

Forum:[Hack Forums](#)

Thread: [Okay, so you can do Javascript alerts.](#)

Phizo - April 12, 2012, 10:46 am

I don't know if it's just me that has noticed this, but this section is being flooded with the following:

[XSS] longdomainnoonehasheardof.com [/XSS]

Okay, I can understand if it was Google, Youtube, Facebook or something that's well known. Most of the people in this section think that it's amazing to make a little alert box saying "XSS By NuLL_Byt3_R00T_HAK3R", is that seriously what the majority of this section is going to post?

Come on guys, it's a bit lame. How about actually trying to gain access instead of displaying alert boxes. There's nothing amazing and unique about it.

Quoted from JoinSeventh:

(Apr 13, 2012 07:22 AM)JoinSeventh Wrote: [\[CITE\]](#) Here is my thoughts on the subject:

XSS is a powerfull vulnerability if you know your shit, but most of these guys doesn't. It would be like if I run a Nessus scan on a random website and posted shit like "OMG LOOK THE SSL IS OLD AND INSECURE".

Pointless? Yes. Illogical? Yes. The same this that is happening? Yes.

I'm not saying that posting making posts about your XSS finds is bad, but:

Why not try to actually exploit them before publish?

I mean if I would find a SQL Injection vulnerability in some company website, I would actually tro the exploit it first.

Not because I necessarily want to dump the DB or own the box, but to show Proof of Concept.

Just my thoughts, hate all you want.

Hycca - April 12, 2012, 10:55 am

Well, it at least keeps the section going. Although some XSS vulns posted here are at sites nobody ever heard of and I admit, that's kind of annoying.

Phizo - April 12, 2012, 10:57 am

(Apr 12, 2012 10:55 AM)-?Exotz- Wrote: [\[CITE\]](#) Well, it at least keeps the section going. Although some XSS vulns posted here are at sites nobody ever heard of and I admit, that's kind of annoying.

Yeah, it keeps the section going which is good.

However, what about other vulnerabilities, what about ones that actually matter.

I'm not saying XSS doesn't matter, but the people on this forum obviously don't know how to unlock it's full potential and flail around with alert boxes.

Sorry, but there's nothing cool about it.

Susp3cT - April 12, 2012, 11:02 am

Yeah I see where ur going. Well people start thinking of XSS attack vectors, is the most dangerous thing.

Also I miss the old days, where the website section was mostly into the rooting! - since rooting is A

FUN SPORT!!

I did a few posts as well, but yeah, to straight it out, I'm stuck at this box, since I need to figure out an exploit.

Shelled website, about to r00t the server.

I tried to enumerate all my enforcements at 1337day, Exploit-DB, securityfocus.

Did not yet tried the command

Code `cd /pentest/exploits/exploitdb`

`cat files.csv | egrep -i "linux|kernel|local" | web | grep 05`

The box which I shelled upon

Code `Linux web05-07 3.0.9-vs2.3.1-20111121-96c063c #1 SMP Mon Nov 21 09:54:21 UTC 2011 x86_64`

Anyways, do you got some advice.. I tried on my own thread, but no one had answer! ? not even my self.

Out & Over

Phizo - April 12, 2012, 11:06 am

(Apr 12, 2012 11:02 AM)Susp3cT Wrote: [\[CITE\]](#) Yeah I see where ur going. Well people start thinking of XSS attack vectors, is the most dangerous...

I did a few posts as well, but yeah, to straight it out, I'm stuck at this box, since I need to figure out an exploit.

Shelled website, about to r00t the server.

I tried to enumerate all my enforcements at 1337day, Exploit-DB, securityfocus.

Did not yet tried the command

Code `cd /pentest/exploits/exploitdb`

`cat files.csv | egrep -i "linux|kernel|local" | web | grep 05`

Code `Linux web05-07 3.0.9-vs2.3.1-20111121-96c063c #1 SMP Mon Nov 21 09:54:21 UTC 2011 x86_64`

Anyways, do you got some advice.. I tried on my own thread, but no one had answer! :evil: not even my self.

Out & Over

XSS attack vectors? Yeah, for more alert boxes xD.

