CSVS PMA

Student ID or IDs for group work	2126529

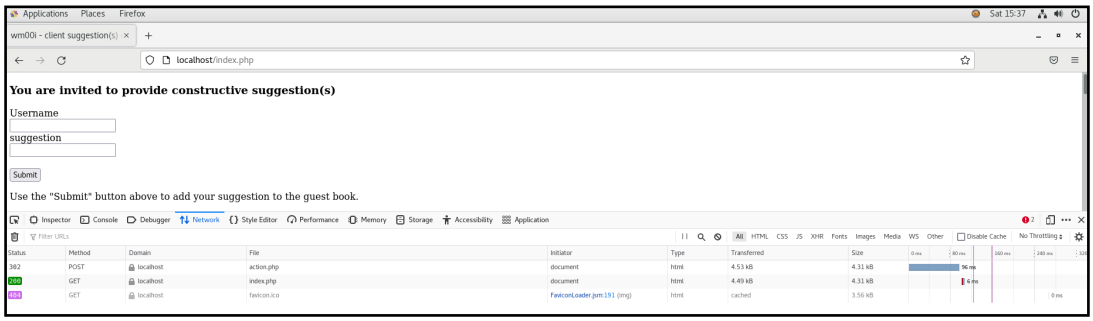
Date set	17th February 2023
Submission date (excluding extensions)	20th March 2023 by 12:00pm (UK time)
Submission guidance	To be submitted electronically via Tabula. Three files of various types to be submitted.
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late. For Postgraduate students only, who started their current course
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More

Module title & code	wm00i - 15 Cyber Security for Virtualisation Systems
Module owner	Peter Norris
Module tutor	Peter Norris
Module marker	Peter Norris
Assessment type	Docker hardening
Weighting of mark	100%

Section1: Set of test cases interactions

Pressure Test (csvs/scripts/u2126529_pressure-test.sh)

- The http status codes can be seen from the webpage and the operation process includes 200 (get) and 302 (post)
- Add the test cases to confirm whether the sent information is received accurately
- The test cases of the database is also identified from http status to confirm the functions



Security Test (csvs/scripts/u2126529_security-test.sh)

- Enter the container to perform high-risk command operations

Section2: Reasoning and evidence for image hardening & image generation

Image hardening (csvs/builds/dbserver/Dockerfile)

- Change db owner from default root to user in dockerfile of dbserver to increase system security

```
# Database Dockerfile

FROM mariadb:10

COPY configfiles/mysqld.cnf  /mysql/mysql.conf.d/mysqld.cnf

# assign user
USER mysql

EXPOSE 3306
```

```
[csc@localhost dbserver]$ docker exec -it u2126529_csvs2023-db_c /bin/bash
bash-5.1$ id -un
mysql
bash-5.1$
```

Image generation (csvs/scripts/u2126529_build-script.sh)

- Generate two original images and images after thinning
- Slimming images are made using docker slims tools [1]
- After running the slimmed images, I find that the containers cannot be started. We debug the logs that come out when starting the containers and add the necessary files and paths to complete the images slims

```
#Build web images
cd ../builds/webserver
docker build . --tag u2126529/csvs2023-web_i
#Build db images
cd ../dbserver
docker build . --tag u2126529/csvs2023-db_i


#Strip
#Docker slim install
curl -sL https://raw.githubusercontent.com/slimtoolkit/slim/master/scripts/install-slim.sh | sudo -E bash -

#manual type csc

#Build webslim images
slim build --target u2126529/csvs2023-web_i:latest --include-path '/var/lib/nginx/tmp/client_body' --include-path '/usr/share/nginx/html' --tag u2126529/csvs2023-web_i.slim

#Build dbslim images
slim build --target u2126529/csvs2023-db_i:latest --http-probe-off --include-path '/etc/mysql/conf.d' --include-path '/run/mysqld/' --tag u2126529/csvs2023-db_i.slim
#Press enter

#list images
docker images
```

Section3: Reasoning and evidence for runtime hardening & verification

Selinux (csvs/builds/webserver/u2126529_web.te)

