Exercise 8.1 - Web Server Security

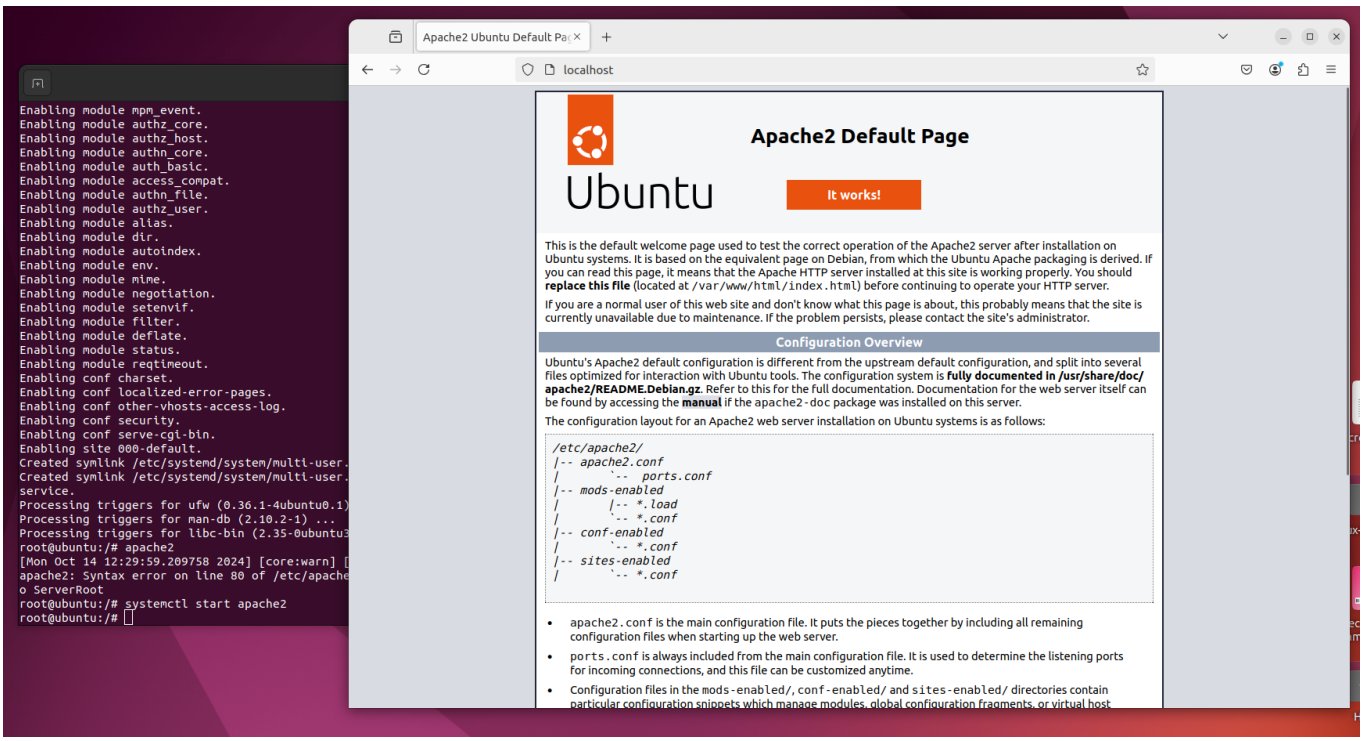
Step 1

```
jordan@ubuntu:~/Downloads$ cd ..
jordan@ubuntu:~$ sudo su
root@ubuntu:/home/jordan# cd /
root@ubuntu:/#
```

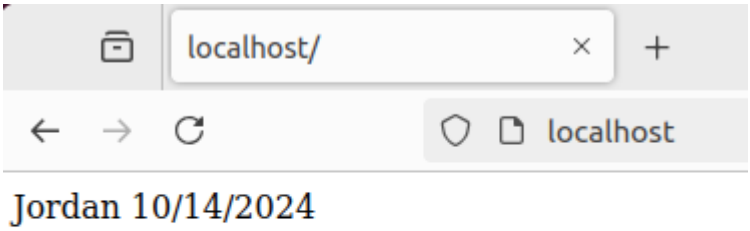
I first swapped to the root directory of my machine to install apache

```
root@ubuntu:/# apache2
[Mon Oct 14 12:29:59.209758 2024] [core:warn] [pid 6889] AH00111: Config variable ${APACHE_RUN_DIR} is not defined
apache2: Syntax error on line 80 of /etc/apache2/apache2.conf: DefaultRuntimeDir must be a valid directory, absolute or relative t
o ServerRoot
root@ubuntu:/#
```

Apache 2 is now installed on my machine



My apache server is now running on my localhost



Echoing to the index.html file displays my name and date onto the web server

Step 2

```
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:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@ubuntu:/# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@ubuntu:/# systemctl restart apache2
root@ubuntu:/#
```

I enabled SSL and default SSL site with apache and restarted my server

```
root@ubuntu:/# openssl req -x509 -nodes -newkey RSA:2048 -keyout root-ca.key -days 365 -out root-ca.crt -subj '/C=US/ST=Denial/L=E
arth/O=Atest/CN=root_CA_for_firefox'
....+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+...........+.......+...+...+...+.....+......+.+...++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..+.......+...+........+......+.........+.........+.........+...
+.....+....+.....+......+......+.+................+......+.......+........+....................+.........+.+...+.....+.+.......
.............+.+...........+...................+......+...+..+...+.........+.+..+....+.....+....+.............+......+.+...+.....
.+...........+...+...+...............+...+.+...........+.........+.+...........+...........+.+...............+........+......+...
......+...............+......+.......+.....+.......+......+..+.......+......+..+...+++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++
..+...+...............+.............+..+....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+......+..+.......+
...+..+...........+...+.......+...+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*..+...+.+.....+..........
.....+....+......+..+...+......+.+..+.......+...+..+..........+........+...............+......+.+.........+.....+.+.....+.+..+...+
...+....+...............+.....+.......+.............+.+...+...+...+...........+....+...........+..+.........+...........+......
+....+.........+...+...+....................+....+........+.......+...+........+.+........+......+....+..+......+.............+..+
.......+...+...+....................+...+.....+.+.....+......+...+.+......+.....+.+.................+......+.+...+..+....+.....+.
........+.........+.....+.+..+.............+.............+...........+................+............+..++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++
-----
root@ubuntu:/#
```

```
bin   cdrom  etc   lib   New Tab   found  mnt  proc  root-ca.crt  run   snap  swapfile  tmp  var
boot  dev    home  lib   Show Menubar      opt  root  root-ca.key  sbin  srv   sys       usr
root@ubuntu:/#
```

