# Other Injection Attacks

Command Injection



# Command Injection

- Execute the `ls` command in DVWA command injection (with Security Level: High)
- If you don’t have DVWA locally you can use the online lab:




# Command Injection - Solution

- If you look at the source code, there are '|' and '||' in blacklists, but the '|' comes first and has a higher priority in $substitutions array. If we input this:
  - 4.4.4.4 || ls
- The first '|' is removed and the second '|' remains and other items in blacklist won't match '|' anymore :)
- Try it!



# ZDResearch Advanced Web Hacking

## ZDResearch

www.zdresearch.com