BÁO CÁO ĐỒ ÁN

Môn học: BẢO MẬT WEB VÀ ỨNG DỤNG

Tên chủ đề: TÌM HIỂU VỀ CÔNG CỤ ACUNETIX

GVHD: ThS. Nguyễn Công Danh

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.O21.ANTT

STT	Họ và tên	MSSV	Email
1	Võ Quốc Huy	21520942	21520942@gm.uit.edu.vn
2	Bùi Quốc Huy	21520911	21520911@gm.uit.edu.vn
3	Nguyễn Minh Phú	21521277	21521277@gm.uit.edu.vn
4	Phạm Phúc Hậu	21520836	21520836@gm.uit.edu.vn

2. PHÂN CÔNG CÔNG VIỆC:

STT	Công việc	Thành viên thực hiện
1	Thu thập thông tin về Acunetix	Cả nhóm
2	Lên ý tưởng các kịch bản	Huy (Võ), Huy (Bùi), Hậu
3	Viết báo cáo đầu kỳ	Cả nhóm
4	Tìm cách tải Acunetix với chi phí thấp	Huy (Bùi), Hậu
5	Viết báo cáo giữa kỳ	Cả nhóm
6	Làm slide báo cáo giữa kỳ	Phú
7	Thực hiện kịch bản 1	Huy (Võ)
8	Thực hiện kịch bản 2	Huy (Võ)
9	Thực hiện kịch bản 3	Hậu
10	Thực hiện kịch bản 4	Hậu
11	Thực hiện kịch bản 5	Hậu
12	Thực hiện kịch bản 6	Huy (Bùi)
13	Viết báo cáo cuối kỳ	Huy (Bùi)
14	Làm slide báo cáo cuối kỳ	Phú
15	Báo cáo cuối kỳ	Cả nhóm

MỤC LỤC

MỤC LỤC 2
DANH MỤC HÌNH ẢNH 5
DANH MỤC BẢNG 10
DANH MỤC VIẾT TẮT 11
CHƯƠNG 1: GIỚI THIỆU TỔNG QUAN ĐỀ TÀI 13
1. Vấn đề đặt ra 13
a. Sự cần thiết của việc kiểm thử bảo mật ứng dụng web 13
b. Sự cần thiết của việc kiểm thử bảo mật tự động 13
2. Giải pháp đề ra 14
3. Mục tiêu của đồ án 14
CHƯƠNG 2: CƠ SỞ LÝ THUYẾT 15
1. Tập đoàn Gartner 15
2. XSS 15
3. SQL Injection 15
4. Directory Traversal Attacks 16
5. Parameter Manipulation 17
6. SSRF 20
7. XXE 20
8. OAuth 21
9. OpenVAS 22
10. SAST, DAST, IAST và RASP 23
CHƯƠNG 3: ACUNETIX 25
1. Acunetix là gì? 25
2. Các chức năng của Acunetix 25
a. Tổng quan 26
b. Khám phá 26
c. Mục tiêu 27
d. Quét 35
e. Lỗ hổng 37
f. Báo cáo 38
g. Người dùng 41
h. Hồ sơ quét 42
i. WAFs 43
j. Engines 44
k. Excluded Hours 45

l. Agents 45
m. Proxy Settings 45
n. Issue Trackers 46
o. Cài đặt 48
3. Một lần quét của Acunetix hoạt động thế nào? 51
4. Acunetix AcuSensor Technology 53
5. AcuSensor Bridge 55
6. Network Vulnerability Scanning 55
7. Cách cài đặt Acunetix 56
a. Yêu cầu hệ thống để cài đặt Acunetix 56
b. Cài đặt trên Windows 57
c. Cài đặt trên Linux 57
d. Kích hoạt Acunetix 57
e. Các cấu hình khác trong quá trình cài đặt Acunetix 58
f. Thêm các công nghệ quét bổ sung 58
8. Acunetix 360 là gì? 58
9. Một vài thông tin về Acunetix 360 On-Premises 62
10. Cách cài đặt Acunetix 360 On-Premises 64
a. Yêu cầu hệ thống cho Acunetix 360 Application Server 64
b. Yêu cầu hệ thống cho Acunetix 360 Agent 64
c. Yêu cầu hệ thống với Authentication Verifier Service và Authentication Verifier Agent 65
d. Yêu cầu hệ thống cho Acunetix 360 Bridge 65
e. Yêu cầu hệ thống với Database Server 66
f. Tóm tắt các bước cài đặt 66
11. Acunetix Manual Tools là gì? 67
12. Các tính năng của Acunextix Manual Tools 67
a. HTTP Editor 67
b. HTTP Fuzzer 69
c. Subdomain Scanner 71
d. HTTP Sniffer 72
e. Blind SQL Injector 74
f. Authentication Tester 76
g. Web Services Editor 79
h. Target Finder 80
13. Phiên bản Acunetix mà nhóm sử dụng 81
14. Acunetix hỗ trợ cho một cuộc tấn công 82

