



# Command injection

BY UNCLE RAT

# Agenda

- ▶ What is Command injection?
  - ▶ How it works?
- ▶ Attack strategy
  - ▶ Separators
  - ▶ Commands
  - ▶ Fuzzing list
  - ▶ Blind command injection



What is Command  
injection?

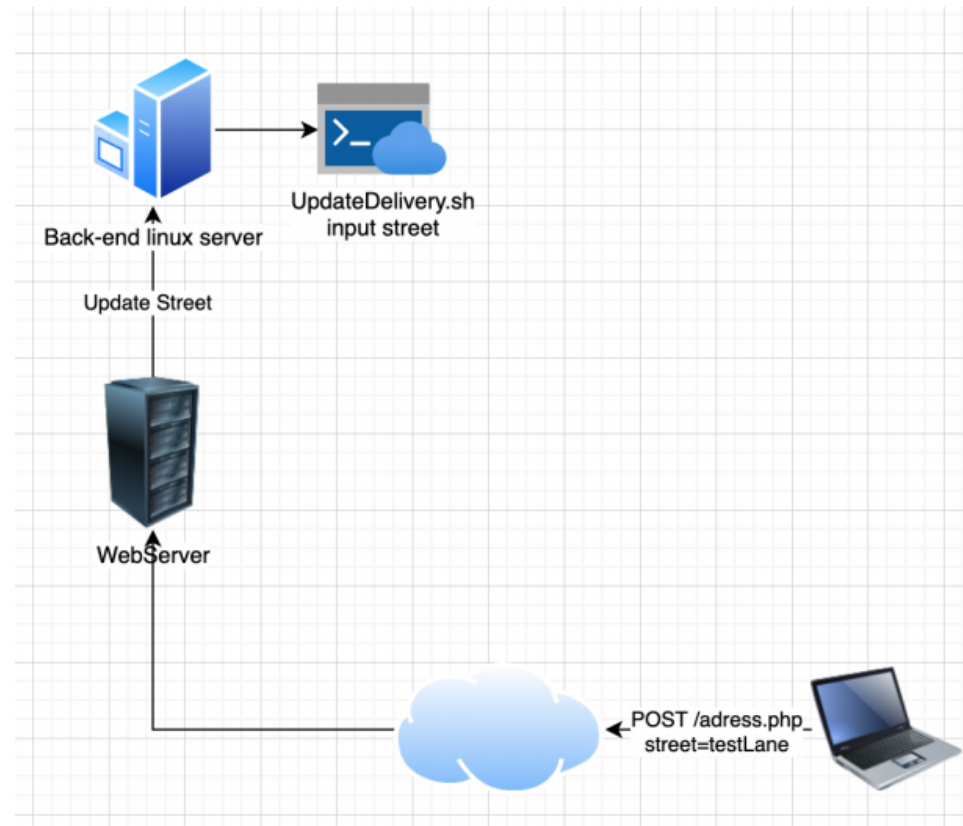


# What is Command injection?

- ▶ Can happen when unsanitised user input get passed to shell script
- ▶ User can insert command seperator and command to execute
  - ▶ User can often pivot using trust relationships
- ▶ Sounds very simple, Is anything but simple
- ▶ Often manifests as blind command injection



# How it works



# Attack strategy



# Attack strategy

- ▶ We have to fuzz every parameters we find
- ▶ Fuzzing list should consist of combination of
  - ▶ Command seperators
  - ▶ Windows/Linux commands
    - ▶ Target dependant
- ▶ Test for blind OS command injection with `ping -c 10 127.0.0.1`
  - ▶ Will cause delay



# Separators

- ▶ Multi platform Examples:

- ▶ &
- ▶ &&
- ▶ |
- ▶ ||

- ▶ Unix Based systems:

- ▶ ;
- ▶ Newline ( 0x0a or \n )