Anyway, to your question.

I have never seen that kernel version before, and it was released in 2011 as it says. I just tried searching up that kernel version on Google and there wasn't much to go on.

Sorry, but I've never seen that kernel version, maybe try rooting it manually instead of relying on local root exploits to perform the task for you, that's all I can suggest.

Good luck.

Susp3cT - April 12, 2012, 11:11 am

(Apr 12, 2012 11:06 AM)Phizo Wrote: [\[CITE\]](#) XSS attack vectors? Yeah, for more alert boxes xD.

Anyway, to your question.

I have never seen that kernel version before, and it was released in 2011 as it says. I just tried searching up that kernel version on Google and there wasn't much to go on.

Sorry, but I've never seen that kernel version, maybe try rooting it manually instead of relying on

local root exploits to perform the task for you, that's all I can suggest.

Good luck.

Yeah the forum did explode with a lot of ways of doing XSS statements.

In this way, we can conclude that this section does preform in mostly XSS attacks. As told, miss the old times!

Now to your answer...

Well, yeah that what I tried as well on Google. But with no luck!. I guess I have to study this kernel for a bit. Never back down! - The greater you dig, the greater chance for success. That is what I have learnt from the past... Anyways, thx for your answer ?

fobber - April 12, 2012, 11:24 am

I don't mind people posting all these XSS'es. As long as it isn't a non-persistent XSS on some stupid 11 year old girl's blog, about her stupid bird.

A sub-forum would be a great idea. Then you guys wouldn't have to bother looking at our awesome XSS finds. And we don't have to look at all your posts about "XSS ==== useless. Stop spamm da forumzz". No offence; but I've seen quite a few of those posts lately.

I'm sure that you, Phizo, is a super pro 1337 hacker (No sarcasm, really. I think you are. You've even helped me.), and you should therefore also understand the "power" of XSS.

When we do make an alert box, we just show that we could do some sick haxor stuff to the website, but we're way too nice to do that.

Again. No offence. Damn, I'd really love a XSS sub forum.

Phizo - April 12, 2012, 11:30 am

(Apr 12, 2012 11:24 AM)fobber Wrote: [\[CITE\]](#) I don't mind people posting all these XSS'es. As long as it isn't a non-persistent XSS on some stupid 11 year old girl's blog, about her stupid bird.

A sub-forum would be a great idea. Then you guys wouldn't have to bother looking at our awesome XSS finds. And we don't have to look at all your posts about "XSS ==== useless. Stop spamm da forumzz". No offence; but I've seen quite a few of those posts lately.

I'm sure that you, Phizo, is a super pro 1337 hacker (No sarcasm, really. I think you are. You've even helped me.), and you should therefore also understand the "power" of XSS.

When we do make an alert box, we just show that we could do some sick haxor stuff to the website, but we're way too nice to do that.

Again. No offence. Damn, I'd really love a XSS sub forum.

As long as it isn't a non-persistent XSS on some stupid 11 year old girl's blog, about her stupid bird.
<--- Seriously loved that.

No offence taken. This is my 2nd day of being back on HF from a year of inactivity, so I haven't seen any of these threads.

I know XSS is 'powerful', however majority of the users do not understand or know it's full potential, they aren't just showing alert boxes because they don't want to damage the site. The truth is they don't know how to.

That's the truth, the truth is inevitable.

Susp3cT - April 12, 2012, 11:39 am

(Apr 12, 2012 11:30 AM)Phizo Wrote: [\[CITE\]](#) As long as it isn't a non-persistent XSS on some stupid 11 year old girl's blog, about her stupid bird. <--- Seriously loved that.

No offence taken. This is my 2nd day of being back on HF from a year of inactivity, so I haven't seen any of these threads.

I know XSS is 'powerful', however majority of the users do not understand or know it's full potential, they aren't just showing alert boxes because they don't want to damage the site. The truth is they don't know how to.

That's the truth, the truth is inevitable.

It's quite easy to lead it into a full OS compromise, if you know how to preform ? ... Like a baws!

Tutorial by a member of Team Intra, has posted this ?

