CVE-2022-24004 & CVE-2022-24127: Vanderbilt REDCap – Stored Cross Site Scripting

By Jordan Pitcairn | June 15, 2022

Nettitude identified two stored Cross Site Scripting (XSS) vulnerabilities within Vanderbilt REDCap. These have been assigned CVE-2022-24004 & CVE-2022-24127.

REDCap is a web application which allows the creation and management of online surveys for research purposes. Version 12.0.11 and below allows a remote authenticated attacker to inject

arbitrary JavaScript or HTML via the Messenger functionality and the administration interface.

CVE-2022-24004 – Proof of Concept

REDCap has a built in messenger function which allows all registered users to communicate within the application. Each conversation created has a title which can only be edited by the user which originally created the conversation. The input field where this title can be edited does not filter input and as a result, it is possible to inject malicious JavaScript and HTML.

Example POST data sent to Messenger_ajax.php:

```
action=change-conversationtitle&amp;thread_id=7&amp;new_title=%22+oncli
```

This payload will then trigger in the browser where the messenger sidebar is toggled of any user which is a participant of the conversation. The following screenshot shows that the payload is injected into the `data-tooltip` parameter of the `h4` tag.

For this simple proof of concept, the user would have to click on the message title, resulting in the execution of a JavaScript alert.

at https://github.com

Popular Recent

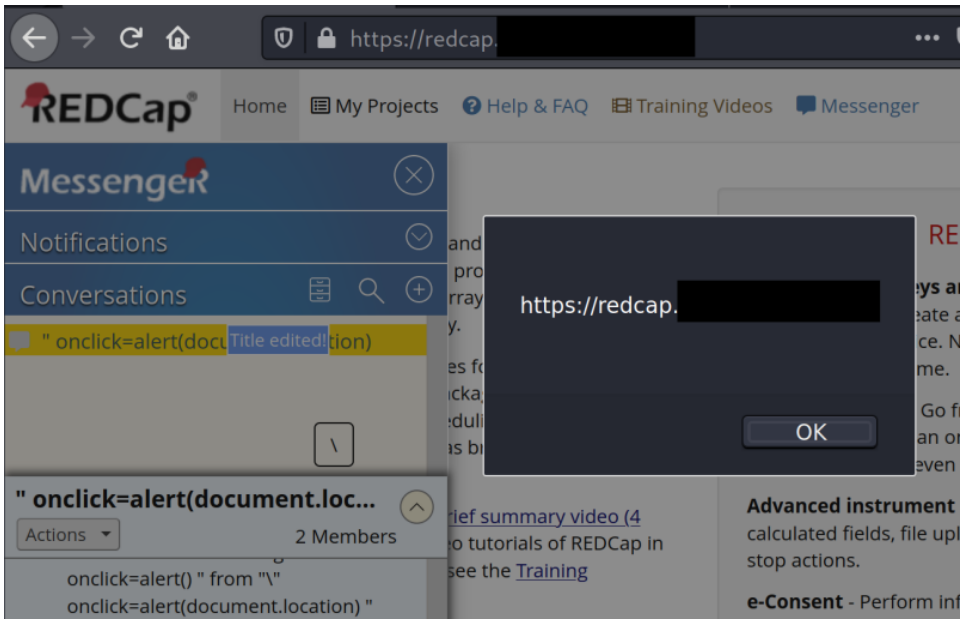
Posh – Introc Nativ macC Impla
April 14, 2021

Apache mod_python for red teams
May 31, 2018

PoshC2 v3 with SOCKS Proxy (SharpSocks)
November 15, 2017

· N 9

What is Cyber squat ting? Take a look at a



The impact of this vulnerability could lead to the disclosure of sensitive application and survey data. Given that the messenger functionality will autocomplete usernames after providing the first character, it is possible to see how an attacker could create a conversation with all application users to maximise chances of compromising application data from an administrator user.

Nettitude demonstrated the impact of this to the application vendor by further improving the proof of concept to automatically trigger on page load and scrape the contents of the users screen, sending this data to a remote server.

