

CSC 154 Lab 06-1

Task 1

1)

I started by getting Apache up and running on my Ubuntu VM, like setting up my own little corner of the internet.

```
Get:22 http://us.archive.ubuntu.com/ubuntu jammy-updates/multiverse i386 Packages [6,028 B]
Get:23 http://us.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [12.0 kB]
Fetched 12.2 MB in 6s (2,204 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
236 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ubuntu:/# apt update -y
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
236 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ubuntu:/# █
```

```
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
root@ubuntu:/# █
```

```
root@ubuntu:/# systemctl start apache2
root@ubuntu:/# systemctl start apache2
```

The screenshot shows a web browser displaying the Apache2 Default Page for Ubuntu. The page features the Ubuntu logo at the top left, followed by the text "Apache2 Default Page". A prominent orange button with the text "It works!" is centered. Below the button, there is a message about the default welcome page and its purpose. A sidebar on the right is titled "Configuration Overview" and contains a tree view of the Apache configuration directory structure:

```
/etc/apache2/  
|--- apache2.conf  
|   |--- ports.conf  
|--- mods-enabled  
|   |--- *.load  
|   |--- *.conf  
|--- conf-enabled  
|   |--- *.conf  
|--- sites-enabled  
|   |--- *.conf
```

At the bottom of the browser window, there is a navigation bar with icons for back, forward, and refresh, along with a search bar containing the text "localhost".

Kevin March 24

2)

Added self signed TLS certificate for security.

```
Considering dependency mime for ssl:  
Module mime already enabled  
Considering dependency socache_shmcb for ssl:  
Enabling module socache_shmcb.  
Enabling module ssl.  
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create  
elf-signed certificates.  
To activate the new configuration, you need to run:  
    systemctl restart apache2  
root@ubuntu:/# a2enmod ssl  
Considering dependency setenvif for ssl:  
Module setenvif already enabled  
Considering dependency mime for ssl:  
Module mime already enabled  
Considering dependency socache_shmcb for ssl:
```

Kevin Cendana

Spring 202

CSC 154

```
Module socache_shmcb already enabled
Module ssl already enabled
root@ubuntu:/# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@ubuntu:/# █
```

Kevin Cendana

Spring 202

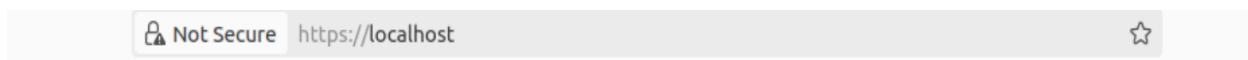
CSC 154

Kevin Cendana

Spring 202

CSC 154

```
root@ubuntu:/# openssl x509 -req -CA root-ca.crt -CAkey root-ca.key -in server.csr -out server.crt -days 365 -CAcreateserial -extfile <(printf "subjectAltName = DNS:localhost\nauthorityKeyIdentifier = keyid,issuer\nbasicConstraints = CA:FALSE\nkeyUsage = digitalSignature, keyEncipherment\\nextendedKeyUsage=serverAuth")  
Certificate request self-signature ok  
subject=C = US, ST = Denial, L = Earth, O = Dis, CN = anything_but_whitespace  
CAcreateserial: command not found  
root@ubuntu:/# openssl x509 -req -CA root-ca.crt -CAkey root-ca.key -in server.csr -out server.crt -days 365 -CAcreateserial -extfile <(printf "subjectAltName = DNS:localhost\nauthorityKeyIdentifier = keyid,issuer\nbasicConstraints = CA:FA  
SE\\nkeyUsage = digitalSignature, keyEncipherment\\nextendedKeyUsage=serverAuth")  
Certificate request self-signature ok  
subject=C = US, ST = Denial, L = Earth, O = Dis, CN = anything_but_whitespace
```



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **localhost**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

