C41NC

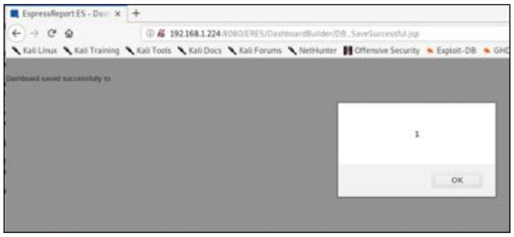
Security site.

CVE-2020-24983

Quadbase – EspressReports ES – Version 7, Update 9 – Cross Site Request Forgery (CSRF) to Cross Site Scripting (XSS).

An unauthenticated attacker can create a malicious website that, when visited, sends a POST request to the Quadbase ERES DashboardBuilder application. This attack is known as a CSRF attack. This makes it possible to utilise the target administrator session and perform an authenticated request, as the target user. In this case, the attacker could chain this vulnerability and execute a Cross-Site Scripting (XSS) payload within the target user's browser, resulting in the execution of arbitrary JavaScript code execution.

Dissecting the attack, we utilise the dashboard name to store the JavaScript payload itself. Under normal web logic, the name would be rejected by the regex validation built within the application. As this is only run on the client-side, the server still accepts malicious values that are later returned.



Dashboard saved successfully to

1

XSS payload executed.

CSRF attacks can often lead to critical risk attacks such as privilege escalation via account takeover. It also allows completely unauthenticated attackers to use a target web application as if they were an admin, performing features that would otherwise be unaccessible.

CSRF Proof of Concept:

```
<form action="http://X.X.X.X:8080/ERES/DashboardBuilder/DB_OverWriteDashboard.jsp?ActionButton=save>
  <input type="hidden" name="DashboardName" value="<script>alert(1)</script>" />
  <input type="hidden" name="SaveAgain" value="true" />
  <input type="hidden" name="OrganizerFolderList" value="9" />
  <input type="hidden" name="OrganizerNodePath" value="Examples" />
  <input type="submit" value="Submit request" />
</form>
```