CVE-2022-24004 – Affected Component

This vulnerability affects REDCap version 12.0.11. Previous versions may also be affected.

- **Vulnerable page:** Messenger_ajax.php
- **Vulnerable parameter:** new_title

CVE-2022-24127 – Proof of Concept

In the project administration section of the application, admin users that have permissions to modify a project can modify the project title. The input field where this value is modified does not

few
com
mon
attack
techn
iques
and
poten
tial
defen
ces in
our
latest
article
.

…
…
C
…

· S 28

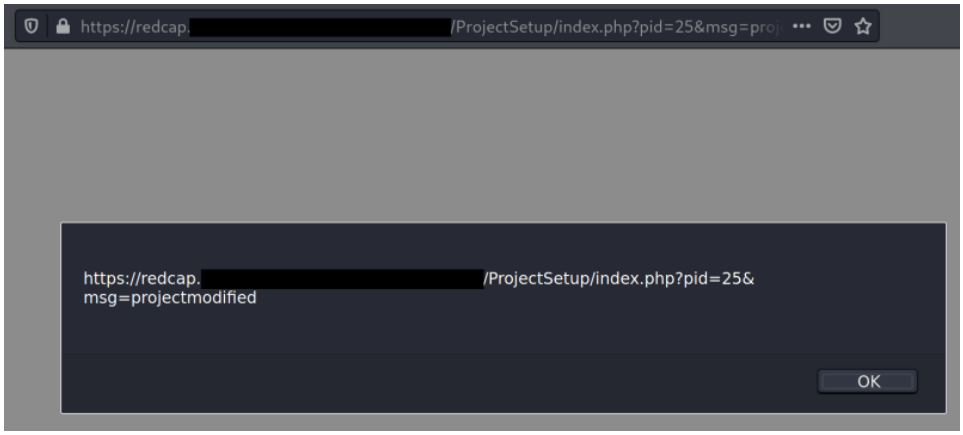
Find
out
how
Circle
bann
ed
the
Torna
do
Cash
crypt
ocurr
ency
mixer
follo
wing
U.S.
sancti
ons
last
mont
h.

filter input and as a result, it is possible to inject malicious JavaScript and HTML.

Example POST Data sent to edit_project_settings.php:

```
surveys_enabled=1&repeatforms=0&scheduling=0&randomizati
f
```

Once the project title is modified, the user is returned to the project administration home page where the payload immediately triggers and will continue to be executed across all administration pages related to the project.



This code execution is triggered due to the project title being reflected in the page `<title>` tag. If a user enters a value which first closes the tag, then any further HTML or JavaScript can be executed as shown in the following screenshot.

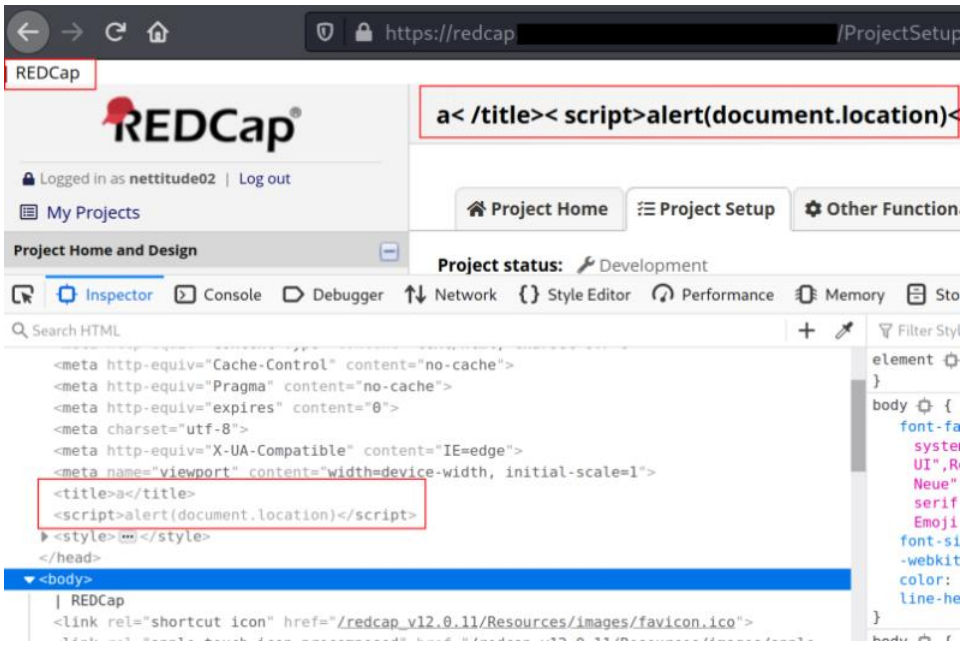
Our latest article explores some key concepts of Ethereum-based blockchains and smart contracts.