Phizo - April 12, 2012, 11:42 am

(Apr 12, 2012 11:39 AM)Susp3cT Wrote: [\[CITE\]](#) It's quite easy to lead it into a full OS compromise, if you know how to preform ? ... Like a baws!

Tutorial by a member of Team Intra, has posted this ?

That's correct, it can indeed lead to a full OS compromise, I have read on it.

Also things like Javascript buffer overflows can be done using XSS, some scary stuff out there.

However, people like to stick with good ol' alert("HAXERRR");

Susp3cT - April 12, 2012, 11:50 am

(Apr 12, 2012 11:42 AM)Phizo Wrote: [\[CITE\]](#) That's correct, it can indeed lead to a full OS compromise, I have read on it.

Also things like Javascript buffer overflows can be done using XSS, some scary stuff out there.

However, people like to stick with good ol' alert("HAXERRR");

Yeah quite sad, that people do not post such as [XSS OS compromise] ?

It would be A LOT more interesting to hear about, like SE your friend to a phishing site, with malicious intent.

Compromise the host, afterwards migrating the session and then, the fun part starts...

And it's also FUN! Anyways, yeah damn it's scary, cause if you got the knowledge, like a baws haha - well then you can do A LOT of damage...

fobber - April 12, 2012, 11:50 am

(Apr 12, 2012 11:42 AM)Phizo Wrote: [\[CITE\]](#) That's correct, it can indeed lead to a full OS compromise, I have read on it.

Also things like Javascript buffer overflows can be done using XSS, some scary stuff out there.

However, people like to stick with good ol' alert("HAXERRR");

Yeah. It's probably true, that quite some on here, don't know what they could actually do with XSS/javascript.

You even do a window.location to some really sick gay website (sorry if you happen to be gay), and then tell your friends to go on that website. Lol. That's a classic.

Phizo - April 12, 2012, 11:52 am

(Apr 12, 2012 11:50 AM)fobber Wrote: [\[CITE\]](#) Yeah. It's probably true, that quite some on here, don't know what they could actually do with XSS/javascript.

You even do a window.location to some really sick gay website (sorry if you happen to be gay), and then tell your friends to go on that website. Lol. That's a classic.

Fuck you, I'll kill you. I'm gay you know.

Haha, just kidding. Yeah, that's funny to do, but it wouldn't be very appropriate to do it on HF, it's still nothing to be like ZOMG HAAXX!11!! about.

MaXoNe - April 12, 2012, 11:57 am

I once suggested that only top 10 alexa sites , worldwide or per country should be allowed for [xss] post.

Eshta - April 12, 2012, 12:00 pm

I don't mean to insult you but I cant express it in any other form; instead of complaining about this can you please do some tuts about the advance XSS ? if your thread gets attention it will sure improve a lot of members skills

Phizo - April 12, 2012, 12:02 pm

(Apr 12, 2012 12:00 PM)Eshta Wrote: [\[CITE\]](#) I don't mean to insult you but I cant express it in any other form; instead of complaining about this can you please do some tuts about the advance XSS ? if your thread gets attention it will sure improve a lot of members skills

I'm guessing you seen my thread on basic XSS then since you're requesting me to make an advanced one.

Since I was gone there have been advanced tutorials posted, why not check them out?

DaNet - April 12, 2012, 12:02 pm

XSS is an indicator about the website security. Releasing these is useless.

But i'm for the release of XSS when it's a big website.

Eshta - April 12, 2012, 12:04 pm

(Apr 12, 2012 12:02 PM)Phizo Wrote: [\[CITE\]](#) I'm guessing you seen my thread on basic XSS then since you're requesting me to make an advanced one.

Since I was gone there have been advanced tutorials posted, why not check them out?

All the tutorials I have read here are about cookie stealing it from the admin, is that what you mean by "advance" ?

Phizo - April 12, 2012, 12:05 pm

(Apr 12, 2012 12:02 PM)Marlowe Wrote: [\[CITE\]](#) XSS is an indicator about the website security. Releasing these is useless.

But i'm for the release of XSS when it's a big website.

You're mistaken. XSS is not an indicator, it's a vulnerability.

