Sri Lanka Institute of Information Technology



4rd Year 1st Semester

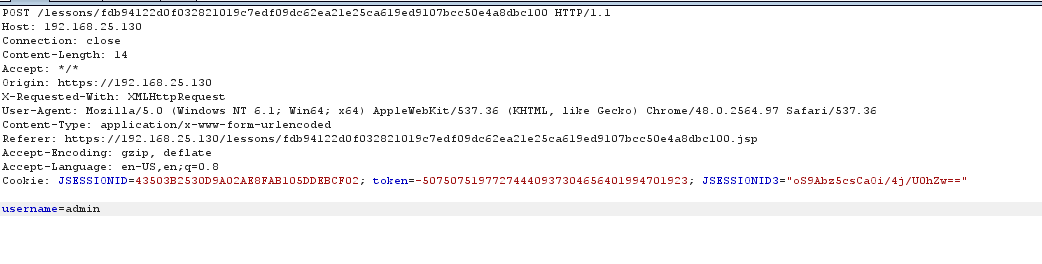
**B.Sc Special (Hons) – Information Technology**

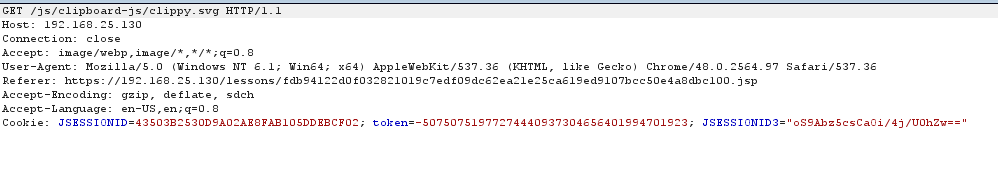
Cyber Security

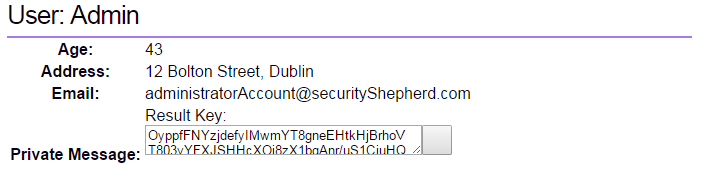
IT13028138 - Sampath S.A.W.S

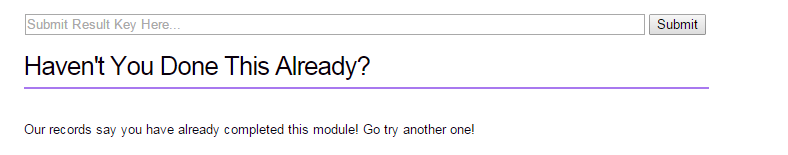
[Insecure Direct Object References](javascript:;)

Here I used Burp suite to get the admin profile by changing guest to admin.



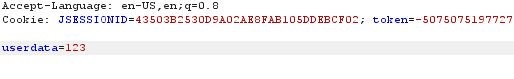


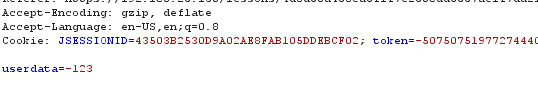


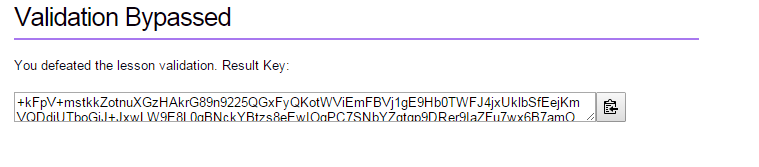


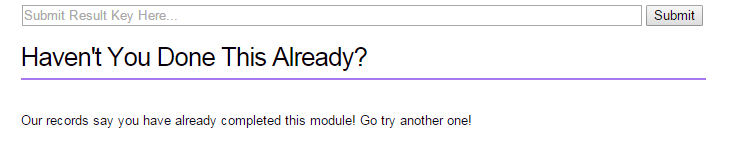
[Poor Data Validation](javascript:;)

Here I added a negative value to post parameter by using burpsuite. Server will accept a negative value.



