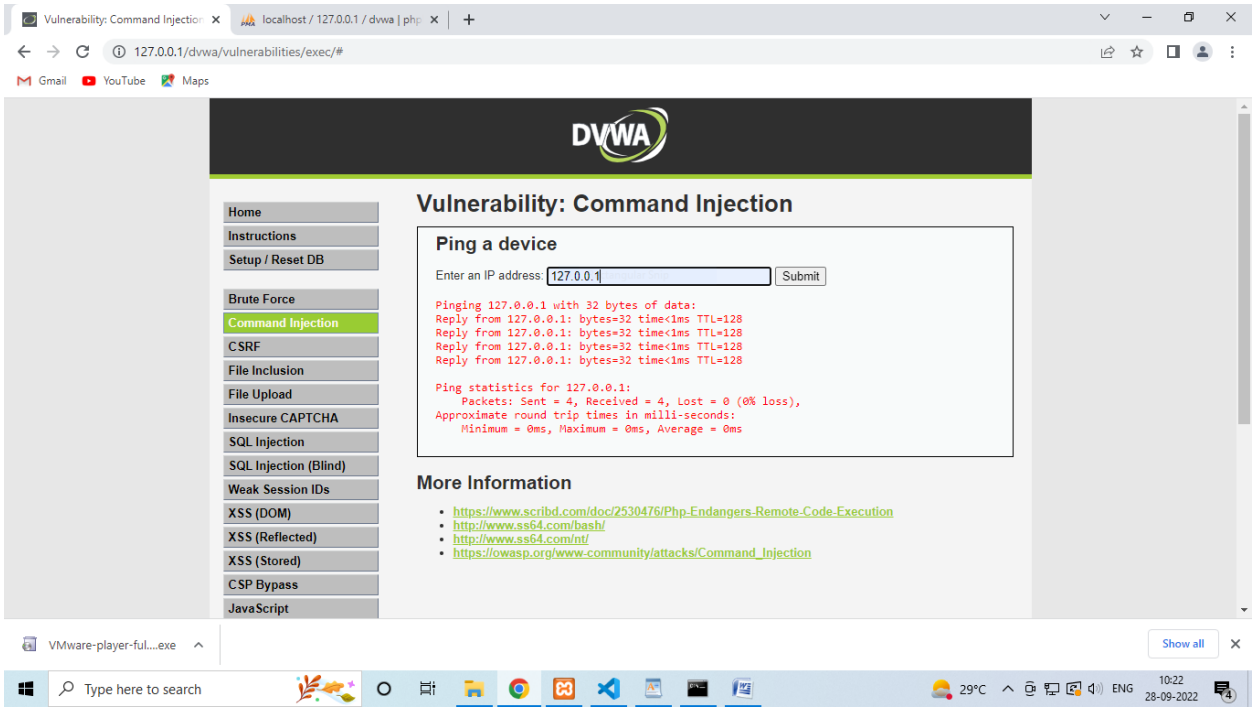
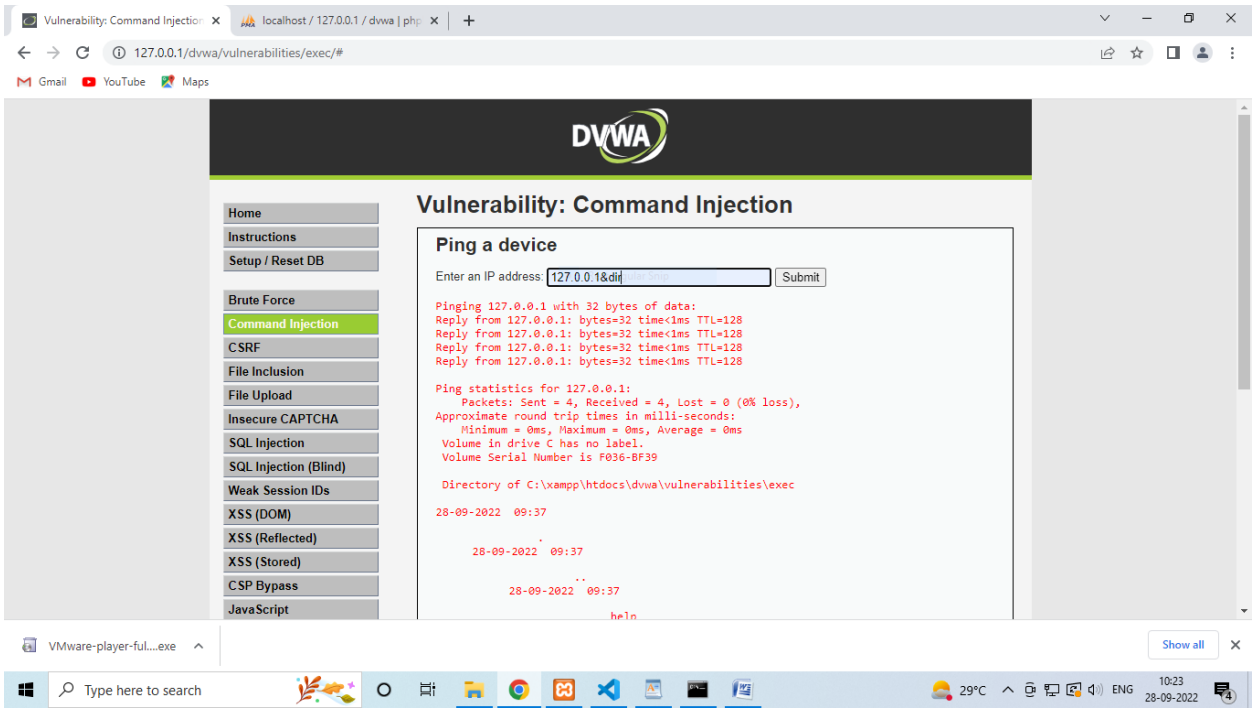
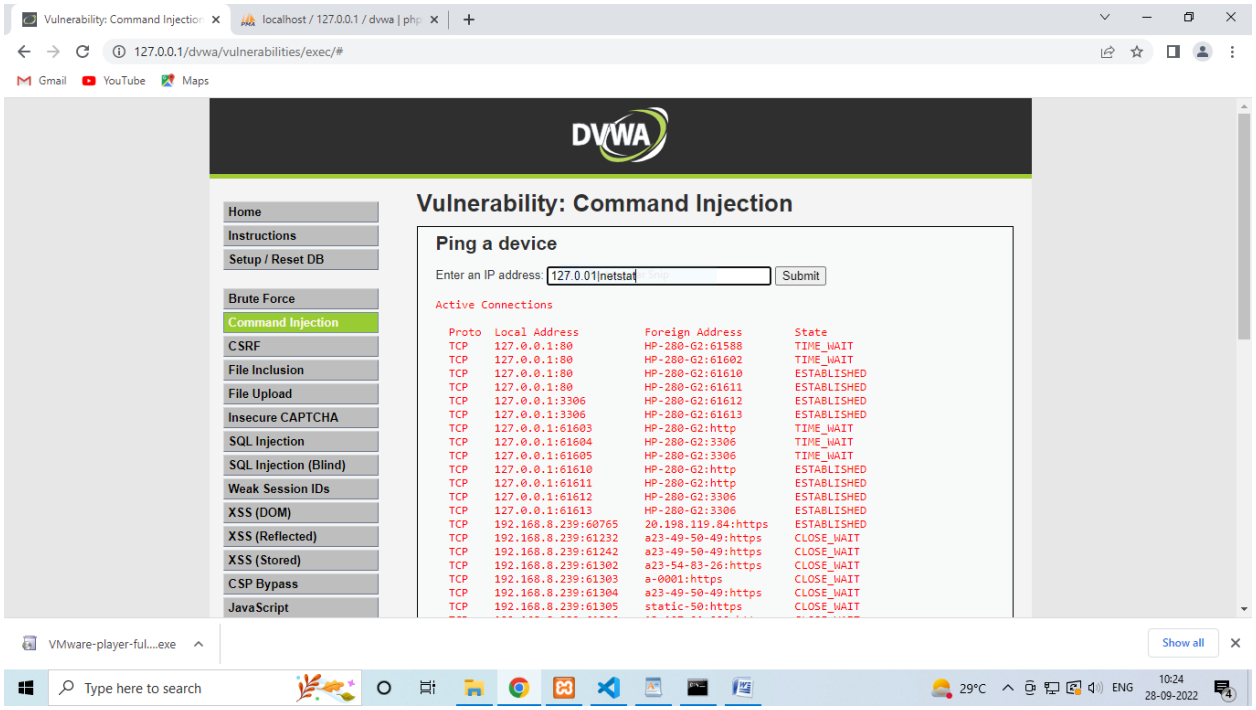
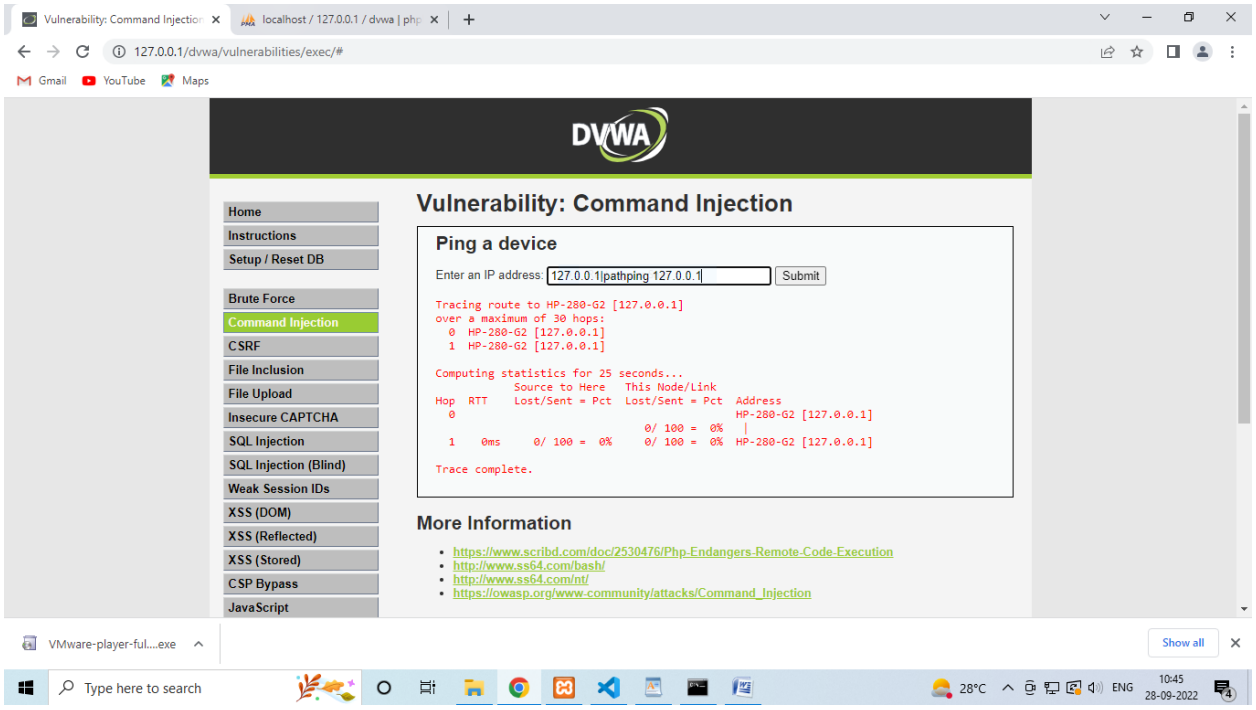
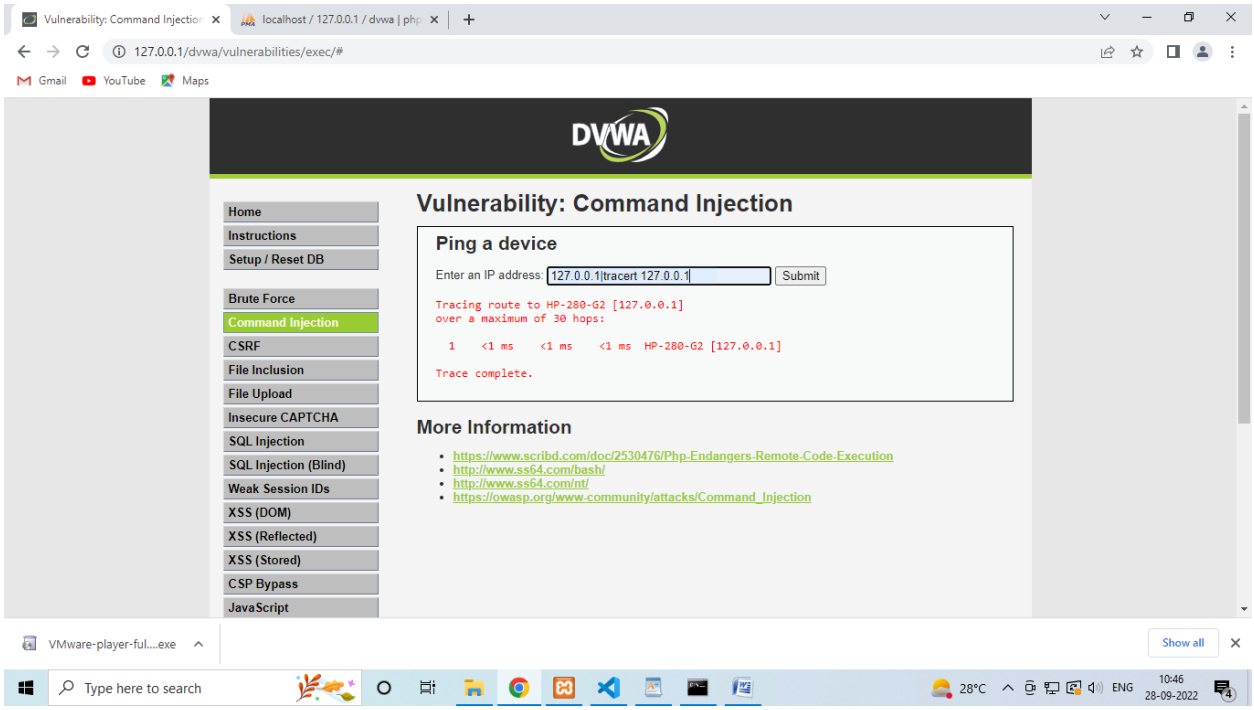
LOW SECURITY



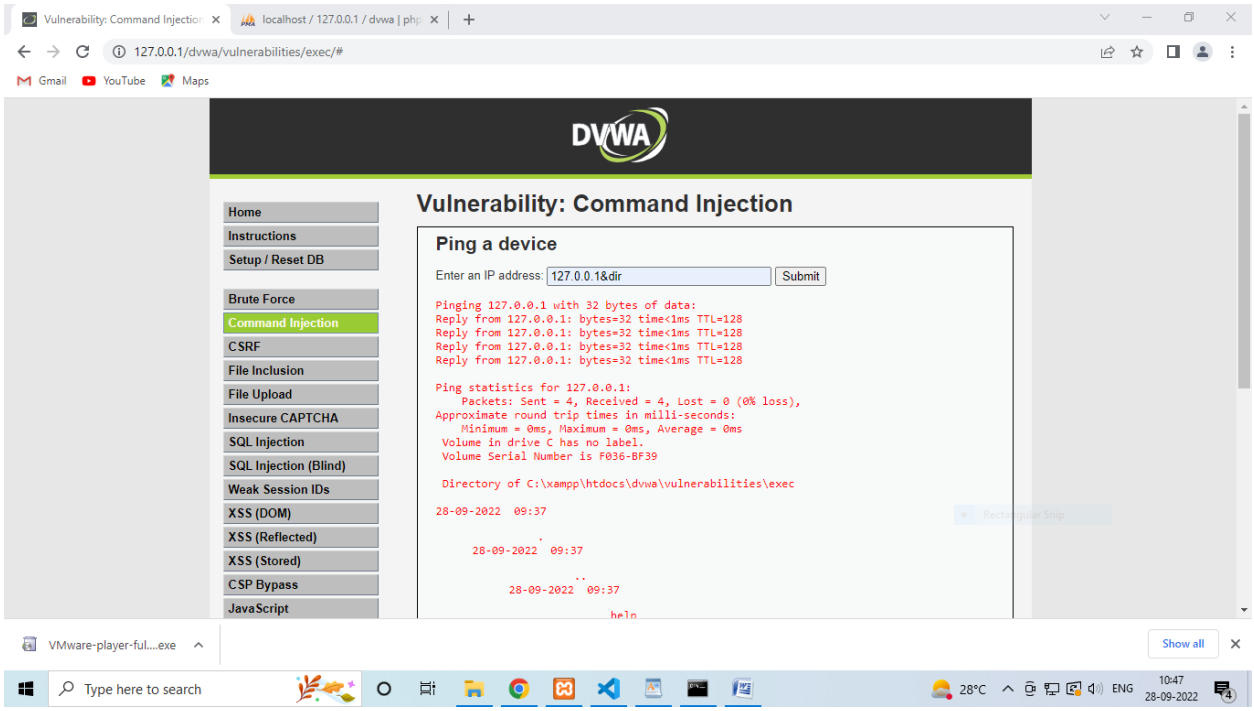


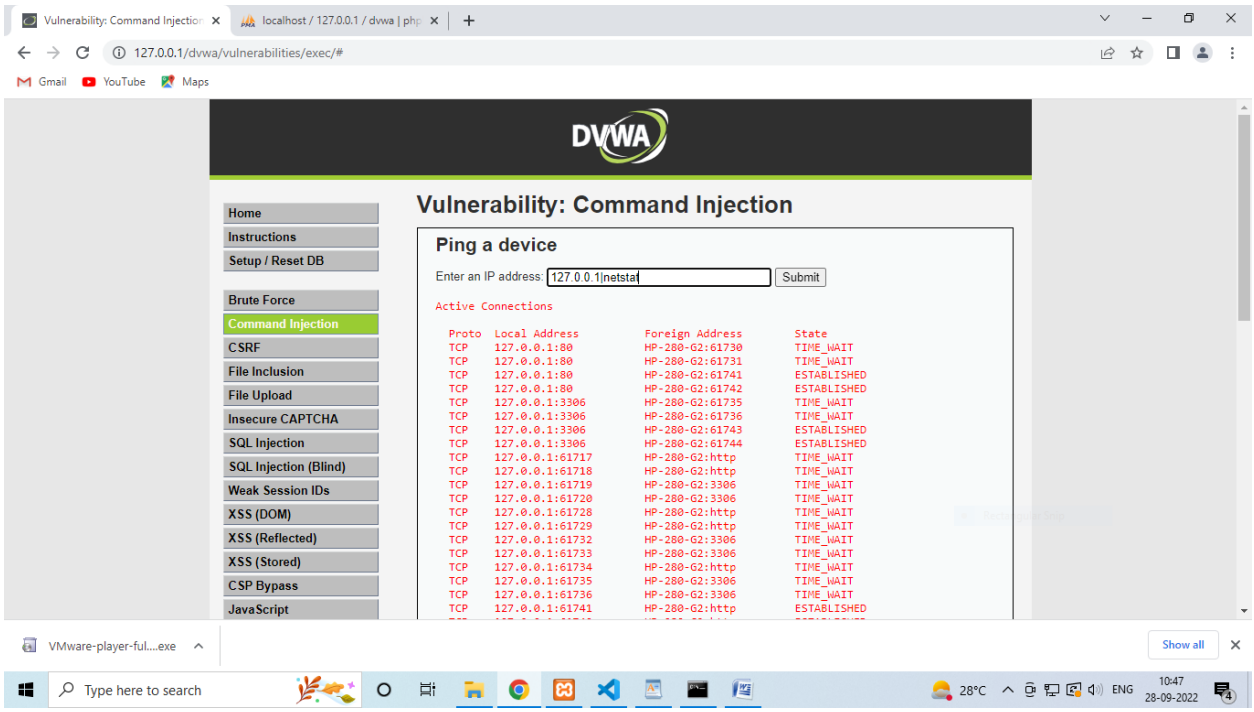

Vulnerability: Command Injection
localhost / 127.0.0.1 / dvwa | php
127.0.0.1/dvwa/vulnerabilities/exec/#
Gmail
YouTube
Maps
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: Command Injection
Ping a device
Enter an IP address: 127.0.01|netstat
Submit
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
Show all
Type here to search
29°C
ENG
10:24
28-09-2022

