

# Pytest-Playwright Test Output Issue

## Playwright

### pytest

```
Starting pytests.... ===== test session starts
===== platform linux -- Python 3.10.12,
pytest-7.4.2, pluggy-1.3.0 rootdir: /home/runner/work/ASTICI/ASTICI plugins:
asyncio-0.21.1, anyio-4.0.0, tornasync-0.6.0.post2, base-url-2.0.0, playwright-0.4.2,
trio-0.8.0 asyncio: mode=strict collected 5 items
```

```
src/testAsyncWebGoatUseCases.py ... [ 60%] src/testWebGoatUseCases.py .. [100%]
```

```
===== 5 passed in 23.92s
```

```
===== Stop pytests....
```

# Metasploit-ParrotOS Test output

## parrotOS metasploit

Interactive Application Security Testing : Making sure that parrot OS docker image has all the latest updates... Get:1 https://deb.parrot.sh/parrot parrot InRelease [14.6 kB] Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB] Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB] Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB] Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB] Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB] Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [526 kB] Get:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B] Get:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1147 kB] Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB] Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB] Fetched 19.9 MB in 2s (10.5 MB/s) Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Hit:1 https://deb.parrot.sh/parrot parrot InRelease Hit:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease Hit:3 https://deb.parrot.sh/parrot parrot-backports InRelease Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Cleaning up any existing old code copies of security tests...

## find a way to read it from secure place.

This is not a secure way to check out code;

## Getting the latest code copy for all security tests...

## Metasploit Framework Exploit Demo :

Target Web Goat Instance IP Address : 20.219.24.255

# Possible Metasploit exploits or auxiliaries or payloads, that can used for attacking

```
[*] Processing ./src/exploitwildflydirtraversal.rc for ERB directives. resource (./src/exploitwildflydirtraversal.rc)> use auxiliary/scanner/http/wildflytraversal resource (./src/exploitwildflydirtraversal.rc)> show options
```

Module options (auxiliary/scanner/http/wildfly\_traversal):

Name	Current	Setting	Required	Description	-----	Proxies
chain	no	A				
format	type:host:port[,type:host:port][...]			RELATIVEFILEPATH		
standalone	yes			Relative path to the file to read RHOSTS		
configuration	standalone.xml					
yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>			RHOSTS		
RPORT	8080	yes		The target port (TCP)		
SSL	false	no		Negotiate SSL/TLS for outgoing connections		
THREADS	1	yes		The number of concurrent threads (max one per host)		
TRAVERSAL_DEPTH	1	yes		Traversal depth		
VHOST	no			HTTP server virtual host		

View the full module info with the info, or info -d command.

```
[*] resource (./src/exploitwildflydirtraversal.rc)> Ruby Code (57 bytes) RHOSTS => resource (./src/exploitwildflydirtraversal.rc)> run [-] Msf::OptionValidateError The following options failed to validate: RHOSTS
```

**resource (./src/exploitwildflydir\_traversal.rc)> exit**

# ZAP Full Scan Report

- Site: <http://20.219.24.255:8080> **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
  - **Cookie Slack Detector** [90027] total: 2:
    - <http://20.219.24.255:8080/WebGoat/login>
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Base64 Disclosure** [10094] total: 1:
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
  - **Non-Storable Content** [10049] total: 1:
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/WebGoat/login>
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/WebGoat/login>
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/WebGoat/login>
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/WebGoat/login>
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
  - **Session Management Response Identified** [10112] total: 2:
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
    - <http://20.219.24.255:8080/WebGoat/start.mvc>
  - **Storable and Cacheable Content** [10049] total: 4:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/sitemap.xml>
    - <http://20.219.24.255:8080/WebGoat/login>
  - **User Agent Fuzzer** [10104] total: 24:
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - ..

View the [following link](#) to download the report. RunnerID:6368622914

# Nmap-ParrotOS Scan output

## parrotOS

### nmap

Nmap vulnerability scanning for 20.219.24.255 Making sure that parrot OS docker image has all the latest updates... Get:1 https://deb.parrot.sh/parrot parrot InRelease [14.6 kB] Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB] Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB] Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB] Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB] Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB] Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [526 kB] Get:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B] Get:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1147 kB] Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB] Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB] Fetched 19.9 MB in 2s (12.4 MB/s) Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Hit:1 https://deb.parrot.sh/parrot parrot InRelease Hit:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease Hit:3 https://deb.parrot.sh/parrot parrot-backports InRelease Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Running basic nmap scan... Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-01 06:31 UTC Nmap scan report for 20.219.24.255 Host is up (0.19s latency). Not shown: 65530 filtered tcp ports (no-response) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0) | ssh-hostkey: | 256 f4:a2:8e:88:24:c3:48:cf:14:fd:53:3f:44:79:e7:08 (ECDSA) |\_ 256 1f:29:98:9c:93:09:d5:ad:9b:6d:e0:16:e7:32:5a:94 (ED25519) 80/tcp closed http 443/tcp closed https 8080/tcp open http-proxy | fingerprint-strings: | FourOhFourRequest, HTTPOptions: | HTTP/1.1 404 Not Found | Connection: close | Content-Length: 0 | Date: Sun, 01 Oct 2023 06:36:10 GMT | GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, Socks5, TLSSessionReq, TerminalServerCookie, WMSRequest, oracle-tns: | HTTP/1.1 400 Bad Request | Content-Length: 0 | Connection: close | GetRequest: | HTTP/1.1 404 Not Found | Connection: close | Content-Length: 0 |\_ Date: Sun, 01 Oct 2023 06:36:09 GMT |http-title: Site doesn't have a title. 9090/tcp open zeus-admin? | fingerprint-strings: | GenericLines, RTSPRequest, SqueezeCenterCLI, WMSRequest, ibm-db2-das: | HTTP/1.1 400 Bad Request | Content-Length: 0 | Connection: close | GetRequest: | HTTP/1.1 404 Not Found | Expires: 0 | Cache-Control: no-cache, no-store, max-age=0, must-revalidate | X-XSS-Protection: 1; mode=block | Pragma: no-cache | X-Frame-Options: DENY | Date: Sun, 01 Oct 2023 06:36:09 GMT | Connection: close | Vary: Origin | Vary: Access-Control-Request-Method | Vary: Access-Control-Request-Headers | X-Content-Type-Options: nosniff | Content-Type: application/json | "timestamp" : "2023-10-01T06:36:09.677+00:00", | "status" : 404, | "error" : "Not