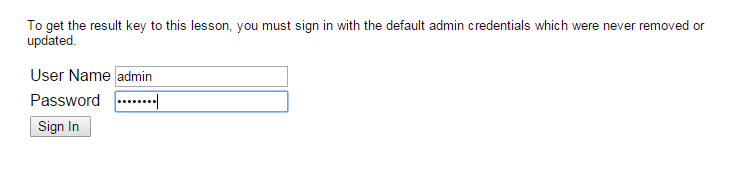


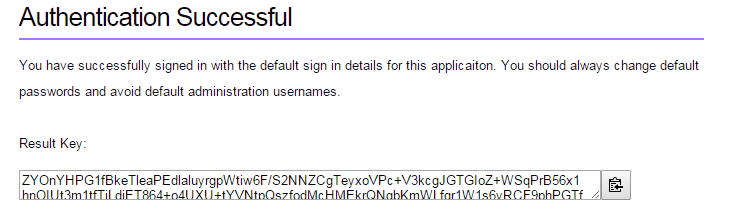


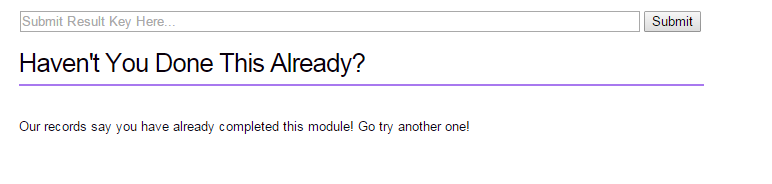


[Security Misconfiguration](javascript:;)

In this level still not changed the username and password so used default username and password to get the result key.

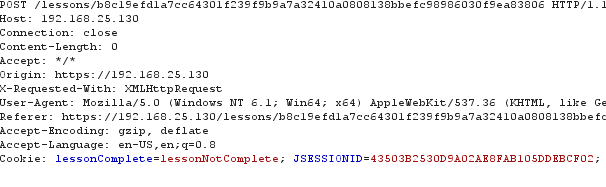




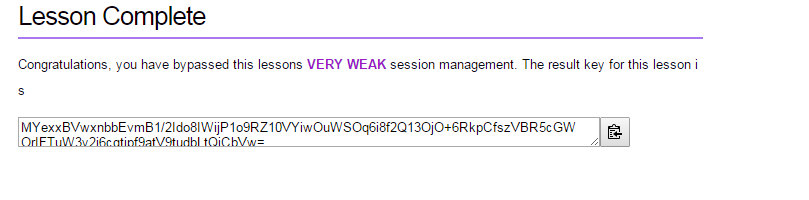


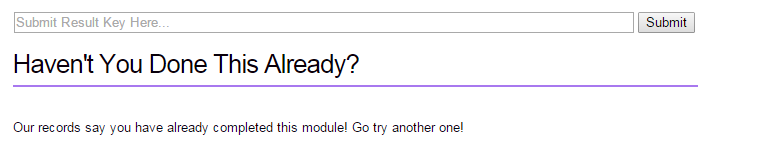
[Broken Session Management](javascript:;)

To complete this level changed the value, non-complete to complete in burp suite.