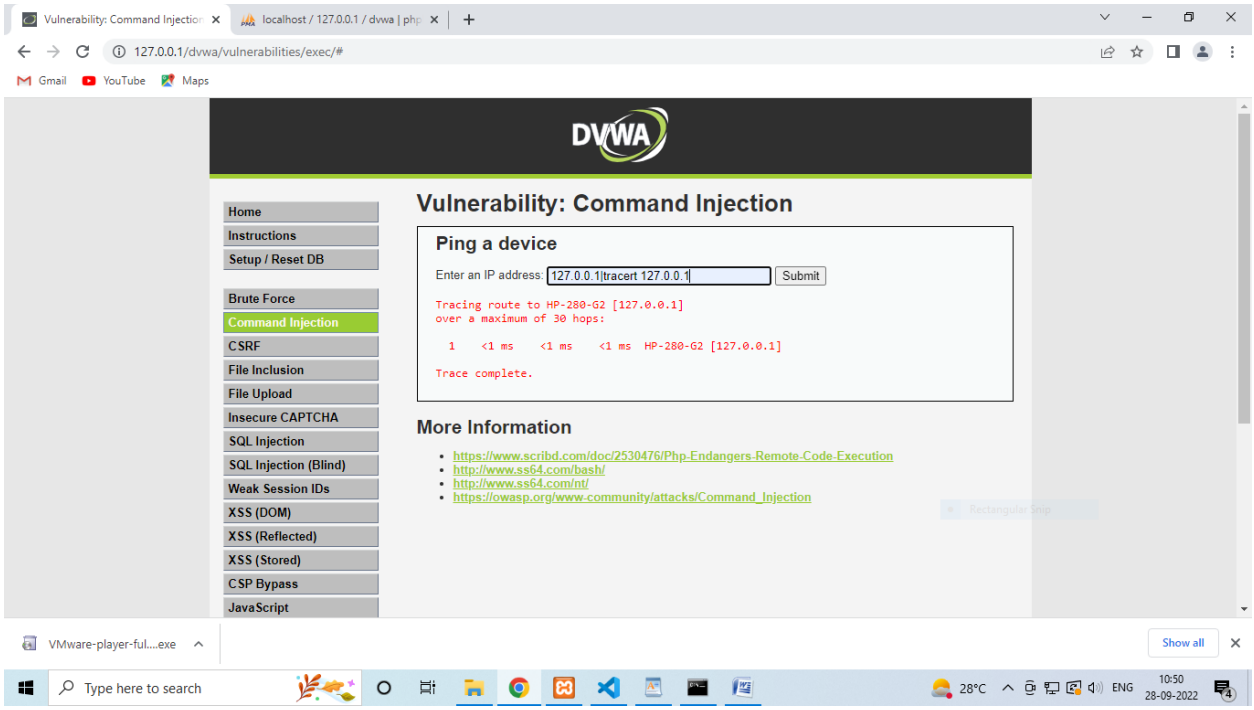

Vulnerability: Command Injection
localhost / 127.0.0.1 / dvwa | php
127.0.0.1/dvwa/vulnerabilities/exec/#
Gmail
YouTube
Maps
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: Command Injection
Ping a device
Enter an IP address: 127.0.0.1|pathping 127.0.0.1
Submit
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...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 HP-280-G2 [127.0.0.1]
0/ 100 = 0% |
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
ENG
10:45
28-09-2022