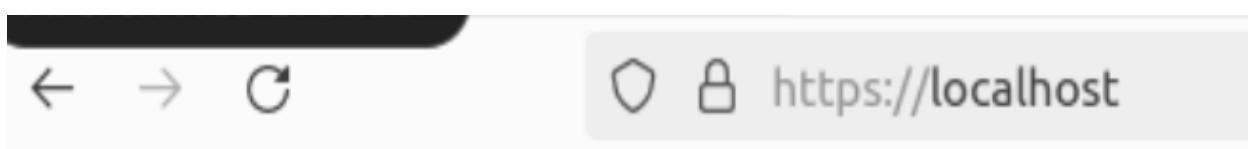
The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

[Learn more...](#)

[Go Back \(Recommended\)](#)

[Advanced...](#)



Kevin March 24

3)

Kevin Cendana

Spring 202

CSC 154

Installed ModSecurity to block any potential intruders.

```
Unpacking liblua5.1-0:amd64 (5.1.5-8.1build4) ...
Selecting previously unselected package libapache2-mod-security2.
Preparing to unpack .../libapache2-mod-security2_2.9.5-1_amd64.deb .
Unpacking libapache2-mod-security2 (2.9.5-1) ...
Selecting previously unselected package modsecurity-crs.
Preparing to unpack .../modsecurity-crs_3.3.2-1_all.deb ...
Unpacking modsecurity-crs (3.3.2-1) ...
Setting up modsecurity-crs (3.3.2-1) ...
Setting up liblua5.1-0:amd64 (5.1.5-8.1build4) ...
Setting up libapache2-mod-security2 (2.9.5-1) ...
apache2_invoke: Enable module security2
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
root@ubuntu:/#
```

```
root@ubuntu:/# mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
root@ubuntu:/#
```

```
root@ubuntu:/# sed -i 's/SecRuleEngine DetectionOnly/SecRuleEngine On/g' /etc/modsecurity/modsecurity.conf
root@ubuntu:/#
```

```
root@ubuntu:/# systemctl restart apache2
root@ubuntu:/#
```

4)

Tested the new security by trying to bypass it with a hack attempt, which failed (successfully!)



https://localhost

Kevin March 24

Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at localhost Port 443

Task 2

1)

Downloaded DVNA, a purposely vulnerable app, so we can learn how to address the issues.

```
Fetched 4,147 kB in 1s (3,194 kB/s)
git clone Selecting previously unselected package liberror-perl.
Reading database ... 227479 files and directories currently installed
Preparing to unpack .../liberror-perl_0.17029-1_all.deb ...
Unpacking liberror-perl (0.17029-1) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1%3a2.34.1-1ubuntu1.10_all.deb ...
Unpacking git-man (1:2.34.1-1ubuntu1.10) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a2.34.1-1ubuntu1.10_amd64.deb ...
Unpacking git (1:2.34.1-1ubuntu1.10) ...
Setting up liberror-perl (0.17029-1) ...
Setting up git-man (1:2.34.1-1ubuntu1.10) ...
Setting up git (1:2.34.1-1ubuntu1.10) ...
Processing triggers for man-db (2.10.2-1) ...
root@ubuntu:/# git clone https://github.com/appsecco/dvna
Cloning into 'dvna'...
remote: Enumerating objects: 645, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 645 (delta 1), reused 2 (delta 0), pack-reused 639
Receiving objects: 100% (645/645), 3.18 MiB | 2.83 MiB/s, done.
Resolving deltas: 100% (279/279), done.
root@ubuntu:/#
```

2)

Downloaded Snyk to help diagnose any possible vulnerabilities.

Enable Snyk Code

To analyze your code for vulnerabilities we temporarily clone the repository or upload your code. Cloned or uploaded code is cached for a maximum of 24h.

With the Snyk Free Plan, Snyk Code offers unlimited scans for open source projects, and limited tests for 1st-party code. [More details on plans](#)



After being enabled, you must import / re-import projects to scan them.

[Save changes](#)

```
snyk-linux.1          [           <=>      ] 98.09M 10.5MB/s  in 9.4s
2024-03-29 23:43:44 (10.4 MB/s) - 'snyk-linux.1' saved [102858752]
```

Authenticate for CLI or IDE

Snyk requires authentication of your machine to associate Snyk CLI or the Snyk IDE plugin with your account.

[Authenticate](#)

3)

Ran an SCA scan with Snyk to find out if there were any known vulnerabilities in the app's components.

```
Organization: kevincendana
Package manager: npm
Open source: yes
Project path: https://github.com/appsecco/dvna
```

```
Tested https://github.com/appsecco/dvna for known vulnerabilities, found 37 vulnerabilities, 53 vulnerable paths.
```

4) Conducted SAST scan to dig deeper into the code, looking for potential security flaws.

```
X [High] Deserialization of Untrusted Data
Path: core/appHandler.js, line 218
Info: Unsanitized input from an uploaded file flows into node-serialize.un
lalize, where it is used to deserialize an object. This may result in an Uns
Deserialization vulnerability.

✓ Test completed

Organization: kevincendana
Test type: Static code analysis
Project path: /dvna

Summary:

37 Code issues found
5 [High] 27 [Medium] 5 [Low]

root@ubuntu:/dvna#
```

Task 3

- 1) Got Docker set up and ran DVNA app running in a container to mess around with safely.

```
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:5 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1,
19 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [602
kB]
Get:7 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages
698 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages
[1,060 kB]
Fetched 4,108 kB in 3s (1,178 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
236 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ubuntu:/dvna#
```

Kevin Cendana

Spring 202

CSC 154

```
Selecting previously unselected package ubuntu-fan.
Preparing to unpack .../5-ubuntu-fan_0.12.16_all.deb ...
Unpacking ubuntu-fan (0.12.16) ...
Setting up runc (1.1.7-0ubuntu1~22.04.2) ...
Setting up bridge-utils (1.7-1ubuntu3) ...
Setting up pigz (2.6-1) ...
Setting up containerd (1.7.2-0ubuntu1~22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/containerd.service →
 /lib/systemd/system/containerd.service.
Setting up ubuntu-fan (0.12.16) ...
Created symlink /etc/systemd/system/multi-user.target.wants/ubuntu-fan.service →
 /lib/systemd/system/ubuntu-fan.service.
Setting up docker.io (24.0.5-0ubuntu1~22.04.1) ...
Adding group `docker' (GID 138) ...
rash
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service →
 /lib/systemd/system/docker.service.
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /lib/
stemd/system/docker.socket.
Processing triggers for man-db (2.10.2-1) ...
root@ubuntu:/dvna#
```

```
root@ubuntu:/dvna# sudo usermod -aG docker $USER
root@ubuntu:/dvna#
```

2) Ran Dastardly to scan the DVNA app while it was running, for any vulnerabilities.

```
eadbf8312262: Pull complete
cf528b18b6ce: Pull complete
075c4f074e90: Pull complete
d0562d9451f1: Pull complete
48671e1607ad: Pull complete
4879e9b180ec: Pull complete
4bcad28e8244: Pull complete
Digest: sha256:2657051b73ac8f879d3a3b419b4618d98e4596a0fe27f8e91582c403541ef1b0
Status: Downloaded newer image for appsecco/dvna:sqlite
b451e56bd1460b2dbce9ec757b3007b6c01cf3cf43d512f0a854bdeec2acdbc6
root@ubuntu:/dvna#
```

3)

Kevin Cendana

Spring 202

CSC 154

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    qdisc default qlen 1000
        link/ether 08:00:27:c3:66:fc brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
            valid_lft 572sec preferred_lft 572sec
        inet6 fe80::d970:dce9:be36:adb1/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    qdisc default
        link/ether 02:42:0d:3e:9f:b5 brd ff:ff:ff:ff:ff:ff
        inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
            valid_lft forever preferred_lft forever
        inet6 fe80::42:dff:fe3e:9fb5/64 scope link
            valid_lft forever preferred_lft forever
5: vethc70bfcd@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
    state UP group default
        link/ether 9a:27:d6:f5:52:8c brd ff:ff:ff:ff:ff:ff link-netnsid 0
        inet6 fe80::9827:d6ff:fe5f:528c/64 scope link
            valid_lft forever preferred_lft forever
root@ubuntu:/dvna#
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
    valid_lft 572sec preferred_lft 572sec
```