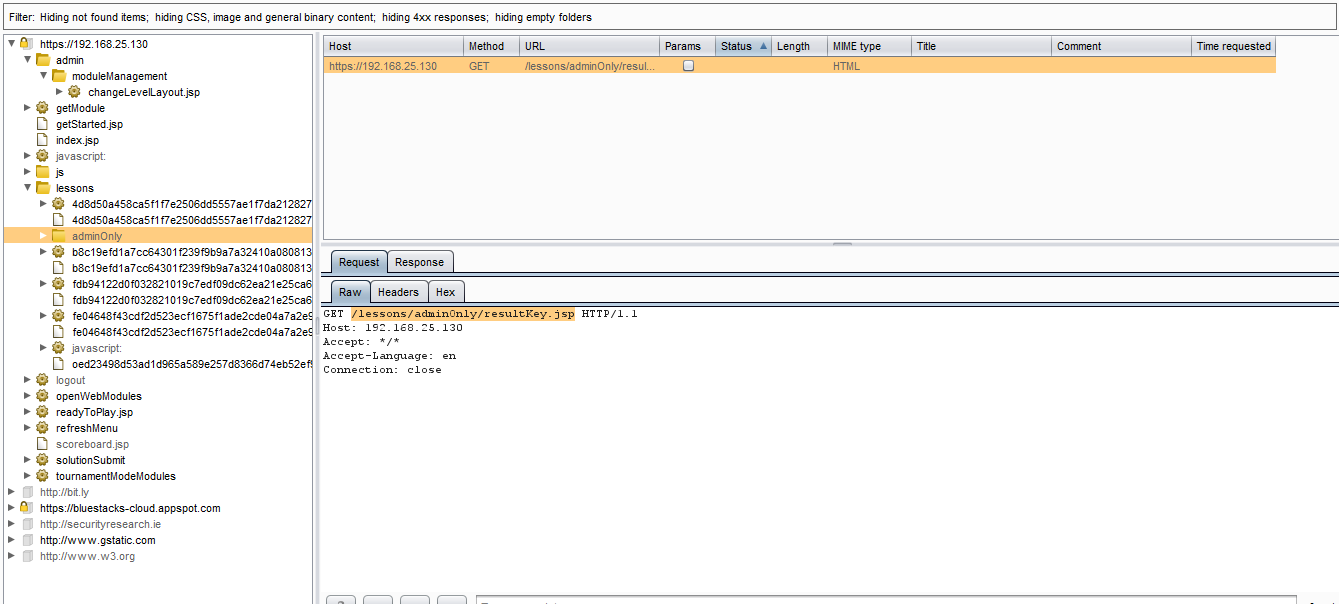




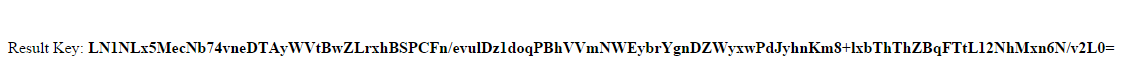


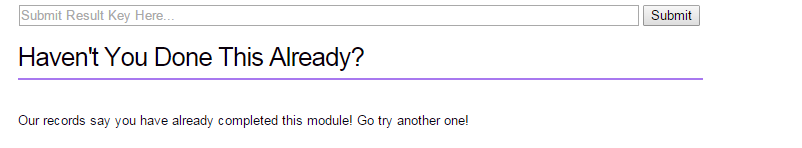
[Failure to Restrict URL Access](javascript:;)

According to the server, it says only the administrator know the page. With that hint, used burp suite and search through the target tab it contained the link under the admin section. Then I got the link and paste it on the URL and got the secret key to the next level.



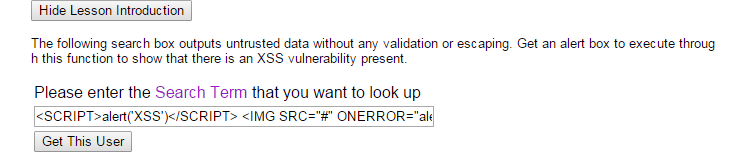


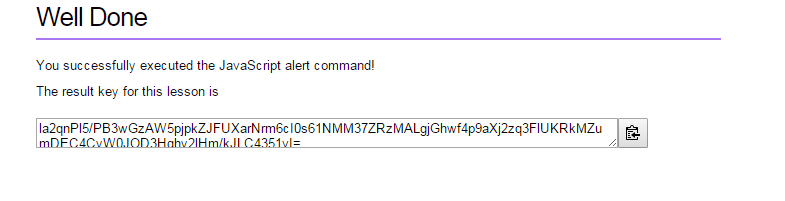


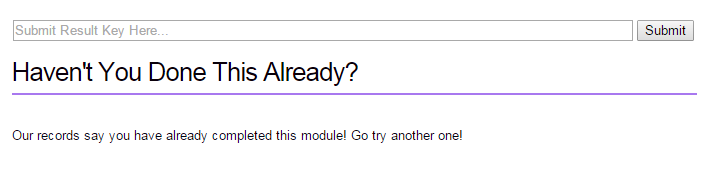


[Cross Site Scripting](javascript:;)

To show that there is XSS vulnerability present got an alert box because there is no any way to validate data whether they are trusted or untrusted.

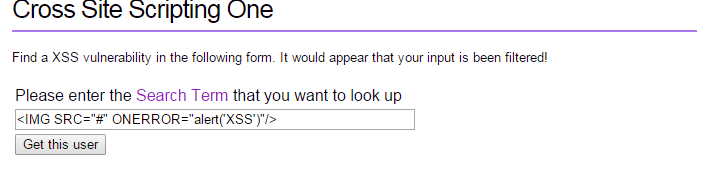


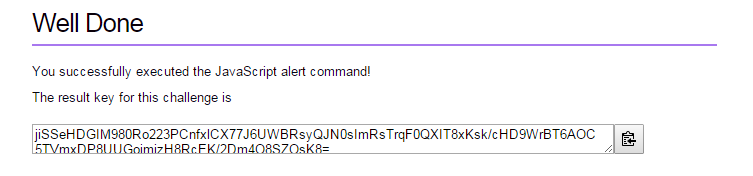


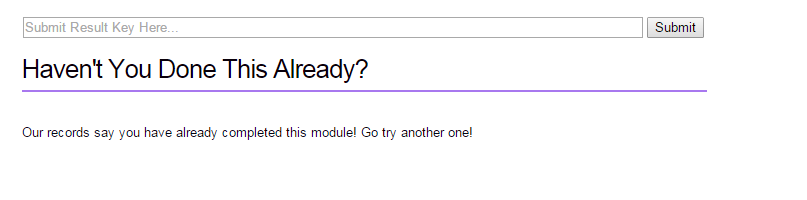


[Cross Site Scripting 1](javascript:;)

In this step I used the alert inside the image tag. Because in here it would appear like input is been filtered.

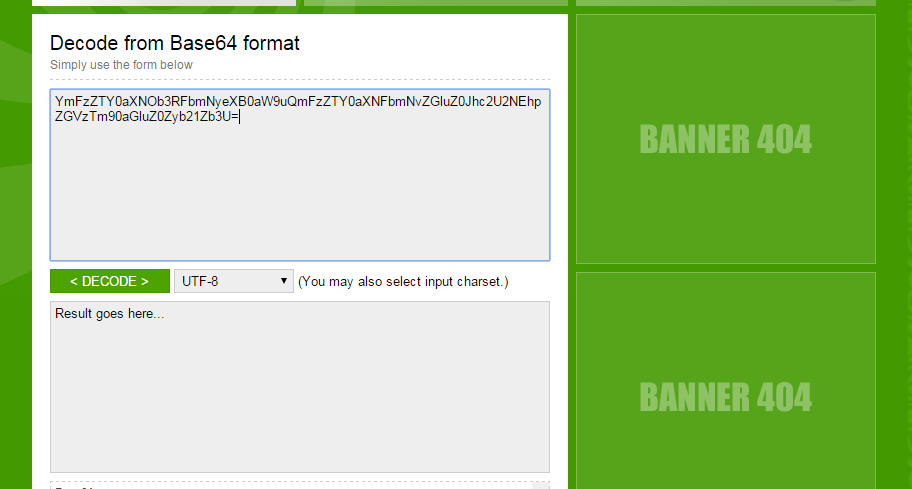


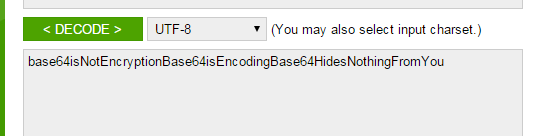


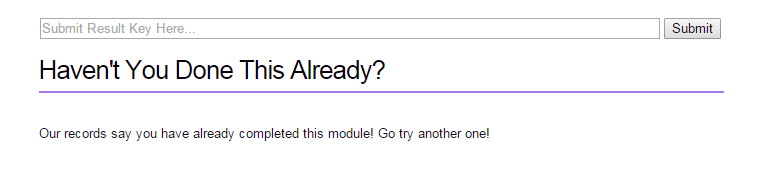


[Insecure Cryptographic Storage](javascript:;)

Used free online tool to decode

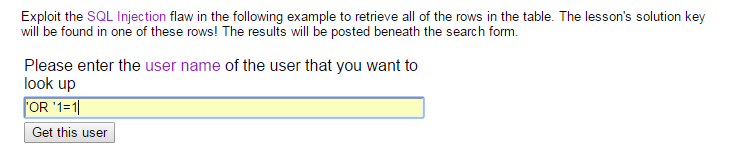


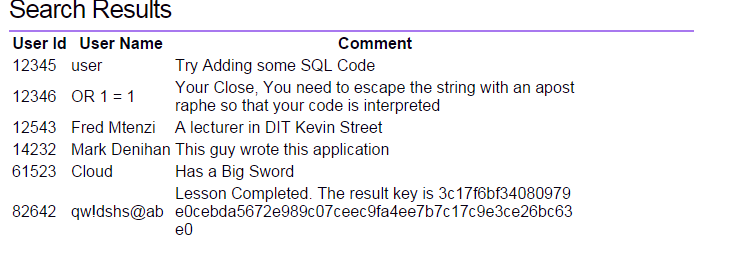


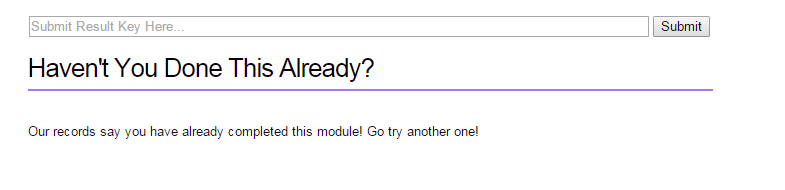


[SQL Injection](javascript:;)

Used a simple sql injection method. Syntax is ‘or ’ 1=1

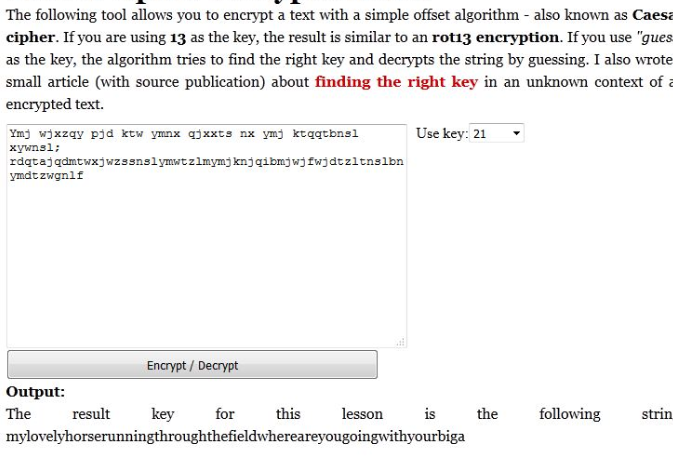


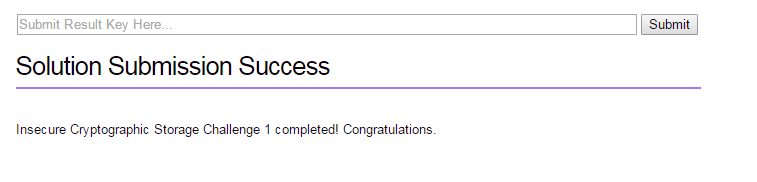




[Insecure Cryptographic Storage Challenge 1](javascript:;)

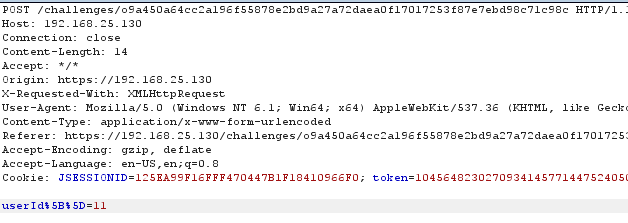
Used online tool and by decoding that, found the key. Key is 21