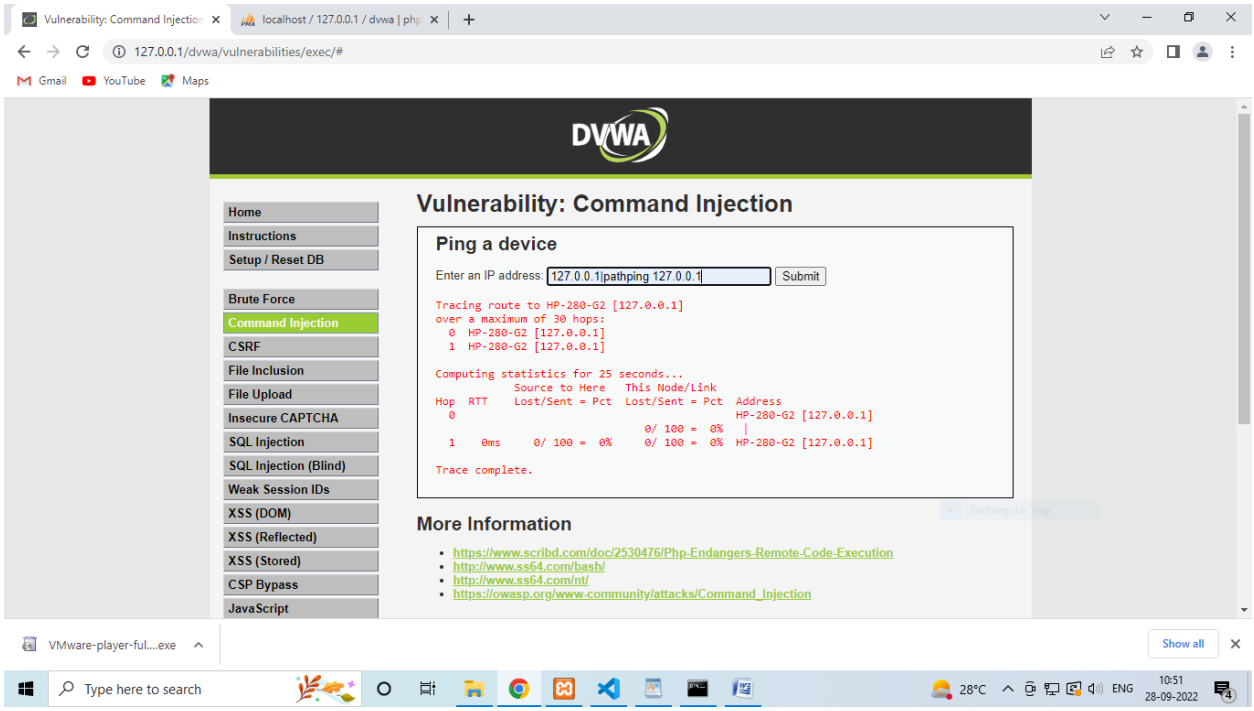

Vulnerability: Command Injection
localhost / 127.0.0.1 / dvwa | php
127.0.0.1/dvwa/vulnerabilities/exec/#
Gmail
YouTube
Maps
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: Command Injection
Ping a device
Enter an IP address: 127.0.0.1|tracert 127.0.0.1
Submit
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
ENG
10:46
28-09-2022