I created a private certificate authority and can see the root-cakey and root-ca.crt files are now created

```
root@ubuntu:/# openssl req -nodes -newkey rsa:2048 -keyout server.key -out server.csr -subj '/C=US/ST=Denial/L=Earth/O=Dis/CN=anyt
hing_but_whitespace'
...+...+...+......+.....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.....+.+..+...++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++*.............+..+...+..........+..+.......+......+.........+...+..............+...+.
+............+..+...+...+......+.+..............+....+...........+...+.......+...........+....+...........+.......................
.+...+......+.+...+..................+...+.........+..+...+..........+........+....+......+..+.+..+............+......+.+.........
............+..............+.+............+...+..+.+...........+....+.........+...............+..+.+..................+.+.....+....
.....+......+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
...+..+.+.....+.............+..+.......+......+......+.....+......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+*....+..+............+......+.+...+...........+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.........+..+
...+.+...+...+...+.........+..+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
-----
root@ubuntu:/# ls
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  root-ca.crt  run   server.csr  snap  swapfile  tmp  var
boot  dev    home  lib32  libx32  media       opt  root  root-ca.key  sbin  server.key  srv   sys       usr
root@ubuntu:/#
```

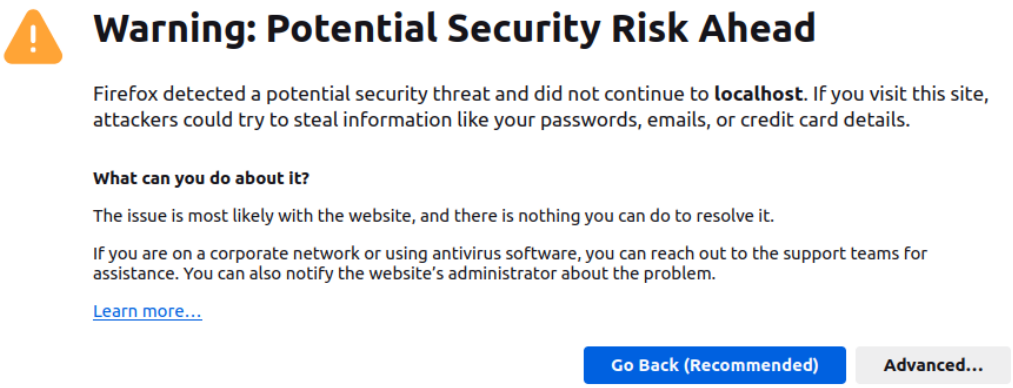
I created a private key and CSR and now see server.cr and server.key

```
root@ubuntu:/# openssl x509 -req -CA root-ca.crt -CAkey root-ca.key -in server.csr -out server.crt -days 365 -CAcreateserial -extf
ile <(printf "subjectAltName = DNS:localhost\nauthorityKeyIdentifier = keyid,issuer\nbasicConstraints = CA:FALSE\nkeyUsage = digit
alSignature, keyEncipherment\nextendedKeyUsage=serverAuth")
Certificate request self-signature ok
subject=C = US, ST = Denial, L = Earth, O = Dis, CN = anything_but_whitespace
root@ubuntu:/# ls
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  root-ca.crt  run   server.crt  server.key  srv   sys  usr
boot  dev    home  lib32  libx32  media       opt  root  root-ca.key  sbin  server.csr  snap        swapfile  tmp  var
root@ubuntu:/#
```

I created TLS self signed certificate and now see server.crt

```
root@ubuntu:/# cp server.crt /etc/ssl/certs/ssl-cert-snakeoil.pem
root@ubuntu:/# cp server.key /etc/ssl/private/ssl-cert-snakeoil.key
root@ubuntu:/# systemctl restart apache2
root@ubuntu:/#
```

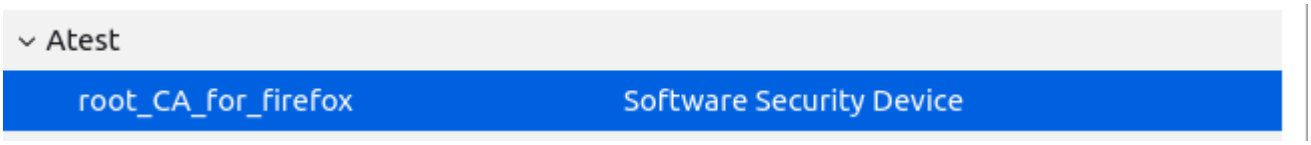
I replaced the default certificate and key for my site



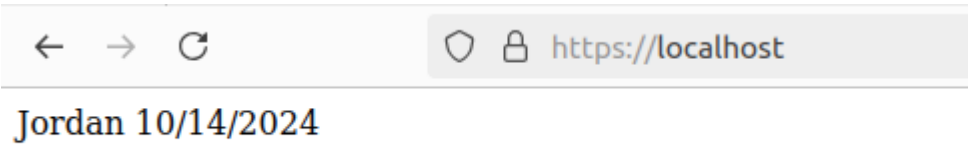
We now get the security risk warning

```
root@ubuntu:/home/jordan/ca# certutil -A -n "My Root CA" -t "C,," -i root-ca.crt -d sql:/home/jordan/snap/firefox/common/.mozilla/
firefox/fq1kgbkr.default/
root@ubuntu:/home/jordan/ca#
```

The instructions never mentioned anything about problems with importing certs with ubuntu firefox but after an hour of troubleshooting I used certutil to directly import the certificate through the terminal.