- Refer to the logs during the audit, add the necessary policy and test it in a loop, so that the container can successfully complete the function of the web page with the minimum permission of selinux
- When the selinux of the web does not add **dac_override**, we will find an error when you open the web page

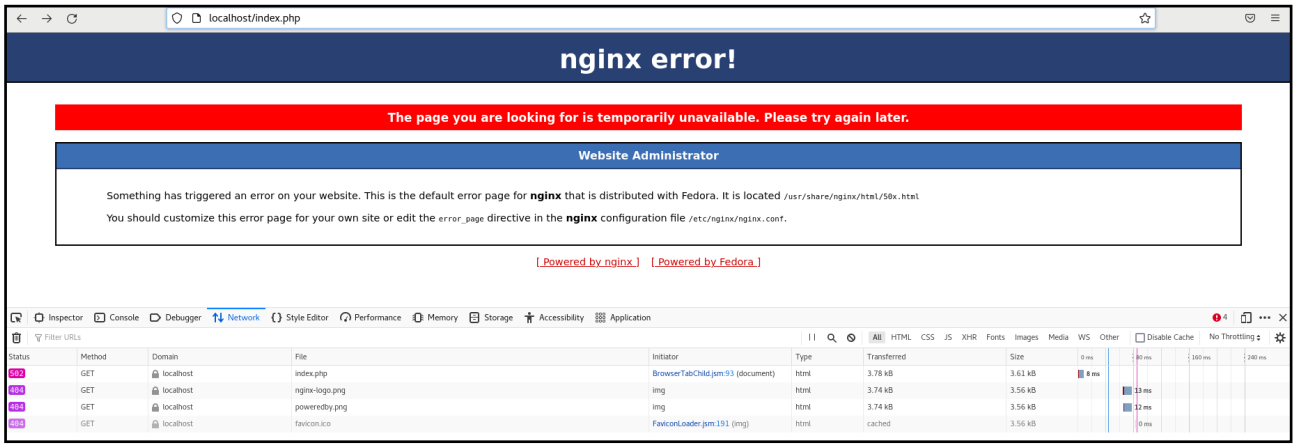
```
#    https://opensource.com/article/18/2/understanding-selinux-labels-container-runtimes

# This template interface creates the u2126529_web_t type as a
# type which can be run as a docker container. To see what it does, look in
# /usr/share/selinux/devel/include/contrib/virt.if
virt_sandbox_domain_template(u2126529_web);

################ put audit2allow rules in here ##############
require {
        type http_port_t;
        type node_t;
        type u2126529_web_t;
        type mysqld_port_t;
        type user_home_t;
        class capability { chown net_bind_service setgid setuid dac_override};
        class tcp_socket { bind create listen name_bind node_bind setopt accept read write connect getattr name_connect getopt};
        #class file { open read };

}
#============= u2126529_web_t ==============
allow u2126529_web_t http_port_t:tcp_socket name_bind;
allow u2126529_web_t node_t:tcp_socket node_bind;
allow u2126529_web_t self:capability { chown net_bind_service setgid setuid dac_override};
allow u2126529_web_t self:tcp_socket { bind create listen name_bind node_bind setopt accept read write connect getattr name_connect getopt};
allow u2126529_web_t mysqld_port_t:tcp_socket name_connect;
#allow u2126529_web_t user_home_t:file { open read };

################ end audit2allow additions #################
```



Seccomp (csvs/scripts/u2126529_build-minimal-syscalls-web.sh, csvs/builds/webserver/u2126529_web.json)

- The http status codes can be seen from the webpage and the operation process includes 200 (get) and 302 (post)
- Add the test cases to confirm whether the sent information is received accurately
- The test cases of the database is also identified from http status to confirm the functions
- If test case without an error page test, the web server will lack **the syscall of sendfile**, resulting in the inability to jump out of the 404 error screen

