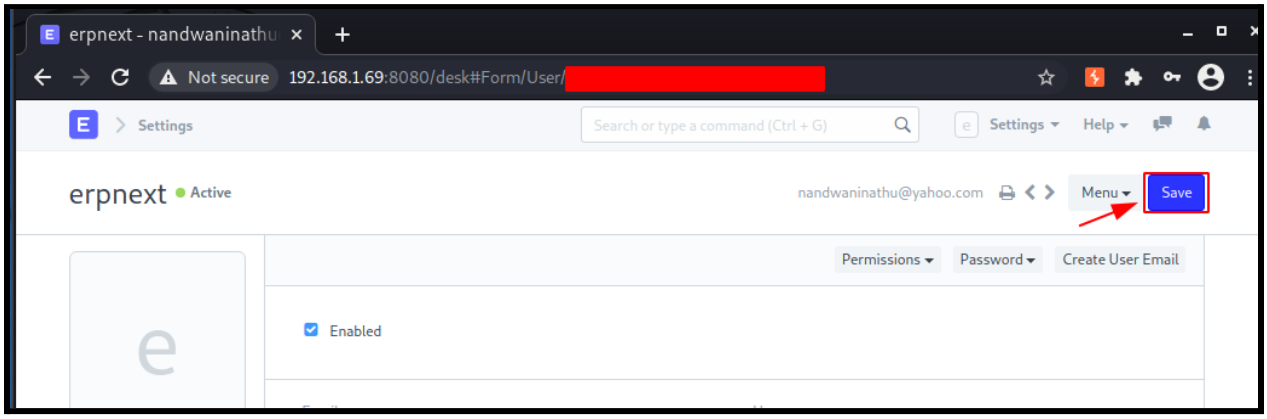
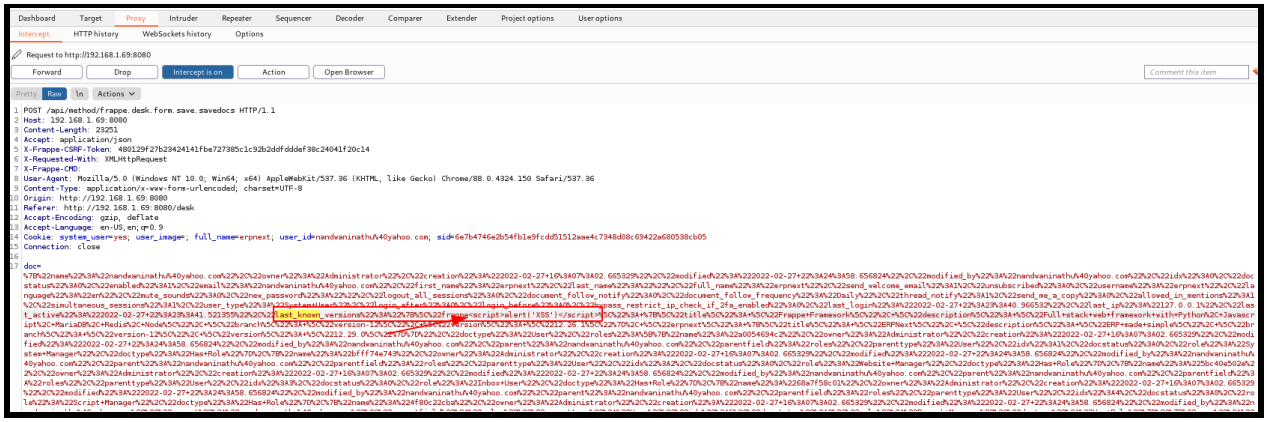
Stored cross-site scripting (XSS) vulnerability in the "last_known_version" field found in the "My Setting" page in ERPNext 12.29.0 allows remote attackers to inject arbitrary web script or HTML via a crafted site name by doing an authenticated POST HTTP request to '/desk#Form/User/(Authenticated User)' and inject the script in the 'last_known_version' field where we are able to view the script by clicking the 'pdf' view form.

This vulnerability is specifically the "last_known_version" field found under the 'My Settings' where we need to first save the my settings.



Under the ‘last_known_version’ field we are going to inject our malicious script.



To view our injected script we need to click the view pdf page, and as seen below we have successfully injected our script.