Lazy Admin

Working Theory

Enumeration

Tools

nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-23 01:45 +08
Nmap scan report for 10.10.195.85
Host is up (0.22s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
|   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
|_  256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
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 32.42 seconds
```

ffuf

```
 :: Method           : GET
 :: URL              : http://10.10.195.85/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10]
content                 [Status: 301, Size: 314, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10]
```

--found sweetrice cms

```
:: Method           : GET
 :: URL              : http://10.10.195.85/content/FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10]
_themes                 [Status: 301, Size: 322, Words: 20, Lines: 10]
as                      [Status: 301, Size: 317, Words: 20, Lines: 10]
attachment              [Status: 301, Size: 325, Words: 20, Lines: 10]
images                  [Status: 301, Size: 321, Words: 20, Lines: 10]
inc                     [Status: 301, Size: 318, Words: 20, Lines: 10]
js                      [Status: 301, Size: 317, Words: 20, Lines: 10]
:: Progress: [20469/20469] :: 172 req/sec :: Duration: [0:01:59] :: Errors: 0 ::
```

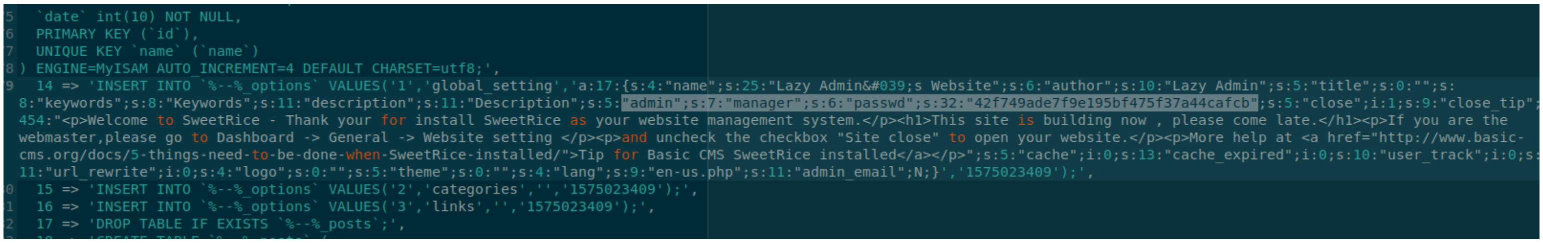
-/as is a login page
-http://10.10.195.85/content/inc/lastest.txt shows SweetRice CMS 1.5.1 version

found interesting file in /content/inc/mysql_backup/ => mysql backup.sql

Targets

mysql backup file

found /as login credential



```
  `date` int(10) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `name` (`name`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;',
  14 => 'INSERT INTO `%--%_options` VALUES('1','global_setting','a:17:{s:4:"name";s:25:"Lazy Admin&#039;s Website";s:6:"author";s:10:"Lazy Admin";s:5:"title";s:0:"";s:
8:"keywords";s:8:"Keywords";s:11:"description";s:11:"Description";s:5:"admin";s:7:"manager";s:6:"passwd";s:32:"42f749ade7f9e195bf475f37a44cafcb";s:5:"close";i:1;s:9:"close_tip";
454:"<p>Welcome to SweetRice - Thank your for install SweetRice as your website management system.</p><h1>This site is building now , please come late.</h1><p>If you are the
webmaster,please go to Dashboard -> General -> Website setting </p><p>and uncheck the checkbox "Site close" to open your website.</p><p>More help at <a href="http://www.basic-
cms.org/docs/5-things-need-to-be-done-when-SweetRice-installed/">Tip for Basic CMS SweetRice installed</a></p>";s:5:"cache";i:0;s:13:"cache_expired";i:0;s:10:"user_track";i:0;s:
11:"url_rewrite";i:0;s:4:"logo";s:0:"";s:5:"theme";s:0:"";s:4:"lang";s:9:"en-us.php";s:11:"admin_email";N;}','1575023409');',
  15 => 'INSERT INTO `%--%_options` VALUES('2','categories','','1575023409');',
  16 => 'INSERT INTO `%--%_options` VALUES('3','links','','1575023409');',
  17 => 'DROP TABLE IF EXISTS `%--%_posts`;',
```

-it's a md5 hash
manager: Password123

Post Exploitation

Privilege Escalation

-www-data have sudo privilege for a perl script in /home/itguy that execute /etc/copy.sh script
-edit copy.sh script with reverse shell script to return root shell

Creds

SweetRice CMS credential
================
manager: Password123

Flags

Write-up Images