Found", | "path" : "/" | HTTPOptions: | HTTP/1.1 404 Not Found | Expires: 0 | Cache-Control: no-cache, no-store, max-age=0, must-revalidate | X-XSS-Protection: 1; mode=block | Pragma: no-cache | X-Frame-Options: DENY | Date: Sun, 01 Oct 2023 06:36:27 GMT | Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH | Connection: close | Vary: Origin | Vary: Access-Control-Request-Method | Vary: Access-Control-Request-Headers | X-Content-Type-Options: nosniff | Content-Type: application/json | "timestamp" : "2023-10-01T06:36:27.230+00:00", | "status" : 404, | "error" : "Not Found", | "path" : "/" 2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at <https://nmap.org/cgi-bin/submit.cgi?new-service> : =====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)===== SF-Port8080-

TCP:V=7.92%I=7%D=10/1%Time=65191359%P=x8664-pc-linux-gnu%(Ge SF:tRequest, 65,"HTTP/1.1\x20404\x20Not\x20Found\r\nConnection:\x20close\r SF:\nContent-Length:\x200\r\nDate:\x20Sun,\x2001\x20Oct\x202023\x2006:36:0 SF:9\x20GMT\r\n\r\n") %r(HTTPOptions,65,"HTTP/1.1\x20404\x20Not\x20Found\r SF:\nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Sun,\x2001\x20Oct\x202023\x2006:36:10\x20GMT\r\n\r\n") %r(RTSPRequest,42,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Sun,\x2001\x20Oct\x202023\x2006:36:10\x20GMT\r\n\r\n") %r(Socks5,42,"HTTP/1.1\x20400 SF:\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n SF:r\n") %r(GenericLines,42,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent- SF:Length:\x200\r\nConnection:\x20close\r\n\r\n") %r(Help,42,"HTTP/1.1\x20 SF:400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r SF:\n\r\n") %r(SSLSessionReq,42,"HTTP/1.1\x20400\x20Bad\x20Request\r\nCont SF:ent-Length:\x200\r\nConnection:\x20close\r\n\r\n") %r(TerminalServerCook SF:ie,42,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nCo SF:nnection:\x20close\r\n\r\n") %r(TLSSessionReq,42,"HTTP/1.1\x20400\x20Ba SF:d\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n") % SF:r(Kerberos,42,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Length:\x2 SF:00\r\nConnection:\x20close\r\n\r\n") %r(SMBProgNeg,42,"HTTP/1.1\x20400 SF:\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\nr SF:\n") %r(LPDString,42,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Leng SF:th:\x200\r\nConnection:\x20close\r\n\r\n") %r(LDAPSearchReq,42,"HTTP/1. SF:1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20cl SF:ose\r\n\r\n") %r(SIPOptions,42,"HTTP/1.1\x20400\x20Bad\x20Request\r\nCo SF:ntent-Length:\x200\r\nConnection:\x20close\r\n\r\n") %r(WMSRequest,42,"H SF:TTP/1.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection SF::\x20close\r\n\r\n") %r(oracle-tns,42,"HTTP/1.1\x20400\x20Bad\x20Reques SF:t\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n");

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)===== SF-Port9090-

TCP:V=7.92%I=7%D=10/1%Time=65191359%P=x8664-pc-linux-gnu%(Ge SF:tRequest, 1EF,"HTTP/1.1\x20404\x20Not\x20Found\r\nExpires:\x200\r\nCach SF:e-Control:\x20no-cache,\x20no-store,\x20max-age=0,\x20must-revalidate\r SF:\nX-XSS-Protection:\x201;\x20mode=block\r\nPragma:\x20no-cache\r\nX-Fra SF:me-Options:\x20DENY\r\nDate:\x20Sun,\x2001\x20Oct\x202023\x2006:36:09\x SF:20GMT\r\nConnection:\x20close\r\nVary:\x20Origin\r\nVary:\x20Access-Con SF:trol-Request-Method\r\nVary:\x20Access-Control-Request-Headers\r\nX-Con SF:tent-Type-Options:\x20nosniff\r\nContent-Type:\x20application/json\r\n SF:r\n{\n\x20\x20"timestamp"\x20:\x20"2023-10-01T06:36:09.677+00:00"\n SF:,\n\x20\x20"status"\x20:\x20404,\n\x20\x20"error"\x20:\x20"Not\x20 SF:Found",\n\x20\x20"path"\x20:\x20"/\n}\n") %r(WMSRequest,42,"HTTP/1. SF:1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20cl SF:ose\r\n\r\n") %r(ibm-db2-das,42,"HTTP/1.1\x20400\x20Bad\x20Request\r\nC SF:ontent-Length:\x200\r\nConnection:\x20close\r\n\r\n") %r(SqueezeCenterC SF:LI,42,"HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nCo SF:nnection:\x20close\r\n\r\n") %r(GenericLines,42,"HTTP/1.1\x20400\x20Bad SF:

\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r SF:  
(HTTPOptions,22B,"HTTP/1.1\x20404\x20Not\x20Found\r\nExpires:\x200\r\n SF:Cache-  
Control:\x20no-cache,\x20no-store,\x20max-age=0,\x20must-revalida SF:te\r\nX-XSS-  
Protection:\x201;\x20mode=block\r\nPragma:\x20no-cache\r\nX SF:-Frame-Options:  
\x20DENY\r\nDate:\x20Sun,\x2001\x20Oct\x202023\x2006:36: SF:27\x20GMT\r\nAllow:  
\x20GET,\x20HEAD,\x20POST,\x20PUT,\x20DELETE,\x20TRA SF:CE,\x20OPTIONS,  
\x20PATCH\r\nConnection:\x20close\r\nVary:\x20Origin\r\n SF:Vary:\x20Access-Control-  
Request-Method\r\nVary:\x20Access-Control-Reque SF:st-Headers\r\nX-Content-Type-  
Options:\x20nosniff\r\nContent-Type:\x20ap SF:plication/  
json\r\n\r\n{\r\n\r\n\x20\x20"timestamp"\r\n\x20:\x20\x20"2023-10-01T06: SF:36:27.230+00:00",  
\r\n\r\n\x20\x20"status"\r\n\x20:\x20\x20404,\r\n\r\n\x20\x20"error" SF:"\r\n\x20:\x20\x20"Not\x20Found",  
\r\n\r\n\x20\x20"path"\r\n\x20:\x20\x20"/"\r\n\r\n}%r(RTSP SF:Request,42,"HTTP/  
1.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\ SF:r\r\nConnection:  
\x20close\r\n\r\n\r\n"); Device type: general purpose|storage-misc|firewall Running (JUST  
GUESSING): Linux 2.6.X|3.X|4.X (86%), Synology DiskStation Manager 5.X (86%),  
FreeBSD 6.X (85%), WatchGuard Fireware 11.X (85%) OS CPE: cpe:/o:linux:linuxkernel:  
2.6.32 cpe:/o:linux:linuxkernel:3 cpe:/o:linux:linuxkernel:4.4 cpe:/o:linux:linuxkernel  
cpe:/a:synology:diskstationmanager:5.1 cpe:/o:freebsd:freebsd:6.2 cpe:/  
o:watchguard:fireware:11.8 Aggressive OS guesses: Linux 2.6.32 (86%), Linux 2.6.39  
(86%), Linux 3.10 - 3.12 (86%), Linux 3.4 (86%), Linux 4.4 (86%), Synology DiskStation  
Manager 5.1 (86%), Linux 3.10 - 3.16 (85%), Linux 4.0 (85%), Linux 2.6.35 (85%), Linux  
3.10 (85%) No exact OS matches for host (test conditions non-ideal). Network Distance:  
2 hops Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 443/tcp) HOP RTT ADDRESS 1 0.02 ms 172.17.0.1 2 5602.63  
ms 20.219.24.255

