CTF - OWASP

Lab Exercises

Name : Pathima Shahama Tamber

Student Number : MS15903020

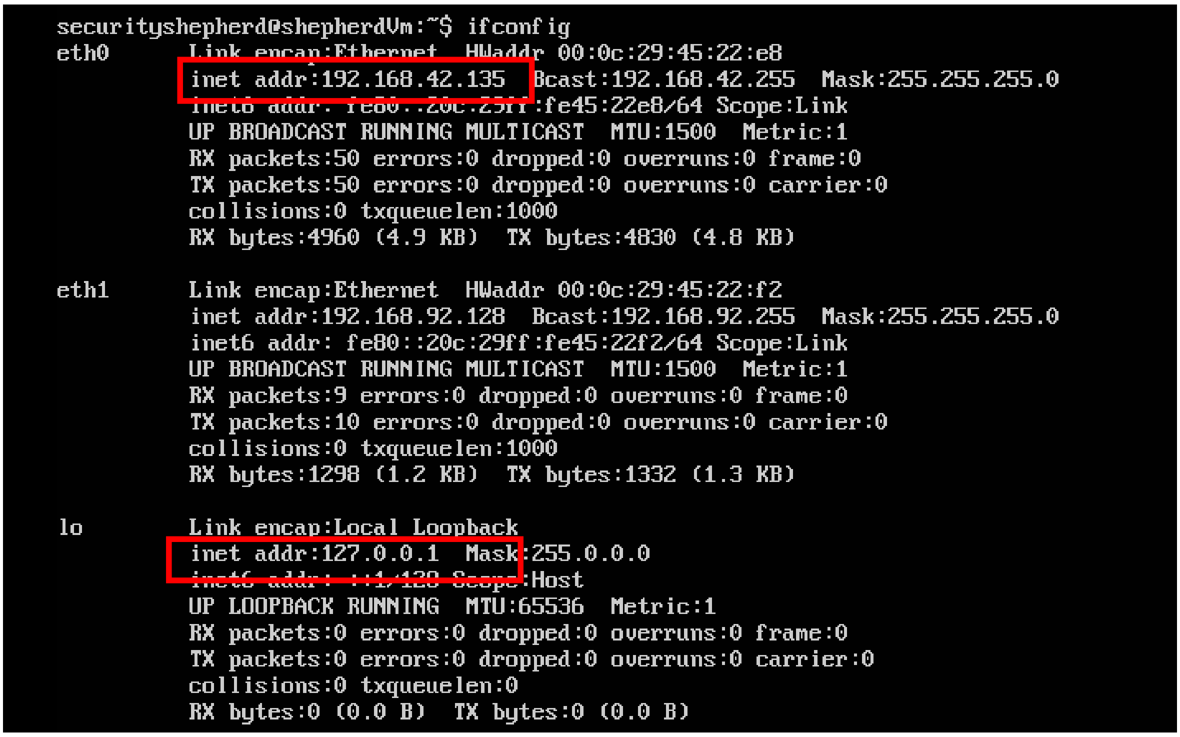
Subject : Penetration Testing

Table of Contents

1. Introduction -OWASP

First install OwaspSecurityShepherdVm_V3.0 operating system in VMware or virtual box as a server.

1) Import the VM to your hyper visor (Eg: Virtual Box)
2) Update the VM Network Adapters to suit what you have available. (Bridged Adapter for Network Availability, Host-Only for local access only and NAT for just outbound access) The VM by default has 2 Network adapters, one NAT and a Host-Only.
3) Boot the VM
4) Sign in with username : securityshepherd and password : owaspSecurityShepherd
5) Change the user password with the passwd command