...
...
T
...

1

· S 14

CVE-2021-44076: Popular file sharing platform Crush FTP affected by stored Cross-Site Scripting.



The impact this vulnerability is reduced because it would require the attacker to have existing access as a user with project administration permissions. An attacker could potentially exploit this issue to redirect the user to a malicious website controlled by the attacker, which may ultimately lead to credential harvesting or the downloading of malware.

CVE-2022-24127 – Affected Component

This vulnerability affects REDCap version 12.0.11. Previous versions may also be affected.

- **Vulnerable page:** edit_project_settings.php
- **Vulnerable parameter:** app_title

Conclusion

All areas of a web application which accept and store user input should not be trusted. Appropriate measures should be taken to sanitize or encode data before being shown in a later browser response.

Nettitude contacted Vanderbilt to disclose these vulnerabilities. Remediation was put in place almost immediately post-disclosure

and a remediated version (12.0.13) was promptly released.

Version 12.0.13 (released on 2022-01-28)

CHANGES IN THIS VERSION:

- **Minor security fix:** A Cross-site Scripting (XSS) vulnerability was discovered where a malicious user could potentially exploit it by inserting HTML tags and/or JavaScript event attributes in a very specific way into the title of a project.
- **Minor security fix:** A Cross-site Scripting (XSS) vulnerability was discovered where a malicious user could potentially exploit it by inserting HTML tags and/or JavaScript event attributes in a very specific way for certain features of REDCap Messenger.

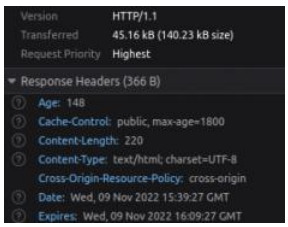
Timeline – CVE-2022-24004

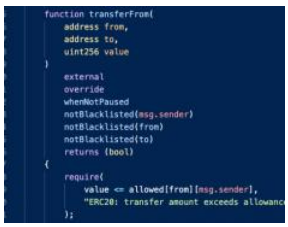
1. Discovered by Nettitude: 25 January 2022
2. Vendor informed: 26 January 2022
3. CVE Assigned: 26 January 2022
4. Vendor fix released: 28 January 2022
5. Nettitude Blog: 15 June 2022

Timeline – CVE-2022-24127

1. Discovered by Nettitude: 28 January 2022
2. Vendor informed: 28 January 2022
3. Vendor fix released: 28 January 2022
4. CVE assigned: 29 January 2022
5. Nettitude Blog: 15 June 2022

Related Posts





USEFUL LINKS

Download PoshC2

Vulnerability Research

Nettitude Cyber

UK

1 Jephson Court

Trancred Close

Leamington Spa

AMERICAS

50 Broad Street

Suite 403

New York City

CONTACT US

Name *

Your name or

Security Tools
Red Team Training
Careers at Nettitude<

NETTITUDE LABS PRESENTED BY

Warwickshire
CV31 3RZ

EUROPE

Leof. Siggrou 348
Kallithea
Athens
Greece
176 74

NY
10004

ASIA

18 Cross Street
#02-101
Suite S2039
Singapore
048423

Email address *

@ your@email.c

Message *

Your message to Nettitude Labs.*

protected by reCAPTCHA
Privacy - Terms

Send your message