Sukhmani Sandhu 18BCE7155
Secure Coding Lab 5
Date: 24 February 2021

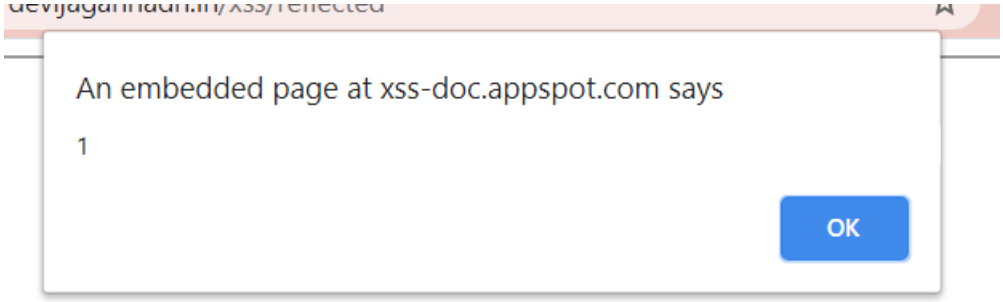
Objective: To understand how secure coding is related to Cross Site Scripting.

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

So it becomes imperative to practice coding securely in order to prevent any such attacks and reduce all these vulnerabilities.

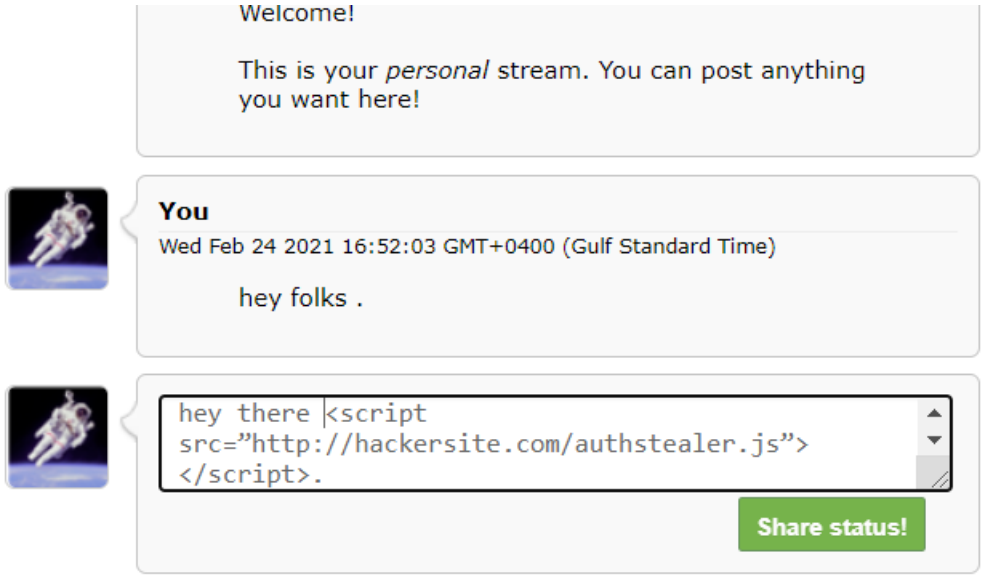
Reflected Cross Site Scripting:

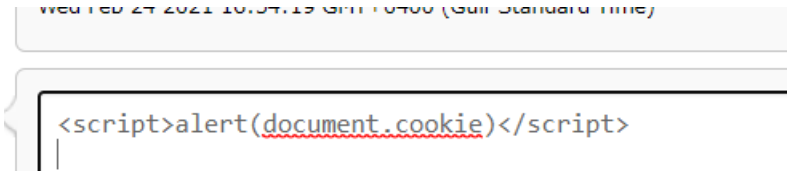
Reflected attacks are those where the injected script is reflected off the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request.



Stored Cross Site Scripting:

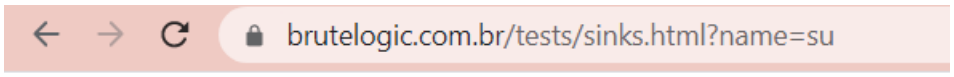
Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information.





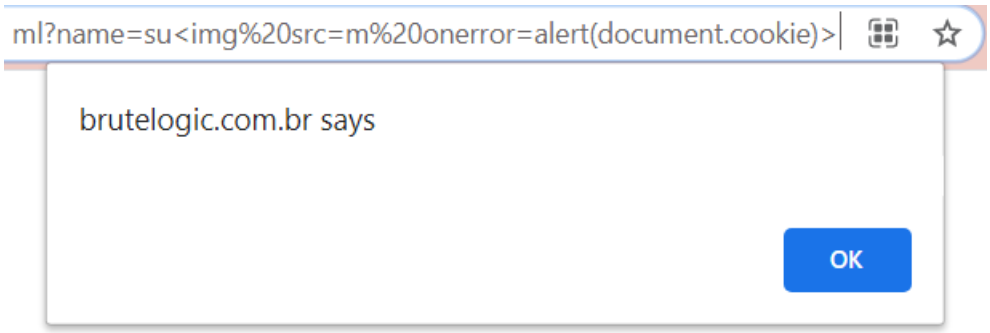
DOM Based Cross Site Scripting:

DOM Based XSS (or as it is called in some texts, “type-0 XSS”) is an XSS attack wherein the attack payload is executed as a result of modifying the DOM “environment” in the victim’s browser used by the original client side script, so that the client side code runs in an “unexpected” manner.

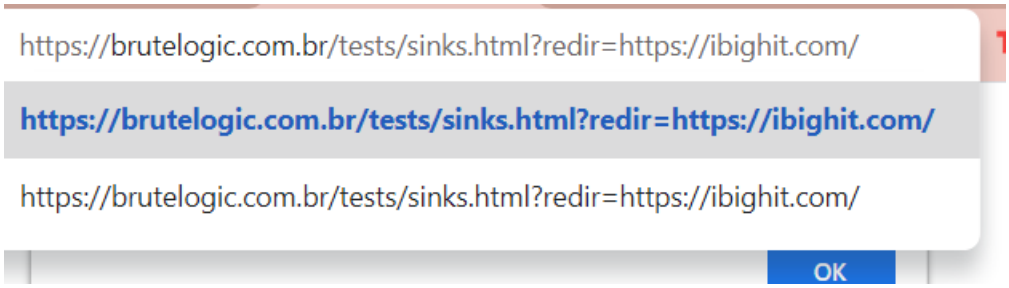


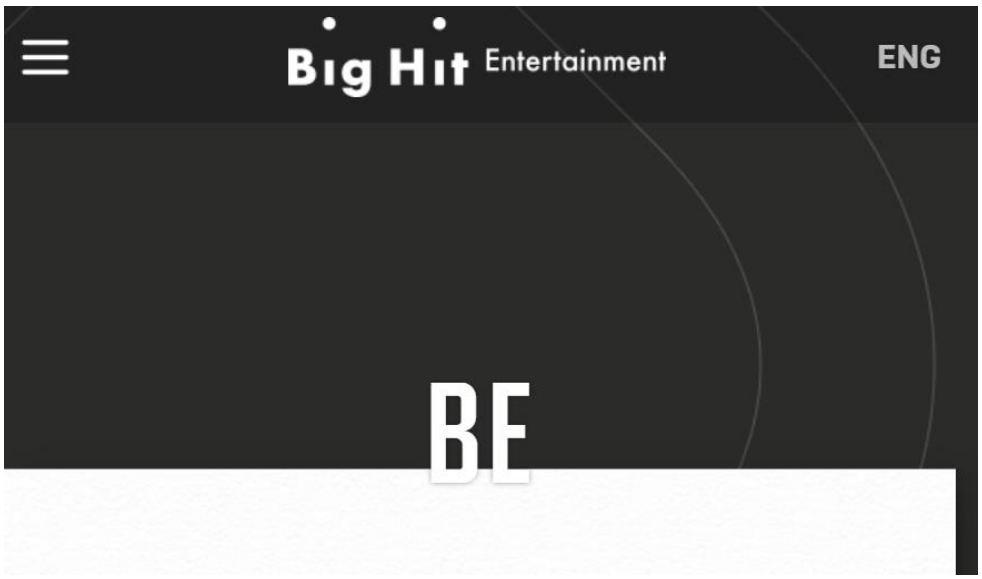
Hello, su!

After locating the source code sink



Now using the “redir” sink





Challenge: Alert(1) to win

alert(1) to win

The code below generates HTML in an unsafe way. Prove it by calling `alert(1)`.

```
function escape(s) {
  return '<script>console.log("'+s+'");</script>';
}
```

Input 14

```
");alert(1);("
```

Output Win!

```
<script>console.log("");alert(1);("");</script>
```

Rate this level: ★★★★★

User	Score	Browser
... ShabbyMe	? 0	Firefox/77
geniusmaster33 don't worry about less than 12 its a hack	? 4	Chrome/86
jay 123	? 11	Chrome/86
ma	? 12	Chrome/88
Kyzer 12	? 12	Firefox/84
aaa 123	? 12	Chrome/87
OvO How less ummm	? 12	Chrome/87
-_- rick roll	? 12	Chrome/88