

# Write Up Kediri Cyber Security Competition 2024



Nama Tim - Asal Sekolah

Nama Peserta 1

Nama Peserta 2

# Daftar Isi

---

|                                                   |   |
|---------------------------------------------------|---|
| [Kategori Soal - Web ].....                       | 2 |
| Judul Soal.....                                   | 2 |
| Flag: a774409a00c21de377cf8ed5c6a56b8547973042 .. | 3 |
| Fotorec #2.....                                   | 4 |
| [Kategori Soal - Crypto].....                     | 6 |
| Fallout #1.....                                   | 6 |
| Flag: c00b8fcc8e12a2543e7c2b1ecbf2661bc668d243 .. | 8 |

# [Web]

## Encode

Screenshoot Soal

Challenge

×

Fotorec #1

100

Sebutkan Flag Nomor 1

Flag

Submit

## Solution

- Penjelasan proses analisa
- Penjelasan proses eksploitasi

Scan semua port menggunakan nmap

```
+ ~ nmap -sV -A 103.183.92.191
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 14:49 WIB
Nmap scan report for 103.183.92.191
Host is up (0.039s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0      0      103 Oct 15 02:12 pesan.txt
| ftp-syst:
| STAT:
| FTP server status:
|   Connected to ::ffff:103.144.15.113
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 6
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
```

ternyata dari hasil scan tersebut, ftp bisa menggunakan user anonymous dan password untuk

anonymous adalah "anonymous".

```
+ ~ ftp 103.183.92.191
Connected to 103.183.92.191.
220 (vsFTPd 3.0.3)
Name (103.183.92.191:roxasz): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||59051|)
150 Here comes the directory listing.
-rw-r--r--  1 0      0      103 Oct 15 02:12 pesan.txt
226 Directory send OK.
ftp> get pesan.txt
local: pesan.txt remote: pesan.txt
229 Entering Extended Passive Mode (|||12019|)
150 Opening BINARY mode data connection for pesan.txt (103 bytes).
100% |*****| 103      304.80 KiB/s      00:00 ETA
226 Transfer complete.
103 bytes received in 00:00 (3.30 KiB/s)
ftp> ^D
221 Goodbye.
```

setelah itu, ternyata terdapat file bernama pesan.txt, dan ternyata isi file tersebut flagnya, menggunakan command get untuk transfer file dari ftp server ke local.

ref : [wikipedia](#)

```
→ ~ cat pesan.txt

Selamat datang di Fotorec System. Berikut pesan anda :
Flag1{a774409a00c21de377cf8ed5c6a56b8547973042}
```

Flag: a774409a00c21de377cf8ed5c6a56b8547973042

# [Reverse]

## Judul Soal

### Screenshot

Challenge ×

## Fallout #1

150

Sebutkan Flag Nomor 1

Flag

Submit

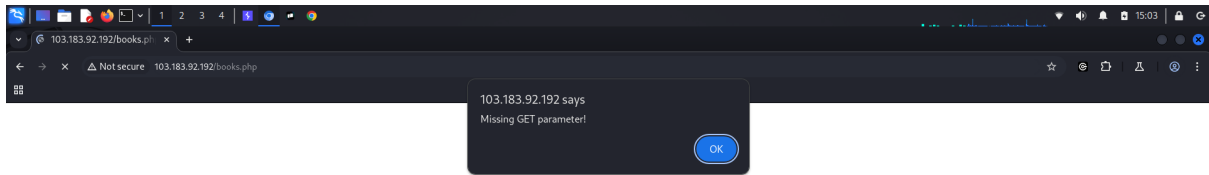
## Solution

- Penjelasan proses analisa
- Penjelasan proses exploits

menggunakan dirsearch untuk mendapatkan url yang tidak muncul di halaman page.

```
+ ~ dirsearch -u http://103.183.92.192/
[15:01:31] 403 - 221B - /.htaccessOLD
[15:01:31] 403 - 221B - /.htaccessBAK
[15:01:31] 403 - 213B - /.htm
[15:01:32] 403 - 222B - /.htaccessOLD2
[15:01:32] 403 - 214B - /.html
[15:01:32] 403 - 220B - /.httr-oauth
[15:01:32] 403 - 223B - /.htpasswd_test
[15:01:32] 403 - 219B - /.htpasswd
[15:01:33] 403 - 218B - /.user.ini
[15:01:34] 403 - 221B - /accounts.cgi
[15:01:34] 403 - 220B - /accounts.pl
[15:01:34] 403 - 216B - /adm.cgi
[15:01:34] 403 - 215B - /adm.pl
[15:01:34] 301 - 236B - /admin -> http://103.183.92.192/admin/
[15:01:35] 403 - 218B - /admin.cgi
[15:01:35] 403 - 217B - /admin.pl
[15:01:35] 302 - 0B - /admin/ -> http://103.183.92.192/admin/login.php
[15:01:35] 200 - 4KB - /admin/login.php
[15:01:35] 302 - 0B - /admin/index.php -> http://103.183.92.192/admin/login.php
[15:01:38] 403 - 218B - /apply.cgi
[15:01:38] 301 - 237B - /assets -> http://103.183.92.192/assets/
[15:01:38] 200 - 2KB - /assets/
[15:01:38] 403 - 221B - /AT-admin.cgi
[15:01:38] 403 - 217B - /auth.cgi
[15:01:38] 403 - 216B - /auth.pl
[15:01:38] 403 - 219B - /awstats.pl
[15:01:39] 200 - 80B - /books.php
[15:01:39] 403 - 221B - /cachemgr.cgi
[15:01:39] 403 - 217B - /cgi-bin/
[15:01:39] 403 - 216B - /cgi.pl/
```