CHƯƠNG 4: THỰC NGHIỆM 83
1. **Các kịch bản** 83
2. **Kịch bản 1** 83
3. **Kịch bản 2** 86
4. **Kịch bản 3** 88
5. **Kịch bản 4** 92
6. **Kịch bản 5** 96
7. **Kịch bản 6** 104

CHƯƠNG 5: KẾT LUẬN VÀ ĐÁNH GIÁ 111
1. **Kết luận** 111
2. **Đánh giá** 111

TÀI LIỆU THAM KHẢO 113

GIẢI TRÌNH CHỈNH SỬA 114

DANH MỤC HÌNH ẢNH

Hình 1: Minh họa tấn công Currency Manipulation....18
Hình 2: Minh họa tấn công Mass Assignment....18
Hình 3: Minh họa tấn công Repeating an Input Parameter Multiple Times....19
Hình 4: Minh họa Data Transfer Object....19
Hình 5: Minh họa cách OAuth 2.0 hoạt động....22
Hình 6: Logo của OpenVAS....22
Hình 7: Kiến trúc của OpenVAS....22
Hình 8: Minh họa giao diện web của Acunetix....25
Hình 9: Minh hoạ trang Discovery trong Acunetix....26
Hình 10: Minh họa Settings của Discovery trong Acunetix....26
Hình 11: Minh họa Inclusions của Discovery trong Acunetix....27
Hình 12: Minh họa Exclusions của Discovery trong Acunetix....27
Hình 13: Minh họa trang Targets của Acunetix....28
Hình 14: Minh họa 5 thuộc tính đầu của Mục tiêu trong Acunetix....29
Hình 15: Minh họa thuộc tính Default Agent, Configure proxy server for agent của Mục tiêu trong Acunetix....29
Hình 16: Minh họa cấu hình Proxy Server cho Agent trong Acunetix....29
Hình 17: Minh họa thuộc tính Site Login của Mục tiêu trong Acunetix....30
Hình 18: Minh họa thuộc tính Crawling của Mục tiêu trong Acunetix....31
Hình 19: Minh họa Import Files / API Definitions của Crawling của Mục tiêu trong Acunetix....31
Hình 20: Minh họa web server yêu cầu xác thực....32
Hình 21: Minh họa HTTP Authentication của HTTP của Mục tiêu trong Acunetix....32
Hình 22: Minh họa các bước thêm Client Certificates của HTTP của Mục tiêu trong Acunetix....32
Hình 23: Minh họa thuộc tính Advanced Options của Mục tiêu trong Acunetix....33
Hình 24: Minh họa Custom Headers của Advanced Options của Mục tiêu trong Acunetix....33
Hình 25: Minh họa Custom Cookies của Advanced Options của Mục tiêu trong Acunetix....34
Hình 26: Minh họa Issue Tracker của Advanced Options của Mục tiêu trong Acunetix 34
Hình 27: Minh họa Allowed Hosts của Advanced Options của Mục tiêu trong Acunetix....34
Hình 28: Minh họa bước 1 cách thêm lần quét mới trong Acunetix....35
Hình 29: Minh họa bước 2 cách thêm lần quét mới trong Acunetix....35
Hình 30: Minh họa bước 3 cách thêm lần quét mới trong Acunetix....35
Hình 31: Minh họa Instant scan khi cấu hình lần quét trong Acunetix....35
Hình 32: Minh họa Future scan khi cấu hình lần quét trong Acunetix....36
Hình 33: Minh họa Recurrent scan....36
Hình 34: Minh họa trang Vulnerabilities trong Acunetix....37
Hình 35: Minh họa trang Reports trong Acunetix....38
Hình 36: Minh họa các loại báo cáo trong Acunetix....40