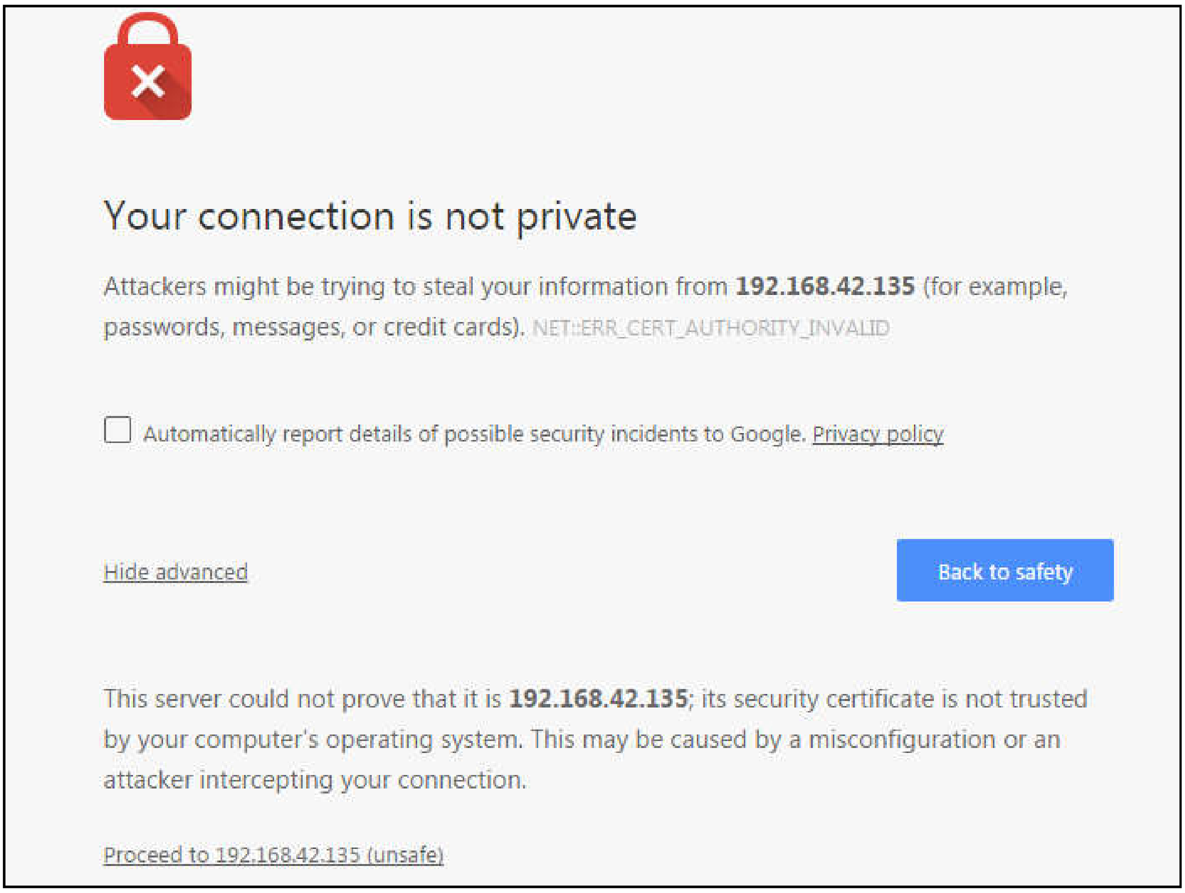


```
securityshepherd@shepherdVm:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:45:22:e8
          inet addr:192.168.42.135  Bcast:192.168.42.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe45:22e8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4960 (4.9 KB)  TX bytes:4830 (4.8 KB)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:45:22:f2
          inet addr:192.168.92.128  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe45:22f2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1298 (1.2 KB)  TX bytes:1332 (1.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Figure 1 : IP configuration of the Security Shepherd

6) In the VM, run "ifconfig" to find the IP address of the network adapter that is not configured for NAT. Make note of this

7) On your host machine, open https://<VM IP Address>/ (ex :<192.168.42.135>) in the security warning go to advanced link proceed to unsafe.



Your connection is not private

Attackers might be trying to steal your information from **192.168.42.135** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

This server could not prove that it is **192.168.42.135**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

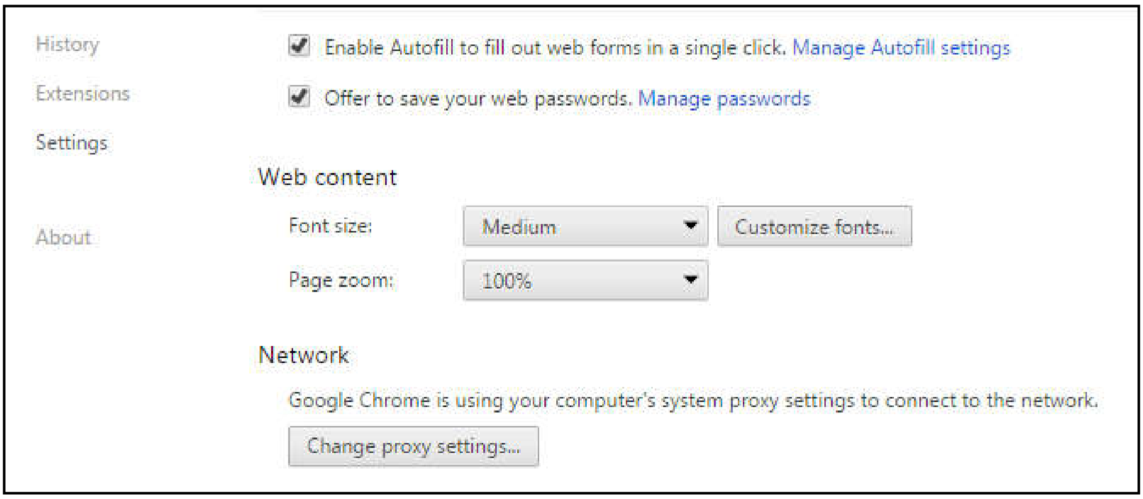
Figure 2 : Proceed to Unsafe

8) Sign in with admin / password

9) Change the admin password (cannot be password again)

10) Go to Admin -> Module Management -> Change Module Layout to change the way levels are presented. Default is CTF Mode (One at a time)

11) If you got any errors, Go to browser settings of your browser and change the proxy setting by clicking the change proxy setting under network tab.



☑ Enable Autofill to fill out web forms in a single click. Manage Autofill settings

☑ Offer to save your web passwords. Manage passwords

Web content

Font size: Medium

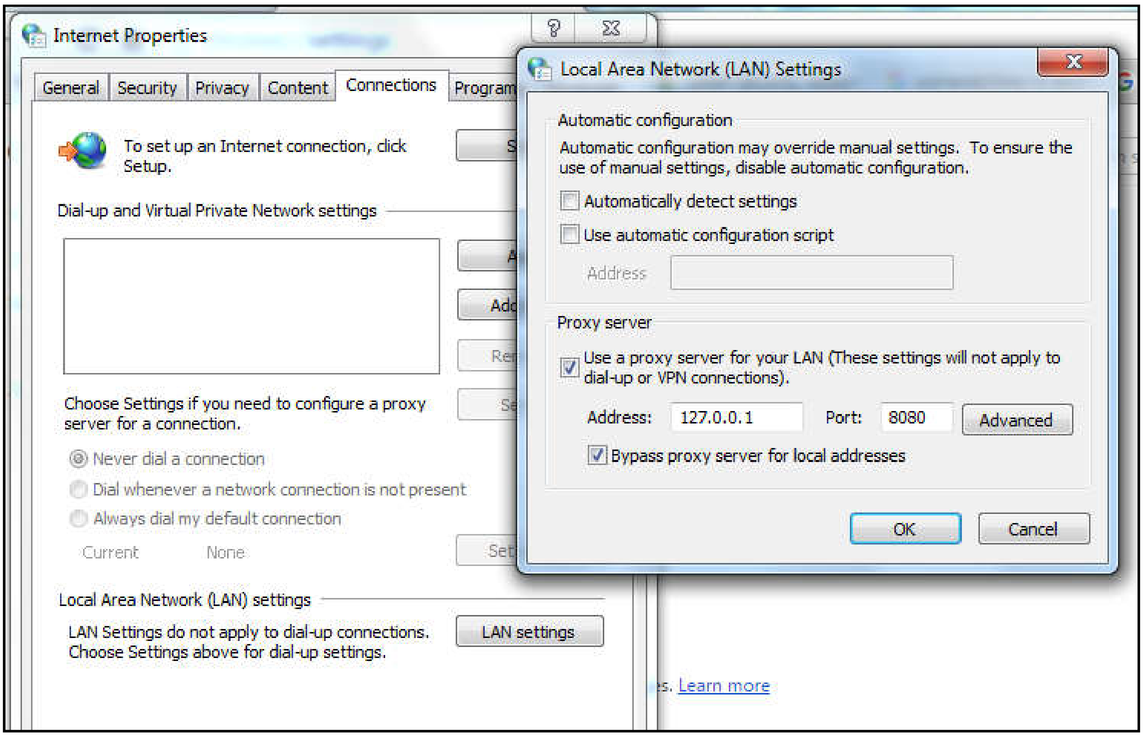
Page zoom: 100%

Network

Google Chrome is using your computer's system proxy settings to connect to the network.

Figure 3

12) Under Connections Click the LAN setting on Internet Options Window. Change proxy setting as below. Proxy Address is your server's Loopback (lo) address. Click ok and refresh your OWASP exercise page.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

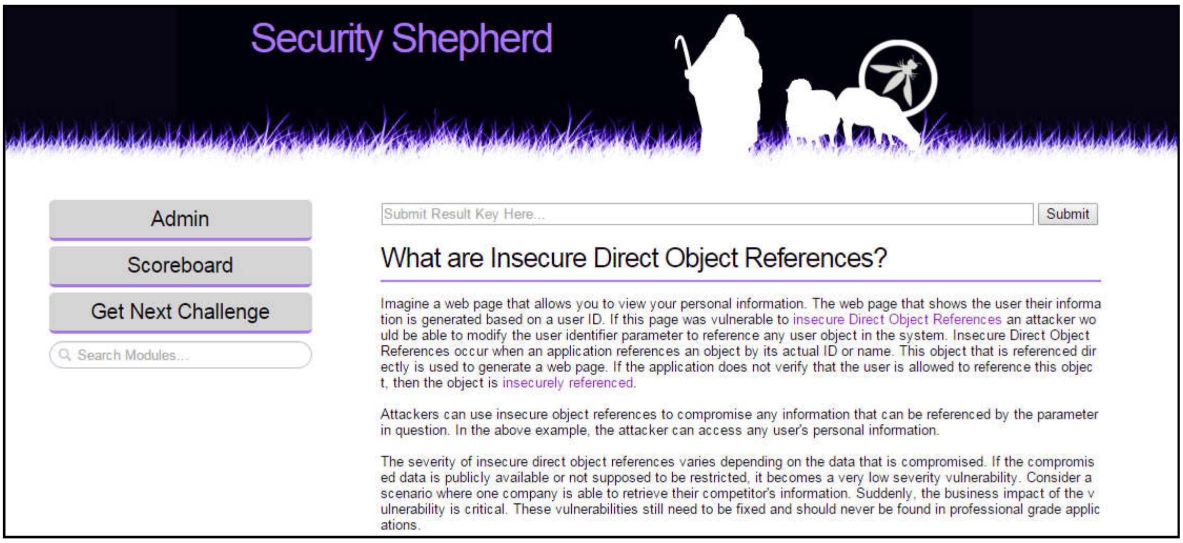
Address: 127.0.0.1 Port: 8080

☑ Bypass proxy server for local addresses

Figure 4

13) Time to play!

14) Go to "Get Next Challenge" and start with first level.



What are Insecure Direct Object References?

Imagine a web page that allows you to view your personal information. The web page that shows the user their information is generated based on a user ID. If this page was vulnerable to insecure Direct Object References an attacker would be able to modify the user identifier parameter to reference any user object in the system. Insecure Direct Object References occur when an application references an object by its actual ID or name. This object that is referenced directly is used to generate a web page. If the application does not verify that the user is allowed to reference this object, then the object is insecurely referenced.

Attackers can use insecure object references to compromise any information that can be referenced by the parameter in question. In the above example, the attacker can access any user's personal information.

The severity of insecure direct object references varies depending on the data that is compromised. If the compromised data is publicly available or not supposed to be restricted, it becomes a very low severity vulnerability. Consider a scenario where one company is able to retrieve their competitor's information. Suddenly, the business impact of the vulnerability is critical. These vulnerabilities still need to be fixed and should never be found in professional grade applications.

Figure 5

Start the burpsuite_free_v1.6.32 (right click→ open with→Java Platform)

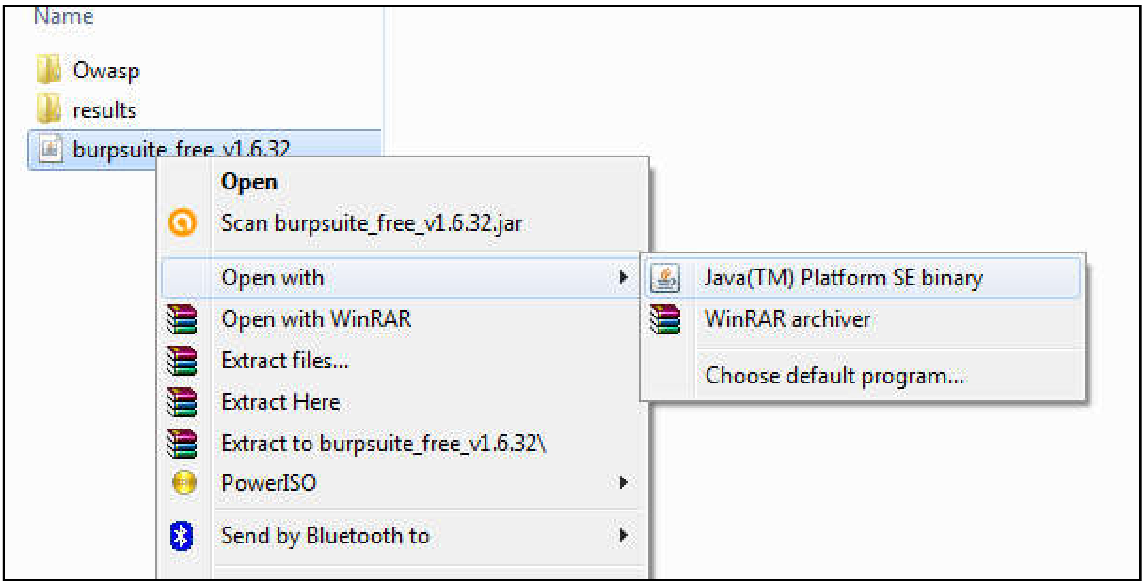
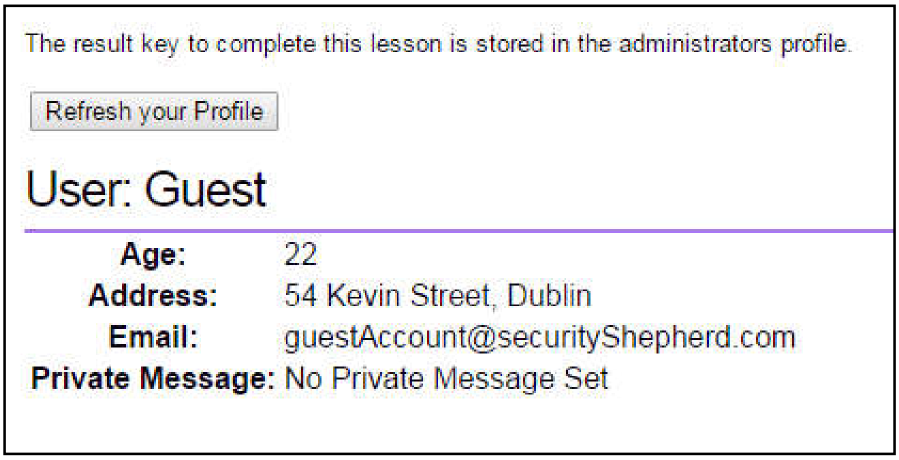


Figure 6

2. Level 1 - What are Insecure Direct Object References?



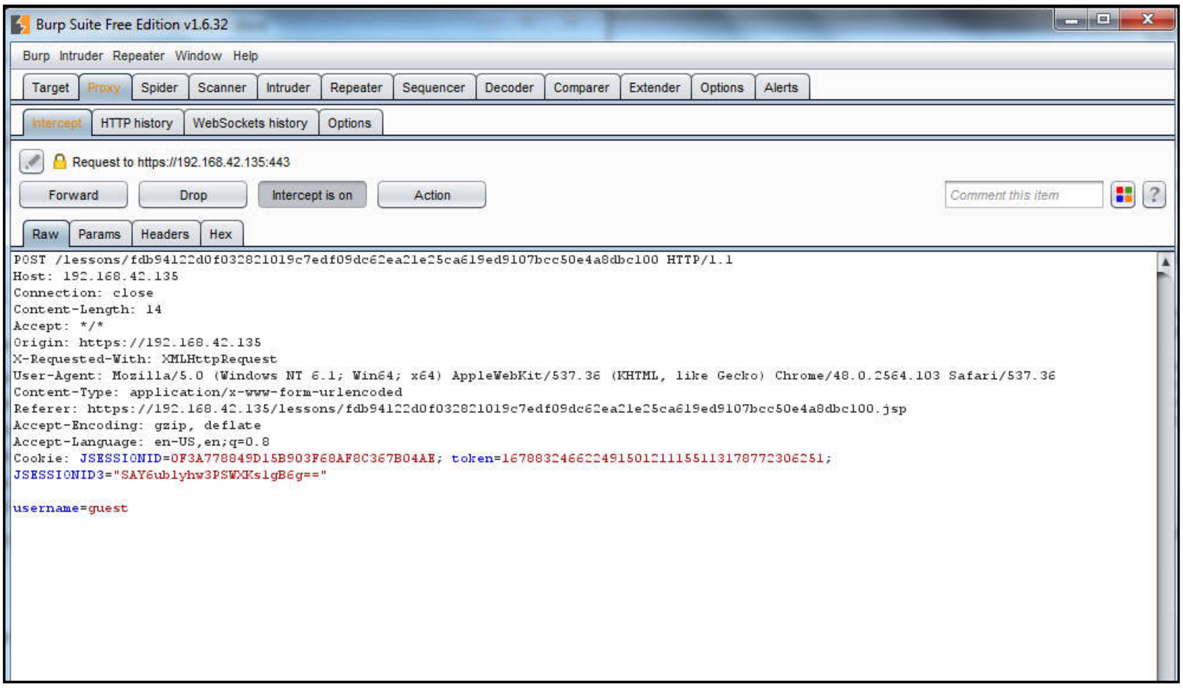
The result key to complete this lesson is stored in the administrators profile.

User: Guest

Age: 22
Address: 54 Kevin Street, Dublin
Email: guestAccount@securityShepherd.com
Private Message: No Private Message Set

Figure 7

To complete this level you have to complete above mentioned requirement. Click refresh button, then it will captured by the burpsuite and you can see the source to change the username as Figure 8.



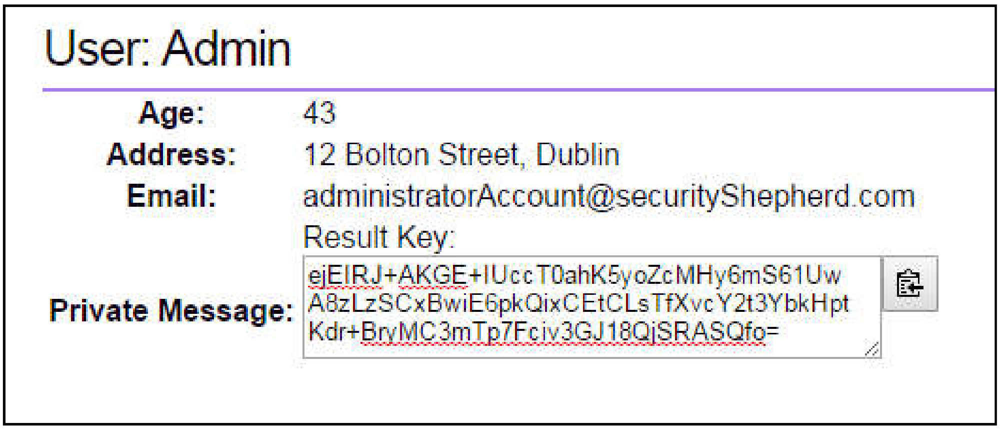
Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex

Request to https://192.168.42.135:443