Majority of this section use it as an indicator, that's the whole point of this thread.

(Apr 12, 2012 12:04 PM)Eshta Wrote: [\[CITE\]](#) All the tutorials I have read here are about cookie stealing it from the admin, is that what you mean by "advance" ?

By advanced I was thinking of WAF bypassing.

Anyway, XSS tutorials aren't going to help you get better. Learn HTML and Javascript if you want to get better.

DaNet - April 12, 2012, 12:08 pm

Yes, it's a vulnerability. Thus, instead of posting the XSS, posting the XSS exploited, with a result. Not just a message box. That's will better.

Hycca - April 12, 2012, 12:15 pm

(Apr 12, 2012 11:57 AM)MaXoNe Wrote: [\[CITE\]](#) I once suggested that only top 10 alexa sites , worldwide or per country should be allowed for [xss] post.

Top 10? Then there will be no XSS at all in this section.

Also, I'd rather see XSS than those random defaces which make me mad >.<

MaXoNe - April 12, 2012, 12:17 pm

Web Application Obfuscation book. It has chapters on bypassing XSS filters.

Phizo - April 12, 2012, 1:46 pm

(Apr 12, 2012 12:15 PM)-?Exotz- Wrote: [\[CITE\]](#) Top 10? Then there will be no XSS at all in this section.

Also, I'd rather see XSS than those random defaces which make me mad >.<

My thoughts exactly haha.

fuku35chars

Dyme - April 12, 2012, 1:57 pm

I actually nudged at the same topic on a thread I posted a while back. What happen? I got flammed. I'm glad that your making more progress.

<https://hackforums.net/showthread.php?tid=2159440>

Sasori - April 12, 2012, 2:29 pm

I can understand what you're saying and I do agree.

Another thing that pisses me off is things like this:

<https://hackforums.net/showthread.php?tid=2395496>

Prominent - April 12, 2012, 2:47 pm

Couldn't have said it better myself, I dislike the amount of lame XSS threads I see daily.. I hope this thread gets some attention.

Phizo - April 12, 2012, 8:01 pm

(Apr 12, 2012 02:29 PM)Sasori Wrote: [\[CITE\]](#) I can understand what you're saying and I do agree. Another thing that pisses me off is things like this:

<https://hackforums.net/showthread.php?tid=2395496>

Oh god, Havij is what I hate the most out of anything else that I can think of.

(Apr 12, 2012 02:47 PM)Prominent Wrote: [\[CITE\]](#) Couldn't have said it better myself, I dislike the amount of lame XSS threads I see daily.. I hope this thread gets some attention.

Yeah, me too.

A lot of users have been telling me to try make a difference and "show them what real hacking is" -- quoted from a few users.

I'm just trying to make a few changes to improve quality in threads, as well as their actual skills in XSS.

Curator - April 12, 2012, 9:33 pm

There's little point in posting a reflective XSS on any site unless it's a really major one, like Google, Youtube, Paypal, Facebook, etc.

However, a persistent XSS on just about any site can be very powerful, so I don't think there's a problem in posting those and using an alert as an example if you find one.

Phizo - April 12, 2012, 9:42 pm

(Apr 12, 2012 09:33 PM)Curator Wrote: [\[CITE\]](#) There's little point in posting a reflective XSS on any

site unless it's a really major one, like Google, Youtube, Paypal, Facebook, etc.

However, a persistent XSS on just about any site can be very powerful, so I don't think there's a problem in posting those and using an alert as an example if you find one.

There is a problem.

That's all they know how to do, they don't know anything other than how to alert.

Persistent XSS on a random site? Self-explanatory.

Nipples.

JoinSeventh - April 13, 2012, 7:22 am

Here is my thoughts on the subject:

XSS is a powerfull vulnerability if you know your shit, but most of these guys doesn't.

It would be like if I run a Nessus scan on a random website and posted shit like "OMG LOOK THE SSL IS OLD AND INSECURE".

Pointless? Yes. Illogical? Yes. The same this that is happening? Yes.

I'm not saying that posting making posts about your XSS finds is bad, but:

Why not try to actually exploit them before publish?

