**BÁO CÁO BÀI THỰC HÀNH SỐ 9**

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

***Họ và tên: Huỳnh Ngọc Bảo Khánh***

***Lớp: 10\_ĐH\_TMĐT***

***MSSV:1050070038***

***Link youtube:https://youtu.be/Z0OqmHvs45o***

***Yêu cầu kết quả thực hành:***

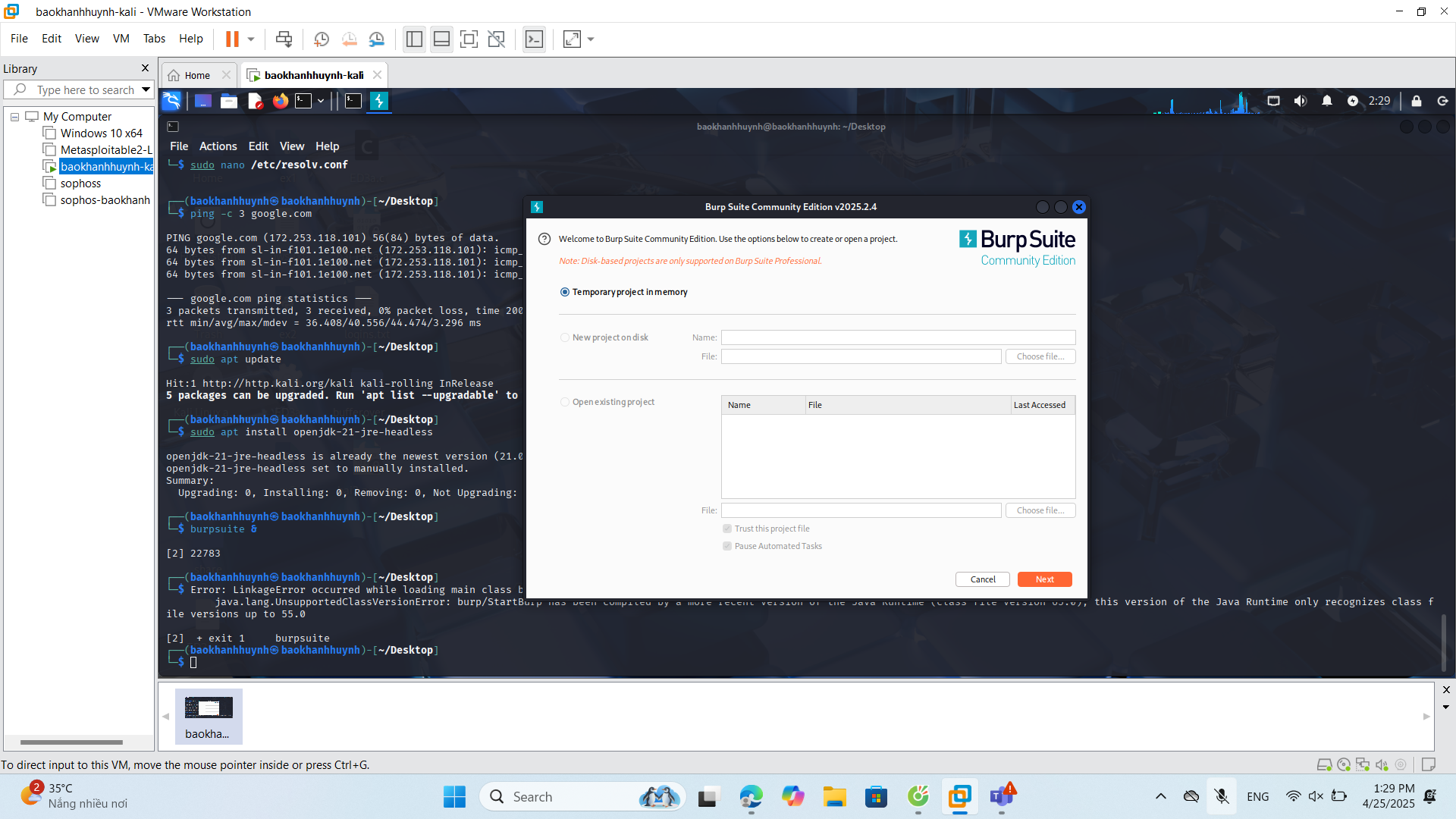
Báo cáo kết quả thực hành có tên theo định dạng HoTenSV\_MSSV\_Lab06.docx

