

## What is Command Injection?

- Command injection is a type of vulnerability that allows an attacker to execute arbitrary commands on the host operating system via a vulnerable application.
- This can occur when an application passes unsafe user supplied data (e.g. form input) to a system shell without proper validation or sanitization.
- An attacker can use command injection to gain unauthorised access to sensitive data, execute malicious code or disrupt the intended functionality of the application.

## How to detect command injection ?

- One way to detect command injection vulnerabilities in a web application is to search the source code for keywords that may indicate the use of system commands with unsanitized user input
- Some keywords to look for include:
  - “Whois”, “dir”, “ls”, “cp”, “cat”, “type”
  - “System”, “etc”, “exec”, “shell\_exec”
  - “Whoami”

## SOC168 - Whoami Command Detected in Request Body

Here is the generated alert,

^ High Feb, 28, 2022, 04:12 AM SOC168 - Whoami Command Detected in Request Body	
EventID :	118
Event Time :	Feb, 28, 2022, 04:12 AM
Rule :	SOC168 - Whoami Command Detected in Request Body
Level :	Security Analyst
Hostname :	WebServer1004
Destination IP Address :	172.16.17.16
Source IP Address :	61.177.172.87
HTTP Request Method :	POST
Requested URL :	https://172.16.17.16/video/
User-Agent :	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Alert Trigger Reason :	Request Body Contains whoami string
Device Action :	Allowed
Show Hint	🔍

- Source IP address (61.177.172.87) attempted “Whoami” command injection attack on Web server 1004 (172.16.17.16).
- Request URL : https://172.16.17.16/video/

Let's check about Source IP address:



3

/ 87

?

X Community Score ✓

⚠ 3 security vendors flagged this IP address as malicious

61.177.172.87 (61.177.128.0/17)  
AS 4134 (Chinanet)

CN

SUMMARY DETECTION DETAILS RELATIONS COMMUNITY 10+

#### Security Vendors' Analysis

Antiy-AVL	⚠ Malicious
Certego	⚠ Malicious
CMC Threat Intelligence	⚠ Malware

This IP address was flagged as malicious. Also attackers make lots of attacks by using this IP address.

**61.177.172.87** was found in our database!

This IP was reported **79,262** times. Confidence of Abuse is **100%**: ?

100%






ISP	ChinaNet Jiangsu Province Network
Usage Type	Data Center/Web Hosting/Transit
Domain Name	chinatelecom.com.cn
Country	China
City	Lianyungang, Jiangsu

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).  
Updated monthly.

REPORT 61.177.172.87

WHOIS 61.177.172.87

Lets, look into the Log Management

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 28, 2022, 04:12 AM	Firewall	61.177.172.87	49821	172.16.17.16	443	
Feb, 28, 2022, 04:11 AM	Firewall	61.177.172.87	49822	172.16.17.16	443	
Feb, 28, 2022, 04:13 AM	Firewall	61.177.172.87	49222	172.16.17.16	443	
Feb, 28, 2022, 04:14 AM	Firewall	61.177.172.87	48822	172.16.17.16	443	
Feb, 28, 2022, 04:15 AM	Firewall	61.177.172.87	46822	172.16.17.16	443	

- There are several command injection were made by this attacker(61.177.172.87).
- All attempts are responded with 200 HTTP Status with different HTTP response sizes.
- We are able to see that all the command injections made by the attacker were executed. By checking the command line History on web server 1004

28.02.2022 04:11 ls

28.02.2022 04:12 whoami

28.02.2022 04:13 uname

28.02.2022 04:14 cat /etc/passwd

28.02.2022 04:17 cat /etc/shadow

## Playbook Answers:

^	High	Feb, 28, 2022, 04:12 AM	SOC168 - Whoami Command Detected in Request Body
EventID :	118		
Event Time :	Feb, 28, 2022, 04:12 AM		
Rule :	SOC168 - Whoami Command Detected in Request Body		
Answer :	True Positive (+5 Point)		
Playbook Answers :	Do You Need Tier 2 Escalation? (+5 Point)		
	Was the Attack Successful? (+5 Point)		
	What Is the Direction of Traffic? (+5 Point)		
	Check If It Is a Planned Test (+5 Point)		
	What Is The Attack Type? (+5 Point)		
	Is Traffic Malicious? (+5 Point)		

- Yes, we need Tier 2 Escalation
- The Attack was successful
- The Direction of Traffic : Internet to company network
- NO, this is not a Planned Test
- This is Command injection attack
- It is a Malicious Traffic