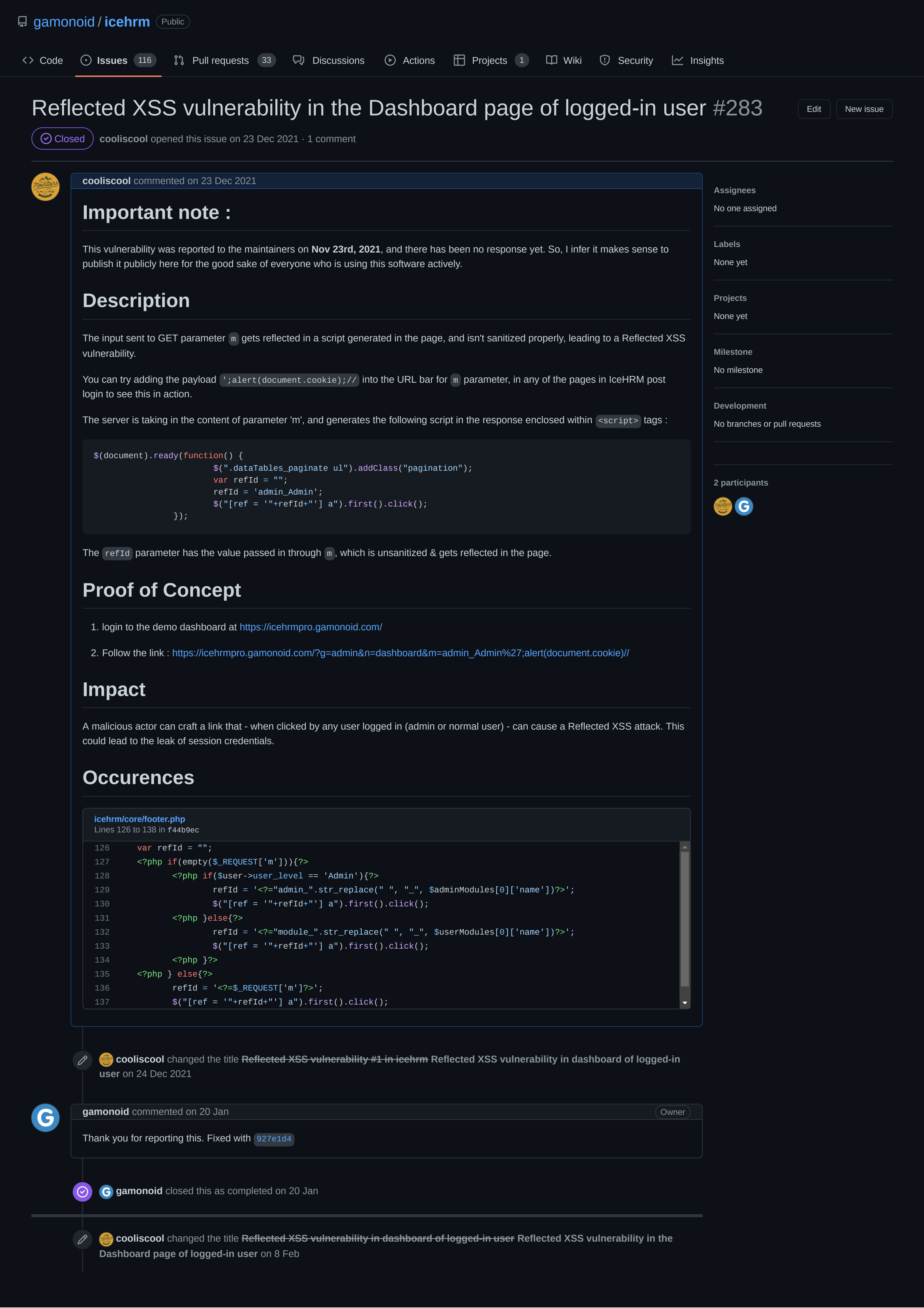

Reflected XSS vulnerability in the Dashboard page of logged-in user #283

Closed **cooliscool** opened this issue on 23 Dec 2021 · 1 comment

cooliscool commented on 23 Dec 2021

Important note :

This vulnerability was reported to the maintainers on **Nov 23rd, 2021**, and there has been no response yet. So, I infer it makes sense to publish it publicly here for the good sake of everyone who is using this software actively.

Description

The input sent to GET parameter `m` gets reflected in a script generated in the page, and isn't sanitized properly, leading to a Reflected XSS vulnerability.

You can try adding the payload `';alert(document.cookie);//` into the URL bar for `m` parameter, in any of the pages in IceHRM post login to see this in action.

The server is taking in the content of parameter 'm', and generates the following script in the response enclosed within `<script>` tags :

```
$(document).ready(function() {
                        $(".dataTables_paginate ul").addClass("pagination");
                        var refId = "";
                        refId = 'admin_Admin';
                        $("[ref = '"+refId+"'] a").first().click();
                });
```

The `refId` parameter has the value passed in through `m`, which is unsanitized & gets reflected in the page.

Proof of Concept

1. login to the demo dashboard at https://icehrmpro.gamonoid.com/
2. Follow the link : https://icehrmpro.gamonoid.com/?g=admin&n=dashboard&m=admin_Admin%27;alert(document.cookie)//

Impact

A malicious actor can craft a link that - when clicked by any user logged in (admin or normal user) - can cause a Reflected XSS attack. This could lead to the leak of session credentials.

Occurences

icehrm/core/footer.php
Lines 126 to 138 in `f44b9ec`

```
126     var refId = "";
127     <?php if(empty($_REQUEST['m'])){?>
128             <?php if($user->user_level == 'Admin'){?>
129                     refId = '<?="admin_".str_replace(" ", "_", $adminModules[0]['name'])?>';
130                     $("[ref = '"+refId+"'] a").first().click();
131             <?php }else{?>
132                     refId = '<?="module_".str_replace(" ", "_", $userModules[0]['name'])?>';
133                     $("[ref = '"+refId+"'] a").first().click();
134             <?php }?>
135     <?php } else{?>
136             refId = '<?=$_REQUEST['m']?>';
137             $("[ref = '"+refId+"'] a").first().click();
```

cooliscool changed the title ~~**Reflected XSS vulnerability #1 in icehrm**~~ **Reflected XSS vulnerability in dashboard of logged-in user** on 24 Dec 2021

gamonoid commented on 20 Jan Owner

Thank you for reporting this. Fixed with `927e1d4`

gamonoid closed this as completed on 20 Jan

cooliscool changed the title ~~**Reflected XSS vulnerability in dashboard of logged-in user**~~ **Reflected XSS vulnerability in the Dashboard page of logged-in user** on 8 Feb

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants