### INTRODUCTION
Passbolt password manager is an open source password manager that uses an OpenPGP encryption standard originally created by Zimmermann and can currently run on few selected browsers (Chrome & Firefox). Passbolt has a feature for protecting phishing attacks using color key. Passbolt is reported to be generally not user-friendly and the vulnerabilities such as inability to reset master passwords, unencrypting of usernames and lack of two factor authentication to validate user’s login details.[6]

### LITERATURE REVIEW
- Wigginton et al discovered a security vulnerability on PHPSeclib which was the PHP cryptography library being use by passbolt and this in turn made passbolt vulnerable to cypher text attacks.[13]
- Golunski in 2016 discovered security vulnerabilities in the open source MySQL database used by passbolt which in turn made passbolt vulnerable to SQL injection attacks.[14]

### RESEARCH QUESTIONS
- How secured is pass bolt password manager than the other password managers.
- What are the major vulnerabilities in a passbolt password manager?
- What are the countermeasures in solving vulnerabilities in pass bolt password managers?

### PROBLEM STATEMENT
The objective of this research is to identify vulnerabilities in passbolt and propose a way to solve the issue of multi-factor authentication.

### METHOD

#### PARTICIPANTS
Students at the university of Cincinnati who use passbolt as a password manager.

#### APARATUS & MATERIALS
- Adobe Dreamweaver Sublime text
- Xampp control panel
- Browser (Firefox and google chrome)
- MSQl server management studio
- Web camera

#### PROCEDURE
- Users will be required to enter their details which will be saved with the passbolt.
- Experiments will be carried out to detect if the vulnerabilities identified with passbolt were resolved with the enhancement made on the passbolt.

### SIGNIFICANCE
The proposed project will add an extra layer of security to the passbolt password manager by implementing the multi-factor authentication.

### REFERENCES