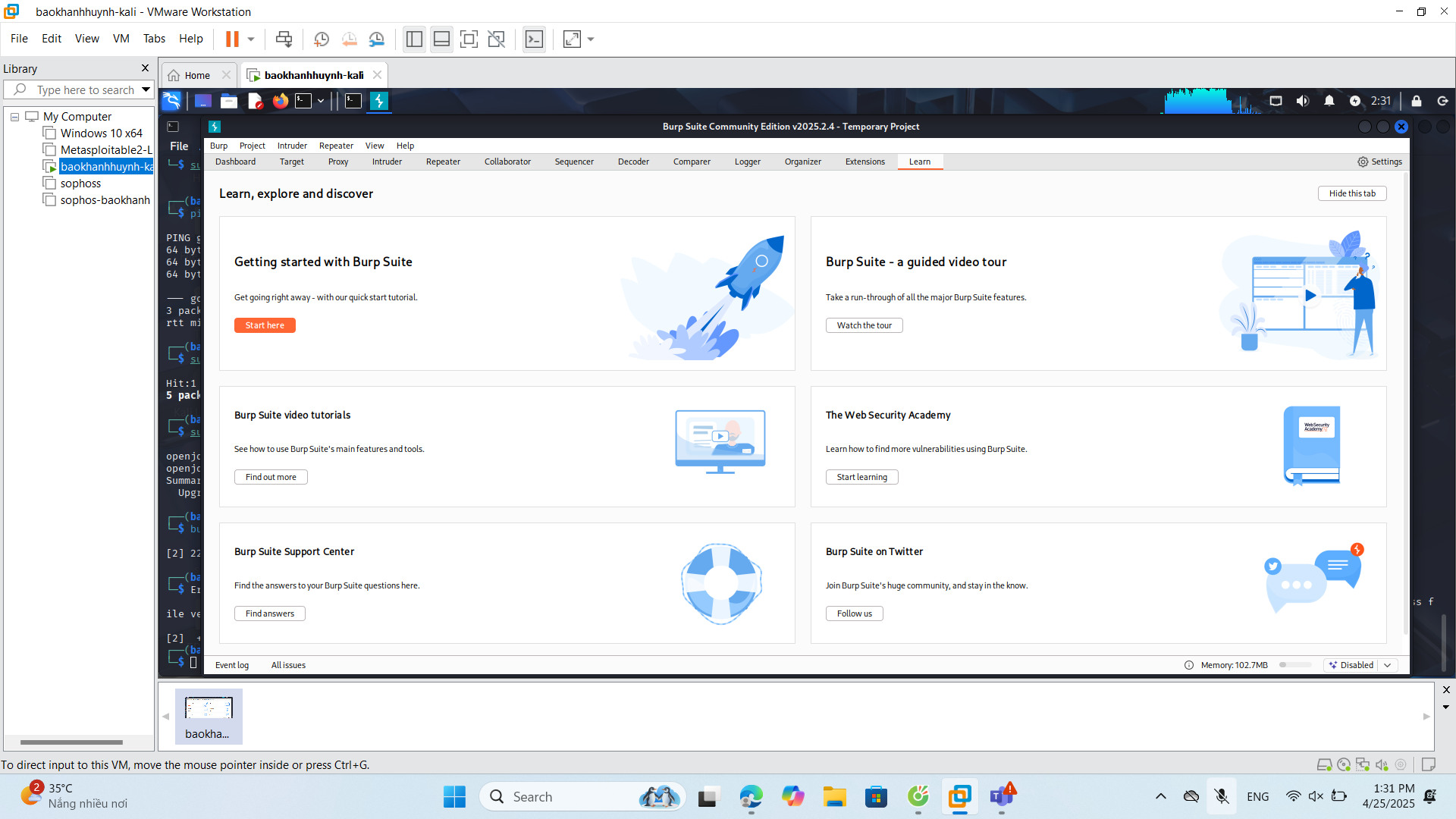
Trình bày quá trình kiểm thử theo mẫu sau

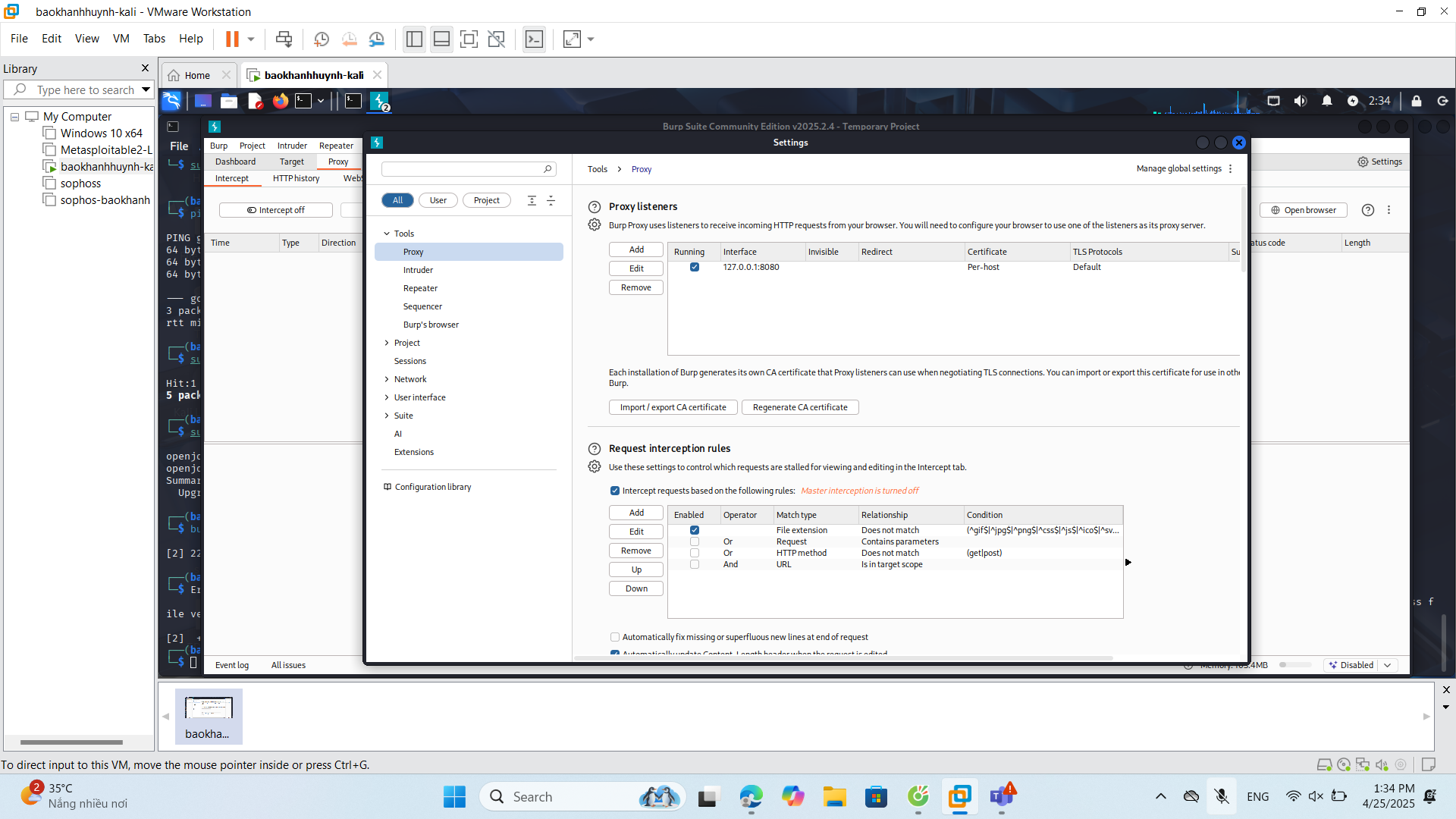
**Phần 1: Kiểm thử XSS**

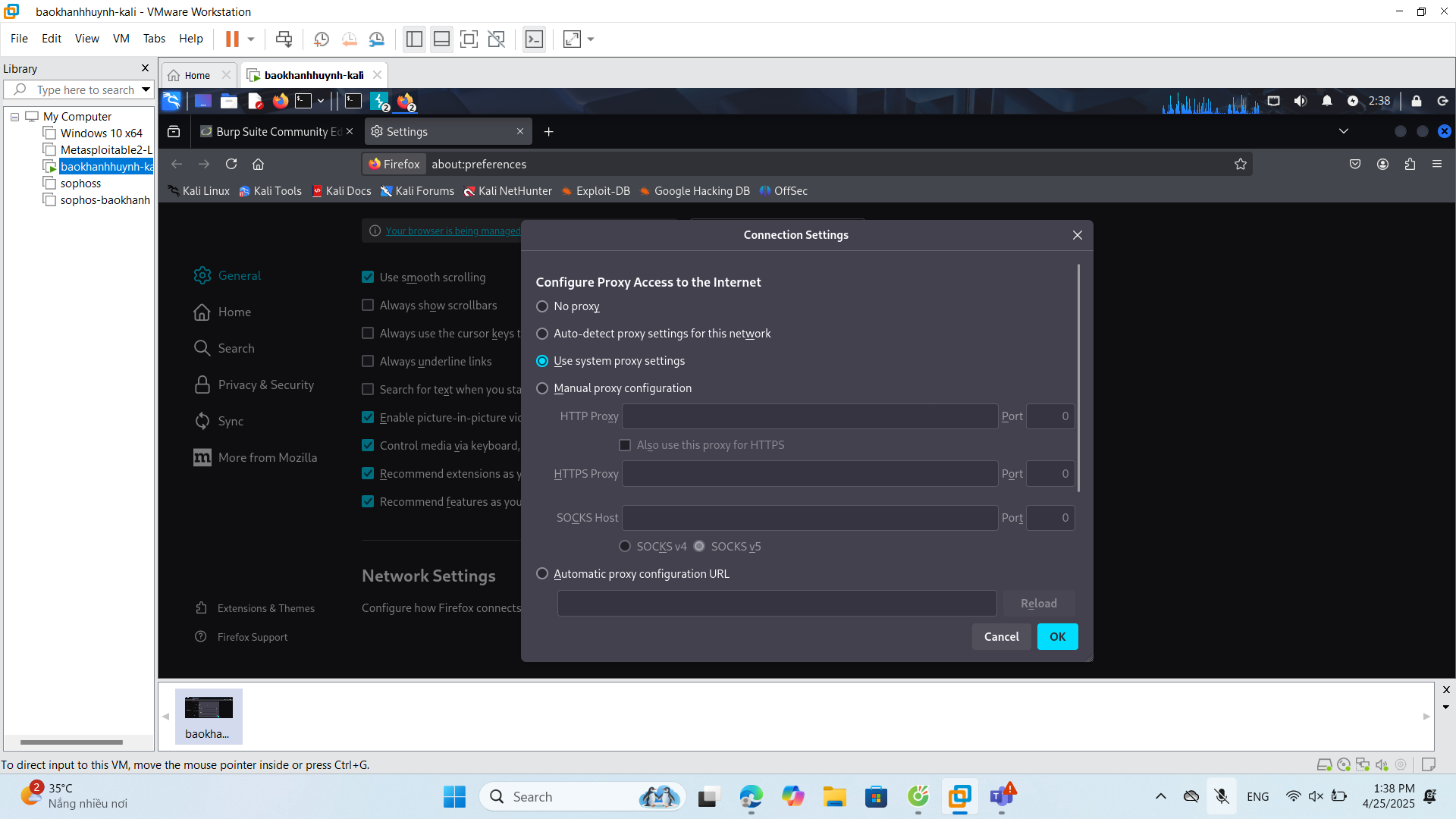
Thực hiện kiểm thử lỗ hổng XSS trên website: chọn 1 trong các trang sau để thử nghiệm

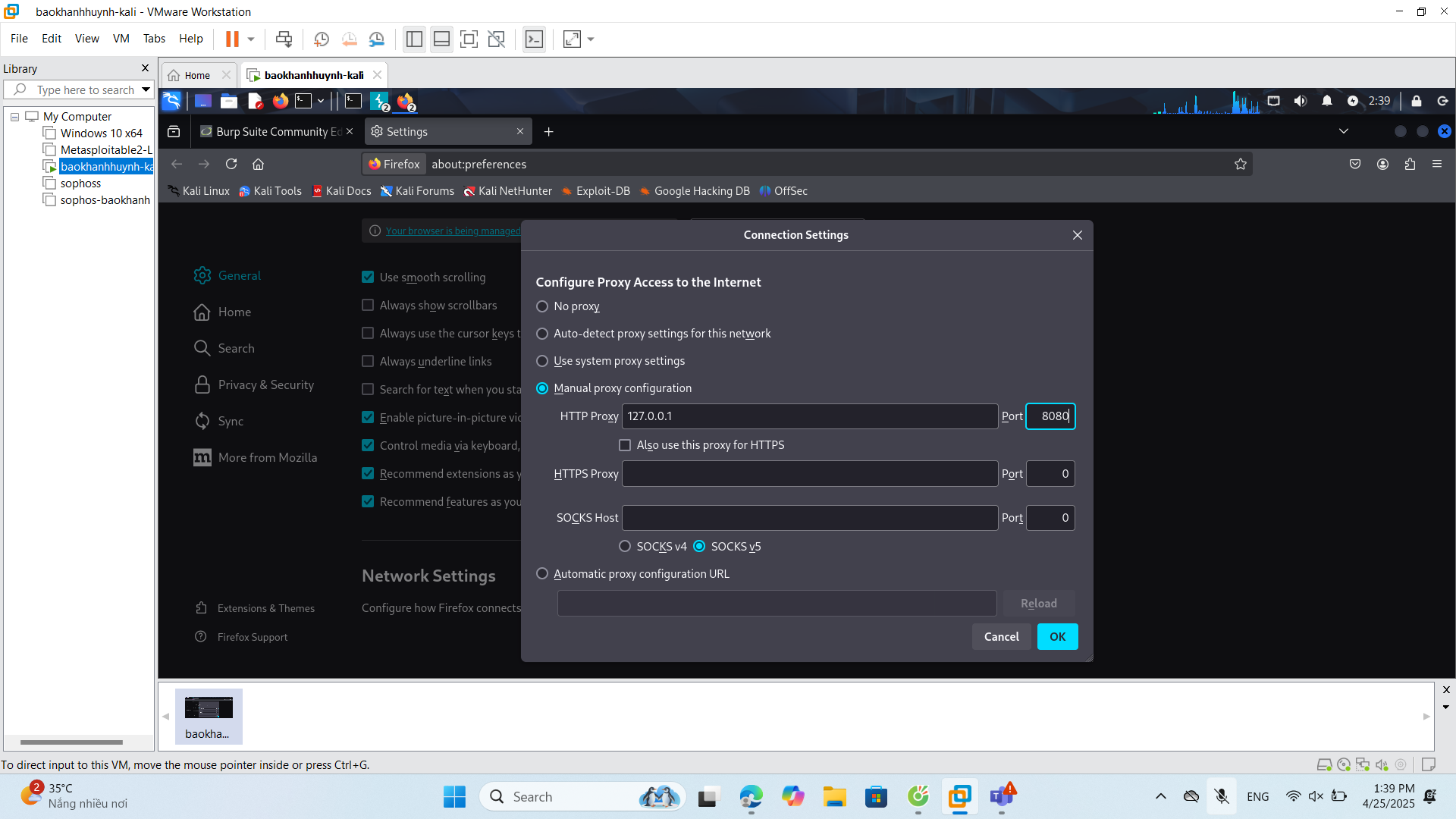
1. [http://demo.testfire.net](http://demo.testfire.net/)`
2. [http://php.testsparker.com](http://php.testsparker.com/)
3. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
4. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
5. [**http://testphp.vulnweb.com**](http://testphp.vulnweb.com/)
6. [http://www.webscantest.com](http://www.webscantest.com/)
7. [http://testhtml5.vulnweb.com](http://testhtml5.vulnweb.com/)
8. [http://aspnet.testsparker.com](http://aspnet.testsparker.com/)
9. [http://zero.webappsecurity.com](http://zero.webappsecurity.com/)

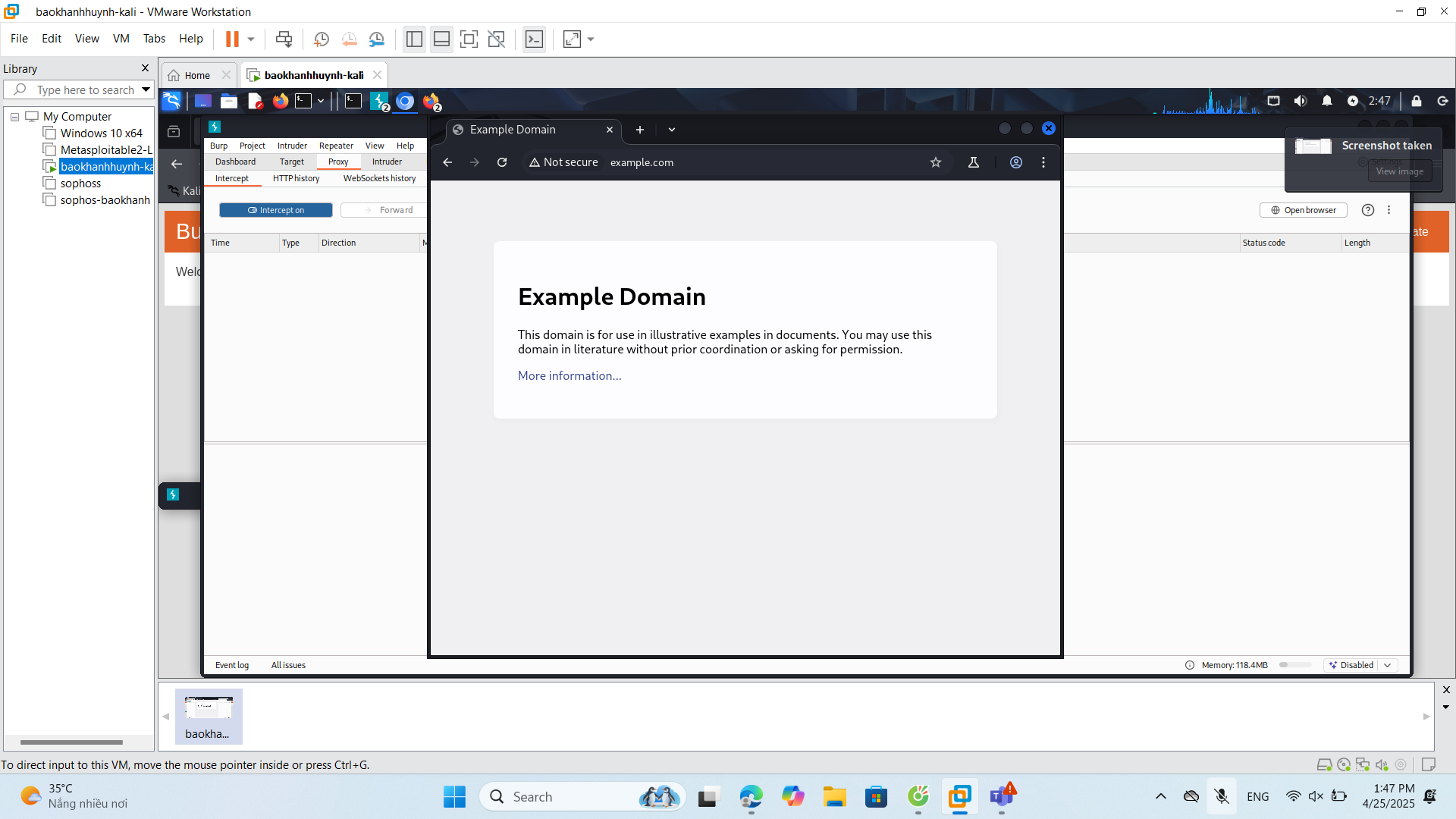
****

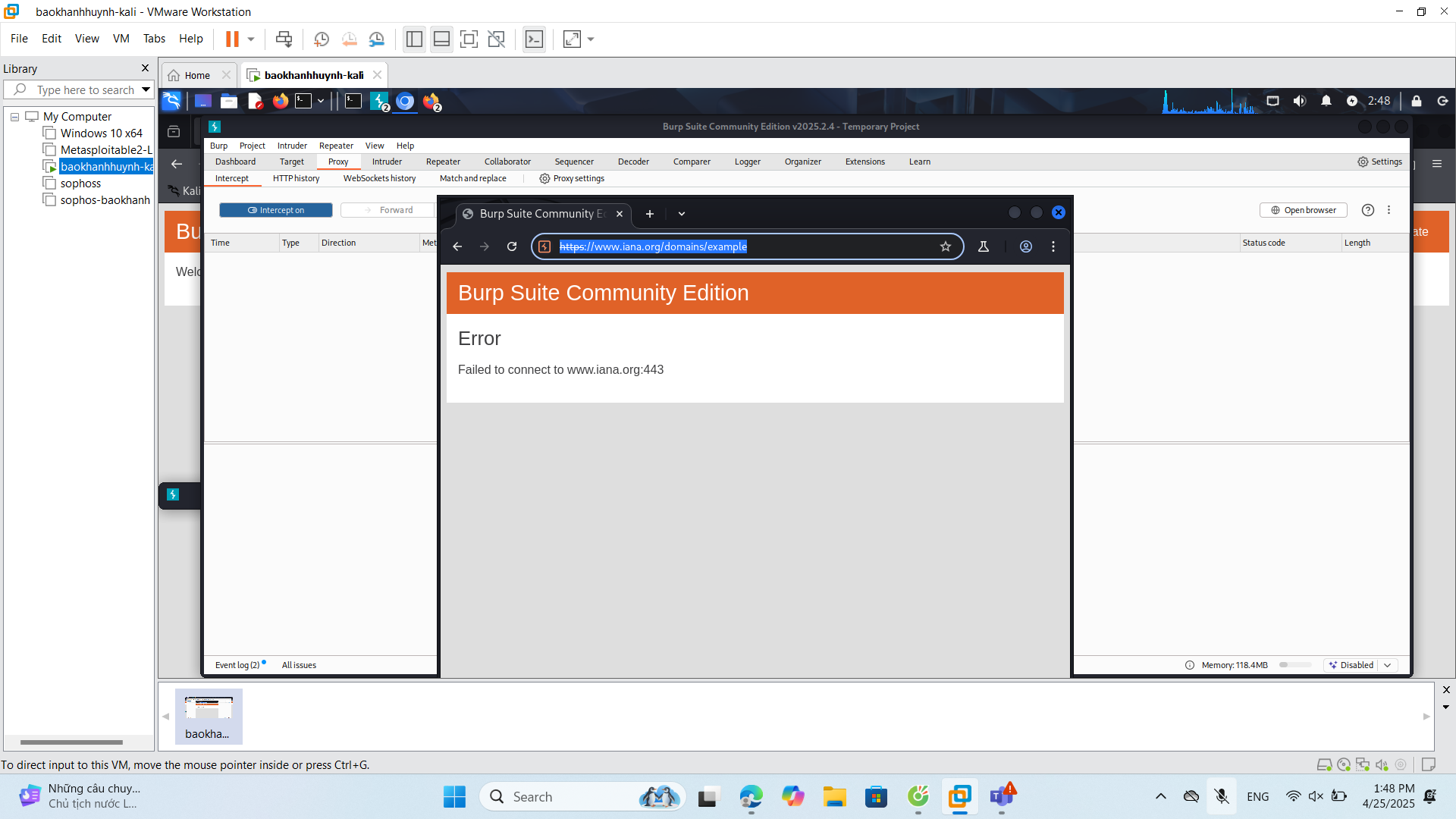
****

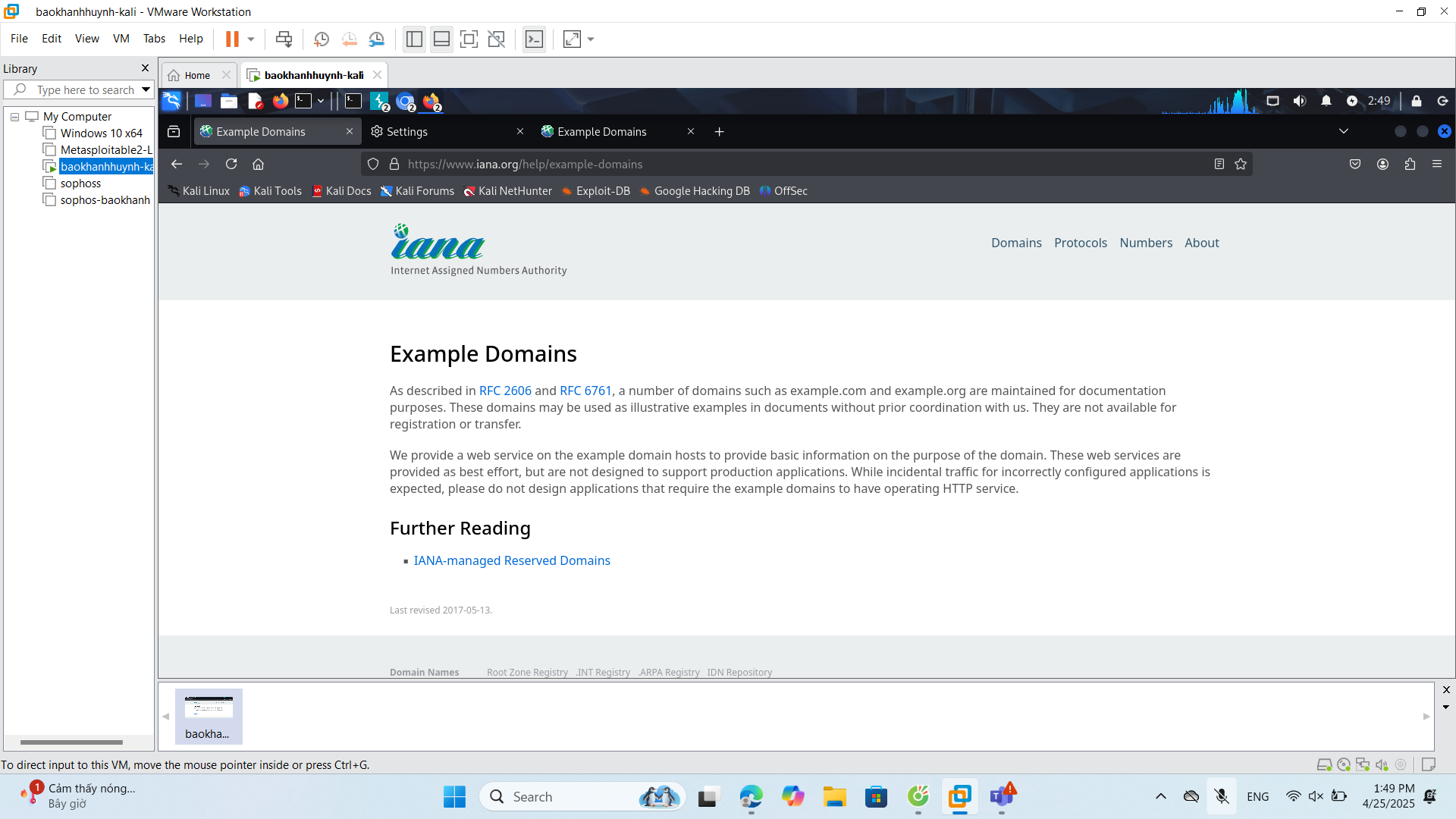
****

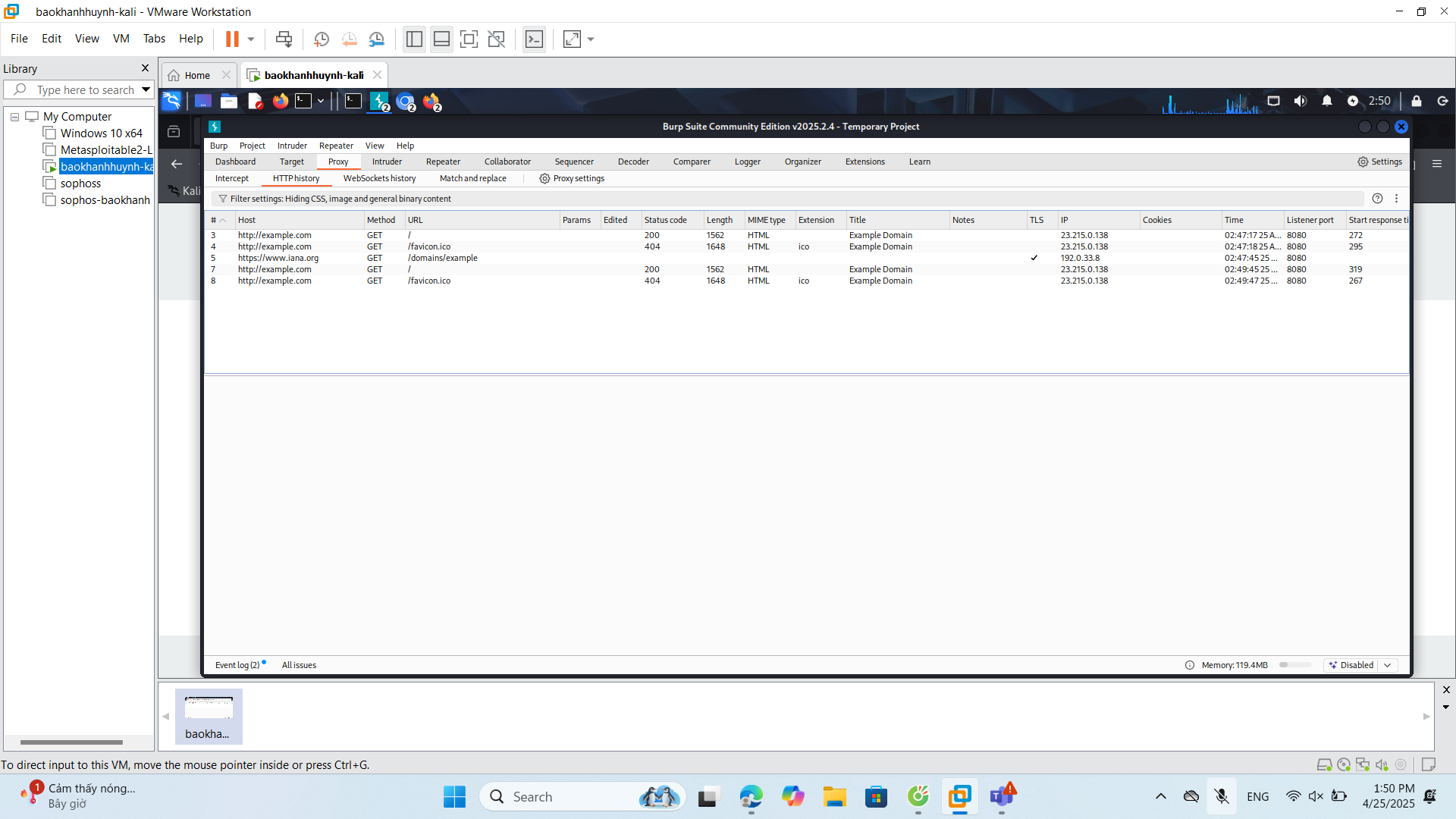
****

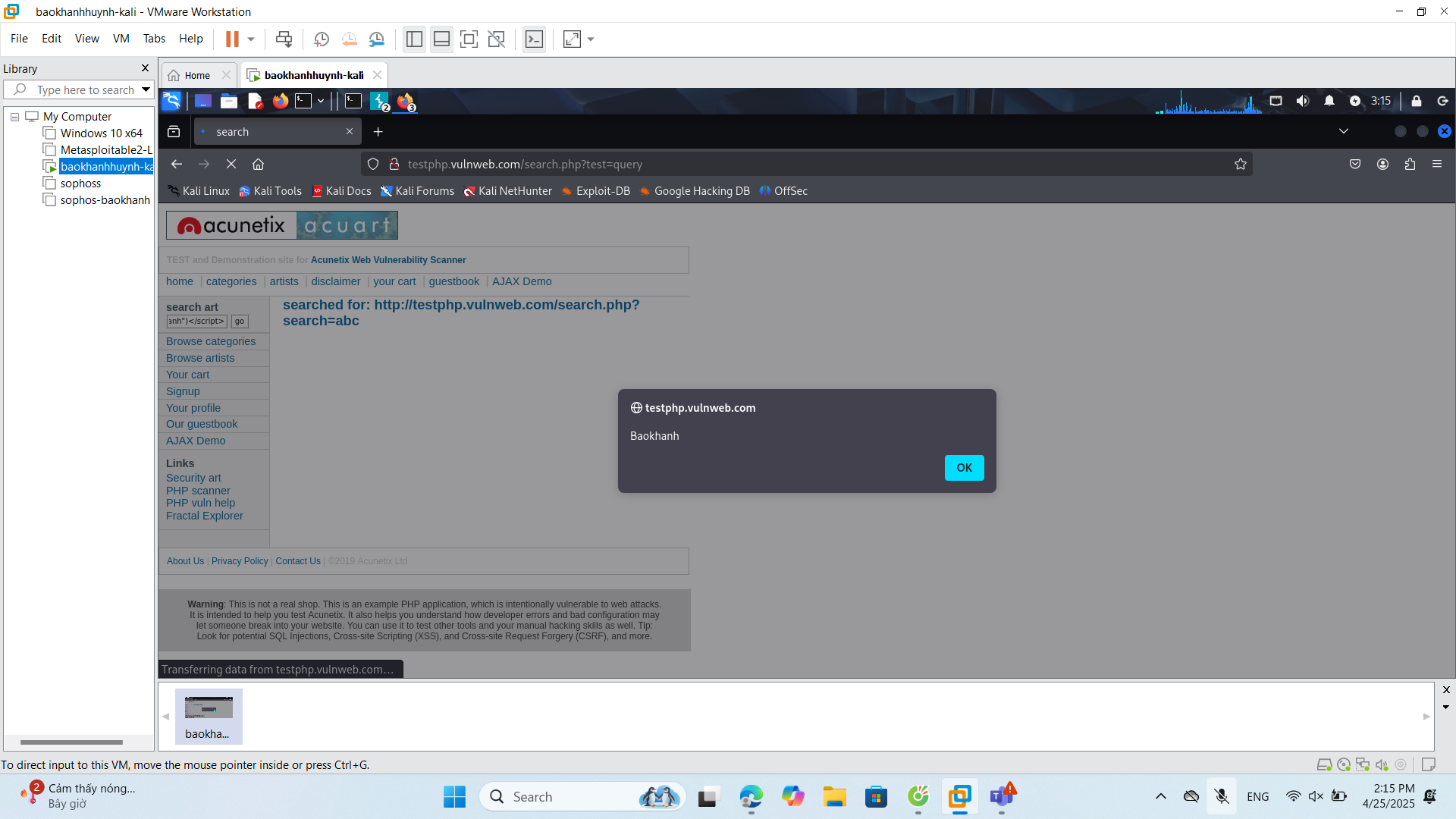
****

****

****

****

****

****

Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa 4 số cuối MSSV. Hãy giải thích:

**-** Xác định các tham số đầu vào: **http://testphp.vulnweb.com/search.php?search=<script>alert("Baokhanh")</script>**

- Xác định giá trị đầu vào xuất hiện trong trang kết quả: **Baokhanh**

**-** Các bước kiểm thử và phán đoán: **Kiểm tra phản hồi từ server có in lại giá trị hay không; thử với payload đơn giản <script>alert("baokhanh")</script> để kiểm tra phản hồi**

- Giá trị kiểm thử cho thấy lỗ hổng và giải thích: **Payload <script>alert("Baokhanh")</script> hiển thị alert ⇒ Trang không lọc dữ liệu đầu vào, có lỗ hổng XSS phản chiếu (Reflected XSS)**