Applications Places Text Editor Sat 16:24

Open u2126529_build-minimal-sycalls-web.sh ~/Desktop/csvs/scripts Save

u2126529_web.te | u2126529_db.te | process | Dockerfile | u2126529_repeated-run-script.sh | u2126529_build-minimal-sycalls-web.sh

```
  docker run -d --rm --net u2126529/csvs2023_n --ip 203.0.113.200 --hostname www.cyber23.test --add-host db.cyber23.test:203.0.113.201 -p 80:80 --name u2126529_csvs2023-web_c \
--security-opt label:type:u2126529_web_t \
--security-opt seccomp:tmp.json u2126529/csvs2023-web_i


  # Wait for container to start
  sleep 5s

  # Send POST request
  value=$RANDOM
  echo $value
  Post_response=$(curl --write-out "%{http_code}" --silent --output /dev/null --max-time 3 -X POST -d "fullname=$value&suggestion=$value" http://localhost/action.php)
  echo $Post_response

  # Send GET request
  Get_response=$(curl --write-out "%{http_code}" --silent --output /dev/null --max-time 3 http://localhost/index.php)
  echo $Get_response

  # Send value request
  Get_value=$(curl --silent --max-time 3 http://localhost/index.php | grep -o "$value")
  echo $Get_value


  # Send error request
  Get_error=$(curl -s --max-time 3 http://localhost/index.php/12345 | grep -o "error")
  echo $Get_error


  if [[ $Get_response -eq 200 && $Get_value == *"$value"* && $Post_response -eq 302 && $Get_error == *"error"* ]]; then
    echo "$s is running properly, do nothing"

  else
    echo "$s is not success, adding to list-of-min-syscalls"
    echo $s >> list-of-min-syscalls

  fi

  # kill docker
  docker kill u2126529_csvs2023-web_c

done < ./moby-syscalls
```

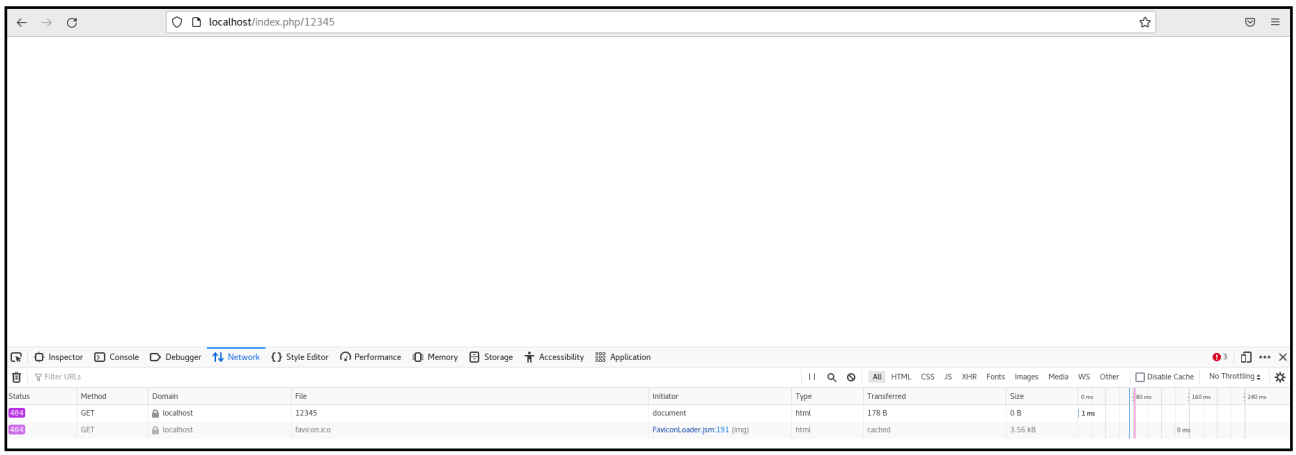
Applications Places Text Editor Sat 16:26