Now we can finally see the certificate in the cert manager



Jordan 10/14/2024

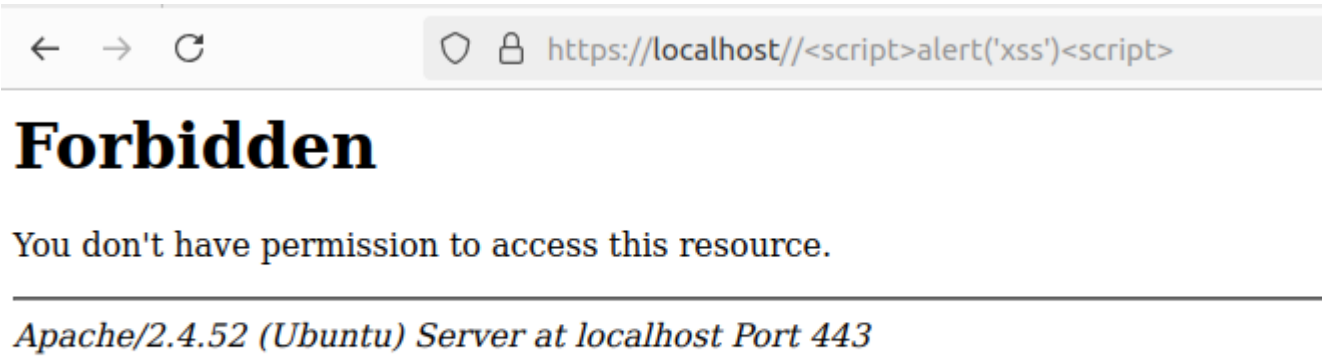
We are able to access the server without warning

Step 3

```
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 (2.35-0ubuntu3.8) ...
root@ubuntu:/# apt install libapache2-mod-security2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libapache2-mod-security2 is already the newest version (2.9.5-1).
The following packages were automatically installed and are no longer required:
  gyp libc-ares2 libjs-events libjs-highlight.js libjs-inherits libjs-is-typedarray libjs-psl libjs-source-map libjs-sprintf-js
  libjs-typedarray-to-buffer libnode-dev libnode72 libssl-dev libuv1-dev node-abbrev node-ansi-regex node-ansi-styles
  node-ansistyles node-are-we-there-yet node-arrify node-asap node-asynckit node-balanced-match node-brace-expansion node-chownr
  node-clean-yaml-object node-color-convert node-color-name node-commander node-core-util-is node-decompress-response
  node-delayed-stream node-delegates node-depd node-diff node-encoding node-end-of-stream node-err-code
  node-escape-string-regexp node-fancy-log node-foreground-child node-fs.realpath node-function-bind node-get-stream node-glob
  node-growl node-has-flag node-has-unicode node-hosted-git-info node-iconv-lite node-iferr node-imurmurhash node-indent-string
  node-inflight node-inherits node-ini node-ip node-ip-regex node-is-buffer node-is-plain-obj node-is-typedarray node-isarray
  node-isexe node-json-parse-better-errors node-jsonparse node-kind-of node-lodash-packages node-lowercase-keys node-lru-cache
  node-mimic-response node-minimatch node-minimist node-minipass node-mute-stream node-negotiator node-npm-bundled node-once
  node-osenv node-p-cancelable node-p-map node-path-is-absolute node-process-nextick-args node-promise-inflight
  node-promise-retry node-promzard node-pump node-quick-lru node-read node-readable-stream node-resolve node-retry
  node-safe-buffer node-set-blocking node-signal-exit node-slash node-slice-ansi node-source-map node-spdx-correct
  node-spdx-exceptions node-spdx-expression-parse node-spdx-license-ids node-sprintf-js node-stealthy-require
  node-string-decoder node-supports-color node-text-table node-time-stamp node-tmatch node-typedarray-to-buffer
  node-universalify node-util-deprecate node-validate-npm-package-license node-webidl-conversions node-whatwg-fetch node-wrappy
  node-yallist nodejs-doc
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 85 not upgraded.
root@ubuntu:/# mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
root@ubuntu:/# sed -i 's/SecRuleEngine DetectionOnly/SecRuleEngine On/g' /etc/modsecurity/modsecurity.conf
root@ubuntu:/# systemctl restart apache2
root@ubuntu:/#
```

Installed modsecurity and setup the config file and updated the config file to turn modsecurity blocking mode on

Step 4



Testing xss we see that the request was blocked by the page

8.2 - Secure Coding

Step 1

```
┌──(jordan㉿kali)-[~]
└─$ git clone https://github.com/appsecco/dvna
Cloning into 'dvna'...
remote: Enumerating objects: 645, done.
remote: Total 645 (delta 0), reused 0 (delta 0), pack-reused 645 (from 1)
Receiving objects: 100% (645/645), 3.18 MiB | 6.63 MiB/s, done.
Resolving deltas: 100% (281/281), done.

┌──(jordan㉿kali)-[~]
└─$
```

I cloned the dvna repo

Enable Snyk Code

To analyze your code for vulnerabilities we temporarily clone the repository or upload your code.
Cloned or uploaded code is cached according to our data retention policy.

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

Enabled

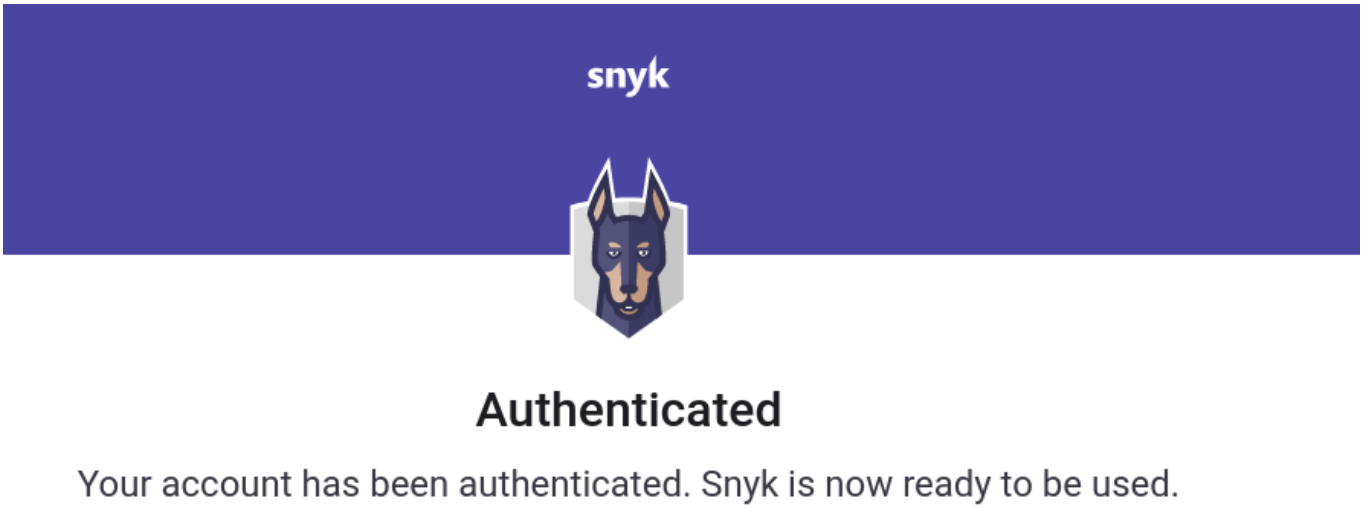
After being enabled, you must import / re-import projects to scan them.