Hình 37: Minh họa trang Users trong Acunetix 41
Hình 38: Minh họa trang Scan Profiles trong Acunetix 42
Hình 39: Minh họa cấu hình WAF trong Acunetix 44
Hình 40: Giao diện Engines của Acunetix 44
Hình 41: Minh họa cấu hình Excluded Hours Profile trong Acunetix 45
Hình 42: Minh họa cấu hình Proxy Settings trong Acunetix 46
Hình 43: Minh họa cấu hình Issue Tracker trong Acunetix 47
Hình 44: Minh họa trường Custom Fields và Tags trong việc cấu hình Issue Tracker trong Acunetix 48
Hình 45: Minh họa trang Settings trong Acunetix 48
Hình 46: Minh họa các cài đặt chung của Acunetix 49
Hình 47: Minh họa cấu hình SMTP server trong Acunetix 49
Hình 48: Vị trí để truy cập Profile 50
Hình 49: Minh họa General của Profile trong Acunetix 50
Hình 50: Minh họa cài đặt thông báo của Profile trong Acunetix 50
Hình 51: Minh họa các cài đặt bảo mật của Profile trong Acunetix 51
Hình 52: Minh họa Online Services của Profile trong Acunetix 51
Hình 53: Minh họa API Key của Profile trong Acunetix 51
Hình 54: Minh họa bản đồ của trang web được tạo bởi Acunetix khi quét 52
Hình 55: Minh họa quét có dùng AcuSensor của Acunetix 52
Hình 56: Minh họa kết quả quét của Acunetix 53
Hình 57: Minh họa cấu hình AcuSensor Bridge trong Acunetix 55
Hình 58: Minh họa bằng chứng khai thác lỗ hổng SQL Injection của Acunetix 360 60
Hình 59: Minh họa báo cáo lỗ hổng XSS của Acunetix 360 với URL là thứ dùng để khai thác lỗ hổng 60
Hình 60: Sơ đồ kiến trúc của Acuntix 360 On-Premises 63
Hình 61: Xem Request header bằng Dev Tool 68
Hình 62: Giao diện HTTP Editor của AMT 68
Hình 63: Tab Request của HTTP Editor 68
Hình 64: Chỉnh sửa các trường và giá trị của Request bằng HTTP Editor 69
Hình 65: Kết quả sau khi gửi Request được chỉnh sửa bởi HTTP Editor 69
Hình 66: Generator của AMT 70
Hình 67: Number generator của AMT 70
Hình 68: Tìm thông tin về các artist trong trang web mục tiêu với HTTP Fuzzer của AMT 71
Hình 69: Kết quả của việc tìm kiếm bằng HTTP Fuzzer của AMT 71
Hình 70: Kết quả quét subdomain của "google.com" 71
Hình 71: Cấu hình Proxy cho trình duyệt Firefox 72
Hình 72: Các request được HTTP Sniffer của AMT ghi lại 72
Hình 73: Giao diện Edit Traps của HTTP Sniffer của AMT 73
Hình 74: Mẫu yêu cầu sẽ bị chặn bởi HTTP Sniffer của AMT 73
Hình 75: Lỗi không thể trích xuất dữ liệu của Blind SQL Injector của AMT 74
Hình 76: Minh họa các dữ liệu cần cấp cho Blind SQL Injector của AMT và bắt đầu tấn công 74
Hình 77: Log ghi lại lịch sử tạo các payload của Blind SQL Injector của AMT 75