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> . Nmap done: 1 IP address (1 host up) scanned in 398.37 seconds  
Running vulnerability scanning using basic nmap scripts - SQL Injection... Starting Nmap  
7.92 ( <https://nmap.org> ) at 2023-10-01 06:38 UTC Nmap scan report for 20.219.24.255  
Host is up (0.19s latency).

PORT STATE SERVICE 8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds Running vulnerability  
scanning using CSS nmap script... Starting Nmap 7.92 ( <https://nmap.org> ) at 2023-10-01  
06:38 UTC Nmap scan report for 20.219.24.255 Host is up (0.19s latency).

PORT STATE SERVICE 8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds



# ZAP Full Scan Report

- Site: <http://20.219.24.255:8080> **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/WebGoat/login>
  - **Storable and Cacheable Content** [10049] total: 4:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/sitemap.xml>
    - <http://20.219.24.255:8080/WebGoat/login>
  - **User Agent Fuzzer** [10104] total: 12:
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - ..

View the [following link](#) to download the report. RunnerID:6368622914

# ZAP Full Scan Report

- Site: <http://20.219.24.255:8080> **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - <http://20.219.24.255:8080/WebGoat/registration>
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - <http://20.219.24.255:8080/WebGoat/registration>
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - <http://20.219.24.255:8080/WebGoat/registration>
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - <http://20.219.24.255:8080/WebGoat/registration>
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/sitemap.xml>
    - <http://20.219.24.255:8080/WebGoat/registration>
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/sitemap.xml>
    - <http://20.219.24.255:8080/WebGoat/registration>
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/sitemap.xml>
    - <http://20.219.24.255:8080/WebGoat/registration>
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/sitemap.xml>
    - <http://20.219.24.255:8080/WebGoat/registration>
  - **Storable and Cacheable Content** [10049] total: 4:
    - <http://20.219.24.255:8080/>
    - <http://20.219.24.255:8080/robots.txt>
    - <http://20.219.24.255:8080/sitemap.xml>
    - <http://20.219.24.255:8080/WebGoat/registration>
  - **User Agent Fuzzer** [10104] total: 12:
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - <http://20.219.24.255:8080/WebGoat>
    - ..

View the [following link](#) to download the report. RunnerID:6368622914

# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO

# Snyk Report

## **Snyk\_scan**

Go to <https://app.snyk.io/org/pradyumna-muppirala> for full report of Snyk with Github SSO

# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO

# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO

# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO

# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO



# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO

# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO

# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO

# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO

# Pytest-Playwright Test Output Issue

## Playwright

### pytest

```
Starting pytests.... ===== test session starts
===== platform linux -- Python 3.10.12,
pytest-7.4.2, pluggy-1.3.0 rootdir: /home/runner/work/ASTICI/ASTICI plugins:
asyncio-0.21.1, anyio-4.0.0, tornasync-0.6.0.post2, base-url-2.0.0, playwright-0.4.2,
trio-0.8.0 asyncio: mode=strict collected 5 items
```

```
src/testAsyncWebGoatUseCases.py ... [ 60%] src/testWebGoatUseCases.py .. [100%]
```

```
===== 5 passed in 29.56s
```

```
===== Stop pytests....
```

# ZAP Full Scan Report

- Site: <http://4.247.148.163:8080> **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
  - **Cookie Slack Detector** [90027] total: 2:
    - <http://4.247.148.163:8080/WebGoat/login>
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Base64 Disclosure** [10094] total: 1:
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
  - **Non-Storable Content** [10049] total: 1:
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/WebGoat/login>
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/WebGoat/login>
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/WebGoat/login>
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/WebGoat/login>
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
  - **Session Management Response Identified** [10112] total: 2:
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
    - <http://4.247.148.163:8080/WebGoat/start.mvc>
  - **Storable and Cacheable Content** [10049] total: 4:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/sitemap.xml>
    - <http://4.247.148.163:8080/WebGoat/login>
  - **User Agent Fuzzer** [10104] total: 24:
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - ..

View the [following link](#) to download the report. RunnerID:6335693005

# Metasploit-ParrotOS Test output

## parrotOS metasploit

Interactive Application Security Testing : Making sure that parrot OS docker image has all the latest updates... Get:1 https://deb.parrot.sh/parrot parrot InRelease [14.6 kB] Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB] Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB] Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB] Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB] Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB] Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [524 kB] Get:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B] Get:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1147 kB] Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB] Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB] Fetched 19.9 MB in 3s (6223 kB/s) Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Hit:1 https://deb.parrot.sh/parrot parrot InRelease Hit:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease Hit:3 https://deb.parrot.sh/parrot parrot-backports InRelease Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Cleaning up any existing old code copies of security tests...

## find a way to read it from secure place.

This is not a secure way to check out code;

## Getting the latest code copy for all security tests...

## Metasploit Framework Exploit Demo :

Target Web Goat Instance IP Address : 4.247.148.163

# Possible Metasploit exploits or auxiliaries or payloads, that can used for attacking

```
[*] Processing ./src/exploitwildflydirtraversal.rc for ERB directives. resource (./src/exploitwildflydirtraversal.rc)> use auxiliary/scanner/http/wildflytraversal resource (./src/exploitwildflydirtraversal.rc)> show options
```

Module options (auxiliary/scanner/http/wildfly\_traversal):

Name	Current	Setting	Required	Description	-----	Proxies
chain	no	A				
format	type:host:port[,type:host:port][...]			RELATIVEFILEPATH		
standalone	yes			Relative path to the file to read RHOSTS		
target	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>			RHOSTS		
RPORT	8080	yes		The target port (TCP)		
SSL	false	no		Negotiate SSL/TLS for outgoing connections		
THREADS	1	yes		The number of concurrent threads (max one per host)		
TRAVERSAL_DEPTH	1	yes		Traversal depth		
VHOST	no			HTTP server virtual host		

View the full module info with the info, or info -d command.

```
[*] resource (./src/exploitwildflydirtraversal.rc)> Ruby Code (57 bytes) RHOSTS => resource (./src/exploitwildflydirtraversal.rc)> run [-] Msf::OptionValidateError The following options failed to validate: RHOSTS
```

**resource (./src/exploitwildflydir\_traversal.rc)> exit**



# Nmap-ParrotOS Scan output

## parrotOS

### nmap

Nmap vulnerability scanning for 4.247.148.163 Making sure that parrot OS docker image has all the latest updates... Get:1 https://deb.parrot.sh/parrot parrot InRelease [14.6 kB] Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB] Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB] Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB] Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB] Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB] Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [524 kB] Get:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B] Get:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1147 kB] Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB] Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB] Fetched 19.9 MB in 3s (6324 kB/s) Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Hit:1 https://deb.parrot.sh/parrot parrot InRelease Hit:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease Hit:3 https://deb.parrot.sh/parrot parrot-backports InRelease Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Running basic nmap scan... Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-28 07:20 UTC Nmap scan report for 4.247.148.163 Host is up (0.24s latency). Not shown: 65530 filtered tcp ports (no-response) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0) | ssh-hostkey: | 256 54:45:44:f8:e3:06:d5:72:af:2e:fa:e9:6d:fb:a5:23 (ECDSA) |\_ 256 1b:83:06:ae:c9:dd:45:99:78:c8:ab:3e:24:02:d2:3b (ED25519) 80/tcp closed http 443/tcp closed https 8080/tcp open http-proxy | fingerprint-strings: | FourOhFourRequest: | HTTP/1.1 404 Not Found | Connection: close | Content-Length: 0 | Date: Thu, 28 Sep 2023 07:24:26 GMT | GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, Socks5, TLSSessionReq, TerminalServerCookie, WMSRequest, oracle-tns: | HTTP/1.1 400 Bad Request | Content-Length: 0 | Connection: close | GetRequest: | HTTP/1.1 404 Not Found | Connection: close | Content-Length: 0 | Date: Thu, 28 Sep 2023 07:24:24 GMT | HTTPOptions: | HTTP/1.1 404 Not Found | Connection: close | Content-Length: 0 |\_ Date: Thu, 28 Sep 2023 07:24:25 GMT |http-title: Site doesn't have a title. 9090/tcp open zeus-admin? | fingerprint-strings: | GenericLines, RTSPRequest, SqueezeCenterCLI, WMSRequest, ibm-db2-das: | HTTP/1.1 400 Bad Request | Content-Length: 0 | Connection: close | GetRequest: | HTTP/1.1 404 Not Found | Expires: 0 | Cache-Control: no-cache, no-store, max-age=0, must-revalidate | X-XSS-Protection: 1; mode=block | Pragma: no-cache | X-Frame-Options: DENY | Date: Thu, 28 Sep 2023 07:24:24 GMT | Connection: close | Vary: Origin | Vary: Access-Control-Request-Method | Vary: Access-Control-Request-Headers | X-Content-Type-Options:

```

nosniff | Content-Type: application/json | "timestamp" :
"2023-09-28T07:24:24.845+00:00", | "status" : 404, | "error" : "Not Found", | "path" : "/"
| HTTPOptions: | HTTP/1.1 404 Not Found | Expires: 0 | Cache-Control: no-cache, no-
store, max-age=0, must-revalidate | X-XSS-Protection: 1; mode=block | Pragma: no-
cache | X-Frame-Options: DENY | Date: Thu, 28 Sep 2023 07:24:43 GMT | Allow: GET,
HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH | Connection: close | Vary: Origin |
Vary: Access-Control-Request-Method | Vary: Access-Control-Request-Headers | X-
Content-Type-Options: nosniff | Content-Type: application/json | "timestamp" :
"2023-09-28T07:24:43.020+00:00", | "status" : 404, | "error" : "Not Found", | "path" : "/"
2 services unrecognized despite returning data. If you know the service/version, please
submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT
INDIVIDUALLY)===== SF-Port8080-
TCP:V=7.92%I=7%D=9/28%Time=65152A28%P=x8664-pc-linux-gnu%(Ge SF:tRequest,
65,"HTTP/1.1|x20404|x20Not|x20Found\r\nConnection:\x20close\r SF:\nContent-Length:
\x200\r\nDate:\x20Thu,\x2028\x20Sep\x202023\x2007:24:2 SF:4\x20GMT\r\n\r\n")
%(HTTPOptions,65,"HTTP/1.1|x20404|x20Not|x20Found\r SF:\nConnection:
\x20close\r\nContent-Length:\x200\r\nDate:\x20Thu,\x2028\x SF:
20Sep\x202023\x2007:24:25\x20GMT\r\n\r\n")%(RTSPRequest,42,"HTTP/1.1|
SF:x20400|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20clos
SF:e\r\n\r\n")%(FourOhFourRequest,65,"HTTP/1.1|x20404|x20Not|x20Found\r|
SF:nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Thu,\x2028\x2 SF:
0Sep\x202023\x2007:24:26\x20GMT\r\n\r\n")%(Socks5,42,"HTTP/1.1|x20400 SF:
|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n SF:r\n")
%(GenericLines,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nContent- SF:Length:
\x200\r\nConnection:\x20close\r\n\r\n")%(Help,42,"HTTP/1.1|x20 SF:
400|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r SF:\n\r\n")
%(SSLSessionReq,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nCont SF:ent-Length:
\x200\r\nConnection:\x20close\r\n\r\n")%(TerminalServerCook SF:ie,42,"HTTP/
1.1|x20400|x20Bad|x20Request\r\nContent-Length:\x200\r\nCo SF:nnection:
\x20close\r\n\r\n")%(TLSSessionReq,42,"HTTP/1.1|x20400|x20Ba
SF:d|x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%
SF:r(Kerberos,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nContent-Length:\x2 SF:
00\r\nConnection:\x20close\r\n\r\n")%(SMBProgNeg,42,"HTTP/1.1|x20400|
SF:x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\nr SF:\n")
%(LPDString,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nContent-Leng SF:th:
\x200\r\nConnection:\x20close\r\n\r\n")%(LDAPSearchReq,42,"HTTP/1. SF:
1|x20400|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20cl
SF:ose\r\n\r\n")%(SIPOptions,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nCo SF:ntent-
Length:\x200\r\nConnection:\x20close\r\n\r\n")%(WMSRequest,42,"H SF:TTP/
1.1|x20400|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection SF::
\x20close\r\n\r\n")%(oracle-tns,42,"HTTP/1.1|x20400|x20Bad|x20Reques
SF:t\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n");
=====NEXT SERVICE FINGERPRINT (SUBMIT
INDIVIDUALLY)===== SF-Port9090-
TCP:V=7.92%I=7%D=9/28%Time=65152A28%P=x8664-pc-linux-gnu%(Ge SF:tRequest,
1EF,"HTTP/1.1|x20404|x20Not|x20Found\r\nExpires:\x200\r\nCach SF:e-Control:\x20no-
cache,\x20no-store,\x20max-age=0,\x20must-revalidate\r SF:\nX-XSS-Protection:
\x201;\x20mode=block\r\nPragma:\x20no-cache\r\nX-Fra SF:me-Options:
\x20DENY\r\nDate:\x20Thu,\x2028\x20Sep\x202023\x2007:24:24\x SF:
20GMT\r\nConnection:\x20close\r\nVary:\x20Origin\r\nVary:\x20Access-Con SF:trol-
Request-Method\r\nVary:\x20Access-Control-Request-Headers\r\nX-Con SF:tent-Type-
Options:\x20nosniff\r\nContent-Type:\x20application/json\r\n\
SF:r\n{\n\x20\x20"timestamp"\x20:\x20"2023-09-28T07:24:24.845+00:00"\ SF:,
\n\x20\x20"status"\x20:\x20404,\n\x20\x20"error"\x20:\x20"Not\x20 SF:Found",
\n\x20\x20"path"\x20:\x20"/\n}\n")%(WMSRequest,42,"HTTP/1. SF:
1|x20400|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20cl
SF:ose\r\n\r\n")%(ibm-db2-das,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nC SF:ontent-
Length:\x200\r\nConnection:\x20close\r\n\r\n")%(SqueezeCenterC SF:LI,42,"HTTP/

