

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

-----





&





-----

**BÁO CÁO LAB 02**

**Bộ môn:** An ninh máy tính

**Giảng viên lý thuyết:** Lê Hà Minh

Lê Giang Thanh



*Hồ Chí Minh, ngày 28 tháng 08 năm 2023*

**Thông tin thành viên**

Họ tên: Phan Trí Tài

MSSV: 20127318

Email: [20127318@student.hcmus.edu.vn](mailto:20127318@student.hcmus.edu.vn)

**Phân công thực hiện**

|  |  |
| --- | --- |
| **Viết report** | Phan Trí Tài |
| **Làm bài tập** | Phan Trí Tài |

**Báo cáo bài tập**

1. **Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Lab: SQL injection vulnerability allowing login bypass**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Lab: Reflected XSS into HTML context with nothing encoded**

A screenshot of a computer

Description automatically generated

A screenshot of a web page

Description automatically generated

1. **Lab: Stored XSS into HTML context with nothing encoded**

A screenshot of a computer

Description automatically generated

A screenshot of a web page

Description automatically generated

# Lab: DOM XSS in document.write sink using source location.search

A screenshot of a computer

Description automatically generated

A screenshot of a web page

Description automatically generated

1. **Lab: DOM XSS in innerHTML sink using source location.search**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Lab: DOM XSS in jQuery anchor href attribute sink using location.search source**

**A screenshot of a computer

Description automatically generated** **A screenshot of a web page

Description automatically generated**

1. **Lab: Reflected XSS into attribute with angle brackets HTML-encoded**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

1. **Lab: Stored XSS into anchor href attribute with double quotes HTML-encoded**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

1. **Lab: Reflected XSS into a JavaScript string with angle brackets HTML encoded**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a web page

Description automatically generated**

1. **Lab: Username enumeration via different responses**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Lab: 2FA simple bypass**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Lab: Password reset broken logic**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Danh sách các Labs**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Loại tấn công | Lab | Hoàn thành |
| 1 | SQL injection | Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data | ☑ |
| 2 | SQL injection | Lab: SQL injection vulnerability allowing login bypass | ☑ |
| 3 | Cross-site scripting | Lab: Reflected XSS into HTML context with nothing encoded | ☑ |
| 4 | Cross-site scripting | Lab: Stored XSS into HTML context with nothing encoded | ☑ |
| 5 | Cross-site scripting | Lab: DOM XSS in document.write sink using source location.search | ☑ |
| 6 | Cross-site scripting | Lab: DOM XSS in innerHTML sink using source location.search | ☑ |
| 7 | Cross-site scripting | Lab: DOM XSS in jQuery anchor href attribute sink using location.search source | ☑ |
| 8 | Cross-site scripting | Lab: Reflected XSS into attribute with angle brackets HTML-encoded | ☑ |
| 9 | Cross-site scripting | Lab: Stored XSS into anchor href attribute with double quotes HTML-encoded | ☑ |
| 10 | Cross-site scripting | Lab: Reflected XSS into a JavaScript string with angle brackets HTML encoded | ☑ |
| 11 | Authentication | Lab: Username enumeration via different responses | ☑ |
| 12 | Authentication | Lab: 2FA simple bypass | ☑ |
| 13 | Authentication | Lab: Password reset broken logic | ☑ |
| 14 |  |  |  |