

Forum:[Hack Forums](#)

Thread: [Beginner XSS Deface Guide](#)

WarOnDrugs - August 8, 2014, 5:18 pm

What is XSS?

cross-site scripting (XSS) is a type of website security vulnerability typically found in web applications that enables client-side script into web pages viewed by other users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

Types of XSS vulnerabilities:

1. Persistent
2. Non persistent

In this post, I'll explain about the non persistent vulnerability.

Non persistent XSS vulnerability is the Most Common Type of XSS Flaw. It is a Server Side Vulnerability

When a Web Server takes any input from a User and returns the same back to the User without any Validation, This leads to a Non-Persistent XSS Vulnerability.

XSS Attacks be used for the following:

- Compromising and Hijacking Accounts
- Stealing User Cookie
- Defacing Websites
- Phishing Attacks
- Posting Hostile Content

Instructions:

Step 1: First of all find the vulnerability using google dorks. You can find dorks online.

Code Most commonly used dorks are as follow:

```
inurl:com_feedpostold/feedpost.php?url=
inurl:/products/orkutclone/scrapbook.php?id=
inurl:/products/classified/headersearch.php?sid=
inurl:/poll/default.asp?catid=
inurl:/search_results.php?search=Search&k=
```

Step 2: Choose a target website:

To do so use the Google Dorks above and once you find a website, refer below for the next step in the process.

Find out the vulnerability:

1)Find a textbox in the site or something where you can submit text.
2)Type in the following and hit Submit Query button.
Code <script>alert("hit");</script>3)If it's vulnerable it will show an alert box with the word "hit" inside it.

Defacing:

There are few ways which can be used to deface a site when you find a XSS vulnerability.

1) Makes A Picture Pop-Up:

Code <script>location="www.website.com/yourdefacepic";</script>

2) Replace The Content Of The Page By An Image:

Code

3)Redirect To A Website

Code <script>window.location="http://www.yoursite.com"</script>

Vanilja - August 8, 2014, 5:20 pm

Hmm, looks pretty nice.

Will take a look tomorrow.

WarOnDrugs - August 8, 2014, 5:24 pm

(Aug 8, 2014 05:20 PM)Katy Perry Wrote: [\[CITE\]](#) Hmm, looks pretty nice.

Will take a look tomorrow.

Take your time, Katy. It's fairly straightforward.

?DutchOps - August 8, 2014, 5:59 pm

Thanks, Learned a few things...!! but its really only changing javascript or html.. Do you know any good persistant xss tuts?

WarOnDrugs - August 8, 2014, 6:47 pm

(Aug 8, 2014 05:59 PM)?DutchOps Wrote: [\[CITE\]](#) Thanks, Learned a few things...!! but its really only changing javascript or html.. Do you know any good persistant xss tuts?

I really don't know any good persistant xss tuts to refer you to. I guess use google.

monuty - August 12, 2014, 8:23 am

(Aug 8, 2014 06:47 PM)Ultimate Wingman Wrote: [\[CITE\]](#) I really don't know any good persistant xss tuts to refer you to. I guess use google.

nice tut bro :D u know any good vulnerability scanner for XSS , SQLi ?

Powindah - August 12, 2014, 1:13 pm

Very basic and straight to the point guide, thanks for posting this.

joneh heil - August 12, 2014, 2:28 pm

Cool tutorial, never really gotten into XSS but I will try this :)

WarOnDrugs - August 12, 2014, 4:48 pm

(Aug 12, 2014 02:28 PM)joneh heil Wrote: [\[CITE\]](#) Cool tutorial, never really gotten into XSS but I will try this :)

It's good just to play around with even, or just to learn something new.

(Aug 12, 2014 01:13 PM)Powindah Wrote: [\[CITE\]](#) Very basic and straight to the point guide, thanks for posting this.

No worries my man. Hopefully you found it of some use.

justsmil3x - *August 13, 2014, 5:58 am*

Basic, yet informative and well structured guide. Sounds perfect for beginners!

aproxyb - *August 13, 2014, 6:34 am*

Thanks for sharing. Will try this out

Dyingsoul - *August 14, 2014, 3:34 am*

Nice and clean guide! :) Thanks for this one!

Blackbullz - *August 21, 2014, 3:39 am*

Great tutorial buddy, I've tested It and is working perfectly.