SPLOIT Vulnerabilities

1. Command injection vulnerability

- In our code we are not blacklisting back quote (`) and thus this can be exploited to perform remote command execution with the compromised application’s privilege

2. Buffer Overflow (1)

- The w command returns the list of logged in users.
- There is no check if the list of users exceed the buffer.
- So an exploit will be logging in on separate machines with different usernames to overflow the buffer.

3. Buffer overflow (2)

- When the user inputs an unknown command the server sends back an error message which includes the command itself.
- So the user can overflow the buffer with required value along with the command he sends.

4. Format string

- If the user sends an unknown command, an error message is displayed along with the command which was entered.

5. Our choice

- We are executing alias commands using popen. But the commands are not using absolute paths.
- Since the user can inject commands, they can change the path variable for commands to anything they want.