```
POST /lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100 HTTP/1.1
Host: 192.168.42.135
Connection: close
Content-Length: 14
Accept: */*
Origin: https://192.168.42.135
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.103 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://192.168.42.135/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=0F3A778849D15B903F68AF8C367B04AE; token=167883246622491501211155113178772306251;
JSESSIONID3="SAY6ublyhw3PSWXKslgB6g=="

username=guest
```

Figure 8

You have to find a resultant key in every level in order to complete the level. The result key to complete this lesson is stored in the administrators profile as mentioned in the request. So, change the username=guest to username=admin then click forward button on the burpsuite.



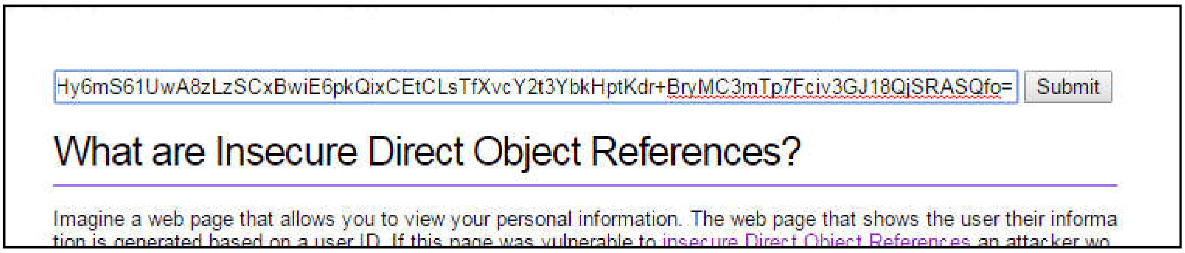
User: Admin

Age: 43
Address: 12 Bolton Street, Dublin
Email: administratorAccount@securityShepherd.com
Private Message: Result Key:
ejEIRJ+AKGE+IUccT0ahK5yoZcMHy6mS61UwA8zLzSCxBwiE6pkQixCEtCLsTfXvcY2t3YbkHptKdr+BryMC3mTp7Fciv3GJ18QjSRASQfo=

Figure 9

On the browser you can see the security key. copy it turn off the intercept is on and paste it on the top text box.

Result key :
ejEIRJ+AKGE+IUccT0ahK5yoZcMHy6mS61UwA8zLzSCxBwiE6pkQixCEtCLsTfXvcY2t3YbkHptKdr+BryMC3mTp7Fciv3GJ18QjSRASQfo=



Hy6mS61UwA8zLzSCxBwiE6pkQixCEtCLsTfXvcY2t3YbkHptKdr+BryMC3mTp7Fciv3GJ18QjSRASQfo=

What are Insecure Direct Object References?

Imagine a web page that allows you to view your personal information. The web page that shows the user their information is generated based on a user ID. If this page was vulnerable to insecure Direct Object References an attacker wo

Figure 10

Then click submit button or press Enter.

Then you will move to next level.

3. Level 2- What is Poor Data Validation?

To get the result key to this lesson, you must bypass the validation in the following function and submit a negative number.

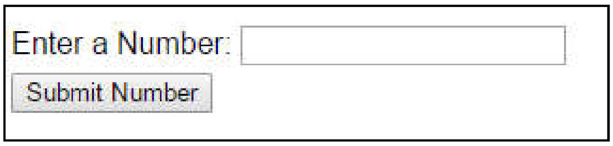
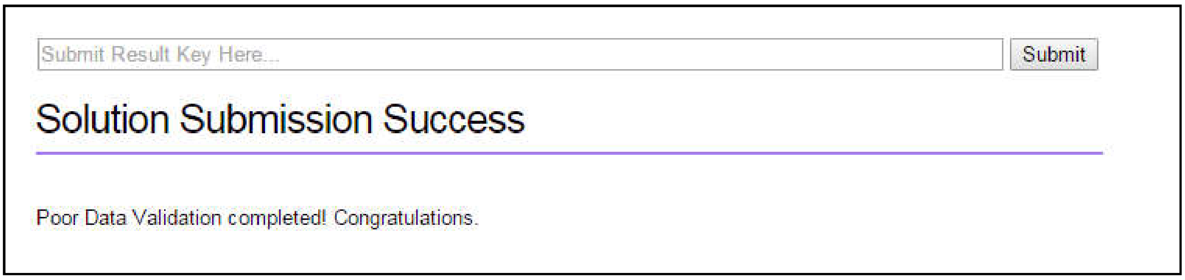


Figure 11

Since you have to submit a negative value, you have to change the respective value in the source such as userdata=2 into userdata=-1 and click forward.

Result key :
f26yIgfiqiO+wbbzBJJHjQf1bRb4Glvd2PBBTdmvJjCoHEMfXQX/lEzc0JNTnSc4i5XxEpD57VRau5L9V7MdHE9JEbarY6OQb+FDWZDVQlrta2WjzPo65Zc2b3O0uu06fFNbYJUliKeZe5/kJzfpAQ==

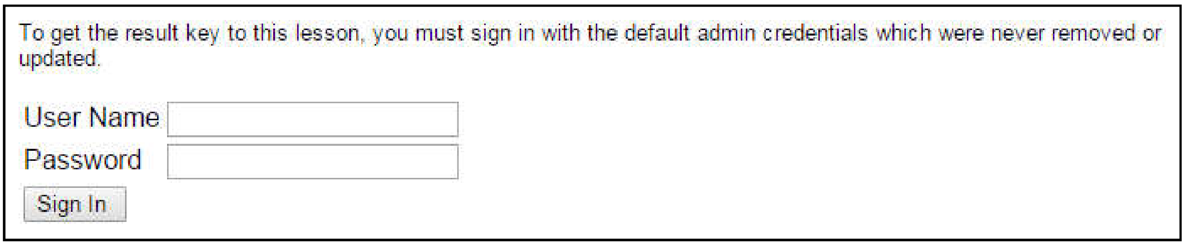
copy that and paste it on the search bar and click submit. You will move to next level. Do the same steps for next levels and bypass the validations and move forward for next level. Carefully read the instructions they have given for each level.



Solution Submission Success

Poor Data Validation completed! Congratulations.

4. level 3 - Security Misconfiguration



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

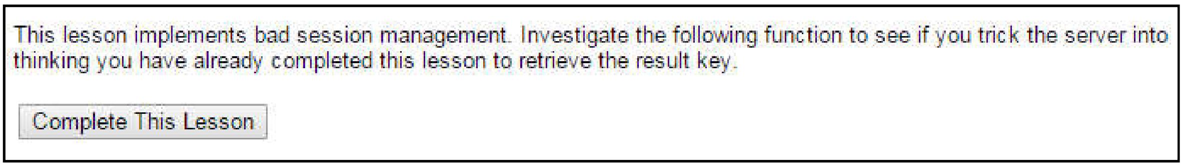
Password

Figure 12

change the userName=admin&userPass=<type your password here> into userName=admin&userPass= password

Result key :
N1AVjRMwx1jZz06ykOT2cKGKFTDPBLrkBogybxLISc16dtI0XYtql9YoFIIUDnbQnqM6CEc
Tc4xeYbuADkj9arlk6TMweU1abqxgLT1g/ZK4dOqGh4AocaBV6a9vw2TGzOXn2lY3tbbWv6
Otb24PAA==

5. level 4 -What is Broken Authentication and Session Management?



This lesson implements bad session management. Investigate the following function to see if you trick the server into thinking you have already completed this lesson to retrieve the result key.

Figure 13

Change lessonComplete=lessonNotComplete; into lessonComplete=lessonComplete;

Result key :
Lha2k8Kau7BR38MIJhaYG+x5SO7j3hP1bUWfMjzIg7g56Nzle86YMOqyXolnxGZKli2Pew8SBxEKQ7fdc8iYyARYD/DDMJGO/DAmA56WfJw=

6. level 5 - What is a Failure to Restrict URL Access?

The result key to this lesson is stored in a web page only administrators know about.

In this page the key is hidden in the web page. To find the key right click on the web page and select Inspect elements.

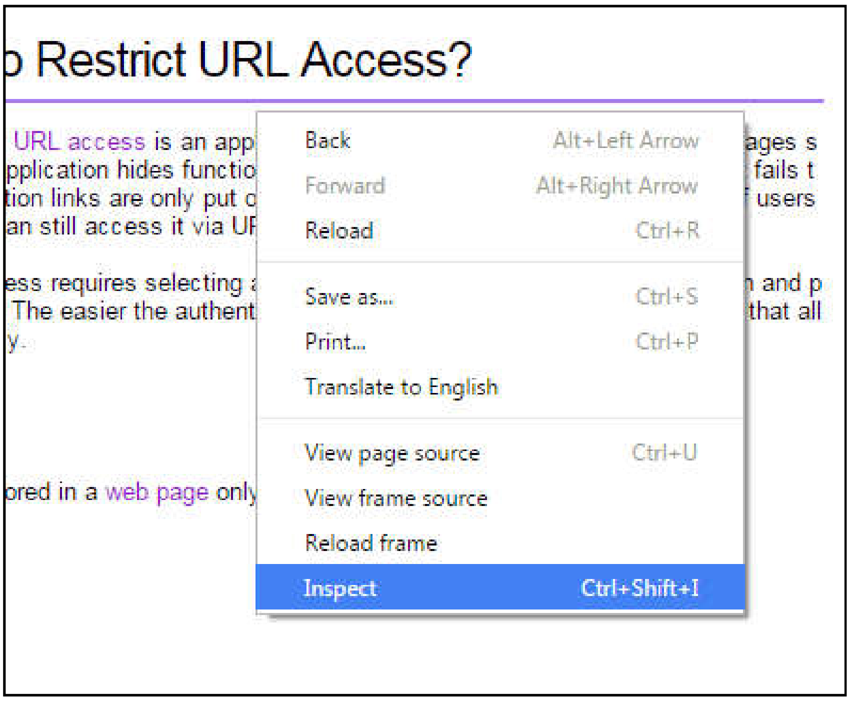
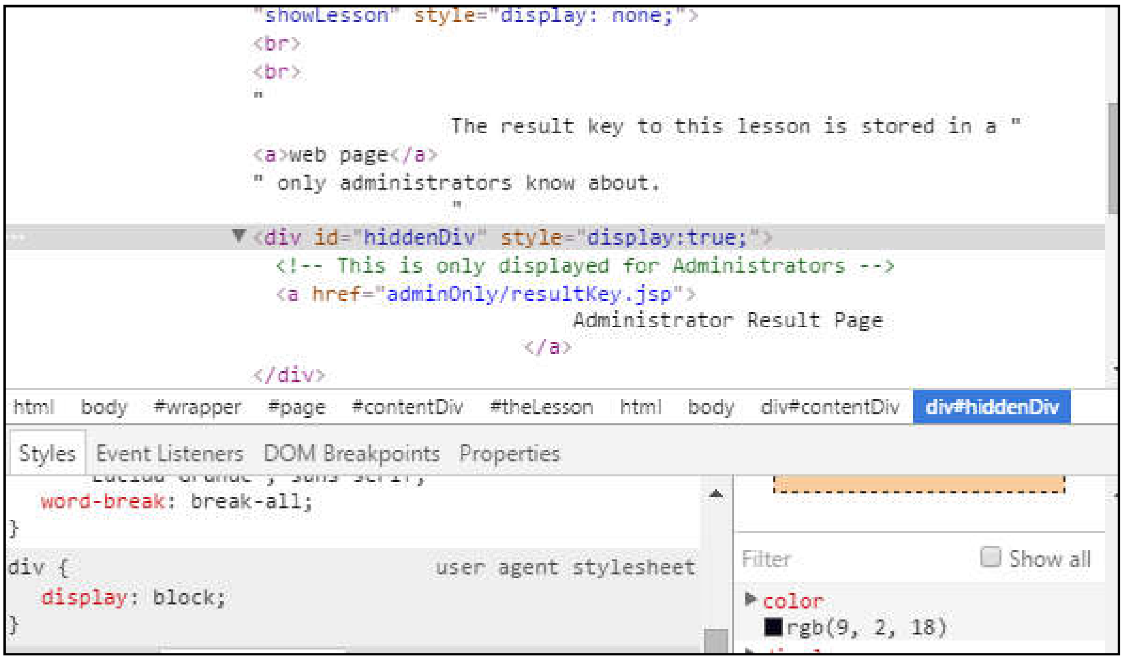


Figure 14

Now find the place where "The result key to this lesson is stored in a web page only administrators know about." is defined. in there you can see <div id="hiddenDiv" style="display:none"> <!--This is ….</div>. Double click on display:none and In this you have to change the style="display:none" into style="display:true". Because the key is display only to administrators.



