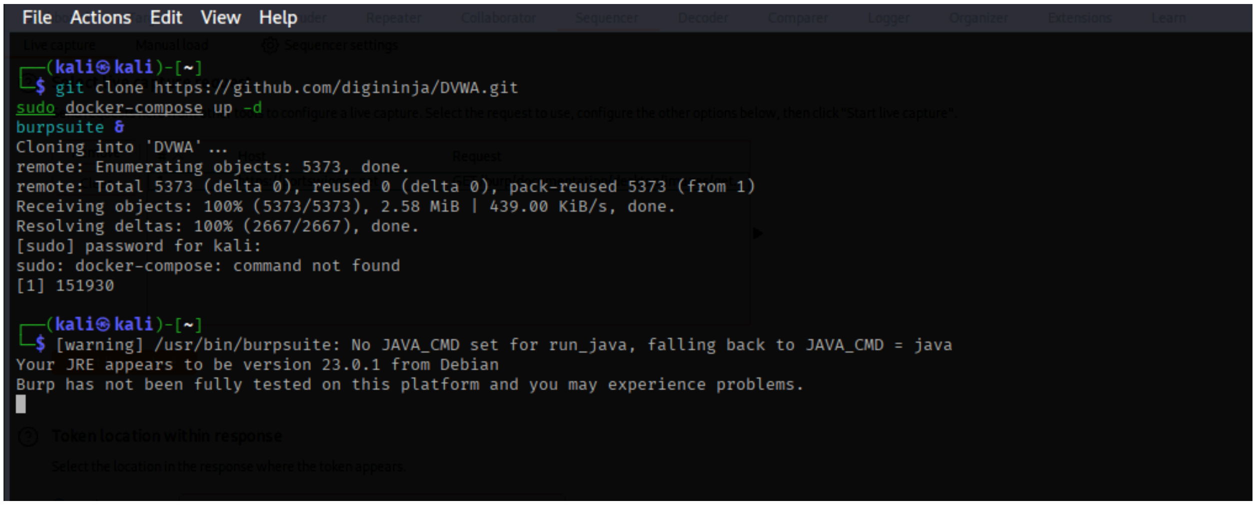
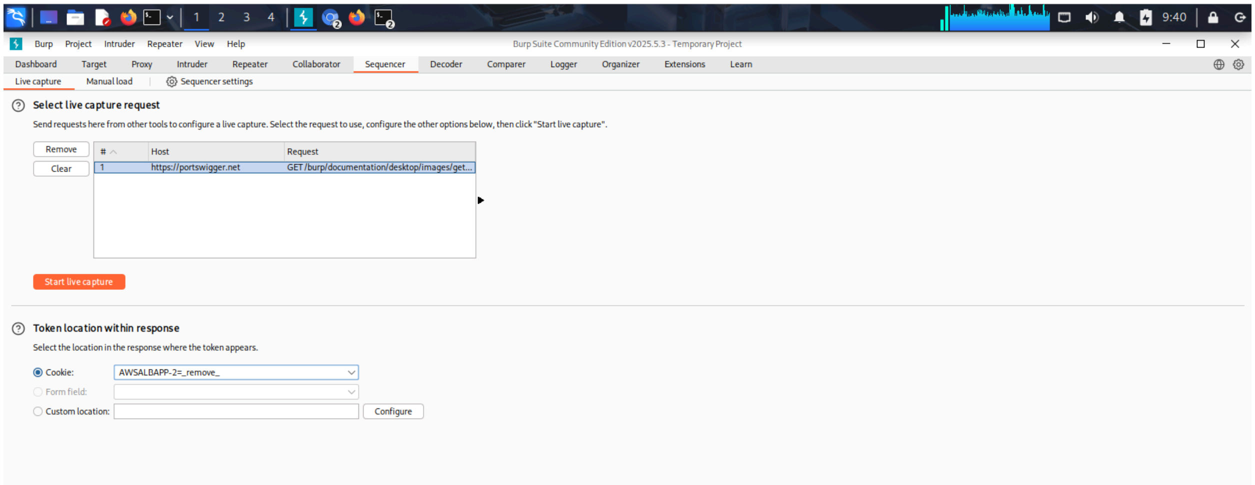
2. API Security Testing Lab;



```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/digininja/DVWA.git
sudo docker-compose up -d
burpsuite &
Cloning into 'DVWA'...
remote: Enumerating objects: 5373, done.
remote: Total 5373 (delta 0), reused 0 (delta 0), pack-reused 5373 (from 1)
Receiving objects: 100% (5373/5373), 2.58 MiB | 439.00 KiB/s, done.
Resolving deltas: 100% (2667/2667), done.
[sudo] password for kali:
sudo: docker-compose: command not found
[1] 151930

┌──(kali㉿kali)-[~]
└─$ [warning] /usr/bin/burpsuite: No JAVA_CMD set for run_java, falling back to JAVA_CMD = java
Your JRE appears to be version 23.0.1 from Debian
Burp has not been fully tested on this platform and you may experience problems.
```

DVDVWA SetupWA Setup



Select live capture request

Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".