Hình 78: Blind SQL Injector của AMT đưa ra thông tin về cơ sở dữ liệu của mục tiêu sau khi hoàn thành tấn công....75
Hình 79: Blind SQL Injector của AMT đưa ra dữ liệu của cơ sở dữ liệu của mục tiêu....76
Hình 80: Các đầu vào cho Authentication Tester của AMT....76
Hình 81: Giao diện web testphp trước khi đăng nhập và khi đăng nhập sai....77
Hình 82: Giao diện web testphp khi đăng nhập đúng....77
Hình 83: Chọn trường user/password cho phương thức bảo mật Web form based....78
Hình 84: Lỗi dương tính giả của Authentication Tester của AMT....78
Hình 85: Lỗi dương tính giả của Authentication Tester của AMT (2)....79
Hình 86: Cấu trúc WSDL của web mục tiêu bởi Web Services Editor của AMT....79
Hình 87: Soạn thảo yêu cầu SOAP tới HelloUser nhờ Web Services Editor của AMT....80
Hình 88: Kết quả yêu cầu SOAP tới dịch vụ HelloWorld nhờ HTTP Editor và Web Services Editor của AMT....80
Hình 89: Đầu vào cho Target Finder của AMT....80
Hình 90: Kết quả quét một dải IP nhờ Target Finder của AMT....81
Hình 91: Kết quả tra cứu IP trên https://mxtoolbox.com/ReverseLookup.aspx....81
Hình 92: Phiên bản của Acunetix CRACK....82
Hình 93: License của Acunetix bản CRACK....82
Hình 94: Tạo target http://testphp.vulnweb.com trên Acunetix....83
Hình 95: Cấu hình Mục tiêu mặc định trên Acunetix....83
Hình 96: Giao diện Acunetix sau khi bắt đầu quét – Trang thông tin của lần quét này..84
Hình 97: Danh sách các lỗ hổng quét được của mục tiêu trong lần quét này....84
Hình 98: Thông tin của một lỗ hổng trong danh sách lỗ hổng....85
Hình 99: Nhập chuỗi khai thác vào ô search art....85
Hình 100: Kết quả khai thác thành công XSS....85
Hình 101: Kết quả quét web juice shop không dùng Site Login trên Acunetix....86
Hình 102: Chọn "New" để tạo trình tự đăng nhập mới cho Site Login trên Acunetix....87
Hình 103: Ghi lại trình tự đăng nhập cho Site Login trên Acunetix....87
Hình 104: Kết quả quét web juice shop có dùng Site Login trên Acunetix....87
Hình 105: So sánh tổng quan giữa có và không dùng Site Login để quét juice shop....88
Hình 106: Challenge HTTP – Cookies của Root Me....88
Hình 107: Cấu hình proxy trên trình duyệt....88
Hình 108: Giao diện trang HTTP Sniffer của AMT....88
Hình 109: Danh sách các gói được "đánh hơi" bởi HTTP Sniffer của AMT....89
Hình 110: Cửa sổ HTTP Traps từ trang HTTP Sniffer của AMT....89
Hình 111: Thêm rule vào HTTP Traps của HTTP Sniffer của AMT....90
Hình 112: Bắt đầu Challenge HTTP - Cookie....90
Hình 113: Phân tích yêu cầu POST có trường Cookie được chặn nhò HTTP Traps....90
Hình 114: Sửa trường Cookie của yêu cầu bị chặn bởi HTTP Trap của HTTP Sniffer của AMT....91
Hình 115: Flag của challeng HTTP – Cookie....91
Hình 116: Challenge Postbook của Root Me....92
Hình 117: Giao diện của trang web mục tiêu của challenge Postbook sau khi đăng nhập thành công....92
Hình 118: Yêu cầu GET bắt được sau khi click "Hello everyone"....93

Hình 119: Thêm $(Gen_5) vào yêu cầu GET ở trên trong HTTP fuzzer của AMT 93
Hình 120: Kết quả của HTTP Fuzzer của AMT sau khi Brute-force để tìm các post 94
Hình 121: Flag 1 được tìm thấy trong post có id=2 94
Hình 122: Tạo post mới trên trang web mục tiêu của challenge Postbook 95
Hình 123: Post được tạo thành công trên trang web mục tiêu của challenge Postbook 95
Hình 124: Bắt được gói yêu cầu POST để chỉnh sửa bài post được gửi tới trang web bằng Dev Tool 95
Hình 125: Payload của yêu cầu bắt được 95
Hình 126: Yêu cầu được chỉnh sửa và phản hồi có chứa flag của nó trong HTTP Editor của AMT 96
Hình 127: Trang chứa Flag 2 của challenge 96
Hình 128: Nội dung index.html sau sửa đổi 97
Hình 129: Nội dung catfile.php 97
Hình 130: Giao diện web được tạo cho kịch bản 5 97
Hình 131: Giao diện của catfile.php 98
Hình 132: Mục tiêu có địa chỉ là IP của máy Kali Linux 98
Hình 133: Bật AcuSensor ở phần cấu hình Mục tiêu 98
Hình 134: Mục tiêu đã tạo trước đó 99
Hình 135: Quét lỗ hổng có mức độ nghiêm trọng cao 99
Hình 136: Kết quả quét trang trang web PHP nội bộ bằng Acunetix 100
Hình 137: Thông tin lỗ hổng Directory traversal quét được nhờ AcuSensor 100
Hình 138: Khuyến nghị sửa lỗ hổng Directory Traversal của Acunetix 101
Hình 139: Tệp catfile.php sau chỉnh sửa để vá lỗ hổng Directory Traversal 101
Hình 140: Thông tin lỗ hổng PHP allow_url_fopen enabled quét được nhờ AcuSensor 102
Hình 141: Khuyến nghị sửa lỗ hổng PHP allow_url_fopen enabled của Acunetix 102
Hình 142: Thông tin lỗ hổng PHP open_basedir is not set quét được nhờ AcuSensor 103
Hình 143: Khuyến nghị sửa lỗ hổng PHP open_basedir is not set của Acunetix 103
Hình 144: Tổng quan kết quả quét trước và sau khi vá lỗ hổng 103
Hình 145: Trang web mục tiêu – DVWA 104
Hình 146: Repository DVWA-Issue-Tracker trên Github để lưu trữ các Issue 104
Hình 147: Mục tiêu nằm trong nhóm mục tiêu Local Web trên Acunetix 105
Hình 148: Thêm Issue Tracker cho Acunetix 105
Hình 149: Thêm tên và chọn nhóm mục tiêu cho Issue Tracker 106
Hình 150: Tạo PAT cho Issue Tracker 106
Hình 151: Tùy chỉnh cho “Issue Tracker Platform and Authentication” 107
Hình 152: Các tag Label trên Github 107
Hình 153: Các tùy chỉnh của “Project and Issue Type” 108
Hình 154: Thêm Issue Tracker cho Mục tiêu trên Acunetix 108
Hình 155: Kết quả quét Mục tiêu của Acunetix 108
Hình 156: Gửi thông tin lỗ hổng đến Issue Tracker 109
Hình 157: Thông báo gửi thành công đến Issue Tracker 109
Hình 158: Repository trên Github nhận được các vấn đề 109
Hình 159: Một vấn đề được gửi lên Issue Track bởi Acunetix 110

Hình 160: Giá Acunetix theo softvn.vn 112
Hình 161: Giá Acunetix 360 theo insight.com 112

DANH MỤC BẢNG

Bảng 1: Bảng phân quyền các vai trò đối với các chức năng 42
Bảng 2: Yêu cầu hệ thống của Acunetix v24.5 57
Bảng 3: Bảng liệt kê các điểm nổi bật của Acunetix 360 60
Bảng 4: Bảng so sánh menu giữa Acunetix 360 On-Demand và On-Premises 62
Bảng 5: Bảng so sánh sơ bộ Acunetix Standard, Premium và 360 62
Bảng 6: Yêu cầu hệ thống cho Acunetix 360 Application Server 64
Bảng 7: Yêu cầu hệ thống cho Acunetix 360 Agent 65
Bảng 8: Yêu cầu hệ thống với Authentication Verifier Service và Authentication Verifier Agent 65
Bảng 9: Yêu cầu hệ thống cho Acunetix 360 Bridge 66
Bảng 10: Yêu cầu hệ thống với Database Server 66
Bảng 11: Bảng giải trình chỉnh sửa cho báo cáo cuối cùng 114

DANH MỤC VIẾT TẮT

Viết tắt	Viết đầy đủ
SQL	Structured query language
URL	Uniform Resource Locator
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Security
XSS	cross-Site Scripting
DOM	Document Object Model
WAF	Web Application Firewall
IPS	Intrusion Prevention System
API	Application Programming Interface
CWE	Common Weakness Enumeration
HIPAA	Federal Health Insurance Portability and Accountability Act
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
DISA	Defense Information Systems Agency
STIG	Security Technical Implementation Guide
WASC	Web Application Security Consortium
CSV	Comma-Separated Values
XML	eXtensible Markup Language
ASM	Application Security Manager
AWS	Amazon Web Services
IP	Internet Protocol
TFS	Team Foundation Server
PAT	Personal Access Token
IAST	Interactive Application Security Testing
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
FTP	File Transfer Protocol
DNS	Domain Name System
IMAP	Internet Message Access Protocol
POP	Post Office Protocol
SSH	Secure SHell
SNMP	Simple Network Management Protocol
CPU	Central Processing Unit
RAM	Random Access Memory
UI	User Interface
SSRF	Server-Side Request Forgery