```
"showLesson" style="display: none;">
<br>
<br>
"
                The result key to this lesson is stored in a "
<a>web page</a>
" only administrators know about.
                "
▼<div id="hiddenDiv" style="display:true;">
  <!-- This is only displayed for Administrators -->
  <a href="adminOnly/resultKey.jsp">
          Administrator Result Page
        </a>
</div>
```

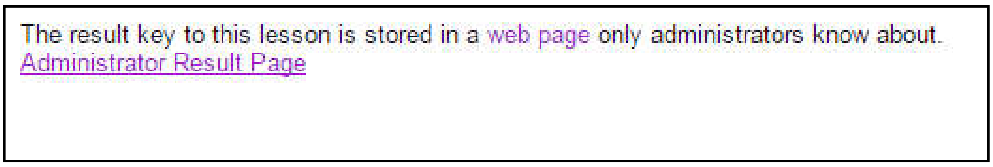
html body #wrapper #page #contentDiv #theLesson html body div#contentDiv div#hiddenDiv
Styles Event Listeners DOM Breakpoints Properties

```
  word-break: break-all;
}
div {                         user agent stylesheet
  display: block;
}
```

Filter
□ Show all
▶ color
■ rgb(9, 2, 18)

Figure 15

Now you can see a link as below. Click the link then your burpsuite will detect the session.



The result key to this lesson is stored in a web page only administrators know about.
Administrator Result Page

Figure 16

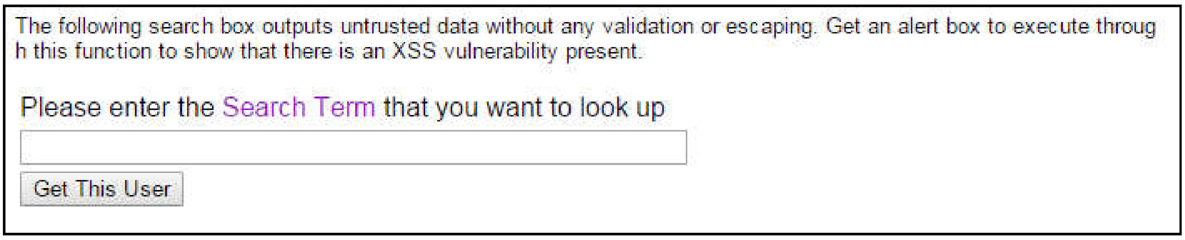
Change the lessonComplete=lessonNotComplete into lessonComplete=lessonComplete and you will get the key.

Result key :
11ipW36JlNkP0eyG+MQIemXJ1TcgOVux27iL+5TF2P9hsOD8Qiizau6uOT61dZuh6Sel7eA6GdzucTCuEpbk2Mmals7v2rJCQPdkwRaTESo=

7. level 6 - What is Cross Site Scripting (XSS)?

```
<SCRIPT>alert('XSS')</SCRIPT>
<IMG SRC="#" ONERROR="alert('XSS')"/>
<INPUT TYPE="BUTTON" ONCLICK="alert('XSS')"/>
<IFRAME SRC="javascript:alert('XSS');"></IFRAME>
```

are XSS script types



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

Figure 17

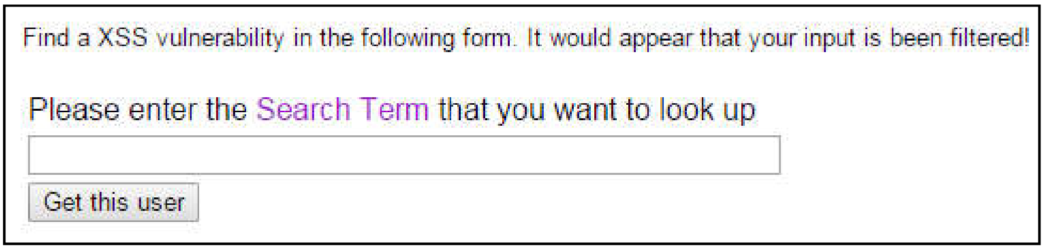
You have to use one of the script to get an alert box. Ex: <SCRIPT>alert('XSS')</SCRIPT>

Then release click intercept is on to off the intercept (you should on the intercept while clicking the Get This User button)

Result Key :
uTrKcSqfrasJYEr/y2LRxbzQTcPf7bcyDZ4Xbcaoad67qtYPMpKQWDRCwlTNG6VP5YfBb1ipyVMhs9/mB2vwHKcgeTN/+sPkfzQL7uP3+fU=

Move to next level.

8. Level 7 - 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

Figure 18

Since it tell about an input type, <INPUT TYPE="BUTTON" ONCLICK="alert('XSS')"/> is used.

on the intercept and click the Get This User button.

Then off the intercept button and you will the key. Copy and paste it on the search and move to next level.

Result Key :
