

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Cross Site Scripting \(XSS\)](#)

Kodaz - January 30, 2017, 4:52 pm

Hello HF members, I'm Kodaz and this will be my first tutorial posted on HackForums. I want to start by saying

I am not responsible of what you use this knowledge for. This tutorial is intended for Educational purposes only.

1. Introduction
2. Finding vulnerable websites
3. Testing for Vulnerabilities
4. Types of Exploits you can execute

1. INTRODUCTION

In this tutorial you will learn about a known vulnerability in websites known as XSS.

Let's start off with the definition of Cross Site Scripting known as XSS.

XSS is a security breach that takes advantage of dynamically generated Web pages. In an XSS attack, a Web application is sent with a script that activates when it is read by an unsuspecting user's browser or by an application that has not protected itself against cross-site scripting.

2. FINDING VULNERABLE WEBSITES

Most people find these type of vulnerable websites by using Google dorks or they run scans on certain websites they are paid for to pentest with permission.

Google Dorks are basically search queries on Google that find the type of website you're looking for... For example:

As you can see I used the dork ".php?q=" and it came up with website links that finish in what I just Googled. This is an example of how to use Google Dorks.

3. TESTING FOR VULNERABILITIES

Once you get the search results on Google, You can go ahead and test to see if the website is vulnerable to XSS.

Once you enter anything on the search bar you can go ahead and do CTRL+U in your browser and it will open up view source. Or just right click anywhere and select view source.

Keep in note where your search query was placed by doing CTRL+F and searching BTS.

So now we are going to go ahead and check if the server sanitizes our code or not. So we will type in <"script"> without quotes on the search query and once again check where the input was placed on view source.

Now we can see that the code went through without being blocked by the website. Which means we can go ahead and execute any code we want.

But first, We want to go ahead and make sure that the website is 100% vulnerable so we're just going to type in this on the search bar,

If it was successful the page will follow up with a pop up that might look like this.

Now we know the website is completely vulnerable and we can proceed to execute all type of code... Malicious or not. There is also different types of XSS which I'm going to explain now.

Persistent XSS = This type of XSS is when the script entered by the hacker is stored on the server. For example, If a person tries to access the search section it will execute the code you saved on the server on their machine and you can proceed to steal their cookies and stealing their accounts.

Non Persistent XSS = This type of XSS is also known as Reflected XSS, Which is the most common one these days. The code entered will be sent to the server as a HTTP Request, So let me explain... If you search something up on a vulnerable search bar it will come up like "search results for 'word' " If the server fails to block the entered code It will execute the injected script. However this type of XSS is not persistent which means only you can see the executed code.

4. TYPES OF EXPLOITS YOU CAN EXECUTE

Stealing identity and Confidential Data

Bypassing website restrictions Session Hijacking

Malware attack Website Defacement

DoS attack

Thank you all for reading and I hope I was of help to somebody in the community.

If you liked it please let me know in the comments and i will continue to write more tutorials.

Megabear - January 30, 2017, 5:03 pm

This tutorial seems very noob friendly.

Anyone can do this to be honest by reading this tutorial.

Thanks for this information you contributed to the community.

Kodaz - January 30, 2017, 5:04 pm

(Jan 30, 2017 06:03 PM)Megabear Wrote: [\[CITE\]](#) This tutorial seems very noob friendly.

Anyone can do this to be honest by reading this tutorial.

Thanks for this information you contributed to the community.

I really appreciate your feedback, I will definitely continue to make more tutorials! :)

Mycroft Holmes - January 30, 2017, 5:06 pm

Excellent job Kodaz. You pretty much cover the basics for people to understand what XSS is and how does it work.

Kodaz - January 30, 2017, 5:08 pm

(Jan 30, 2017 06:06 PM)The Enigma Wrote: [\[CITE\]](#) Excellent job Kodaz. You pretty much cover the basics for people to understand what XSS is and how does it work.

Appreciate it and, Yes sir, it was actually what I aimed to do.

bdawn - January 31, 2017, 4:59 pm

A bit basic but I got to say that I really enjoyed how you formatted this. Keep up the work, dude

(Yes, I stalked your profile and found this post :P)

Desert03 - January 31, 2017, 5:26 pm

Keep up the good bru,ilearned alot

Kodaz - January 31, 2017, 6:08 pm

Thanks for the feedback guys. I hope i helped :)

SpeedDemonx - February 1, 2017, 10:01 am

Great tutorial, Very noob friendly and easy to follow. Its great that you added the images as well.

Kodaz - February 1, 2017, 3:45 pm

(Feb 1, 2017 11:01 AM)SpeedDemonx Wrote: [\[CITE\]](#) Great tutorial, Very noob friendly and easy to follow. Its great that you added the images as well.

Thank you, Appreciate your feedback.

EvilL0rd - February 1, 2017, 7:09 pm

Well done brother. This helped me a lot

Kodaz - February 2, 2017, 11:49 am

(Feb 1, 2017 08:09 PM)EvilL0rd Wrote: [\[CITE\]](#) Well done brother. This helped me a lot
I'm glad it did. Thank you

Mr. Robot - February 2, 2017, 11:51 am

Baha I am referring people to this thread from now on, So easy for noobs to understand.

Thanks OP

Kodaz - February 2, 2017, 11:55 am

(Feb 2, 2017 12:51 PM)Mr. Robot Wrote: [\[CITE\]](#) Baha I am referring people to this thread from now on, So easy for noobs to understand.

Thanks OP

Awesome Mr. Robot, Thanks for the feedback... Would be glad to work with you ;)

Tyler0410 - June 21, 2017, 9:55 am

Dude, how can I create a site which recives their cookies?

k1llph1ll - July 5, 2018, 2:10 pm

nice tutorial it was simple yet effective.

LGiver - May 19, 2021, 10:28 pm

Hmmhm Interesting. I'd be interested in more of a youtube explanation. does anyone have some of those?