

# COMMAND INJECTION

# OS COMMAND INJECTION

OS command 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, and typically fully compromise the application and all its data.



1

Attacker found website  
Is vulnerable to command  
injection he can find  
find which OS running  
On remote and can inject  
OS level commands



2

Command is passed either  
in url or vulnerable input  
field and the commands get  
executed on the server

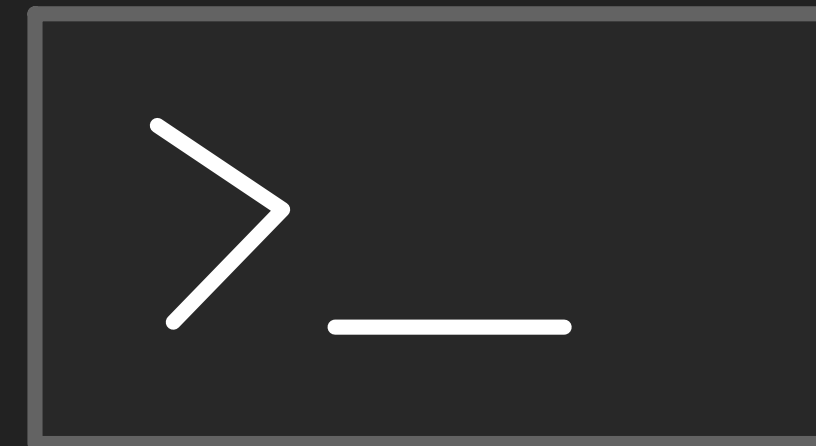


3

On successful command execution  
attacker gets a full control  
one can access the entire  
server and can manipulate data  
and many more things.



# LINUX COMMANDS



OPEN YOUR TERMINAL

**LINUX BOOTCAMP**

**ls**

Lists the files in the current directory

USAGE

`ls -t`

sorts according to last modified time

`ls -l`

lists files with all the details

`ls -1`

displays list one per line

#Linux #ClickAndRun #Ubuntu

Linux Commands and their usage | Linux BootCamp | Open Source Starter Pack

1,111 views · Streamed live on 15-Jan-2021

93 DISLIKE SHARE SAVE ...

GNU/Linux Users' Group, NIT Durgapur  
1.22K subscribers

SUBSCRIBED

Hello Everyone!



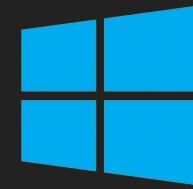
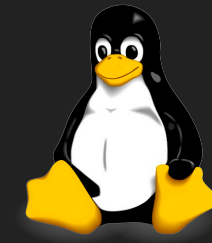
^^

CHECKOUT

# DIFFERENT WAYS OF INJECTION

## > COMMAND SEPARATORS

1. &
2. &&
3. |
4. ||



1. ;
2. \n



# PRACTICE



For further reading:

<https://portswigger.net/web-security/os-command-injection>

**THANK YOU**