Medium Security

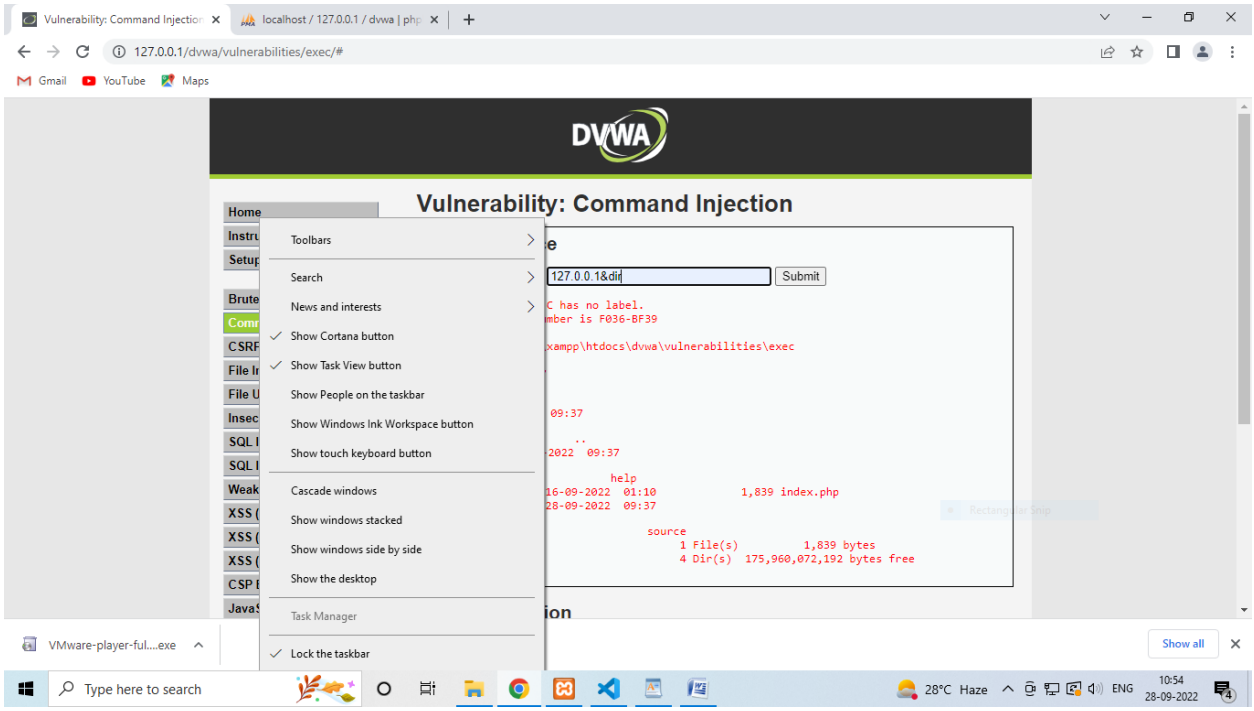


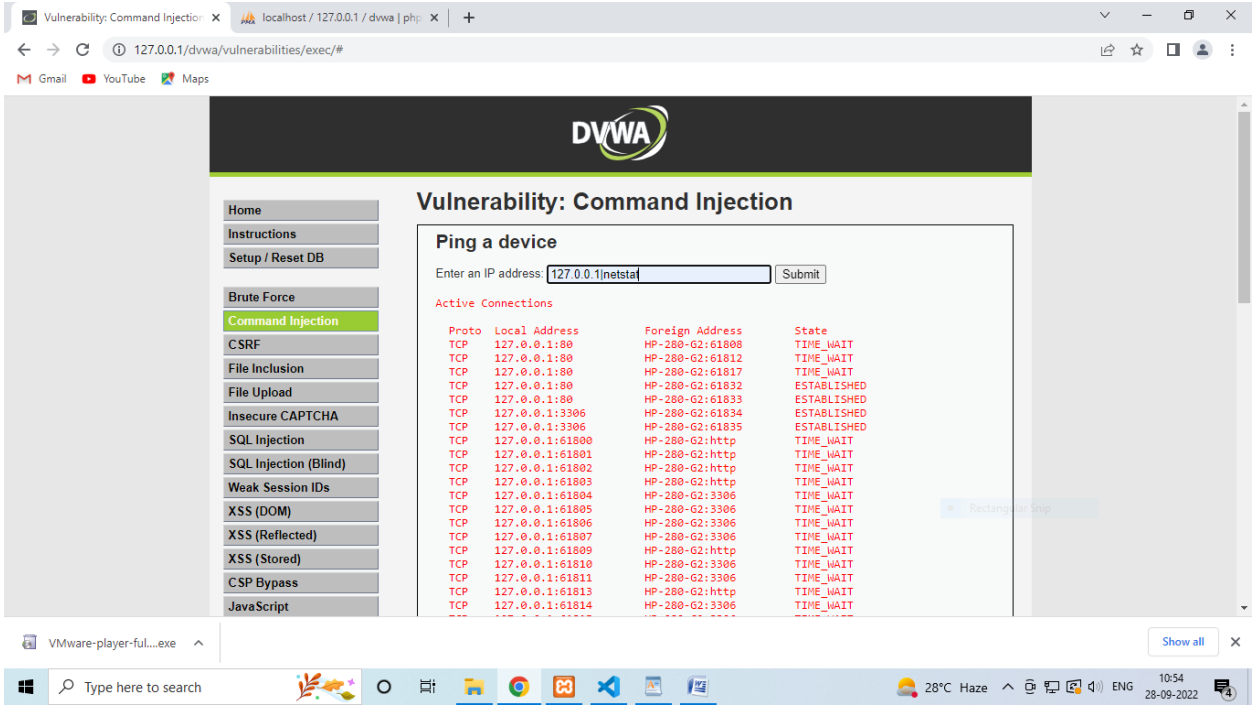


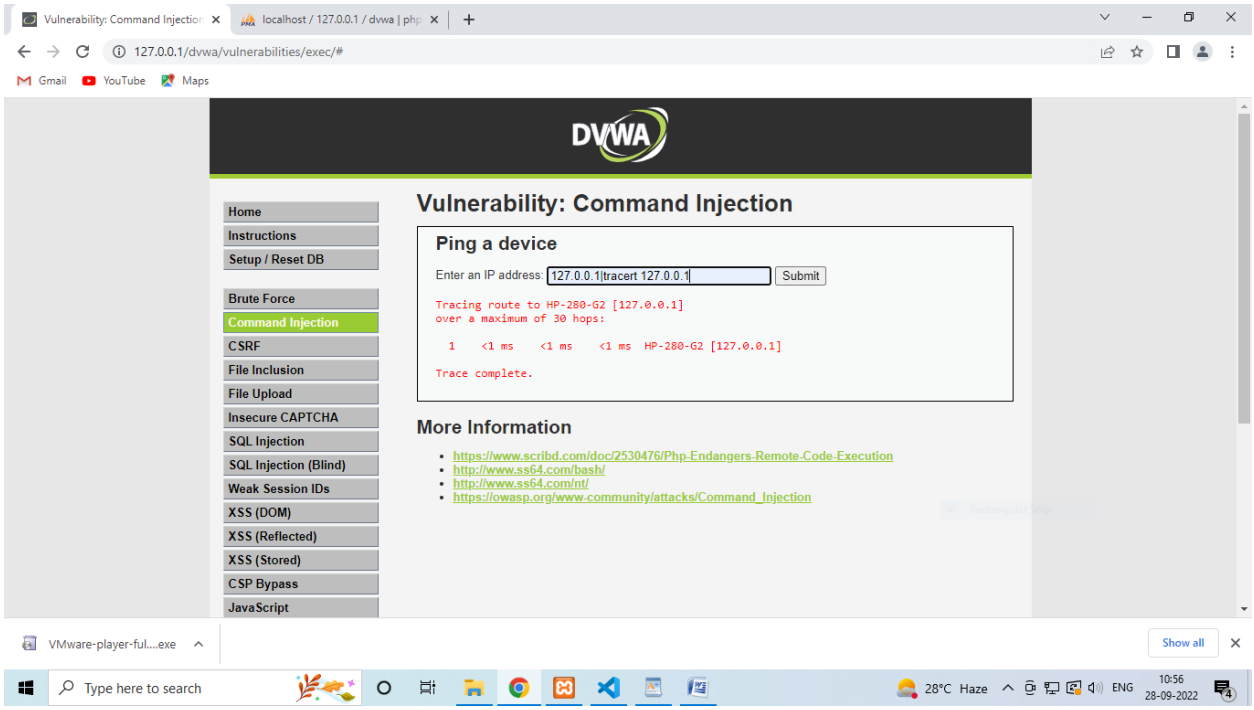

Vulnerability: Command Injection
localhost / 127.0.0.1 / dvwa | php
127.0.0.1/dvwa/vulnerabilities/exec/#
Gmail
YouTube
Maps
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: Command Injection
Ping a device
Enter an IP address: 127.0.0.1|tracert 127.0.0.1
Submit
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
ENG
10:50
28-09-2022

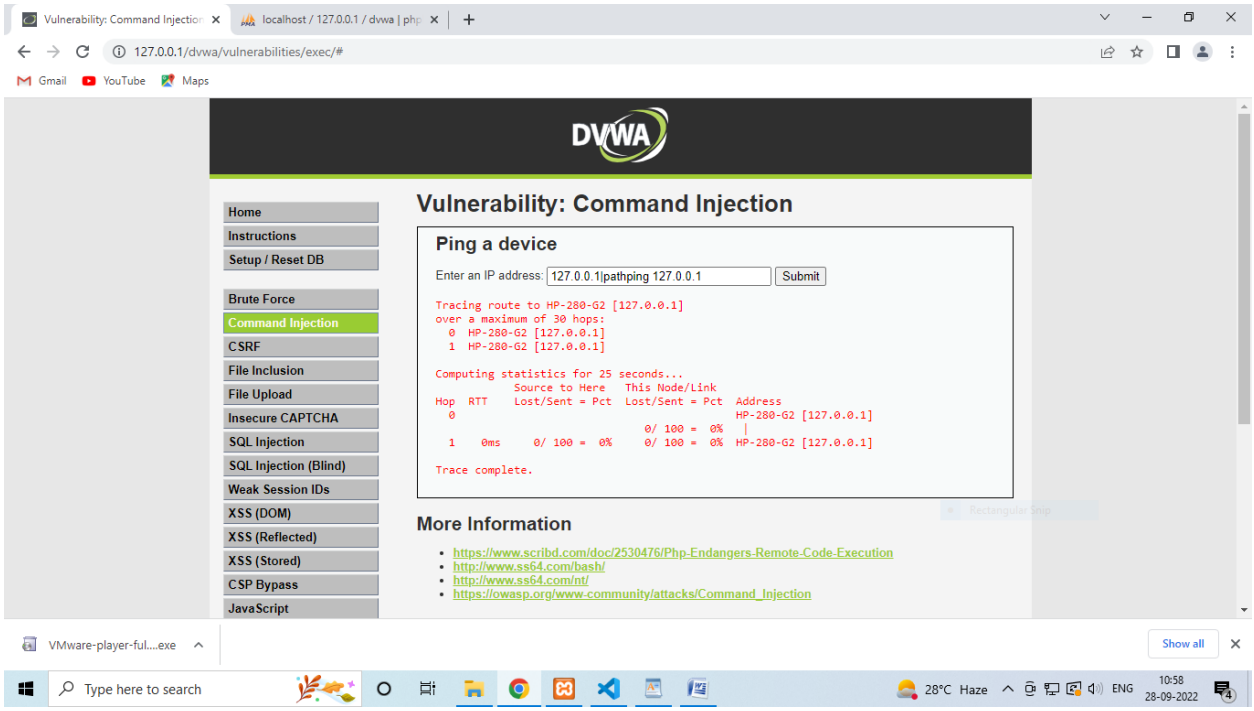

Vulnerability: Command Injection
localhost / 127.0.0.1 / dvwa | php
127.0.0.1/dvwa/vulnerabilities/exec/#
Gmail
YouTube
Maps
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: Command Injection
Ping a device
Enter an IP address: 127.0.0.1|pathping 127.0.0.1
Submit
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...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 HP-280-G2 [127.0.0.1]
0/ 100 = 0% |
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
ENG
10:51
28-09-2022

High security






Vulnerability: Command Injection
localhost / 127.0.0.1 / dvwa | php
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: 127.0.0.1|tracert 127.0.0.1
Submit
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
ENG
10:56
28-09-2022


Vulnerability: Command Injection
localhost / 127.0.0.1 / dvwa | php
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: 127.0.0.1|pathping 127.0.0.1
Submit
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...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 HP-280-G2 [127.0.0.1]
0/ 100 = 0% |
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
ENG
10:58
28-09-2022