KwuqJtBvKXS8TnE0Zvdl4NpK/K8hGhrNP94a5n3pcA8TvV3mzhOrMgXhmgnYpySlRBdJeWFxE5tL56x6yE4Ji2hBRnGPjPrsqmvtARbLdQE=

move to next level.

9. What is Insecure Cryptographic Storage?

The decision has been made that the result key to this lesson should not be publicly available. To achieve this, the development team have decided to encode the result key with base64... recover it to complete the lesson.

Result Key (encoded):

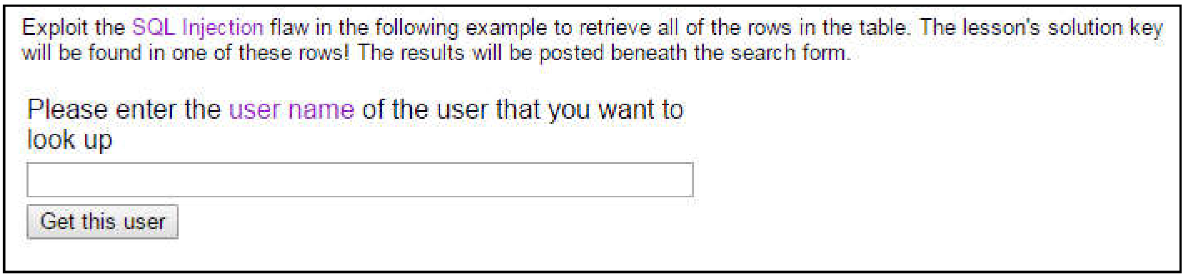
YmFzZTY0aXNOb3RFbmNyeXB0aW9uQmFzZTY0aXNFbmNvZGluZ0Jhc2U2NEhpZGVzTm 90aGluZ0Zyb21Zb3U=

This is the key to move to next level. it is encrypted using base64 and you have to decrypt it using a decryption tool(online or a software). Then copy and paste decrypted phase on the search bar and move to next level.

Result Key (Decoded):

base64isNotEncryptionBase64isEncodingBase64HidesNothingFromYou

10. SQL Injection Lesson



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

Figure 19

Right click on the user name which is in purple colour and select Inspect.

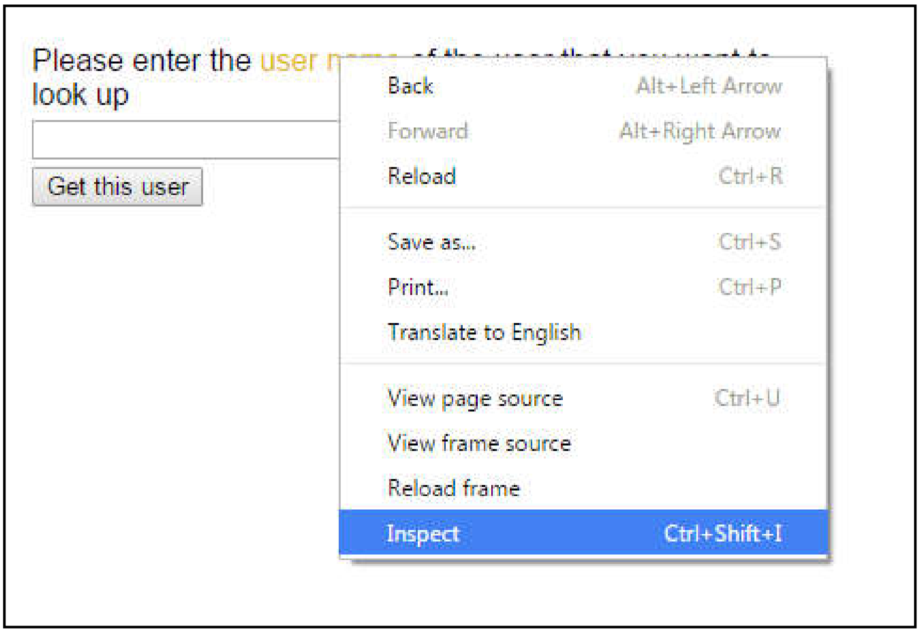
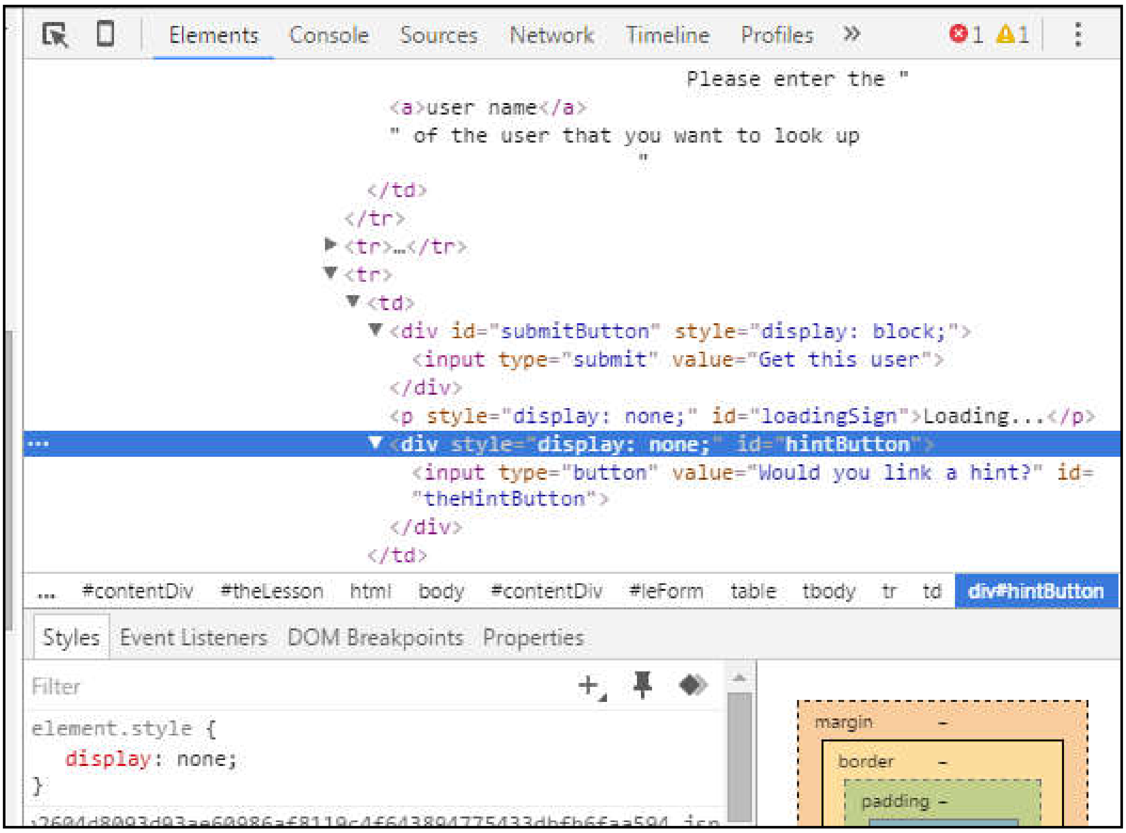


Figure 20

Go down on the source code and find div of hintButton and change the style=”display:none” to style=”display:true”.



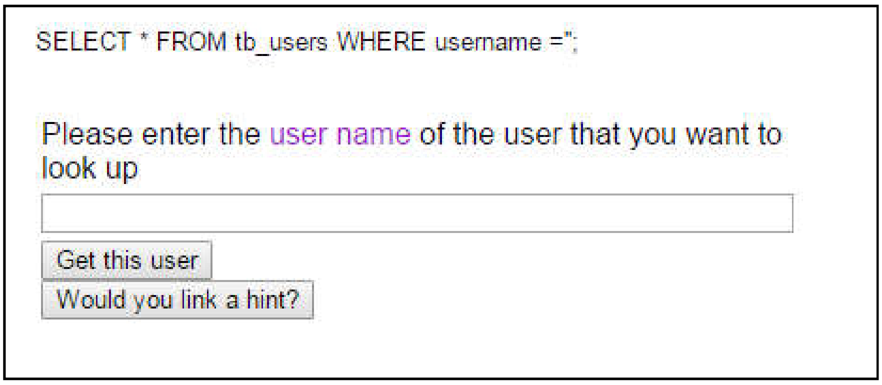
```
                                            Please enter the "
                        <a>user name</a>
                        " of the user that you want to look up
                                          "
                      </td>
                    </tr>
                  ▶ <tr>…</tr>
                  ▼ <tr>
                    ▼ <td>
                      ▼ <div id="submitButton" style="display: block;">
                          <input type="submit" value="Get this user">
                        </div>
                        <p style="display: none;" id="loadingSign">Loading...</p>
…                     ▼ <div style="display: none;" id="hintButton">
                          <input type="button" value="Would you link a hint?" id=
                          "theHintButton">
                        </div>
                      </td>
```

… #contentDiv #theLesson html body #contentDiv #leForm table tbody tr td div#hintButton
Styles
Event Listeners
DOM Breakpoints
Properties
Filter

