Implementation & Recognition of the solutions for OWASP ZAP

1)

Located the Options +Indexes line in the apache config file. Apache2.conf. Removed the +Indexes from that line.

```
276     # for more information.
277     #
278     Options +FollowSymLinks +Multiviews
279
280     #
```

2)

Implemented X-Frame. Apache config file. Apache2.conf.

```
#Setting of X-Frame Options to deny regardless of the site attempting to do so.
Header set X-Frame-Options DENY
```

3)

Header set for cache control and pragma. Apache2.conf.

```
#Prevent Cache
<IfModule mod_headers.c>
        Header set Cache-Control "no-cache, no-store, must-revalidate"
        Header set Pragma "no-cache"
        Header set Expires 0
</IfModule>
```

4)

Implemented the autocomplete feature to be off. login.html.

```
<br>
<form action="" class="form-inline" method="post" autocomplete="off">
```

5)

Web browser XSS protection has been enabled. Apache config file. Apache2.conf.

```
# Enables XSS filtering. Rather than sanitizing the page,
# the browser will prevent rendering of the page if an attack is detected.
Header set X-XSS-Protection "1; mode=block"
```

6)

The Anti-MIME-Sniffing Header X-Content-Type-Options has been set to nosniff. Apache config file. Apache2.conf

```
# Setting of MIME types advertised in the content-type
# headers should not be changed and be followed
LoadModule headers_module modules/mod_headers.so
<IfModule mod_headers.c>
  Header set X-Content-Type-Options nosniff
</IfModule>
```