Command injection

BY UNCLE RAT

Agenda

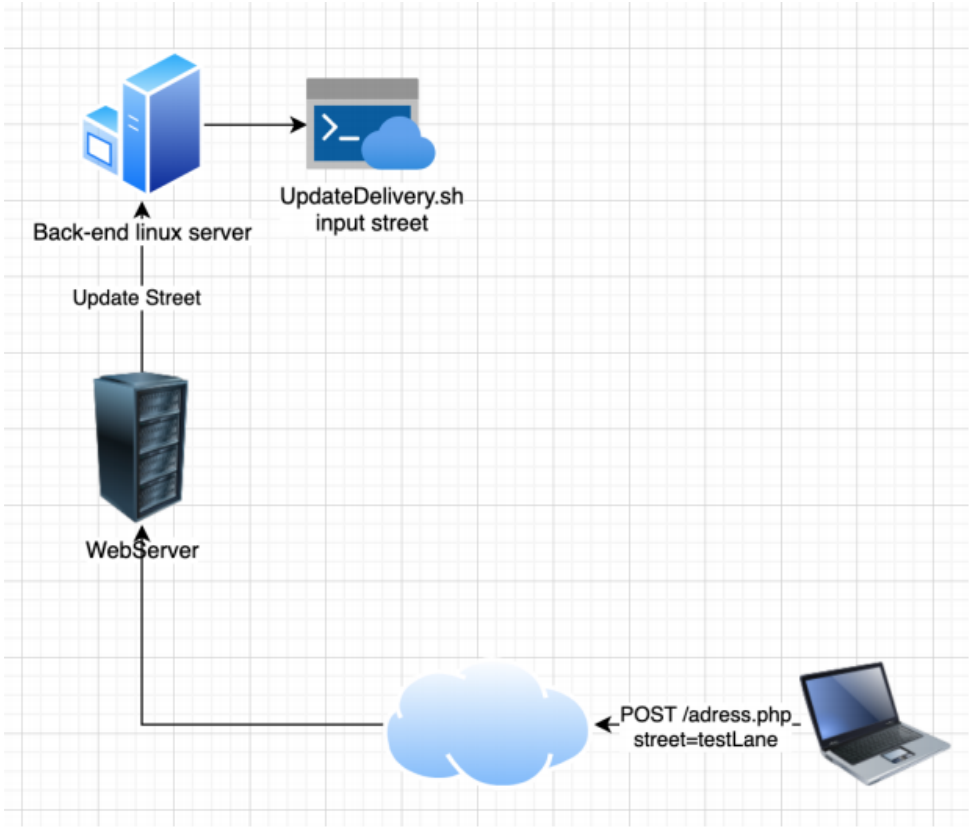
- What is Command injection?
  - How it works?
- Attack strategy
  - Separators
  - Commands
  - Fuzzing list
  - Blind command injection

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

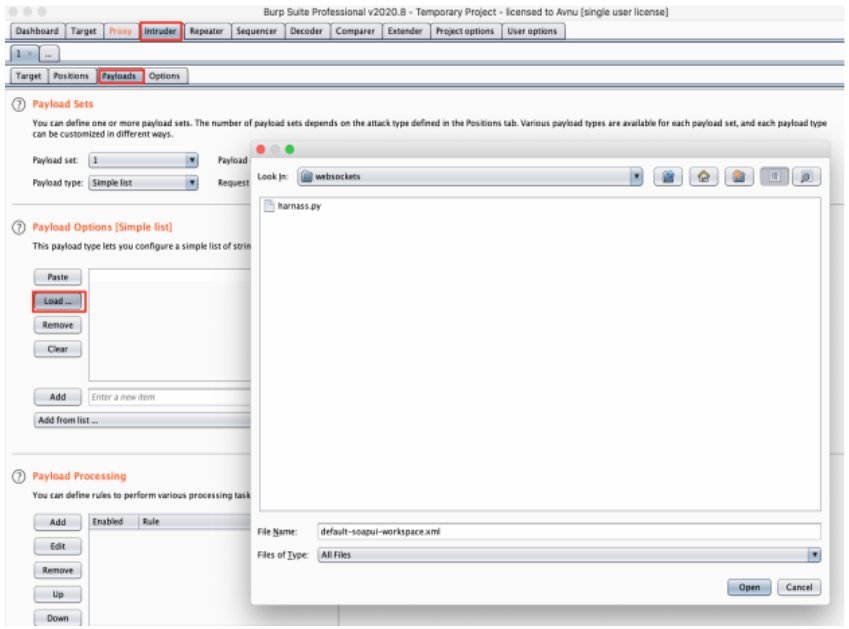
- Multi platform Examples:
  - &
  - &&
  - |
  - | |
- Unix Based systems:
  - ;
  - Newline (0x0a or \n)
- Backticks
- `` `injected command` ``
- $(*injected command*)

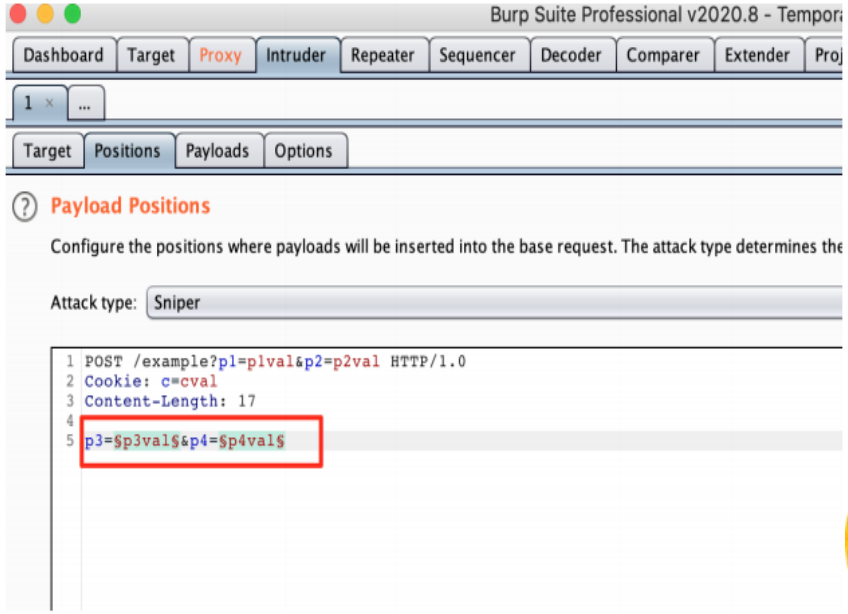
Commands

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

Fuzzing List

- Utilizing Burp intruder





Blind Command Injection

- Testing

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

- False positives