```
element.style {
    display: none;
}
\2604d8093d93ae60986af8119c4f643894775433dbfb6faa594.jcn
```

Figure 21

Then you can see a hint button under Get this User button and a database statement. (Previously hint button was hidden)



SELECT * FROM tb_users WHERE username =";

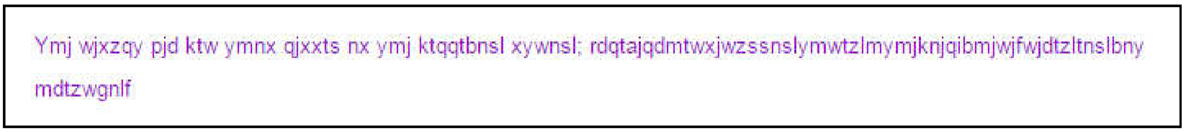
Please enter the user name of the user that you want to look up

Figure 22

Copy and paste the database statement in the textbox.

11. Insecure Cryptographic Storage Challenge 1

The result key has been encrypted to ensure that nobody can finish the challenge without knowing the secret key to decrypt it. However, the result key has been encrypted with a famous, but easily broken, Roman cipher. The Plain text is in English.



Ymj wjxzqy pjd ktw ymnx qjxxts nx ymj ktqqtbnsl xywnsl; rdqtajqdmtwxjwzssnslymwtzlmymjknjqibmjwjfwjdtzltnslbny mdtzwgnlf

Figure 23

Copy the above text and decrypt it by using a Roman Cipher or Caesar cipher decryption tool.

The key for Roman cipher is 21.

Result Key : The result key for this lesson is the following string; *mylovelyhorserunningthroughthefieldwhereareyougoingwithyourbiga*

copy and paste the selected result key on the search bar and submit.

move to next level.

12. 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...

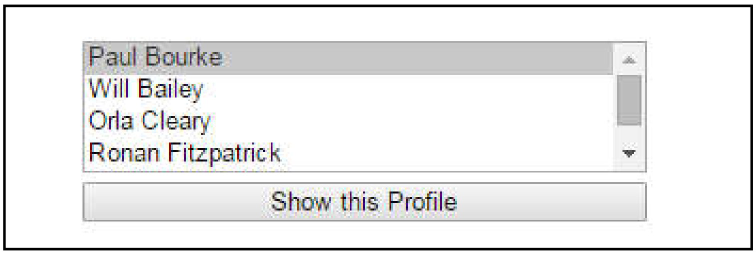


Figure 24

select one by one from the list above and click the Show this Profile button. You'll get a message like below for each name. Go through each name and collect the message it shows.

Paul Bourke's Message

No Message Set

Will Bailey's Message

I love Go Karting

Orla Cleary's Message

As if!

Ronan Fitzpatrick's Message

I have retired

Pat McKenana's Message

I have a car!

13. 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...

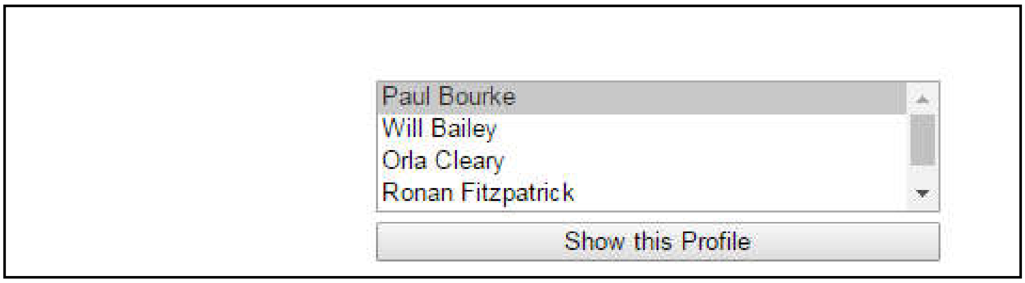
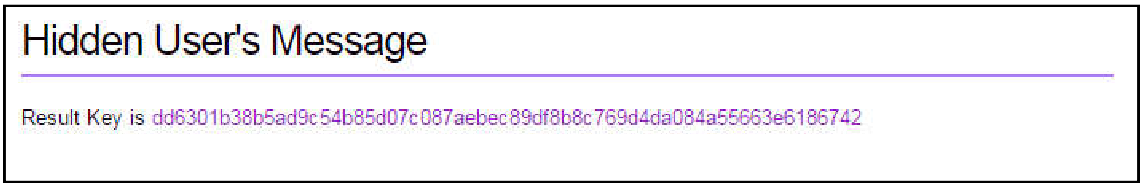


Figure 25

The private message is stored inside the user that not listed in drop down. Right click on the Show this Profile Button and select Inspect. From there Identify the pattern of the list box values or IDs. You can realized user IDs are set as 1,3,5,7,9. So, what I have done is I tried 0,2,4,6,8,10,11,12..etc. To do this, click the "Intercept is on" button on Burp Suite and go to your OWASP exercise page and select one of the user from the list and click the Show this Profile button. Then go to Burp Suite page and change the user IDs to 0 and click Forward button. Check the OWASP page whether you got the Key.

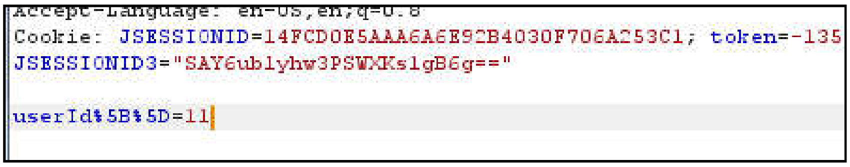


Hidden User's Message

Result Key is dd6301b38b5ad9c54b85d07c087aebec89df8b8c769d4da084a55663e6186742

Figure 26

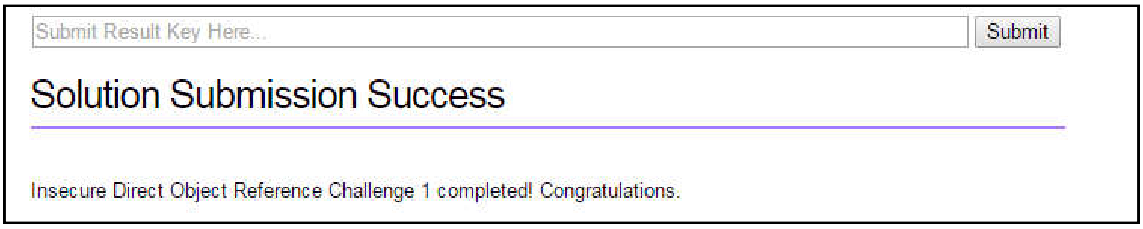
dd6301b38b5ad9c54b85d07c087aebec89df8b8c769d4da084a55663e6186742