terlihat disana ternyata ada books.php



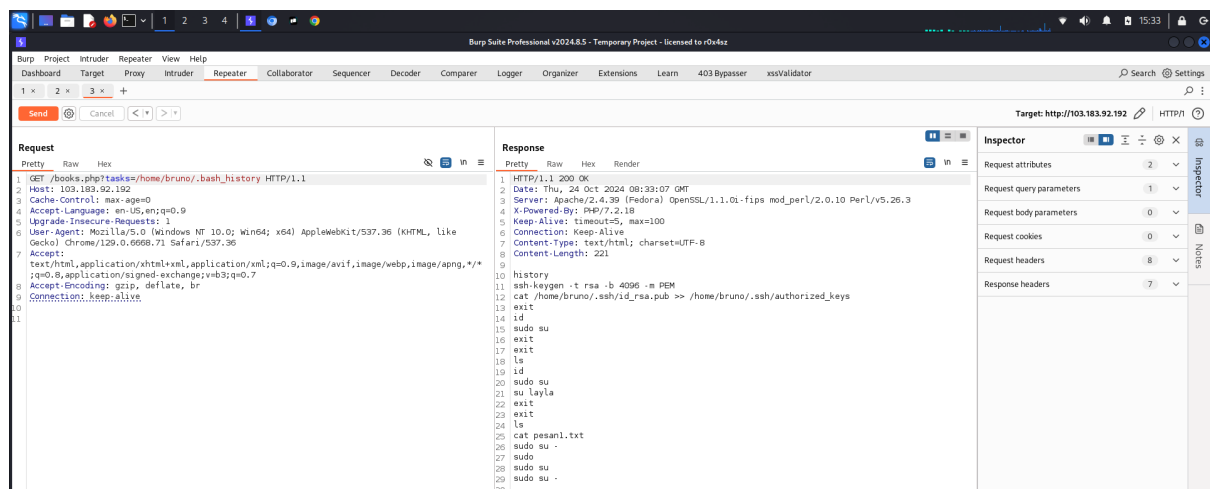
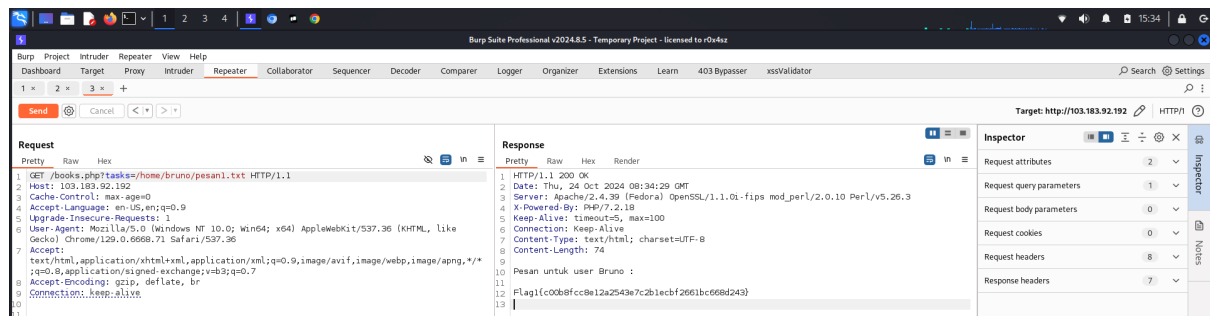
ternyata butuh param, mari kita brute paramnya apa aja yang dipakai menggunakan ffuf



ternyata dari fuzzing tersebut kita dapatkan param tasks langsung saja kita dapatkan /etc/passwdnya.



karena sama seperti vulnhub jadi tinggal ke dir /home/bruno/.bash\_history untuk melihat apa aja sih yang user bruno lakukan, lalu ternyata



flag ada di /home/bruno/pesan1.txt

Flag: KCSC{text}

# Terimakasih