

Vulnerability: Command Injection

localhost / 127.0.0.1 / dvwa | php | x | +

← → ↻ ⓘ 127.0.0.1/dvwa/vulnerabilities/exec/#

Gmail YouTube Maps

DVWA

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

VMware-player-ful...exe

Show all

Type here to search

29°C

10:22

28-09-2022

Vulnerability: Command Injection x localhost / 127.0.0.1 / dvwa | php x +

127.0.0.1/dvwa/vulnerabilities/exec/#

Gmail YouTube Maps

[Home](#)[Instructions](#)[Setup / Reset DB](#)
[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:80	HP-280-G2:61588	TIME_WAIT
TCP	127.0.0.1:80	HP-280-G2:61602	TIME_WAIT
TCP	127.0.0.1:80	HP-280-G2:61610	ESTABLISHED
TCP	127.0.0.1:80	HP-280-G2:61611	ESTABLISHED
TCP	127.0.0.1:3306	HP-280-G2:61612	ESTABLISHED
TCP	127.0.0.1:3306	HP-280-G2:61613	ESTABLISHED
TCP	127.0.0.1:61603	HP-280-G2:http	TIME_WAIT
TCP	127.0.0.1:61604	HP-280-G2:3306	TIME_WAIT
TCP	127.0.0.1:61605	HP-280-G2:3306	TIME_WAIT
TCP	127.0.0.1:61610	HP-280-G2:http	ESTABLISHED
TCP	127.0.0.1:61611	HP-280-G2:http	ESTABLISHED
TCP	127.0.0.1:61612	HP-280-G2:3306	ESTABLISHED
TCP	127.0.0.1:61613	HP-280-G2:3306	ESTABLISHED
TCP	192.168.8.239:60765	20.198.119.84:https	ESTABLISHED
TCP	192.168.8.239:61232	a23-49-50-49:https	CLOSE_WAIT
TCP	192.168.8.239:61242	a23-49-50-49:https	CLOSE_WAIT
TCP	192.168.8.239:61302	a23-54-83-26:https	CLOSE_WAIT
TCP	192.168.8.239:61303	a-0001:https	CLOSE_WAIT
TCP	192.168.8.239:61304	a23-49-50-49:https	CLOSE_WAIT
TCP	192.168.8.239:61305	static-50:https	CLOSE_WAIT

VMware-player-ful...exe

Type here to search

29°C

10:24 28-09-2022

Vulnerability: Command Injection x localhost / 127.0.0.1 / dvwa | php x +

127.0.0.1/dvwa/vulnerabilities/exec/#

Gmail YouTube Maps

[Home](#)[Instructions](#)[Setup / Reset DB](#)
[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Tracing route to HP-280-G2 [127.0.0.1]
over a maximum of 30 hops:
0 HP-280-G2 [127.0.0.1]
1 HP-280-G2 [127.0.0.1]

Computing statistics for 25 seconds...

Hop	RTT	Source to Here	This Node/Link	Address
0				HP-280-G2 [127.0.0.1]
1	0ms	0/ 100 = 0%	0/ 100 = 0%	HP-280-G2 [127.0.0.1]

Trace complete.

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

VMware-player-ful...exe

Type here to search

28°C

10:45 28-09-2022

Vulnerability: Command Injection xlocalhost / 127.0.0.1 / dvwa | php x+127.0.0.1/dvwa/vulnerabilities/exec/#GmailYouTubeMaps

DVWA

HomeInstructionsSetup / Reset DBBrute ForceCommand InjectionCSRFFile InclusionFile UploadInsecure CAPTCHASQL InjectionSQL Injection (Blind)Weak Session IDsXSS (DOM)XSS (Reflected)XSS (Stored)CSP BypassJavaScript

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Tracing route to HP-280-G2 [127.0.0.1]
over a maximum of 30 hops:

```
1    <1 ms    <1 ms    <1 ms    HP-280-G2 [127.0.0.1]
```

Trace complete.

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

VMware-player-ful...exeShow all xType here to search28°CENG10:4628-09-2022

Vulnerability: Command Injection

localhost / 127.0.0.1 / dvwa | php | x

127.0.0.1/dvwa/vulnerabilities/exec/#

Gmail YouTube Maps

DVWA

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Pinging 127.0.0.1 with 32 bytes of data:
 Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
 Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
 Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
 Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
 Volume in drive C has no label.
 Volume Serial Number is F036-BF39

Directory of C:\xampp\htdocs\dvwa\vulnerabilities\exec

28-09-2022 09:37

28-09-2022 09:37

28-09-2022 09:37

help

VMware-player-ful...exe

Show all

Type here to search

28°C

ENG

10:47

28-09-2022

Vulnerability: Command Injection x localhost / 127.0.0.1 / dvwa | php x +

127.0.0.1/dvwa/vulnerabilities/exec/#

Gmail YouTube Maps

[Home](#)[Instructions](#)[Setup / Reset DB](#)
[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Tracing route to HP-280-G2 [127.0.0.1]
over a maximum of 30 hops:

```
  1    <1 ms    <1 ms    <1 ms  HP-280-G2 [127.0.0.1]
```

Trace complete.