Step 2

After setting up synk, synk code was already enabled

```
┌──(jordan㉿kali)-[~]
└─$ wget https://static.snyk.io/cli/latest/snyk-linux
--2024-10-14 14:28:47--  https://static.snyk.io/cli/latest/snyk-linux
Resolving static.snyk.io (static.snyk.io)... 23.38.224.207, 2600:1406:2e00:78d::ecd, 2600:1406:2e00:7a0::ecd
Connecting to static.snyk.io (static.snyk.io)|23.38.224.207|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [binary/octet-stream]
Saving to: 'snyk-linux'

snyk-linux                                          [

2024-10-14 14:28:58 (9.27 MB/s) - 'snyk-linux' saved [110141700]


┌──(jordan㉿kali)-[~]
└─$ chmod +x snyk-linux

┌──(jordan㉿kali)-[~]
└─$ sudo mv snyk-linux /usr/local/bin/snyk
[sudo] password for jordan:

┌──(jordan㉿kali)-[~]
└─$
```

Installed synk linux binary and configured it to use



After running synk auth, I was able to authenticate into synk

Step 3

```
┌──(jordan㉿kali)-[~]
└─$ snyk test https://github.com/appsecco/dvna

Testing https://github.com/appsecco/dvna...

✗ Low severity vulnerability found in tar
  Description: Regular Expression Denial of Service (ReDoS)
  Info: https://security.snyk.io/vuln/SNYK-JS-TAR-1536758
  Introduced through: bcrypt@1.0.3
  From: bcrypt@1.0.3 > node-pre-gyp@0.6.36 > tar@2.2.2
  From: bcrypt@1.0.3 > node-pre-gyp@0.6.36 > tar-pack@3.4.1 > tar@2.2.2

✗ Medium severity vulnerability found in validator
  Description: Regular Expression Denial of Service (ReDoS)
  Info: https://security.snyk.io/vuln/SNYK-JS-VALIDATOR-1090599
  Introduced through: sequelize@4.44.4
  From: sequelize@4.44.4 > validator@10.11.0

✗ Medium severity vulnerability found in validator
  Description: Regular Expression Denial of Service (ReDoS)
  Info: https://security.snyk.io/vuln/SNYK-JS-VALIDATOR-1090601
  Introduced through: sequelize@4.44.4
  From: sequelize@4.44.4 > validator@10.11.0

✗ Medium severity vulnerability found in validator
  Description: Regular Expression Denial of Service (ReDoS)
  Info: https://security.snyk.io/vuln/SNYK-JS-VALIDATOR-1090602
  Introduced through: sequelize@4.44.4
  From: sequelize@4.44.4 > validator@10.11.0

✗ Medium severity vulnerability found in tough-cookie
  Description: Prototype Pollution
  Info: https://security.snyk.io/vuln/SNYK-JS-TOUGHCOOKIE-5672873
  Introduced through: bcrypt@1.0.3
  From: bcrypt@1.0.3 > node-pre-gyp@0.6.36 > request@2.88.2 > tough-cookie@2.5.0

✗ Medium severity vulnerability found in tar
  Description: Uncontrolled Resource Consumption ('Resource Exhaustion')
  Info: https://security.snyk.io/vuln/SNYK-JS-TAR-6476909
  Introduced through: bcrypt@1.0.3
  From: bcrypt@1.0.3 > node-pre-gyp@0.6.36 > tar@2.2.2
  From: bcrypt@1.0.3 > node-pre-gyp@0.6.36 > tar-pack@3.4.1 > tar@2.2.2

✗ Medium severity vulnerability found in sequelize
  Description: Information Exposure
  Info: https://security.snyk.io/vuln/SNYK-JS-SEQUELIZE-3324089
  Introduced through: sequelize@4.44.4
  From: sequelize@4.44.4

✗ Medium severity vulnerability found in sequelize
  Description: Access of Resource Using Incompatible Type ('Type Confusion')
  Info: https://security.snyk.io/vuln/SNYK-JS-SEQUELIZE-3324090
  Introduced through: sequelize@4.44.4
```

After running synk test a large amount of security risks were found

```
✗ High severity vulnerability found in mathjs
  Description: Arbitrary Code Execution
  Info: https://security.snyk.io/vuln/npm:mathjs:20171118
  Introduced through: mathjs@3.10.1
  From: mathjs@3.10.1
```

Let's take a look at this mathjs vulnerability
It is an Arbitrary Coded Execution vulnerability with a 7.3 CVSS rating so it is pretty high. Mathjjs is a math library for javascript and node.js. It is an easy fix and can be fixed by simply upgrading mathjs to 3.17.0 or higher. Affected versions of the package are vulnerable to arbitrary code execution by the typed-function. A user can execute arbitrary code in the JS engine by creating a typed function with JS code in the name.

Step 4

```
┌──(jordan㉿kali)-[~/dvna]
└─$ snyk code test

Testing /home/jordan/dvna  ...

 ✗ [Low] Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
   Path: server.js, line 27
   Info: Cookie has the Secure attribute set to false. Set it to true to protect the cookie from man-in-the-middle attacks.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: core/authHandler.js, line 49
   Info: MD5 hash (used in md5) is insecure. Consider changing it to a secure hashing algorithm.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: core/authHandler.js, line 78
   Info: MD5 hash (used in md5) is insecure. Consider changing it to a secure hashing algorithm.

 ✗ [Low] Improper Type Validation
   Path: core/appHandler.js, line 150
   Info: The type of this object, coming from body and the value of its length property can be controlled by the user. An attacker may craft the properties of the object to crash the application or bypass its logic. Consider c
e type of the object.

 ✗ [Low] Improper Type Validation
   Path: core/appHandler.js, line 151
   Info: The type of this object, coming from body and the value of its length property can be controlled by the user. An attacker may craft the properties of the object to crash the application or bypass its logic. Consider c
e type of the object.

 ✗ [Medium] Information Exposure
   Path: server.js, line 11
   Info: Disable X-Powered-By header for your Express app (consider using Helmet middleware), because it exposes information about the used framework to potential attackers.

 ✗ [Medium] Open Redirect
   Path: core/appHandler.js, line 188
   Info: Unsanitized input from an HTTP parameter flows into redirect, where it is used as an URL to redirect the user. This may result in an Open Redirect vulnerability.

 ✗ [Medium] Cross-Site Request Forgery (CSRF)
   Path: server.js, line 11
   Info: CSRF protection is disabled for your Express app. This allows the attackers to execute requests on a user's behalf.

 ✗ [Medium] Cross-site Scripting (XSS)
   Path: views/app/adminusers.ejs, line 40
   Info: Unsanitized input from data from a remote resource flows into innerHTML, where it is used to dynamically construct the HTML page on client side. This may result in a DOM Based Cross-Site Scripting attack (DOMXSS).

 ✗ [Medium] Cross-site Scripting (XSS)
   Path: views/app/adminusers.ejs, line 41
   Info: Unsanitized input from data from a remote resource flows into innerHTML, where it is used to dynamically construct the HTML page on client side. This may result in a DOM Based Cross-Site Scripting attack (DOMXSS).

 ✗ [Medium] Cross-site Scripting (XSS)
   Path: views/app/adminusers.ejs, line 42
```

running another snyk scan in the dvna directory we see many vulnerabilities again

```
✗ [High] SQL Injection
  Path: core/appHandler.js, line 11
  Info: Unsanitized input from the HTTP request body flows into query, where it is used in an SQL query. This may result in an SQL Injection vulnerability.
```

Let's take a look at this one. SQL injection is an attack where an adversary can type into an input box and escape the input box by inputting a SQL closing/opening char to input a SQL query. This app is vulnerable because it does not sanitize the input from the http request body meaning queries can be made by anyone maliciously. SQLi can be detected by using prepared statements or parameterized queries to prevent malicious input from being executed as SQL

8.3 - DAST Scan

Step 1

```
┌──(jordan㉿kali)-[~/dvna]
└─$ docker

Usage:  docker [OPTIONS] COMMAND

A self-sufficient runtime for containers

Common Commands:
  run         Create and run a new container from an image
  exec        Execute a command in a running container
  ps          List containers
  build       Build an image from a Dockerfile
  pull        Download an image from a registry
  push        Upload an image to a registry
  images      List images
  login       Log in to a registry
  logout      Log out from a registry
  search      Search Docker Hub for images
  version     Show the Docker version information
  info        Display system-wide information
```

Docker is already installed on my machine

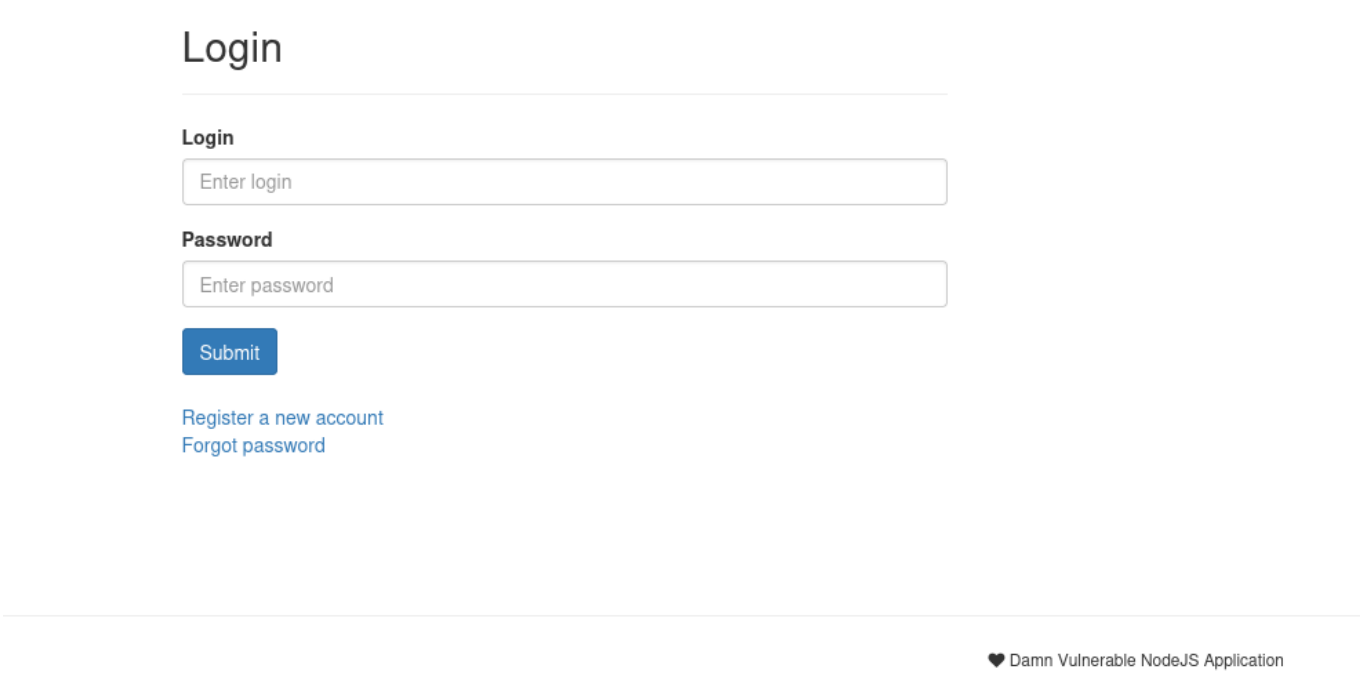
```
┌──(jordan㉿kali)-[~/dvna]
└─$ sudo usermod -aG docker jordan
```

I added jordan to the docker group so they can use docker commands

Step 2

```
┌──(jordan㉿kali)-[~]
└─$ docker run --name dvna -p 9090:9090 -d appsecco/dvna:sqlite
Unable to find image 'appsecco/dvna:sqlite' locally
sqlite: Pulling from appsecco/dvna
57936531d1ee: Pull complete
b186cf19f9ed: Pull complete
eadbf8312262: Pull complete
cf528b18b6ce: Pull complete
075c4f074e90: Pull complete
d0562d9451f1: Pull complete
48671e1607ad: Pull complete
4879e9b180ec: Pull complete
4bcad28e8244: Pull complete
```