```
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=14FCD0E5AAA6A6E92B4030F706A253C1; token=-135
JSESSIONID3="SAY6ublyhw3PSWXKs1gB6g=="

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

Figure 27

Copy the displayed key in the submit result key textbox and click the submit button.



Solution Submission Success

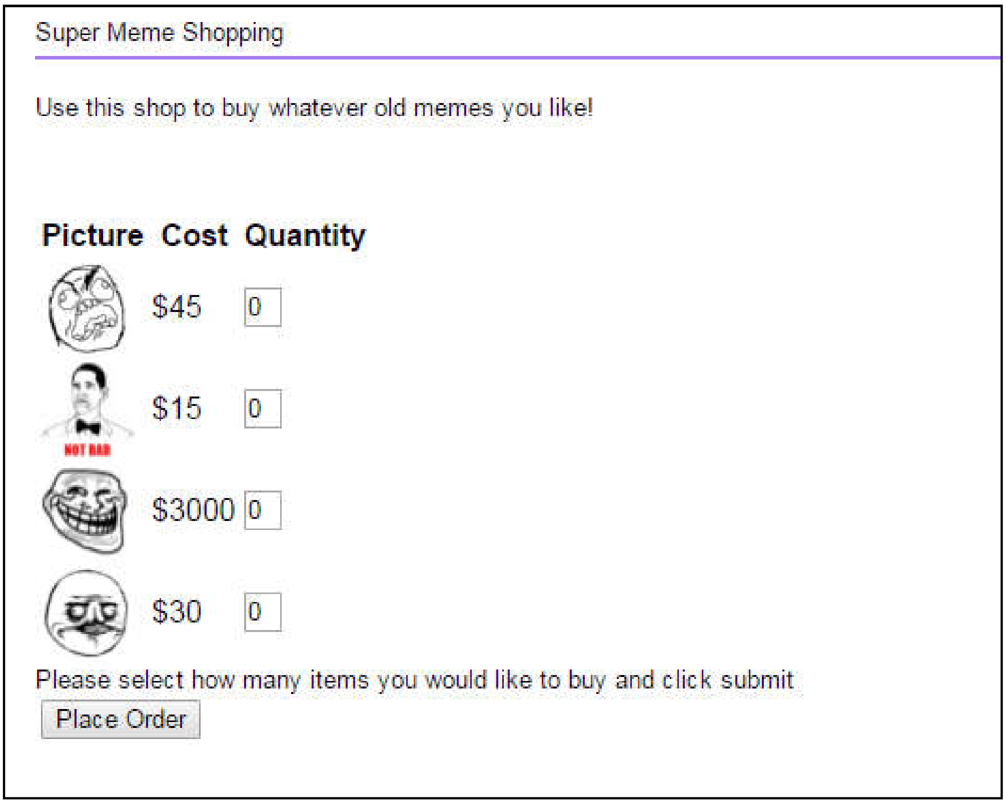
Insecure Direct Object Reference Challenge 1 completed! Congratulations.

Figure 28

Move to next level.

14. Poor Validation One

If you can buy trolls for free you'll receive the key for this level!



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

Figure 29