README.md

Vendor:

```
Redcap app
```

Affected version:

The issue exists to version 10.3.4 and 10.0.20 (LTS)

Description:

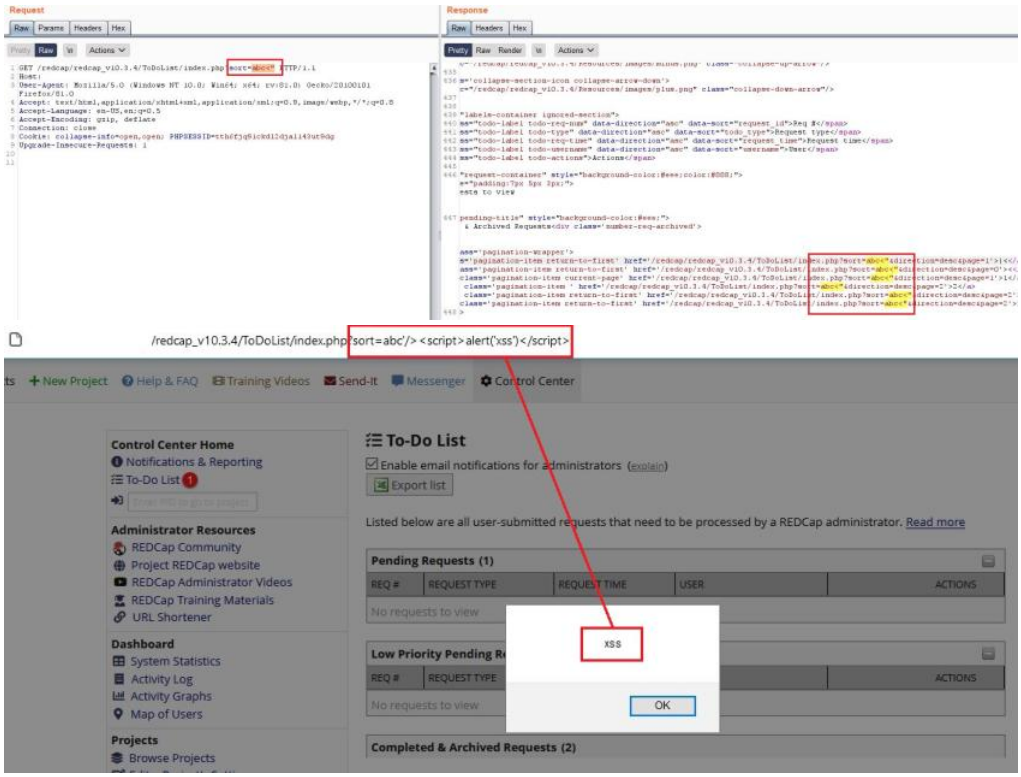
1. SQL injection attack allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server

2. The XSS vulnerability exists in the ToDoList function with parameter sort, the information submitted by the user is immediately returned in the response and not escaped leading to the Reflect XSS vulnerability. Attackers can exploit vulnerabilities to steal login session information or borrow user rights to perform unauthorized acts This vulnerability occurs when Completed & Archived Requests has more than 10 records, the application starts paging, and the vulnerability exists here.

Proof of Concept:

1. SQLInjection : redcap_v10.3.4/ToDoList/index.php?sort=(select case when (1=2) then 1 else 1*((select*from(select(sleep(5)))a))end)

2. XSS : redcap_v10.3.4/ToDoList/index.php?sort=abc%27/%3E%3Cscript%3Ealert(%27xss%27)%3C/script%3E



Reference

https://www.project-redcap.org/

Releases

No releases published

Packages

No packages published