

Forum:[Hack Forums](#)

Thread: [\[TuT\] XSS - Tamper Data to Persistent \[TuT\]](#)

zer0pwn - January 3, 2012, 10:05 am

[TuT] XSS - Tamper Data to Persistent [TuT]

Hello there, Hack Forums. I haven't made a tutorial in quite a while, and decided to post one today ^_^ . I'm posting a tutorial on a very useful XSS method I discovered (I'm not sure if lots of people know it or not :S). To successfully complete this method, you will need Tamper Data, and Firefox. That's all.

Finding a vulnerability

To successfully exploit this vulnerability, you will need a form that is select only. The form should look like this:

Also, this (obviously) must be on a page where it will save the selection we pick. I usually find these vulnerabilities in a Profile page, where it will say what kind of business you work in. Or what kind of job you do. Now for the next part, we need tamper data. So if you don't have it, go to the mozilla firefox addons home, and search for Tamper Data.

Tamper data is an HTTP Headers editor, so we'll be able to edit what we select in the boxes. Note that not every site is vulnerable, but the site I tested this on is called "F2C.com". It's one of the biggest (popular) sites in the world. And it's worth a lot of points on rankmyhack.com. Anyways, get Tamper data open. But don't start tampering yet. Select the option in the form, then start tampering, and hit "Save". Now on Tamper data, a little box should have appeared. It'll say the link of the request we're tampering. Now, you should see on the right side, what you put in for the form. Edit that to "><script>alert(/XSS/)</script>". Now you're done!

Sorry if this is a disorganized tutorial, hopefully it helped you out with XSS. If you have ANY questions, about XSS, this tutorial, my other tutorials. DO NOT HESITATE to PM me, I will respond to you as soon as I can! I am online a lot, so you should get a reply in the first 10-20 minutes. Enjoy this method, and please reply saying thanks just to keep the thread alive. :)

Anne - January 3, 2012, 10:07 am

Not a bad idea. I guess someone else must have thought of this, since it's suprisingly easy.

First time I've heard of though. Good tutorial, though I don't think people who haven't tried XSS will know what to do with it.

Girby2K11 - January 3, 2012, 10:35 am

Great tutorial, gonna try it out now!

AnoNimTeck - January 3, 2012, 10:41 am

Really nice guide! I was looking for some XSS guides because it seems really interesting ;D

Hooded Robin - January 3, 2012, 10:42 am

I am sure a lot of folks dont think (or remember) to tamper with other fields/forms when trying to inject but you would be surprised on the affects they might have. Good share, and original!

zer0pwn - January 3, 2012, 10:43 am

I'm thinking of making a video, so that everyone will understand more clearly. I kinda hoped there would be more feedback. Oh well :P

Anne - January 3, 2012, 10:45 am

Yea it's sad that many great tutorials like this one get's ignored.

Was this the method you used on co.cc?

-DownFall - January 3, 2012, 10:48 am

(Jan 3, 2012 11:45 AM)Anne Lindfjeld Wrote: [\[CITE\]](#) Yea it's sad that many great tutorials like this one get's ignored.

Was this the method you used on co.cc?

Great tutorials like this usually get ignored because the only people who leave feedback are the ones actually willing to fucking learn something (15% of the section?).

Great tut Zer0Pwn, Zer0Lulz strikes again :3

zer0pwn - January 3, 2012, 10:51 am

(Jan 3, 2012 11:45 AM)Anne Lindfjeld Wrote: [\[CITE\]](#) Yea it's sad that many great tutorials like this one get's ignored.

Was this the method you used on co.cc?

Haha, no.

I used it on other huge sites though.

If you want me to tell you the one for co.cc just PM me :P

United Kingdom - January 3, 2012, 10:53 am

Nice tut dude.

If you get accepted for uber pm I might buy you it.

Anne - January 3, 2012, 10:55 am

(Jan 3, 2012 11:51 AM)//#- Zer0Pwn -#// Wrote: [\[CITE\]](#) Haha, no.

I used it on other huge sites though.

If you want me to tell you the one for co.cc just PM me :P

Nah it's okay, I'm just interested in seeing how new exploits get developed. I won't be needing it myself.

Girby2K11 - January 3, 2012, 11:04 am

(Jan 3, 2012 11:43 AM)//#- Zer0Pwn -#// Wrote: [\[CITE\]](#) I'm thinking of making a video, so that everyone will understand more clearly. I kinda hoped there would be more feedback. Oh well :P

Well, it is a great tutorial, but when i use tamper data i get a box pop up saying Tamper, Submit, Abort. Which one do i pick? Thanks. ?

Hooded Robin - January 3, 2012, 2:45 pm

Tamper = allows you to edit fields and then submit; Submit = submit the request as is; Abort = cancel the request and nothing is sent. You will want to tamper with it then send the request when you are done editing the fields you need...

.Satan - January 3, 2012, 3:09 pm

Very cool method! thanks for sharing, ill try this soon

AcidSuit - January 3, 2012, 3:13 pm

Good job I've never heard of this before. Also good luck with uber!

FastFive - January 3, 2012, 6:47 pm

very good tutorial. never heard of this before, very unique method. hope to see more advanced XSS tutorials like this. thanks

Ayumu "Osaka" Kasuga - January 5, 2012, 4:57 pm

Very good tutorial sir! most people don't think of messing with other fields, but luckily that means most companies don't either :)