#	Host	Request
1	https://portswigger.net	GET /burp/documentation/desktop/images/get...

Token location within response

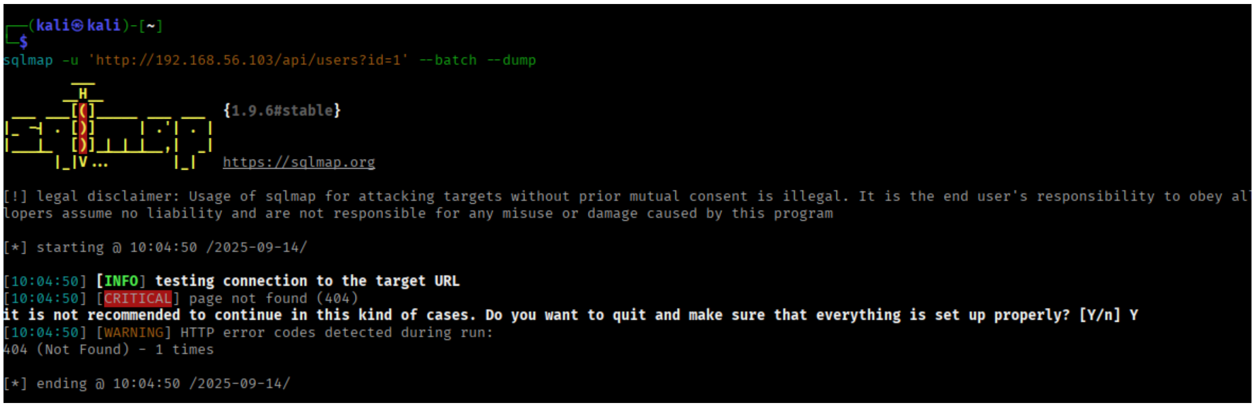
Select the location in the response where the token appears.

● Cookie: AWSALBAPP-2=_remove_

○ Form field:

○ Custom location:

SQL Injection Testing



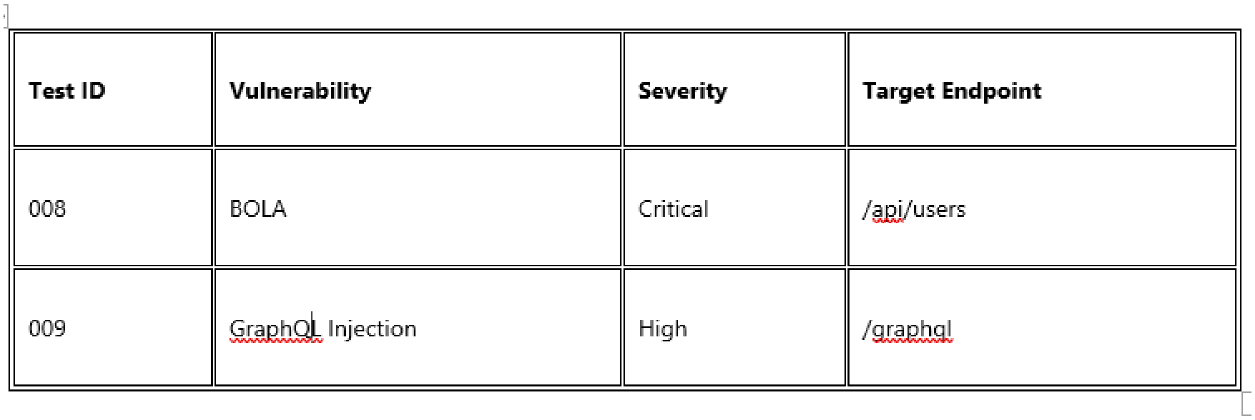
```
┌──(kali㉿kali)-[~]
└─$
sqlmap -u 'http://192.168.56.103/api/users?id=1' --batch --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.6#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey al
lopers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:04:50 /2025-09-14/

[10:04:50] [INFO] testing connection to the target URL
[10:04:50] [CRITICAL] page not found (404)
it is not recommended to continue in this kind of cases. Do you want to quit and make sure that everything is set up properly? [Y/n] Y
[10:04:50] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times

[*] ending @ 10:04:50 /2025-09-14/
```



Test ID	Vulnerability	Severity	Target Endpoint
008	BOLA	Critical	/api/users
009	GraphQL Injection	High	/graphql

BOLA Exploitation

Demonstrated Broken Object Level Authorization by manipulating API requests in Burp Suite, accessing unauthorized user data through parameter modification (GET /api/users/1 → GET /api/users/2).

GraphQL Testing

Executed introspection queries and injection attacks, revealing schema information and exploiting weak input validation for unauthorized data access.

Summary: Conducted comprehensive API security assessment targeting OWASP API Top 10 vulnerabilities, identifying critical BOLA vulnerability and high-severity GraphQL injection through manual testing and automated scanning.