

# **Secure Coding 2010**

## **XSS warmup**

**D.V.S MOHITH GUPTA**  
**18BCN7072**

## **How secure coding related to XSS?**

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.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script.

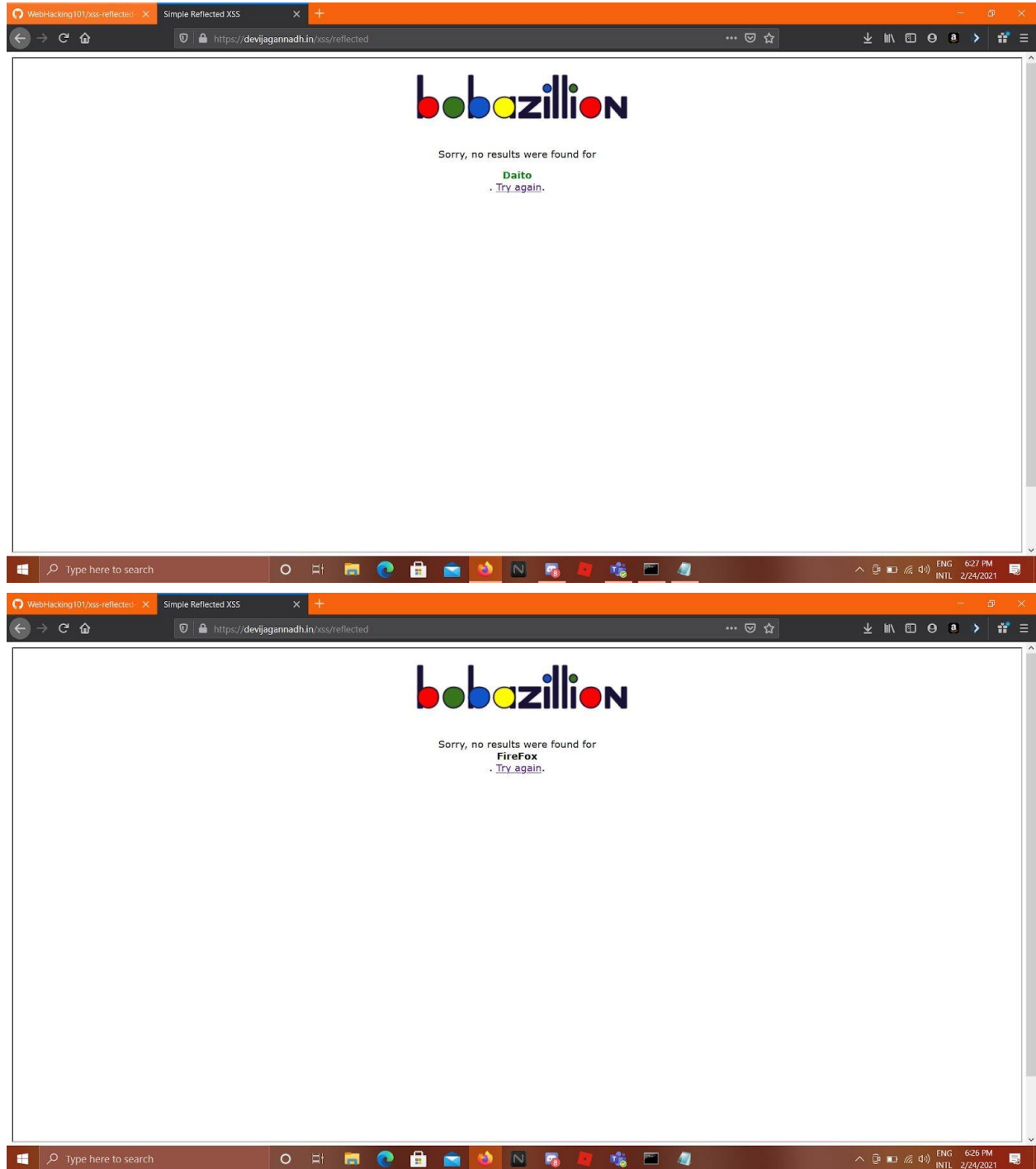
Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

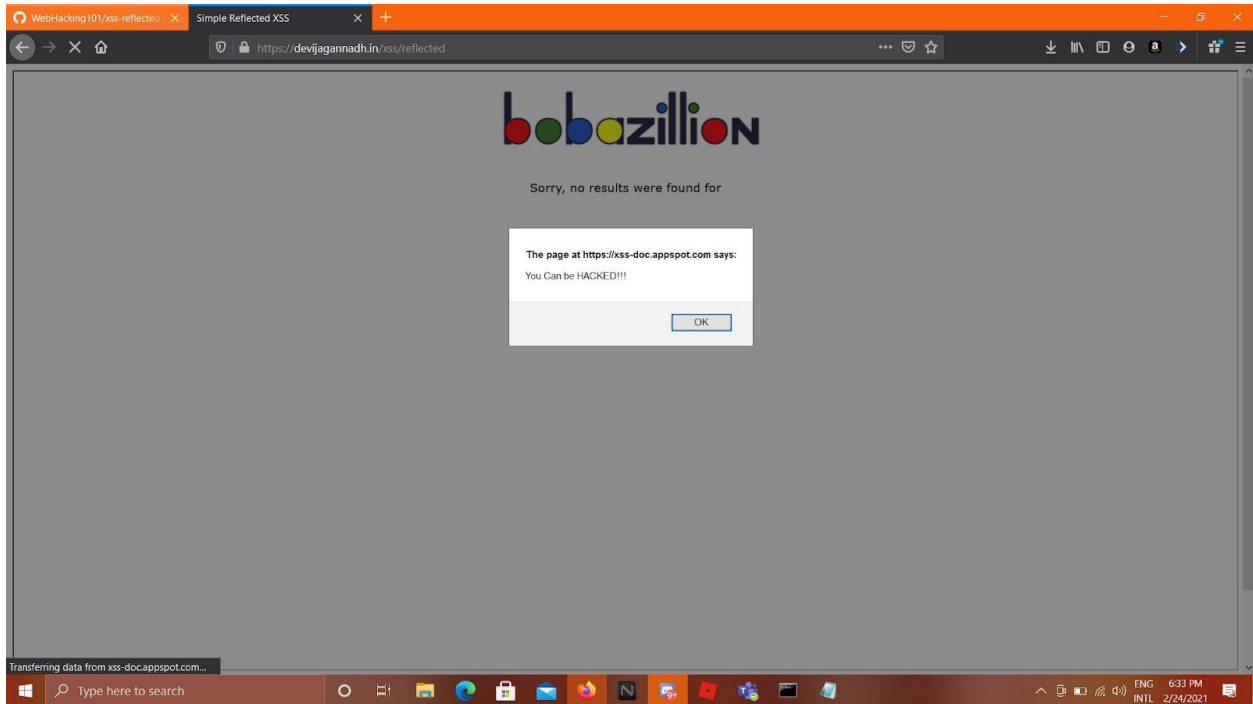
# XSS Reflected

<br>FireFox</br>

<div style=color:green>Daito</div>

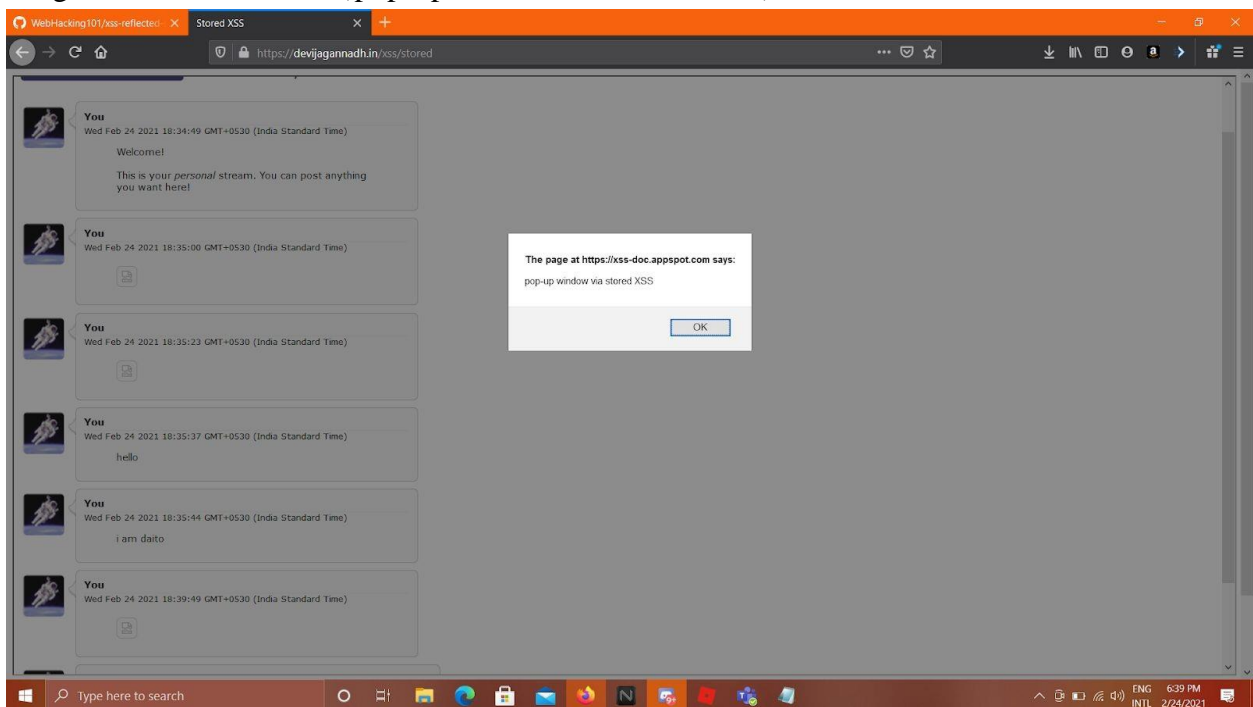
<script>alert("You Can be HACKED!!!")</script>





## XSS Stored

`<img src=x onerror="alert('pop-up window via stored XSS');"`



# XSS DOM

<http://brutelologic.com.br/tests/sinks.html>

[http://brutelologic.com.br/tests/sinks.html?name=daito<img src=x onerror=alert\(document.cookie\)>](http://brutelologic.com.br/tests/sinks.html?name=daito<img src=x onerror=alert(document.cookie)>)

[http://brutelologic.com.br/tests/sinks.html?redir=javascript:alert\(101\)](http://brutelologic.com.br/tests/sinks.html?redir=javascript:alert(101))