Open u2126529_web.json ~/Desktop/csvs/builds/webserver Save

u2126529_web.te | u2126529_db.te | process | u2126529_repeated-run-script.sh | u2126529_web.json

```
"ioperm",
"listen",
"lstat",
"mkdir",
"mmap",
"mprotect",
"newfstatat",
"open",
"openat",
"poll",
"prctl",
"pread64",
"ptrace",
"read",
"readv",
"recvfrom",
"rt_sigaction",
"rt_sigprocmask",
"rt_sigreturn",
"s390_runtime_instr",
"sendfile",
"sendto",
"setgid",
"setgroups",
"set_mempolicy",
"setsid",
"setsockopt",
"set_tls",
"setuid",
"shutdown",
"socket",
"socketpair",
"stat",
"uname",
"unshare",
"wait4",
"write",
"writev",
"getcwd"


                    ],
                    "action": "SCMP_ACT_ALLOW",
                    "args": [],
```


localhost/index.php/12345
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Disable Cache
No Throttling
Status
Method
Domain
File
Initiator
Type
Transferred
Size
404
GET
localhost
12345
document
html
178 B
0 B
1 ms
404
GET
localhost
favicon.ico
FaviconLoader.jsm:191 (img)
html
cached
3.56 kB
0 ms

Capability (csvs/scripts/u2126529_repeated-run-script.sh)

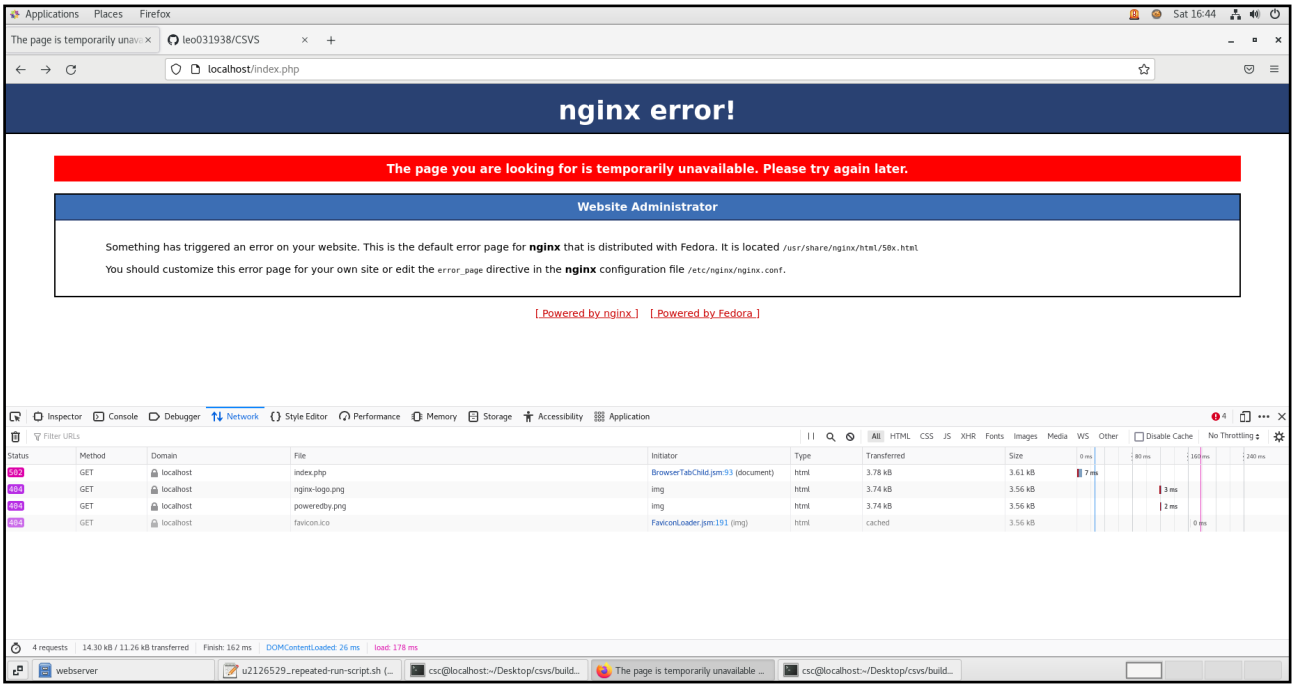
- Add capabilities found from the audit logs of selinux
- Db server does not require capabilities
- If the web does not add **dac_override**, the page will not be displayed correctly

```
#Run webserver
cd ../builds/webserver
docker run -d --rm --net u2126529/csvs2023_n --ip 203.0.113.200 --hostname www.cyber23.test --add-host db.cyber23.test:203.0.113.201 -p 80:80 --name u2126529_csvs2023-web_c \
--security-opt label:type:u2126529_web_t \
--security-opt seccomp:u2126529_web.json \
--cap-drop=ALL \
--cap-add=chown \
--cap-add=net_bind_service \
--cap-add=dac_override \
--cap-add=setgid \
--cap-add=setuid \
u2126529/csvs2023-web_i.slim



#Run dbserver
cd ../dbserver
docker run -d --rm --net u2126529/csvs2023_n --ip 203.0.113.201 --hostname db.cyber23.test -e MYSQL_ROOT_PASSWORD="CorrectHorseBatteryStaple" -e MYSQL_DATABASE="csvs23db" --name u2126529_csvs2023-db_c \
--security-opt label:type:u2126529_db_t \
--security-opt seccomp:u2126529_db.json \
--cap-drop=ALL \
-v mysql_volume:/var/lib/mysql \
u2126529/csvs2023-db_i.slim

#list images
docker images
```



Volume (csvs/scripts/u2126529_repeated-run-script.sh)

- After the volume is created and mounted, the database needs to be imported for the first time, and there is no need to import it later
- The data will continue to exist and complete the function of persistence

```
Applications  Places  Terminal                                                    Sat 16:49
csc@localhost:~/Desktop/csvs/builds/webserver
File  Edit  View  Search  Terminal  Help
[csc@localhost webserver]$ docker volume inspect mysql_vol
[
    {
        "CreatedAt": "2023-03-24T22:55:57Z",
        "Driver": "local",
        "Labels": {},
        "Mountpoint": "/var/lib/docker/volumes/mysql_vol/_data",
        "Name": "mysql_vol",
        "Options": {},
        "Scope": "local"
    }
]
[csc@localhost webserver]$
```

```
Applications  Places  Text Editor                                                 Sat 16:46
Open   u2126529_repeated-run-script.sh   Save
~/Desktop/csvs/scripts
u2126529_web.te   process   u2126529_repeated-run-script.sh

#Run webserver
cd ../builds/webserver
docker run -d --rm --net u2126529/csvs2023_n --ip 203.0.113.200 --hostname www.cyber23.test --add-host db.cyber23.test:203.0.113.201 -p 80:80 --name u2126529_csvs2023-web_c \
--security-opt label:type:u2126529_web_t \
--security-opt seccomp:u2126529_web.json \
--cap-drop=ALL \
--cap-add=chown \
--cap-add=net_bind_service \
--cap-add=dac_override \
--cap-add=setgid \
--cap-add=setuid \
u2126529/csvs2023-web_i.slim


#Run dbserver
cd ../dbserver
docker run -d --rm --net u2126529/csvs2023_n --ip 203.0.113.201 --hostname db.cyber23.test -e MYSQL_ROOT_PASSWORD="CorrectHorseBatteryStaple" -e MYSQL_DATABASE="csvs23db" --name u2126529_csvs2023-db_c \
--security-opt label:type:u2126529_db_t \
--security-opt seccomp:u2126529_db.json \
--cap-drop=ALL \
-v mysql_volume:/var/lib/mysql \
u2126529/csvs2023-db_i.slim

#list images
docker images
```

Section4: Additional part

The table below presents the options for completion:

	Web	**DB**
Selinux	V	V
Seccomp	V	V
Capabilities	V	V
Strip	V	V
User	N/A	V
Volumn	N/A	V

References:

[1] GitHub. (2023). Optimize Your Experience with Containers. Make Your Containers Better, Smaller, More Secure and Do Less to Get There (free and open source!). [online] Available at: https://github.com/slimtoolkit/slim.