**BẢN BÁO CÁO VỀ LỖ HỔNG TỒN TẠI TRÊN WEBSITE**

1. Các lỗ hổng:
   1. SQLi In-band:

* Chức năng search của website
  1. SQLi Blind:
* Chức năng đăng nhập của website
  1. Stored XSS:
* Chức năng đăng bài viết của website
  1. Reflected XSS:
* Chức năng search của website
  1. DOM XSS:
  2. Directory Traversal (impact != read files):
  3. Directory Traversal (impact = read files):
  4. Vertical access controls:
* Chức năng sửa xóa người dùng dành cho admin
  1. Horizontal access controls:
* Chức năng xóa bài đăng của người dùng khác
  1. Context-dependent access controls:
  2. CSRF:
* Chức năng đổi email của người dùng

1. Nguyên nhân (root-cause):
   1. SQLi In-band:
   2. SQLi Blind:
   3. Stored XSS:
   4. Reflected XSS:
   5. DOM XSS:
   6. Directory Traversal (impact != read files):
   7. Directory Traversal (impact = read files):
   8. Vertical access controls:
   9. Horizontal access controls:
   10. Context-dependent access controls:
   11. CSRF:
2. Tác động (impact):
   1. SQLi In-band:
   2. SQLi Blind:
   3. Stored XSS:
   4. Reflected XSS:
   5. DOM XSS:
   6. Directory Traversal (impact != read files):
   7. Directory Traversal (impact = read files):
   8. Vertical access controls:
   9. Horizontal access controls:
   10. Context-dependent access controls:
   11. CSRF:
3. Cách khắc phục(fix, patch) lỗ hổng:
   1. SQLi In-band:
   2. SQLi Blind:
   3. Stored XSS:
   4. Reflected XSS:
   5. DOM XSS:
   6. Directory Traversal (impact != read files):
   7. Directory Traversal (impact = read files):
   8. Vertical access controls:
   9. Horizontal access controls:
   10. Context-dependent access controls:
   11. CSRF: