

# Forum:[Hack Forums](#)

Thread: [\[Vulnerability\] New Minecraft.net XSS Vulnerability](#)

**Norman Bates** - June 13, 2015, 2:21 pm

[Video: <https://vimeo.com/130542892>]

This exploit was found by [this](#) awesome guy.  
(Didn't know he had HF, but he's been on my skype for awhile lol)

**Fractal** - June 13, 2015, 2:22 pm

Nice find man. ?

**ThePenumbra** - June 13, 2015, 2:23 pm

Good job on finding that. Would report it to them if I were you.

**Norman Bates** - June 13, 2015, 3:14 pm

(Jun 13, 2015 02:23 PM)ThePenumbra Wrote: [\[CITE\]](#) Good job on finding that. Would report it to them if I were you.

Don't want to report it, want to see if anyone can do anything with this

**HaxOr?** - June 13, 2015, 3:18 pm

It's POST XSS mate. Pretty much useless.

**ThePenumbra** - June 13, 2015, 3:20 pm

(Jun 13, 2015 03:18 PM)HaxOr? Wrote: [\[CITE\]](#) It's POST XSS mate. Pretty much useless.

Sorry Haxxy baby, but are you dumb o.o?

I can make a link which on click auto-submits a POST request.

OP, got skype/xmpp?

If yes, PM me it.

**Fractal** - June 13, 2015, 3:21 pm

Harder to use, yes, but it's more dangerous as you don't see it in the requested URL. Either way this should be reported to Mojang, maybe you'll get some money for finding the exploit.

**ThePenumbra** - June 13, 2015, 3:23 pm

(Jun 13, 2015 03:21 PM)Fractal Wrote: [\[CITE\]](#) Harder to use, yes, but it's more dangerous as you don't see it in the requested URL. Either way this should be reported to Mojang, maybe you'll get some money for finding the exploit.

Why is it harder to use?

It's really easy.

Make a form, use js to auto-submit it.

Ez fucking pz.

**Fractal** - June 13, 2015, 3:25 pm

(Jun 13, 2015 03:23 PM)ThePenumbra Wrote: [\[CITE\]](#) Why is it harder to use?

It's really easy.

Make a form, use js to auto-submit it.

Ez fucking pz.

Exactly, JavaScript/HTML is required to make it work. Hence why it's harder to use on people, or

implement. I totally agree with you, it's not useless.

**SIM-1241186** - June 13, 2015, 7:49 pm

(Jun 13, 2015 03:20 PM)ThePenumbra Wrote: [\[CITE\]](#) Sorry Haxxy baby, but are you dumb o.o?  
I can make a link which on click auto-submits a POST request.

OP, got skype/xmpp?

If yes, PM me it.

You did not just call HaxOr? dumb ?

**Angel-sama?** - June 13, 2015, 7:51 pm

Wow what a great find. I've been trying to do something with it so far. :)

**Norman Bates** - June 13, 2015, 11:45 pm

(Jun 13, 2015 07:51 PM)Angel-sama Wrote: [\[CITE\]](#) Wow what a great find. I've been trying to do something with it so far. :)

No one done anything with it yet? Waiting for a big haxOr to get something done

**ThePenumbra** - June 14, 2015, 12:22 am

(Jun 13, 2015 11:47 PM)Yani Wrote: [\[CITE\]](#) That form has CSRF protection and your auto-submit thing would never work.

Didn't notice that. I guess i'll look around the site in abit.

**nullifiedvoid** - June 14, 2015, 2:38 pm

I found this vulnerability in December of 2014. It is pretty much useless unless any of you have any suggestions of how to capture the authenticityToken?

It has already been reported to Mojang. When I emailed them, they stated that there will be no payouts for vulnerability disclosures. I kind of kept it to myself for a few months hoping to find bypasses with authenticityToken. Unfortunately, I failed.

I have a few more vulnerabilities but am not sure if I want to release them.

**SuicidalManiac** - June 14, 2015, 6:36 pm

Pretty sure this isn't going to work, but I'll edit once I come up with something.

**?Criminal** - June 14, 2015, 6:43 pm

<http://kuza55.blogspot.com/2008/02/exploiting-csrf-protected-xss.html>

Using something like this may still work depending on how the session cookies work on minecrafts site.

**Im gone brah** - June 14, 2015, 7:01 pm

(Jun 13, 2015 03:20 PM)ThePenumbra Wrote: [\[CITE\]](#) Sorry Haxxy baby, but are you dumb o.o?  
I can make a link which on click auto-submits a POST request.

OP, got skype/xmpp?

If yes, PM me it.No, that won't work at all. Rifk

**Gee4rce** - June 15, 2015, 2:08 am

(Jun 13, 2015 03:20 PM)ThePenumbra Wrote: [\[CITE\]](#) I can make a link which on click auto-submits a POST request.

This is true, but if the website i.e. has no other vulnerability (which you may could use in combination to auto-launch the XSS),

AND further is even CSRF protected, then there is no real chance for a proper exploitation.

(Jun 13, 2015 03:20 PM)ThePenumbra Wrote: [\[CITE\]](#) Sorry Haxxy baby, but are you dumb o.o? You not call HaxOr dumb mate... ? If he says something, then it has a reason.

(Jun 13, 2015 11:45 PM)?Norman Bates Wrote: [\[CITE\]](#) No one done anything with it yet? Waiting for a big haxOr to get something done  
So why not do something by your own?

Greetings, Gee.

**ThePenumbra** - June 15, 2015, 3:55 am

(Jun 14, 2015 07:01 PM)Zayne Wrote: [\[CITE\]](#) No, that won't work at all. Rifk Why not?

(Jun 15, 2015 02:08 AM)Gee4rce Wrote: [\[CITE\]](#) This is true, but if the website i.e. has no other vulnerability (which you may could use in combination to auto-launch the XSS), AND further is even CSRF protected, then there is no real chance for a proper exploitation. Why do you need another vulnerability?  
If you have a proper POST XSS without csrf protection in it, you can just upload html with js on another site. You dont need to get the response, you just need to make the request.

**Gee4rce** - June 15, 2015, 4:03 am

(Jun 15, 2015 03:55 AM)ThePenumbra Wrote: [\[CITE\]](#) Why do you need another vulnerability? As for this one, there was a CSRF protection.

So as long as you not find another vulnerability, this XSS alone is not pretty much to exploit something interesting from it.

(Jun 15, 2015 03:55 AM)ThePenumbra Wrote: [\[CITE\]](#) You dont need to get the response, you just need to make the request.

You must be new here, calling HaxOr dumb and explaining me how XSS works ?  
(it's ok though, no problem ;)

Greetings, Gee.

**ThePenumbra** - June 15, 2015, 4:23 am

(Jun 15, 2015 04:03 AM)Gee4rce Wrote: [\[CITE\]](#) As for this one, there was a CSRF protection. So as long as you not find another vulnerability, this XSS alone is not pretty much to exploit something interesting from it.

You must be new here, calling HaxOr dumb and explaining me how XSS works ?  
(it's ok though, no problem ;)

Greetings, Gee.

If you take a look at my previous post in this thread, I said I didnt notice the CSRF protection.

**Gee4rce** - June 15, 2015, 4:30 am

Yes, sure,

but if you also take a look at your pre-previous post, you stated "Why do you need another vulnerability?", so i just explained why i put this statement before.

But np, lets move on here and get back to the topic guys...

Greetings, Gee.

**Im gone brah** - June 15, 2015, 7:10 am

ThePenumbra Wrote:Why not?

Are you for real, last time I checked this is not possible due to CSRF protection mechanism. Prove me wrong and I'd be happy to change my opinion. I'd also like to state that this XSS vulnerability is pretty much limited and really useless. Edit: If you want feel proudly with piping alerts, I won't stop you.

**LevelUp** - June 15, 2015, 10:03 am

You realise you can just use the XSS to extract the token using javascript right? Why are people crying over the token being some kind of ultimate protection?

It's 2015 now, step it up guys.

**Gee4rce** - June 15, 2015, 10:09 am

(Jun 15, 2015 10:03 AM)LevelUp Wrote: [\[CITE\]](#) You realise you can just use the XSS to extract the token using javascript right? Why are people crying over the token being some kind of ultimate protection?

It's 2015 now, step it up guys.

Nice to see you back LevelUp!!

But looks like you was sleeping while writing your answer ? ->

how would you extract the session or CSRF token, if the CSRF token already prevents an attacker from launching the XSS 'remotely' ? ...(as that would be required to extract anything Session related)

Greetings, Gee.

**LevelUp** - June 15, 2015, 10:16 am

(Jun 15, 2015 10:09 AM)Gee4rce Wrote: [\[CITE\]](#) Nice to see you back LevelUp!!

But looks like you was sleeping while writing your answer ? ->

how would you extract the session or CSRF token, if the CSRF token already prevents an attacker from launching the XSS 'remotely' ? ...(as that would be required to extract anything Session related)

Greetings, Gee.

To leave you wanting more I suggest you look into the Sammy Worm which used javascript to bypass myspace anti-csrf, but I wasn't sleeping.

Quick edit: Because I don't think any of you will actually bother looking into that you can just go on Owasp and it will set you straight.

**Gee4rce** - June 15, 2015, 10:49 am

(Jun 15, 2015 10:39 AM)Yani Wrote: [\[CITE\]](#) He was able to bypass CSRF because he got a persistent XSS that was running on the MySpace domain

^ Thats what i tried to explain LevelUp, OP's scenario is just a reflected POST XSS, thus it will not work extracting stuff.

**Cathal** - September 11, 2015, 3:35 pm

(Jun 15, 2015 10:16 AM)LevelUp Wrote: [\[CITE\]](#) To leave you wanting more I suggest you look into the Sammy Worm which used javascript to bypass myspace anti-csrf, but I wasn't sleeping.

Quick edit: Because I don't think any of you will actually bother looking into that you can just go on Owasp and it will set you straight.

Leaving this here in the hopes LevelUp sees it. I can't PM you at the moment, gimme a buzz when you're round.

