is 'testtest'. The status is '302', and the length is 633. The response is shown in the 'Response' tab, indicating a redirect to the login page.