```

```

1.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nCo SF:nnection:
\x20close\r\n\r\n")%r(GenericLines,42,"HTTP/1.1\x20400\x20Bad SF:
\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r SF:
(HTTPOptions,22B,"HTTP/1.1\x20404\x20Not\x20Found\r\nExpires:\x200\r\n SF:Cache-
Control:\x20no-cache,\x20no-store,\x20max-age=0,\x20must-revalida SF:tel\r\nX-XSS-
Protection:\x201;\x20mode=block\r\nPragma:\x20no-cache\r\nX SF:-Frame-Options:
\x20DENY\r\nDate:\x20Thu,\x2028\x20Sep\x202023\x2007:24: SF:43\x20GMT\r\nAllow:
\x20GET,\x20HEAD,\x20POST,\x20PUT,\x20DELETE,\x20TRA SF:CE,\x20OPTIONS,
\x20PATCH\r\nConnection:\x20close\r\nVary:\x20Origin\r\n SF:Vary:\x20Access-Control-
Request-Method\r\nVary:\x20Access-Control-Reque SF:st-Headers\r\nX-Content-Type-
Options:\x20nosniff\r\nContent-Type:\x20ap SF:plication/
json\r\n\r\n{\r\n\r\n\x20\timestamp"\x20:\x20\t2023-09-28T07: SF:24:43.020+00:00",
\r\n\r\n\x20\tatus"\x20:\x20404,\r\n\r\n\x20\terror\ SF:"\x20:\x20\tNot\x20Found",
\r\n\r\n\x20\tath"\x20:\x20\t/\r\n\r\n}%r(RTSP SF:Request,42,"HTTP/
1.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\ SF:r\nConnection:
\x20close\r\n\r\n"); Device type: general purpose|storage-misc|firewall Running (JUST
GUESSING): Linux 4.X|2.6.X|3.X (86%), Synology DiskStation Manager 5.X (86%),
WatchGuard Firewall 11.X (86%) OS CPE: cpe:/o:linux:linuxkernel:4.0 cpe:/
o:linux:linuxkernel:2.6.32 cpe:/o:linux:linuxkernel:3.10 cpe:/o:linux:linuxkernel cpe:/
a:synology:diskstationmanager:5.1 cpe:/o:watchguard:fireware:11.8 Aggressive OS
guesses: Linux 4.0 (86%), Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (86%), Linux 3.5
(86%), Linux 4.2 (86%), Linux 4.4 (86%), Synology DiskStation Manager 5.1 (86%),
WatchGuard Firewall 11.8 (86%), Linux 2.6.35 (85%), Linux 3.10 (85%) No exact OS
matches for host (test conditions non-ideal). Network Distance: 27 hops Service Info: OS:
Linux; CPE: cpe:/o:linux:linux_kernel

```

TRACEROUTE (using port 80/tcp) HOP RTT ADDRESS 1 0.02 ms 172.17.0.1 2 ... 26 27  
244.65 ms 4.247.148.163

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> . Nmap done: 1 IP address (1 host up) scanned in 365.91 seconds  
Running vulnerability scanning using basic nmap scripts - SQL Injection... Starting Nmap 7.92 ( <https://nmap.org> ) at 2023-09-28 07:26 UTC Nmap scan report for 4.247.148.163  
Host is up (0.26s latency).

PORT STATE SERVICE 8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds Running vulnerability scanning using CSS nmap script... Starting Nmap 7.92 ( <https://nmap.org> ) at 2023-09-28 07:26 UTC Nmap scan report for 4.247.148.163 Host is up (0.24s latency).

PORT STATE SERVICE 8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds

# ZAP Full Scan Report

- Site: <http://4.247.148.163:8080> **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/WebGoat/login>
  - **Storable and Cacheable Content** [10049] total: 4:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/sitemap.xml>
    - <http://4.247.148.163:8080/WebGoat/login>
  - **User Agent Fuzzer** [10104] total: 12:
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - ..

View the [following link](#) to download the report. RunnerID:6335693005

# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO

# Snyk Report

## **Snyk\_scan**

Go to <https://app.snyk.io/org/pradyumna-muppirala> for full report of Snyk with Github SSO

# Pytest-Playwright Test Output Issue

## Playwright

### pytest

Starting pytest.... ===== test session starts  
===== platform linux -- Python 3.10.12,  
pytest-7.4.2, pluggy-1.3.0 rootdir: /home/runner/work/ASTICI/ASTICI plugins:  
asyncio-0.21.1, tornasync-0.6.0.post2, base-url-2.0.0, playwright-0.4.2, anyio-4.0.0,  
trio-0.8.0 asyncio: mode=strict collected 5 items

src/testAsyncWebGoatUseCases.py ... [ 60%] src/testWebGoatUseCases.py .. [100%]

===== 5 passed in 28.78s

===== Stop pytest....

# ZAP Full Scan Report

- Site: <http://20.193.229.71:8080> **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
  - **Cookie Slack Detector** [90027] total: 2:
    - <http://20.193.229.71:8080/WebGoat/login>
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Base64 Disclosure** [10094] total: 1:
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
  - **Non-Storable Content** [10049] total: 1:
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - <http://20.193.229.71:8080/>
    - <http://20.193.229.71:8080/robots.txt>
    - <http://20.193.229.71:8080/WebGoat/login>
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - <http://20.193.229.71:8080/>
    - <http://20.193.229.71:8080/robots.txt>
    - <http://20.193.229.71:8080/WebGoat/login>
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - <http://20.193.229.71:8080/>
    - <http://20.193.229.71:8080/robots.txt>
    - <http://20.193.229.71:8080/WebGoat/login>
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - <http://20.193.229.71:8080/>
    - <http://20.193.229.71:8080/robots.txt>
    - <http://20.193.229.71:8080/WebGoat/login>
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
  - **Session Management Response Identified** [10112] total: 2:
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
    - <http://20.193.229.71:8080/WebGoat/start.mvc>
  - **Storable and Cacheable Content** [10049] total: 4:
    - <http://20.193.229.71:8080/>
    - <http://20.193.229.71:8080/robots.txt>
    - <http://20.193.229.71:8080/sitemap.xml>
    - <http://20.193.229.71:8080/WebGoat/login>
  - **User Agent Fuzzer** [10104] total: 24:
    - <http://20.193.229.71:8080/WebGoat>
    - <http://20.193.229.71:8080/WebGoat>
    - <http://20.193.229.71:8080/WebGoat>
    - <http://20.193.229.71:8080/WebGoat>
    - <http://20.193.229.71:8080/WebGoat>
    - ..



View the [following link](#) to download the report. RunnerID:6333630416

- Site: <http://4.247.148.163:8080> **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - <http://4.247.148.163:8080/WebGoat/registration>
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - <http://4.247.148.163:8080/WebGoat/registration>
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - <http://4.247.148.163:8080/WebGoat/registration>
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - <http://4.247.148.163:8080/WebGoat/registration>
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/sitemap.xml>
    - <http://4.247.148.163:8080/WebGoat/registration>
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/sitemap.xml>
    - <http://4.247.148.163:8080/WebGoat/registration>
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/sitemap.xml>
    - <http://4.247.148.163:8080/WebGoat/registration>
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/sitemap.xml>
    - <http://4.247.148.163:8080/WebGoat/registration>
  - **Storable and Cacheable Content** [10049] total: 4:
    - <http://4.247.148.163:8080/>
    - <http://4.247.148.163:8080/robots.txt>
    - <http://4.247.148.163:8080/sitemap.xml>
    - <http://4.247.148.163:8080/WebGoat/registration>
  - **User Agent Fuzzer** [10104] total: 12:
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - <http://4.247.148.163:8080/WebGoat>
    - ..

View the [following link](#) to download the report. RunnerID:6335693005

# Metasploit-ParrotOS Test output

## parrotOS metasploit

Interactive Application Security Testing : Making sure that parrot OS docker image has all the latest updates... Get:1 https://deb.parrot.sh/parrot parrot InRelease [14.6 kB] Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB] Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB] Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB] Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB] Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB] Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [524 kB] Get:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B] Get:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1147 kB] Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB] Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB] Fetched 19.9 MB in 2s (9245 kB/s) Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Hit:1 https://deb.parrot.sh/parrot parrot InRelease Hit:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease Hit:3 https://deb.parrot.sh/parrot parrot-backports InRelease Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Cleaning up any existing old code copies of security tests...

## find a way to read it from secure place.

This is not a secure way to check out code;

## Getting the latest code copy for all security tests...

## Metasploit Framework Exploit Demo :

Target Web Goat Instance IP Address : 20.193.229.71

# Possible Metasploit exploits or auxiliaries or payloads, that can used for attacking

```
[*] Processing ./src/exploitwildflydirtraversal.rc for ERB directives. resource (./src/exploitwildflydirtraversal.rc)> use auxiliary/scanner/http/wildflytraversal resource (./src/exploitwildflydirtraversal.rc)> show options
```

Module options (auxiliary/scanner/http/wildfly\_traversal):

Name	Current	Setting	Required	Description	-----	Proxies
chain	no	A				
format	type:host:port[,type:host:port][...]			RELATIVEFILEPATH		
standalone	yes			Relative path to the file to read RHOSTS		
target	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>			RHOSTS		
RPORT	8080	yes		The target port (TCP)		
SSL	false	no		Negotiate SSL/TLS for outgoing connections		
THREADS	1	yes		The number of concurrent threads (max one per host)		
TRAVERSAL_DEPTH	1	yes		Traversal depth		
VHOST	no			HTTP server virtual host		

View the full module info with the info, or info -d command.

```
[*] resource (./src/exploitwildflydirtraversal.rc)> Ruby Code (57 bytes) RHOSTS => resource (./src/exploitwildflydirtraversal.rc)> run [-] Msf::OptionValidateError The following options failed to validate: RHOSTS
```