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

Rectangular Snip

VMware-player-ful...exe

Type here to search

28°C 10:50 28-09-2022

Vulnerability: Command Injection x localhost / 127.0.0.1 / dvwa | php x +

127.0.0.1/dvwa/vulnerabilities/exec/#

Gmail YouTube Maps

[Home](#)[Instructions](#)[Setup / Reset DB](#)
[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Tracing route to HP-280-G2 [127.0.0.1]
over a maximum of 30 hops:

```
  0  HP-280-G2 [127.0.0.1]
  1  HP-280-G2 [127.0.0.1]
```

Computing statistics for 25 seconds...

Hop	RTT	Source to Here	This Node/Link	Address
0				HP-280-G2 [127.0.0.1]
1	0ms	0/ 100 = 0%	0/ 100 = 0%	HP-280-G2 [127.0.0.1]

Trace complete.

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

Rectangular Snip

VMware-player-ful...exe

Type here to search

28°C 10:51 28-09-2022

High security

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The left sidebar contains a menu with options: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, and JavaScript. The main content area is titled "Vulnerability: Command Injection". It features a text input field containing "127.0.0.1&dir" and a "Submit" button. Below the input field, the output of the command execution is displayed in a monospaced font, showing a directory listing of the file system. The output includes the path "C:\xampp\htdocs\dwva\vulnerabilities\exec" and lists files and directories with their sizes and permissions.

127.0.0.1&dir

Submit

C has no label.
number is F036-BF39
xampp\htdocs\dwva\vulnerabilities\exec

09:37
2022 09:37

help
16-09-2022 01:10 1,839 index.php
28-09-2022 09:37

source
1 File(s) 1,839 bytes
4 Dir(s) 175,960,072,192 bytes free

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The left sidebar contains a menu with options: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection (highlighted), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, and JavaScript. The main content area is titled "Vulnerability: Command Injection". It features a text input field containing "127.0.0.1netstat" and a "Submit" button. Below the input field, the output of the command execution is displayed in a monospaced font, showing a list of active network connections. The output is organized into columns: Proto, Local Address, Foreign Address, and State.

127.0.0.1netstat

Submit

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:80	HP-280-G2:61808	TIME_WAIT
TCP	127.0.0.1:80	HP-280-G2:61812	TIME_WAIT
TCP	127.0.0.1:80	HP-280-G2:61817	TIME_WAIT
TCP	127.0.0.1:80	HP-280-G2:61832	ESTABLISHED
TCP	127.0.0.1:80	HP-280-G2:61833	ESTABLISHED
TCP	127.0.0.1:3306	HP-280-G2:61834	ESTABLISHED
TCP	127.0.0.1:3306	HP-280-G2:61835	ESTABLISHED
TCP	127.0.0.1:61800	HP-280-G2:http	TIME_WAIT
TCP	127.0.0.1:61801	HP-280-G2:http	TIME_WAIT
TCP	127.0.0.1:61802	HP-280-G2:http	TIME_WAIT
TCP	127.0.0.1:61803	HP-280-G2:http	TIME_WAIT
TCP	127.0.0.1:61804	HP-280-G2:3306	TIME_WAIT
TCP	127.0.0.1:61805	HP-280-G2:3306	TIME_WAIT
TCP	127.0.0.1:61806	HP-280-G2:3306	TIME_WAIT
TCP	127.0.0.1:61807	HP-280-G2:3306	TIME_WAIT
TCP	127.0.0.1:61809	HP-280-G2:http	TIME_WAIT
TCP	127.0.0.1:61810	HP-280-G2:3306	TIME_WAIT
TCP	127.0.0.1:61811	HP-280-G2:3306	TIME_WAIT
TCP	127.0.0.1:61813	HP-280-G2:http	TIME_WAIT
TCP	127.0.0.1:61814	HP-280-G2:3306	TIME_WAIT

Vulnerability: Command Injection x localhost / 127.0.0.1 / dvwa | php x +

127.0.0.1/dvwa/vulnerabilities/exec/#

Gmail YouTube Maps

[Home](#)[Instructions](#)[Setup / Reset DB](#)
[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Tracing route to HP-280-G2 [127.0.0.1]
over a maximum of 30 hops:

```
  1    <1 ms    <1 ms    <1 ms  HP-280-G2 [127.0.0.1]
```

Trace complete.

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

VMware-player-ful...exe

Show all

Type here to search

28°C Haze 10:56 28-09-2022

Vulnerability: Command Injection x localhost / 127.0.0.1 / dvwa | php x +

127.0.0.1/dvwa/vulnerabilities/exec/#

Gmail YouTube Maps

[Home](#)[Instructions](#)[Setup / Reset DB](#)
[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Tracing route to HP-280-G2 [127.0.0.1]
over a maximum of 30 hops:

```
  0  HP-280-G2 [127.0.0.1]
  1  HP-280-G2 [127.0.0.1]
```

Computing statistics for 25 seconds...

Hop	RTT	Source to Here	This Node/Link	Address
0				HP-280-G2 [127.0.0.1]
1	0ms	0/ 100 = 0%	0/ 100 = 0%	HP-280-G2 [127.0.0.1]

Trace complete.

More Information

- <https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- https://owasp.org/www-community/attacks/Command_Injection

VMware-player-ful...exe

Show all

Type here to search

28°C Haze 10:58 28-09-2022