I mean if I would find a SQL Injection vulnerability in some company website, I would actually tro the exploit it first.

Not because I necessarily want to dump the DB or own the box, but to show Proof of Concept.

Just my thoughts, hate all you want.

Phizo - April 13, 2012, 7:24 am

(Apr 13, 2012 07:22 AM)JoinSeventh Wrote: [\[CITE\]](#) Here is my thoughts on the subject:

XSS is a powerfull vulnerability if you know your shit, but most of these guys doesn't.

It would be like if I run a Nessus scan on a random website and posted shit like "OMG LOOK THE SSL IS OLD AND INSECURE".

Pointless? Yes. Illogical? Yes. The same this that is happening? Yes.

I'm not saying that posting making posts about your XSS finds is bad, but:

Why not try to actually exploit them before publish?

I mean if I would find a SQL Injection vulnerability in some company website, I would actually tro the exploit it first.

Not because I necessarily want to dump the DB or own the box, but to show Proof of Concept.

Just my thoughts, hate all you want.

Putting this in the original post if that's okay with you. That's a good post.

Exactly what I'm trying to get at. There's nothing wrong with doing it, but at least try and gain access.

JoinSeventh - April 13, 2012, 7:27 am

(Apr 13, 2012 07:24 AM)Phizo Wrote: [\[CITE\]](#) Putting this in the original post if that's okay with you. That's a good post.

Exactly what I'm trying to get at. There's nothing wrong with doing it, but at least try and gain

access.

No problem.

Glad to see people agree with me.

Hycca - April 13, 2012, 7:31 am

If you're reporting a vulnerability, you're hoping for a reward, a company WON'T give you a reward if you're gonna actually perform an attack that could harm the site in any way, that's why I'm doing ONLY alert boxes and I report my finds right away.

JoinSeventh - April 13, 2012, 7:37 am

(Apr 13, 2012 07:31 AM)-?Exotz- Wrote: [\[CITE\]](#) If you're reporting a vulnerability, you're hoping for a reward, a company WON'T give you a reward if you're gonna actually perform an attack that could harm the site in any way, that's why I'm doing ONLY alert boxes and I report my finds right away.

Sure, I get that.

But let's face it, most if the XSS posted in here is never reported and if they are the websites admin doesn't care about it.

Phizo - April 13, 2012, 7:39 am

(Apr 13, 2012 07:37 AM)JoinSeventh Wrote: [\[CITE\]](#) Sure, I get that.

But let's face it, most if the XSS posted in here is never reported and if they are the websites admin doesn't care about it.

That and the fact majority of HF don't know how to do anything other than display an alert box.

Razor4x 5_0 - April 13, 2012, 7:54 am

(Apr 13, 2012 07:39 AM)Phizo Wrote: [\[CITE\]](#) That and the fact majority of HF don't know how to do anything other than display an alert box.

thats right but most of the site is quite losted by the administrators and are useless and they post it here so the think that are 1337 h4x0rs

HaxOr? - April 13, 2012, 8:03 am

Why are pepole always talk about me? :P

Yea i agree!

If it isn't on some big site it's garbage.

DaNet - April 13, 2012, 8:18 am

I give an example from me : <https://hackforums.net/showthread.php?tid=1775089>

It's a big XSS release, only big french websites (medias, aerian company, television channel and more ...). I reported all these XSS. Now, verify XSS. The 3/4 of these stay activated !

Reporting to webmaster, it's ... a bullshit, totally useless. In most of cases, Webmasters don't know how to fixing the vulnerability. Or they think XSS is totally useless, so they don't give response.

A grammatic question, "Webmaster don't know how to fixing the vulnerability" It's fixing, or fix ?
Raah, french is more easy Lulzcat has his place here.

Cordially

Phizo - April 13, 2012, 8:44 am

(Apr 13, 2012 08:03 AM)?? ? x O r ? Wrote: [\[CITE\]](#) Why are pepole always talk about me? :P

Yea i agree!

If it isn't on some big site it's garbage.

Yeah, it's just a waste. Who cares about sites you find by using vulnerability scanners ?