**resource (./src/exploitwildflydir\_traversal.rc)> exit**

# Nmap-ParrotOS Scan output

## parrotOS

### nmap

Nmap vulnerability scanning for 20.193.229.71 Making sure that parrot OS docker image has all the latest updates... Get:1 https://deb.parrot.sh/parrot parrot InRelease [14.6 kB] Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB] Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB] Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB] Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB] Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB] Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [524 kB] Get:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B] Get:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1147 kB] Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB] Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB] Fetched 19.9 MB in 3s (6128 kB/s) Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Reading package lists... Building dependency tree... Reading state information... Calculating upgrade... The following packages will be upgraded: bind9-dnsutils bind9-host bind9-libs dnsutils file libaom0 libgssapi-krb5-2 libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0 libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 openssh-client openssh-server openssh-sftp-server openssl python3-typing-extensions 23 upgraded, 0 newly installed, 0 to remove and 0 not upgraded. Need to get 9186 kB of archives. After this operation, 63.5 kB disk space will be freed. Do you want to continue? [Y/n] Abort. Hit:1 https://deb.parrot.sh/parrot parrot InRelease Hit:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease Hit:3 https://deb.parrot.sh/parrot parrot-backports InRelease Reading package lists... Building dependency tree... Reading state information... 23 packages can be upgraded. Run 'apt list --upgradable' to see them. Running basic nmap scan... Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-28 02:09 UTC Nmap scan report for 20.193.229.71 Host is up (0.23s latency). Not shown: 65521 filtered tcp ports (no-response) PORT STATE SERVICE VERSION 21/tcp closed ftp 22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0) | ssh-hostkey: | 256 5e:ed:a1:cd:2f:be:fd:6c:53:0a:ce:d4:01:0b:ca:f2 (ECDSA) |\_ 256 75:33:de:48:ae:d0:5a:42:9d:47:45:d3:88:ec:c0:d8 (ED25519) 80/tcp closed http 111/tcp closed rpcbind 135/tcp closed msrpc 143/tcp closed imap 443/tcp closed https 587/tcp closed submission 993/tcp closed imaps 995/tcp closed pop3s 1025/tcp closed NFS-or-IIS 3306/tcp closed mysql 8080/tcp open http-proxy |http-title: Site doesn't have a title. | fingerprint-strings: | FourOhFourRequest: | HTTP/1.1 404 Not Found | Connection: close | Content-Length: 0 | Date: Thu, 28 Sep 2023 02:13:23 GMT | GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, Socks5, TLSSessionReq, TerminalServerCookie, WMSRequest, oracle-tns: | HTTP/1.1 400 Bad Request | Content-Length: 0 | Connection: close | GetRequest: | HTTP/1.1 404 Not Found | Connection: close | Content-Length: 0 | Date: Thu, 28 Sep 2023 02:13:21 GMT | HTTPOptions: | HTTP/1.1 404 Not Found | Connection: close | Content-Length: 0 | Date: Thu, 28 Sep 2023 02:13:22 GMT 9090/tcp open zeus-admin? | fingerprint-strings: | GenericLines, RTSPRequest, SqueezeCenterCLI, WMSRequest, ibm-db2-das: | HTTP/1.1 400 Bad Request | Content-Length: 0 | Connection: close | GetRequest: | HTTP/1.1 404 Not Found | Expires: 0 | Cache-Control: no-cache, no-store, max-age=0, must-revalidate | X-XSS-Protection: 1; mode=block | Pragma: no-cache | X-

Frame-Options: DENY | Date: Thu, 28 Sep 2023 02:13:21 GMT | Connection: close | Vary: Origin | Vary: Access-Control-Request-Method | Vary: Access-Control-Request-Headers | X-Content-Type-Options: nosniff | Content-Type: application/json | "timestamp" : "2023-09-28T02:13:21.961+00:00", | "status" : 404, | "error" : "Not Found", | "path" : "/" | HTTPOptions: | HTTP/1.1 404 Not Found | Expires: 0 | Cache-Control: no-cache, no-store, max-age=0, must-revalidate | X-XSS-Protection: 1; mode=block | Pragma: no-cache | X-Frame-Options: DENY | Date: Thu, 28 Sep 2023 02:13:39 GMT | Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH | Connection: close | Vary: Origin | Vary: Access-Control-Request-Method | Vary: Access-Control-Request-Headers | X-Content-Type-Options: nosniff | Content-Type: application/json | "timestamp" : "2023-09-28T02:13:39.903+00:00", | "status" : 404, | "error" : "Not Found", | "path" : "/"

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)===== SF-Port8080-

TCP:V=7.92%I=7%D=9/28%Time=6514E142%P=x8664-pc-linux-gnu%(Ge SF:tRequest, 65,"HTTP/1.1|x20404|x20Not|x20Found\r\nConnection:\x20close\r SF:\nContent-Length:\x200\r\nDate:\x20Thu,\x2028\x20Sep\x202023\x2002:13:2 SF:1\x20GMT\r\n\r\n") %r(HTTPOptions,65,"HTTP/1.1|x20404|x20Not|x20Found\r SF:\nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Thu,\x2028\x SF:20Sep\x202023\x2002:13:22\x20GMT\r\n\r\n")%r(RTSPRequest,42,"HTTP/1.1| SF:x20400|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20clos SF:e\r\n\r\n")%r(FourOhFourRequest,65,"HTTP/1.1|x20404|x20Not|x20Found\r SF:nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Thu,\x2028\x2 SF:0Sep\x202023\x2002:13:23\x20GMT\r\n\r\n")%r(Socks5,42,"HTTP/1.1|x20400 SF:\x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n SF:r\n") %r(GenericLines,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nContent- SF:Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(Help,42,"HTTP/1.1|x20 SF:400|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r SF:\n\r\n") %r(SSLSessionReq,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nCont SF:ent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(TerminalServerCook SF:ie,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nContent-Length:\x200\r\nCo SF:nnection:\x20close\r\n\r\n")%r(TLSSessionReq,42,"HTTP/1.1|x20400|x20Ba SF:d|x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")% SF:r(Kerberos,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nContent-Length:\x2 SF:00\r\nConnection:\x20close\r\n\r\n")%r(SMBProgNeg,42,"HTTP/1.1|x20400| SF:x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\nr SF:\n") %r(LPDString,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nContent-Leng SF:th:\x200\r\nConnection:\x20close\r\n\r\n")%r(LDAPSearchReq,42,"HTTP/1. SF:1|x20400|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20cl SF:ose\r\n\r\n")%r(SIPOptions,42,"HTTP/1.1|x20400|x20Bad|x20Request\r\nCo SF:ntent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(WMSRequest,42,"H SF:TTP/1.1|x20400|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection SF::\x20close\r\n\r\n")%r(oracle-tns,42,"HTTP/1.1|x20400|x20Bad|x20Reques SF:t\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n");