IK first ran the dvna docker container and forwarded it to porn 9090



The page looks to be a simple login page

```
┌──(jordan㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c3:3e:30 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.37/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 86187sec preferred_lft 86187sec
    inet6 fe80::a00:27ff:fec3:3e30/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:d0:02:fc:46 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:d0ff:fe02:fc46/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
5: vethcf9e0a5@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether 56:24:80:53:05:a1 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::5424:80ff:fe53:5a1/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(jordan㉿kali)-[~]
└─$
```

My eth0 ip is 192.168.1.37

```
┌──(jordan㉿kali)-[~]
└─$ docker run --user $(id -u) --rm -v $(pwd):/dastardly -e DASTARDLY_TARGET_URL=http://192.168.1.37:9090/ -e DASTARDLY_OUTPUT_FILE=/dastardly/dastardly-report.xml public.ecr.aws/portswigger/dastardly:latest
Unable to find image 'public.ecr.aws/portswigger/dastardly:latest' locally
latest: Pulling from portswigger/dastardly
560c024910be: Pull complete
eb7adb7470c6: Pull complete
76046a519ec5: Pull complete
50c254587221: Pull complete
f5dc0d66069a: Pull complete
aaabbeb8b035: Pull complete
5b86a0188786: Pull complete
bbd797cb2bef: Pull complete
4f4fb700ef54: Pull complete
5dcd964b8fb4: Pull complete
57899c18a1ef: Pull complete
a213d3ba650b: Pull complete
7249b8d2d98c: Pull complete
dd9f51efd91b: Pull complete
87b5bb8586f2: Pull complete
Digest: sha256:8d7a4db225d80a1eb7cbce93e573a73ff0ad5eaff7a540355edff3b0a416fbfb
Status: Downloaded newer image for public.ecr.aws/portswigger/dastardly:latest


    §§§§§§§§§§§§§§§§§§§§§§§\
    §                     § |
    §          ||         § |    §§§§§§§\                          §§\
    §         //          § |    §§  __§§\                         §§ |
    §      /////|         § |    §§ |  §§ | §§§§§§\   §§§§§§§\ §§§§§§\    §§§§§§\   §§§§§§\   §§§§§§§ |§§ |§§\   §§\
    §         ||          § |    §§ |  §§ | \____§§\ §§  _____|\_§§  _|   \____§§\ §§  __§§\ §§  __§§ |§§ |§§ |  §§ |
    §         |/////      § |    §§ |  §§ | §§§§§§§ |\§§§§§§\    §§ |    §§§§§§§ |§§ |  \__|§§ /  §§ |§§ |§§ |  §§ |
    §           //        § |    §§ |  §§ |§§  __§§ | \____§§\   §§ |§§\ §§  __§§ |§§ |      §§ |  §§ |§§ |§§ |  §§ |
    §          //         § |    §§§§§§§  |\§§§§§§§ |§§§§§§§  |   \§§§§  |\§§§§§§§ |§§ |      \§§§§§§§ |§§ |\§§§§§§§ |
    §          ||         § |    \_______/ \_______|\_______/    \____/ \_______|\__|       \_______|\__| \____§§ |
    §                     § |                                                                                §§\   §§ |
    §§§§§§§§§§§§§§§§§§§§§§§ |                                                  from Burp Suite   v2024.9-18509    \§§§§§§  |
    \_______________________|                                                                                    \______/

Installing or running Dastardly affirms your agreement to the Terms of Service https://portswigger.net/burp/dastardly/eula

2024-10-14 22:51:15 INFO  dastardly.StartDastardly - Using Java version 21.0.4
2024-10-14 22:51:15 WARN  d.DeprecatedEnvironmentVariableMapper - The environment variable DASTARDLY_OUTPUT_FILE is deprecated - please use BURP_REPORT_FILE_PATH instead. Treating DASTARDLY_OUTPUT_FILE as BURP_REPORT_FILE_PATH.
2024-10-14 22:51:15 WARN  d.DeprecatedEnvironmentVariableMapper - The environment variable DASTARDLY_TARGET_URL is deprecated - please use BURP_START_URL instead. Treating DASTARDLY_TARGET_URL as BURP_START_URL.
2024-10-14 22:51:16 INFO  bsee.BurpProcess.scan.scan-1 - Oct 14, 2024 10:51:16 PM java.util.prefs.FileSystemPreferences$1 run
2024-10-14 22:51:16 INFO  bsee.BurpProcess.scan.scan-1 - INFO: Created user preferences directory.
2024-10-14 22:51:21 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:21: REST API running on http://localhost:45799/
2024-10-14 22:51:21 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 39] 2024-10-14 10:51:21.909 409903194928, net.portswigger.Zdt INFO - connectedSocket, opened new socket: 1348376212
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 37] 2024-10-14 10:51:22.412 410405591389, net.portswigger.Zh INFO - Closing socket due to timeout: 1348376212
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 37] 2024-10-14 10:51:22.412 410405941626, net.portswigger.Zh INFO - Closing socket: 1348376212
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 37] 2024-10-14 10:51:22.412 410406229001, net.portswigger.Zh INFO - Socket closed: 1348376212
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:22: Failed to send NOT_READY heartbeat to http://127.0.0.1:1234/da6665bf-3e78-48f0-9837-52ba3b90df01/api/heartbeat
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - java.net.SocketTimeoutException: Communication timed out: sent = true, receivedEmptyResponse = true, timedOut = true
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at net.portswigger.Zh.Zz(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at net.portswigger.Zh.ZA(Unknown Source)
```

```
2024-10-14 22:51:15 WARN  d.DeprecatedEnvironmentVariableMapper - The environment variable DASTARDLY_TARGET_URL is deprecated - please use BURP_START_URL instead. Treating DASTARDLY_TARGET_URL as BURP_START_URL.
2024-10-14 22:51:16 INFO  bsee.BurpProcess.scan.scan-1 - Oct 14, 2024 10:51:16 PM java.util.prefs.FileSystemPreferences$1 run
2024-10-14 22:51:16 INFO  bsee.BurpProcess.scan.scan-1 - INFO: Created user preferences directory.
2024-10-14 22:51:21 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:21: REST API running on http://localhost:45799/
2024-10-14 22:51:21 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 39] 2024-10-14 10:51:21.909 409903194928, net.portswigger.Zdt INFO - connectedSocket, opened new socket: 1348376212
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 37] 2024-10-14 10:51:22.412 410405591389, net.portswigger.Zh INFO - Closing socket due to timeout: 1348376212
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 37] 2024-10-14 10:51:22.412 410405941626, net.portswigger.Zh INFO - Closing socket: 1348376212
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 37] 2024-10-14 10:51:22.412 410406229001, net.portswigger.Zh INFO - Socket closed: 1348376212
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:22: Failed to send NOT_READY heartbeat to http://127.0.0.1:1234/da6665bf-3e78-48f0-9837-52ba3b90df01/api/heartbeat
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - java.net.SocketTimeoutException: Communication timed out: sent = true, receivedEmptyResponse = true, timedOut = true
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at net.portswigger.Zh.Zz(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at net.portswigger.Zh.ZA(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at net.portswigger.Zh.Zl(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at net.portswigger.Zdt.Zl(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at net.portswigger.Zjs.Zf(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zs_v.ZD(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zs_v.lambda$new$0(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.concurrent.Executors$RunnableAdapter.call(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.concurrent.FutureTask.runAndReset(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.lang.Thread.run(Unknown Source)
2024-10-14 22:51:22 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 39] 2024-10-14 10:51:22.414 410408240621, net.portswigger.Zh INFO - Closing socket: 1348376212
2024-10-14 22:51:23 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:23: Using longer timeout due to failure
2024-10-14 22:51:23 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 64] 2024-10-14 10:51:23.580 411573950225, net.portswigger.Zdt INFO - connectedSocket, opened new socket: 2145852177
2024-10-14 22:51:23 INFO  bsee.BurpProcess.scan.scan-1 - Debug ID: 3907ztrfgf2jwa0kzdtm:lgrz
2024-10-14 22:51:23 INFO  bsee.BurpProcess.scan.scan-1 - Burp Version: 2024.7.6-32146
2024-10-14 22:51:23 INFO  bsee.BurpProcess.scan.scan-1 - Product Name: Dastardly from Burp Suite
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 - Exception report:
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -     Category: UNHANDLED
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -     Detail:
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 - java.lang.IndexOutOfBoundsException: Index 4 out of bounds for length 4
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/jdk.internal.util.Preconditions.outOfBounds(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/jdk.internal.util.Preconditions.outOfBoundsCheckIndex(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/jdk.internal.util.Preconditions.checkIndex(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.Objects.checkIndex(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.ArrayList.get(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at com.sun.javafx.collections.ObservableListWrapper.get(ObservableListWrapper.java:88)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdi1.lambda$getPendingValueAt$5(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zfwu.Zw(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdi1.Zm(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zz7z.ZC(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvfh.Ze(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zf8m.Zr(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zf8m.compareTo(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.Arrays.binarySearch0(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.Arrays.binarySearch(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvfh.ZY(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvfh.ZJ(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvfh.rowsUpdated(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvgg.lambda$rowsUpdated$6(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zfwu.Zq(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvgg.rowsUpdated(Unknown Source)
```

```
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/javax.swing.table.AbstractTableModel.fireTableChanged(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdi1.fireTableChanged(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/javax.swing.table.AbstractTableModel.fireTableRowsUpdated(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdi1.fireTableRowsUpdated(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdik.fireTableRowsUpdated(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdis.Zx(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zexl.ZY(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zav.lambda$nodeUpdated$22(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.event.InvocationEvent.dispatch(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.EventQueue.dispatchEventImpl(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.EventQueue$4.run(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.EventQueue$4.run(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.security.AccessController.doPrivileged(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.security.ProtectionDomain$JavaSecurityAccessImpl.doIntersectionPrivilege(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.EventQueue.dispatchEvent(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.EventDispatchThread.pumpOneEventForFilters(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.EventDispatchThread.pumpEventsForFilter(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.EventDispatchThread.pumpEventsForHierarchy(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.EventDispatchThread.pumpEvents(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.EventDispatchThread.pumpEvents(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/java.awt.EventDispatchThread.run(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 - ------------------------------------------------------------------------------
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 - java.lang.IndexOutOfBoundsException: Index 4 out of bounds for length 4
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/jdk.internal.util.Preconditions.outOfBounds(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/jdk.internal.util.Preconditions.outOfBoundsCheckIndex(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/jdk.internal.util.Preconditions.checkIndex(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.Objects.checkIndex(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.ArrayList.get(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at com.sun.javafx.collections.ObservableListWrapper.get(ObservableListWrapper.java:88)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdi1.lambda$getPendingValueAt$5(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zfwu.Zw(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdi1.Zm(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zz7z.ZC(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvfh.Ze(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zf8m.Zr(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zf8m.compareTo(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.Arrays.binarySearch0(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.base/java.util.Arrays.binarySearch(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvfh.ZY(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvfh.ZJ(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvfh.rowsUpdated(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvgg.lambda$rowsUpdated$6(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zfwu.Zq(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zvgg.rowsUpdated(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/javax.swing.JTable.notifySorter(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/javax.swing.JTable.sortedTableChanged(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/javax.swing.JTable.tableChanged(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/javax.swing.table.AbstractTableModel.fireTableChanged(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdi1.fireTableChanged(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at java.desktop/javax.swing.table.AbstractTableModel.fireTableRowsUpdated(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdi1.fireTableRowsUpdated(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdik.fireTableRowsUpdated(Unknown Source)
2024-10-14 22:51:25 INFO  bsee.BurpProcess.scan.scan-1 -        at burp.Zdis.Zx(Unknown Source)
```

```
2024-10-14 22:51:26 INFO  bsee.BurpProcess.scan.scan-1 - [Thread: 110] 2024-10-14 10:51:26.892 414885742796, net.portswigger.Zdt INFO - connectedSocket, opened new socket: 1931756092
2024-10-14 22:51:26 INFO  b.s.LoggingScanProgressCollector - Event log updated:
2024-10-14 22:51:26 INFO  b.s.LoggingScanProgressCollector - 2024-10-14 22:51:23 INFORMATION - Crawl started.
2024-10-14 22:51:26 INFO  b.s.LoggingScanProgressCollector - 2024-10-14 22:51:24 DEBUG - cdnjs.cloudflare.com is using HTTP/2
2024-10-14 22:51:26 INFO  b.s.LoggingScanProgressCollector - 2024-10-14 22:51:24 DEBUG - maxcdn.bootstrapcdn.com is using HTTP/2
2024-10-14 22:51:26 INFO  bsee.BurpProcess.scan.scan-1 - Received metric CRAWLING 0 3
2024-10-14 22:51:31 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:31: CRAWLING → crawlUniqueLocationsVisited:6, crawlRequestsMade:59, auditQueueItemsWaiting:0, auditQueueItemsCompleted:0, auditRequestsMade:0, insertionPointCoun
t:0
2024-10-14 22:51:31 INFO  bsee.BurpProcess.scan.scan-1 - Received metric CRAWLING 0 6
2024-10-14 22:51:32 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:32: Crawl finished
2024-10-14 22:51:32 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:32: Audit started
2024-10-14 22:51:36 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:36: AUDITING → crawlUniqueLocationsVisited:7, crawlRequestsMade:62, auditQueueItemsWaiting:9, auditQueueItemsCompleted:2, auditRequestsMade:212, insertionPointCo
unt:110
2024-10-14 22:51:36 INFO  b.s.LoggingScanProgressCollector - Event log updated:
2024-10-14 22:51:36 INFO  b.s.LoggingScanProgressCollector - 2024-10-14 22:51:32 INFORMATION - Crawl finished.
2024-10-14 22:51:36 INFO  b.s.LoggingScanProgressCollector - 2024-10-14 22:51:32 INFORMATION - Identifying items to audit.
2024-10-14 22:51:36 INFO  b.s.LoggingScanProgressCollector - 2024-10-14 22:51:32 INFORMATION - Audit started.
2024-10-14 22:51:36 INFO  b.s.IssueLoggingScanProgressCollector - Issue identified. Path: /login, Issue Type: Vulnerable JavaScript dependency, Severity: LOW
2024-10-14 22:51:36 INFO  b.s.IssueLoggingScanProgressCollector - Issue identified. Path: /register, Issue Type: Vulnerable JavaScript dependency, Severity: LOW
2024-10-14 22:51:36 INFO  b.s.IssueLoggingScanProgressCollector - Issue identified. Path: /forgotpw, Issue Type: Vulnerable JavaScript dependency, Severity: LOW
2024-10-14 22:51:36 INFO  b.s.IssueLoggingScanProgressCollector - Issue identified. Path: /assets/jquery-3.2.1.min.js, Issue Type: Vulnerable JavaScript dependency, Severity: LOW
2024-10-14 22:51:36 INFO  bsee.BurpProcess.scan.scan-1 - Received metric AUDITING 212 7
2024-10-14 22:51:41 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:41: AUDITING → crawlUniqueLocationsVisited:7, crawlRequestsMade:62, auditQueueItemsWaiting:3, auditQueueItemsCompleted:8, auditRequestsMade:355, insertionPointCo
unt:110
2024-10-14 22:51:41 INFO  bsee.BurpProcess.scan.scan-1 - Received metric AUDITING 355 7
2024-10-14 22:51:46 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:46: AUDITING → crawlUniqueLocationsVisited:7, crawlRequestsMade:62, auditQueueItemsWaiting:1, auditQueueItemsCompleted:10, auditRequestsMade:408, insertionPointC
ount:110
2024-10-14 22:51:46 INFO  bsee.BurpProcess.scan.scan-1 - Received metric AUDITING 408 7
2024-10-14 22:51:47 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:47: Audit finished
2024-10-14 22:51:51 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:51: SUCCEEDED → crawlUniqueLocationsVisited:7, crawlRequestsMade:62, auditQueueItemsWaiting:0, auditQueueItemsCompleted:11, auditRequestsMade:410, insertionPoint
Count:110
2024-10-14 22:51:51 INFO  b.s.LoggingScanProgressCollector - Event log updated:
2024-10-14 22:51:51 INFO  b.s.LoggingScanProgressCollector - 2024-10-14 22:51:47 INFORMATION - Audit finished.
2024-10-14 22:51:51 INFO  bsee.BurpProcess.scan.scan-1 - Received metric SUCCEEDED 410 7
2024-10-14 22:51:51 INFO  b.s.LoggingScanProgressCollector - Scan has completed successfully
2024-10-14 22:51:52 INFO  b.s.EventLogPrintingScanProgressCollector - Oct 14 2024 22:51:23 INFORMATION Crawl started.
2024-10-14 22:51:52 INFO  b.s.EventLogPrintingScanProgressCollector - Oct 14 2024 22:51:24 DEBUG cdnjs.cloudflare.com is using HTTP/2
2024-10-14 22:51:52 INFO  b.s.EventLogPrintingScanProgressCollector - Oct 14 2024 22:51:24 DEBUG maxcdn.bootstrapcdn.com is using HTTP/2
2024-10-14 22:51:52 INFO  b.s.EventLogPrintingScanProgressCollector - Oct 14 2024 22:51:32 INFORMATION Crawl finished.
2024-10-14 22:51:52 INFO  b.s.EventLogPrintingScanProgressCollector - Oct 14 2024 22:51:32 INFORMATION Identifying items to audit.
2024-10-14 22:51:52 INFO  b.s.EventLogPrintingScanProgressCollector - Oct 14 2024 22:51:32 INFORMATION Audit started.
2024-10-14 22:51:52 INFO  b.s.EventLogPrintingScanProgressCollector - Oct 14 2024 22:51:47 INFORMATION Audit finished.
2024-10-14 22:51:52 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:52: Burp shutting down due to DELETE request
2024-10-14 22:51:52 INFO  bsee.BurpProcess.scan.scan-1 - Deleting temporary files - please wait ... done.
2024-10-14 22:51:55 INFO  bsee.BurpProcess.scan.scan-1 - 2024-10-14 10:51:55: Burp shutdown because Project was closed / suite was told to exit
2024-10-14 22:51:56 INFO  dastardly.ScanManager - Scan finished, exiting
2024-10-14 22:51:56 ERROR dastardly.ScanFinishedHandler - Failing build as scanner identified issue(s) with severity higher than "INFO":
2024-10-14 22:51:56 ERROR dastardly.ScanFinishedHandler - Path: /register Issue Type: Vulnerable JavaScript dependency Severity: LOW
2024-10-14 22:51:56 ERROR dastardly.ScanFinishedHandler - Path: /forgotpw Issue Type: Vulnerable JavaScript dependency Severity: LOW
2024-10-14 22:51:56 ERROR dastardly.ScanFinishedHandler - Path: /assets/jquery-3.2.1.min.js Issue Type: Vulnerable JavaScript dependency Severity: LOW
2024-10-14 22:51:56 ERROR dastardly.ScanFinishedHandler - Path: /login Issue Type: Vulnerable JavaScript dependency Severity: LOW
```

Looks like the scan found a few LOW findings. Particularly in the /login /register /forgotpw and /assets. There is vulnerable javascript code. This scan cannot go to authenticated pages unless we login.