- ▶ Backticks

- ▶ ``injected command``

- ▶ `$(injected command)`





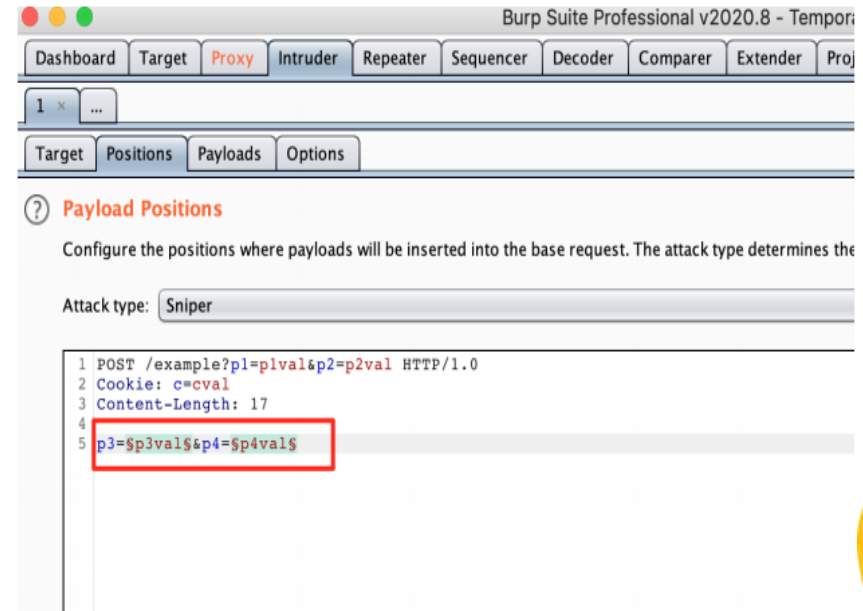
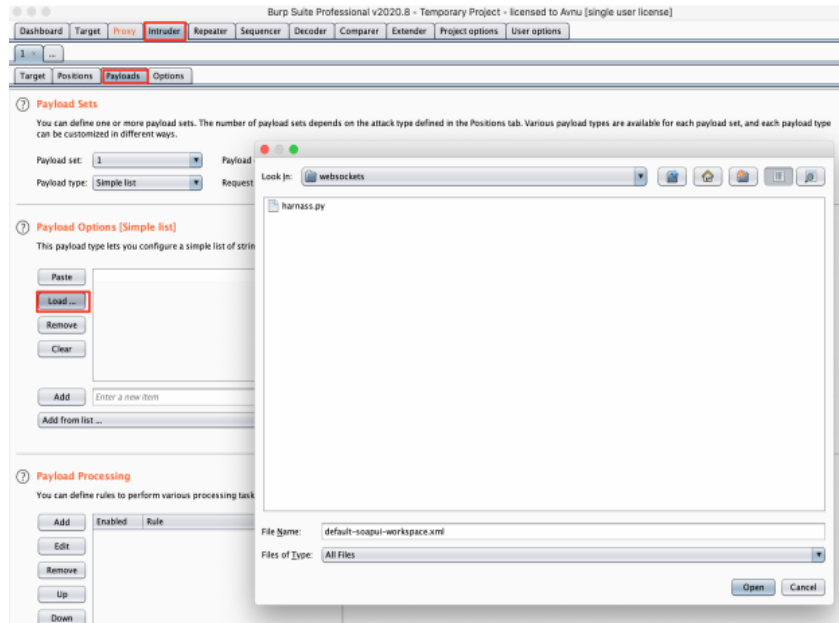
# Commands

<u>Aa</u> Purpose of command	☰ Linux	☰ Windows
<u>Name of current user</u>	<code>whoami</code>	<code>whoami</code>
<u>Operating system</u>	<code>uname -a</code>	<code>ver</code>
<u>Network configuration</u>	<code>ifconfig</code>	<code>ipconfig /all</code>
<u>Network connections</u>	<code>netstat -an</code>	<code>netstat -an</code>
<u>Running processes</u>	<code>ps -ef</code>	<code>tasklist</code>



# Fuzzing List

## ► Utilizing Burp intruder



# Blind Command Injection

- ▶ Testing

```
& ping -c 10 127.0.0.1 &
```

- ▶ False positives