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)===== SF-Port9090-

TCP:V=7.92%I=7%D=9/28%Time=6514E142%P=x8664-pc-linux-gnu%(Ge SF:tRequest, 1EF,"HTTP/1.1|x20404|x20Not|x20Found\r\nExpires:\x200\r\nCach SF:e-Control:\x20no-cache,\x20no-store,\x20max-age=0,\x20must-revalidate\r SF:\nX-XSS-Protection:\x201;\x20mode=block\r\nPragma:\x20no-cache\r\nX-Fra SF:me-Options:\x20DENY\r\nDate:\x20Thu,\x2028\x20Sep\x202023\x2002:13:21\x SF:20GMT\r\nConnection:\x20close\r\nVary:\x20Origin\r\nVary:\x20Access-Con SF:trol-Request-Method\r\nVary:\x20Access-Control-Request-Headers\r\nX-Con SF:tent-Type-Options:\x20nosniff\r\nContent-Type:\x20application/json\r\n SF:r\n{ \n\x20\x20"timestamp"\x20:\x20"2023-09-28T02:13:21.961+00:00" SF:,\n\x20\x20"status"\x20:\x20404,\n\x20\x20"error"\x20:\x20"Not\x20 SF:Found",\n\x20\x20"path"\x20:\x20"/\n}\n")%r(WMSRequest,42,"HTTP/1. SF:1|x20400|x20Bad|x20Request\r\nContent-Length:\x200\r\nConnection:\x20cl

SF:ose\r\n\r\n")%r(ibm-db2-das,42,"HTTP/1.1\x20400\x20Bad\x20Request\r\nC SF:ontent-  
Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(SqueezeCenterC SF:LI,42,"HTTP/  
1.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nCo SF:nnection:  
\x20close\r\n\r\n")%r(GenericLines,42,"HTTP/1.1\x20400\x20Bad SF:  
\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r SF:  
(HTTPOptions,22B,"HTTP/1.1\x20404\x20Not\x20Found\r\nExpires:\x200\r\n SF:Cache-  
Control:\x20no-cache,\x20no-store,\x20max-age=0,\x20must-revalida SF:tel\r\nX-XSS-  
Protection:\x201;\x20mode=block\r\nPragma:\x20no-cache\r\nX SF:-Frame-Options:  
\x20DENY\r\nDate:\x20Thu,\x2028\x20Sep\x202023\x2002:13: SF:39\x20GMT\r\nAllow:  
\x20GET,\x20HEAD,\x20POST,\x20PUT,\x20DELETE,\x20TRA SF:CE,\x20OPTIONS,  
\x20PATCH\r\nConnection:\x20close\r\nVary:\x20Origin\r\n SF:Vary:\x20Access-Control-  
Request-Method\r\nVary:\x20Access-Control-Reque SF:st-Headers\r\nX-Content-Type-  
Options:\x20nosniff\r\nContent-Type:\x20ap SF:plication/  
json\r\n\r\n{\r\n\r\n\x20\x20"timestamp"\r\n\r\n\x20:\x20\x20"2023-09-28T02: SF:13:39.903+00:00",  
\r\n\r\n\x20\x20"status"\r\n\r\n\x20:\x20\x20404,\r\n\r\n\x20\x20"error" SF:"\r\n\r\n\x20:\x20\x20"Not\x20Found",  
\r\n\r\n\x20\x20"path"\r\n\r\n\x20:\x20\x20"/"\r\n\r\n}"}%r(RTSP SF:Request,42,"HTTP/  
1.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\ SF:r\r\nConnection:  
\x20close\r\n\r\n"); OS fingerprint not ideal because: Didn't receive UDP response. Please  
try again with -sSU No OS matches for host Network Distance: 2 hops Service Info: OS:  
Linux; CPE: cpe:/o:linux:linuxkernel

TRACEROUTE (using port 80/tcp) HOP RTT ADDRESS 1 0.02 ms 172.17.0.1 2 5480.66 ms  
20.193.229.71

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> . Nmap done: 1 IP address (1 host up) scanned in 364.33 seconds  
Running vulnerability scanning using basic nmap scripts - SQL Injection... Starting Nmap  
7.92 ( <https://nmap.org> ) at 2023-09-28 02:15 UTC Nmap scan report for 20.193.229.71  
Host is up (0.23s latency).

PORT STATE SERVICE 8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds Running vulnerability  
scanning using CSS nmap script... Starting Nmap 7.92 ( <https://nmap.org> ) at 2023-09-28  
02:15 UTC Nmap scan report for 20.193.229.71 Host is up (0.24s latency).

PORT STATE SERVICE 8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds

# ZAP Full Scan Report

- Site: <http://20.193.229.71:8080> **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - <http://20.193.229.71:8080/>
    - <http://20.193.229.71:8080/robots.txt>
    - <http://20.193.229.71:8080/sitemap.xml>
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - <http://20.193.229.71:8080/>
    - <http://20.193.229.71:8080/robots.txt>
    - <http://20.193.229.71:8080/sitemap.xml>
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - <http://20.193.229.71:8080/>
    - <http://20.193.229.71:8080/robots.txt>
    - <http://20.193.229.71:8080/sitemap.xml>
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - <http://20.193.229.71:8080/>
    - <http://20.193.229.71:8080/robots.txt>
    - <http://20.193.229.71:8080/sitemap.xml>
    - <http://20.193.229.71:8080/WebGoat/login>
  - **Storable and Cacheable Content** [10049] total: 4:
    - <http://20.193.229.71:8080/>
    - <http://20.193.229.71:8080/robots.txt>
    - <http://20.193.229.71:8080/sitemap.xml>
    - <http://20.193.229.71:8080/WebGoat/login>
  - **User Agent Fuzzer** [10104] total: 12:
    - <http://20.193.229.71:8080/WebGoat>
    - <http://20.193.229.71:8080/WebGoat>
    - <http://20.193.229.71:8080/WebGoat>
    - <http://20.193.229.71:8080/WebGoat>
    - <http://20.193.229.71:8080/WebGoat>
    - ..

View the [following link](#) to download the report. RunnerID:6333630416

# Sonar Cloud Code Scan Report

## **SonarQube Cloud code scan**

Go to [https://sonarcloud.io/project/overview?id=pradyumna-muppirala\\_WebGoatSAST](https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST) for full report of SonarCloud with Github SSO



# Snyk Report

## **Snyk\_scan**

Go to <https://app.snyk.io/org/pradyumna-muppirala> for full report of Snyk with Github SSO