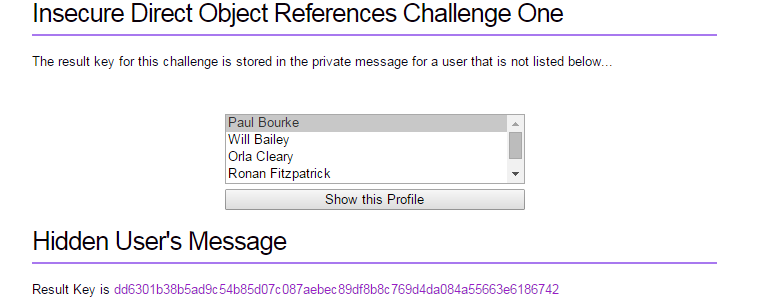


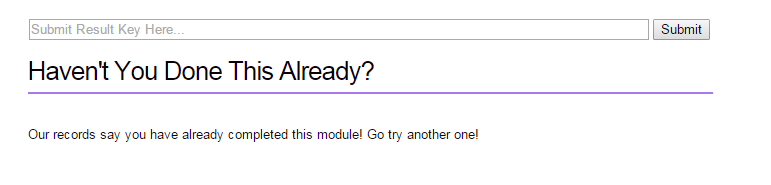


[Insecure Direct Object Reference Challenge 1](javascript:;)

I check the drop down box which contains name and captured it by using burp suite and finally came up with a pattern like (1,3,5,7,9) simply I guessed the next one should be 11. So I try it as post parameter

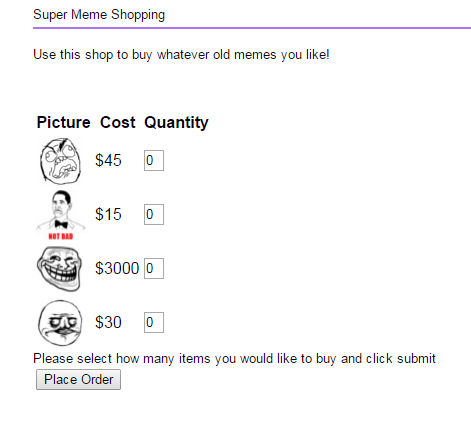


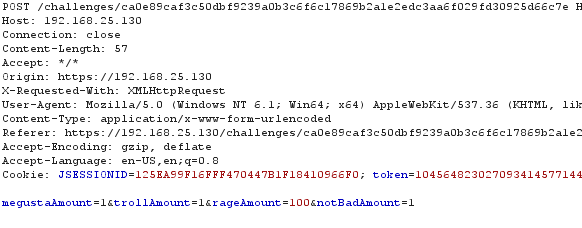


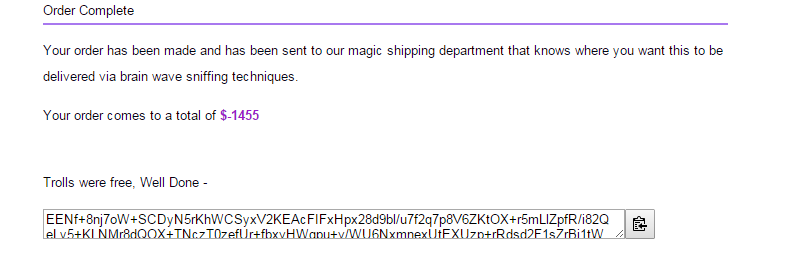


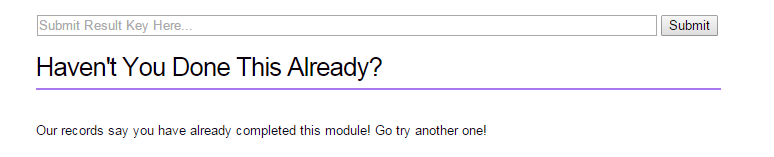
[Poor Data Validation 1](javascript:;)

To complete this level used burpsuite and when I insert the negative values to all products, app noticed it. But when I insert all positive values to all of them except troll meme and put negative value to it, app didn’t recognize it and just passed without any detection.



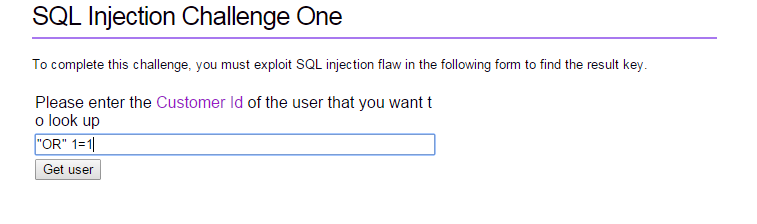






[SQL Injection 1](javascript:;)

To complete this challenge I used “or”1=1 syntax and do the sql injection in the text field. This time I used double quotes.



Get the result key and input the key in field and complete the mission