XXE	XML eXternal Entity
POE	Proof Of Exploit
POC	Proof Of Concept
SDLC	Systems Development Life Cycle
CI	Continuous Integration
LFI	Local File Inclusion
RFI	Remote File Inclusion
IIS	Internet Information Services
RDP	Remote Desktop Protocol
ZAP	Zed Attack Proxy
CORS	Cross-Origin Resource Sharing
AI	Artificial Intelligence
OAuth	Open Authorization
OpenVAS	Open Vulnerability Assessment Scanner
GVM	Greenbone Vulnerability Management
GPL	GNU General Public License
NASL	Nessus Attack Scripting Language
GVMd	Greenbone Vulnerability Manager daemon
GSA	Greenbone Security Assistant
OSP	Open Scanner Protocol
GMP	Greenbone Management Protocol
NVT	Network Vulnerability Test
SAST	Static Application Security Testing
DAST	Dynamic Application Security Testing
RASP	Run-time Application Security Protection
DTD	Document Type Definition
XE	eXternal Entity
AMT	Acunetix Manual Tools
WSDL	Web Services Description Language
SOAP	Simple Object Access Protocol
DVWA	Damn Vulnerable Web App

CHƯƠNG 1: GIỚI THIỆU TỔNG QUAN ĐỀ TÀI

Ở chương này, nhóm sẽ giới thiệu một cách tổng quan về đề tài và đồ án mà nhóm thực hiện.

1. Vấn đề đặt ra

a. Sự cần thiết của việc kiểm thử bảo mật ứng dụng web

Bảo mật trang web là vấn đề bị bỏ qua nhiều nhất hiện nay trong việc bảo mật doanh nghiệp và nên là ưu tiên hàng đầu trong bất kỳ tổ chức nào. Ngày càng có nhiều tin tặc tập trung tấn công vào các ứng dụng web như giỏ hàng, biểu mẫu, trang đăng nhập, nội dung động, ... Việc có thể truy cập 24/7 từ mọi nơi trên thế giới của các ứng dụng web không an toàn có thể cung cấp quyền truy cập vào cơ sở dữ liệu của công ty cho tin tặc và tạo điều kiện cho tin tặc thực hiện các hoạt động bất hợp pháp bằng cách sử dụng các trang web bị tấn công. Trang web của nạn nhân có thể được sử dụng để tổ chức các hoạt động bất hợp pháp như lưu trữ các trang web lừa đảo hoặc vận chuyển nội dung bất hợp pháp, đồng thời lạm dụng băng thông của trang web và khiến chủ sở hữu phải chịu trách nhiệm về những hành vi bất hợp pháp này.

Tin tặc đã tổ chức hàng loạt các cuộc tấn công SQL Injection, Cross Site Scripting, Directory Traversal Attacks, Parameter Manipulation (ví dụ: URL, Cookie, HTTP header, web form), Authentication Attacks, Directory Enumeration, ..., nhằm vào các doanh nghiệp.

Cộng đồng hacker cũng rất đoàn kết, các cuộc tấn công ứng dụng web mới hoàn toàn, được gọi là khai thác Zero Day, được đăng trên một số diễn đàn và trang web chỉ được biết đến với các thành viên của nhóm "ngầm" độc quyền đó. Các bài đăng được cập nhật hàng ngày và được sử dụng để tuyên truyền và tạo điều kiện cho cuộc tấn công mới.

Các ứng dụng web như giỏ hàng, biểu mẫu, trang đăng nhập, nội dung động, ..., được thiết kế để cho phép khách truy cập trang web của ta để truy xuất và gửi nội dung động bao gồm dữ liệu cá nhân và dữ liệu nhạy cảm ở nhiều mức độ khác nhau. Nếu các ứng dụng web này không an toàn, thì toàn bộ cơ sở dữ liệu chứa thông tin nhạy cảm sẽ gặp rủi ro nghiêm trọng. Một nghiên cứu của Tập đoàn Gartner cho thấy 75% các cuộc tấn công mạng được thực hiện ở cấp độ ứng dụng web.

Việc kiểm thử bảo mật web để vá các lỗ hổng sẽ giảm thiểu được tình trạng trên. Việc liên tục cập nhật tính năng đi kèm với liên tục tìm và vá các lỗ hổng mới sẽ gây khó cho các hacker trong việc thực hiện khai thác Zero Day.

b. Sự cần thiết của việc kiểm thử bảo mật tự động

Việc kiểm thử lỗ hổng bảo mật một cách thủ công đối với các ứng dụng web rất phức tạp và tốn thời gian vì nó thường liên quan đến việc xử lý một khối lượng lớn dữ liệu. Nó cũng đòi hỏi trình độ chuyên môn cao và khả năng theo dõi khối lượng mã đáng kể được sử dụng trong ứng dụng web. Ngoài ra, tin tặc liên tục tìm ra những cách mới để khai thác ứng dụng web của ta, điều đó có nghĩa là ta sẽ phải liên tục theo dõi cộng

đồng bảo mật và tìm ra các lỗ hổng mới trong mã ứng dụng web của mình trước khi tin tặc phát hiện ra chúng.

Việc có thể quét lỗ hổng tự động cho phép ta tập trung hơn vào nhiệm vụ vốn đã đầy thử thách là xây dựng ứng dụng web. Một trình quét bảo mật ứng dụng web tự động sẽ luôn tìm kiếm các đường tấn công mà tin tặc có thể sử dụng để truy cập vào ứng dụng web của ta hoặc dữ liệu của nó.

2. Giải pháp đề ra

Công cụ Acunetix bởi Invicti Security là một công cụ kiểm tra bảo mật ứng dụng web tự động giúp kiểm tra các ứng dụng web của ta bằng cách kiểm tra các lỗ hổng như SQL Insert, Cross-site scripting và các lỗ hổng có thể khai thác khác. Nói chung, Acunetix quét bất kỳ trang web hoặc ứng dụng web nào có thể truy cập được qua trình duyệt web và sử dụng giao thức HTTP/HTTPS.

3. Mục tiêu của đồ án

Nhóm sẽ tìm hiểu thật kỹ về Acunetix về mặt thông tin như Acunetix là gì, hoạt động thế nào, có các chức năng gì, các chức năng hoạt động ra sao, ...

Nhóm sẽ cố gắng tìm cách cài đặt một bản Acunetix với chi phí thấp nhất có thể và dùng nó thể triển khai các kịch bản mà nhóm cho rằng có thể sử dụng Acunetix như thế.

Qua đó giới thiệu tới người đọc về Acunetix - một công cụ kiểm thử tiên tiến.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

Ở chương này, nhóm sẽ tổng hợp các khái niệm, lý thuyết về các lĩnh vực, thuật ngữ có liên quan đến đề tài.

1. Tập đoàn Gartner

Tập đoàn Gartner là một công ty tư vấn và nghiên cứu công nghệ hàng đầu thế giới của Mỹ có trụ sở tại Stamford, Connecticut, chuyên tiến hành nghiên cứu về công nghệ và chia sẻ nghiên cứu này thông qua tư vấn tư nhân cũng như các chương trình và hội nghị điều hành.

2. XSS

XSS là viết tắt của Cross-site Scripting, có nghĩa là chèn mã độc (thường là Javascript) vào các ứng dụng trang web. Khi người dùng truy cập vào trang web bị nhiễm mã độc, trình duyệt sẽ tự động thực thi mã độc đó.

Có 3 loại tấn công lỗ hổng XSS phổ biến, gồm:

- Reflected XSS: Mã độc được chèn vào các URL, khi người dùng click vào URL đó thì mã độc sẽ được thực thi.
- Stored XSS: Mã độc được lưu trữ trên máy chủ, khi người dùng truy cập vào trang web sẽ kích hoạt mã độc.
- DOM - based XSS: Sử dụng các kỹ thuật JavaScript để thay đổi nội dung trang web và chèn mã độc vào DOM.

Kẻ tấn công lợi dụng lỗ hổng XSS thường hướng đến các mục đích như:

- Đánh cắp thông tin người dùng (cookie, token,...).
- Điều khiển hoạt động của ứng dụng trang web.
- Phát tán mã độc sang các máy khác.
- Đánh cắp quyền điều khiển tài khoản người dùng.

Cách phát hiện, ngăn chặn:

- Sử dụng công cụ quét lỗ hổng: Các công cụ như Acunetix, Burp Suite,... có thể tìm ra các lỗ hổng XSS trên trang web.
- Mã hóa dữ liệu đầu vào: Mã hóa, chuẩn hóa, lọc các dữ liệu do người dùng nhập vào để tránh chèn mã độc vào cơ sở dữ liệu.
- Sử dụng thư viện chống XSS: Các thư viện như DOMPurify, js-xss giúp làm sạch các đoạn mã độc trước khi hiển thị lên website.
- Cấu hình CORS: Giới hạn truy cập tài nguyên giữa các trang web khác nhau để ngăn chặn XSS.

3. SQL Injection

SQL injection – còn được gọi là SQLi – sử dụng những lỗ hổng trong các kênh đầu vào (input) của trang web để nhắm mục tiêu vào cơ sở dữ liệu nằm trong phần back-end

của ứng dụng web, nơi lưu giữ những thông tin nhạy cảm và có giá trị nhất. Chúng có thể được kẻ tấn công sử dụng để ăn cắp hoặc xáo trộn dữ liệu, cản trở sự hoạt động của các ứng dụng, và trong trường hợp xấu nhất, nó có thể chiếm được quyền truy cập quản trị vào máy chủ cơ sở dữ liệu.

Phân loại SQL Injection:

- In-band SQLi: Xảy ra khi hacker có thể tổ chức tấn công và thu thập kết quả trực tiếp trên cùng một kênh liên lạc. Phân làm 2 loại:
    - Error-based SQLi: Là một kỹ thuật tấn công SQL Injection dựa vào thông báo lỗi được trả về từ Database Server có chứa thông tin về cấu trúc của cơ sở dữ liệu.
    - Union-based SQLi: Là một kỹ thuật tấn công SQL Injection dựa vào chức năng của toán tử UNION trong ngôn ngữ SQL cho phép tổng hợp kết quả của 2 hay nhiều câu truy vấn SELECTION trong cùng 1 kết quả và được trả về như một phần của HTTP response.
- Inferential SQLi (Blind SQLi): Kẻ tấn công cố gắng xây dựng lại cấu trúc cơ sở dữ liệu bằng việc gửi đi các payloads, dựa vào kết quả phản hồi của web application và kết quả hành vi của database server. Phân làm 2 loại:
    - Blind-boolean-based: Là kĩ thuật tấn công SQL Injection dựa vào việc gửi các truy vấn tới cơ sở dữ liệu bắt buộc ứng dụng trả về các kết quả khác nhau phụ thuộc vào câu truy vấn là True hay False.
    - Time-based Blind SQLi: Là kĩ thuật tấn công dựa vào việc gửi những câu truy vấn tới cơ sở dữ liệu và buộc cơ sở dữ liệu phải chờ một khoảng thời gian (thường tính bằng giây) trước khi phản hồi.
- Out-of-band SQLi: Kiểu tấn công này xảy ra khi hacker không thể trực tiếp tấn công và thu thập kết quả trực tiếp trên cùng một kênh (In-band SQLi), và đặc biệt là việc phản hồi từ server là không ổn định, phụ thuộc vào các tính năng được bật trên Database Server được sử dụng bởi ứng dụng Web.

Cách ngăn chặn:

- Không tin tưởng vào input của người dùng, giữ suy nghĩ này khi thiết kế.
- Kiểm tra các chuỗi input ở phía máy chủ, đảm bảo input là hợp lệ và vô hiệu hóa bất kỳ lệnh độc hại tiềm ẩn nào có thể được nhúng trong chuỗi nhập.
- Sử dụng các câu lệnh tham số hay placeholder.
- Khai báo rõ ràng kiểu input.
- Tránh dùng quyền quản trị để kết nối ứng dụng web với máy chủ cơ sở dữ liệu.
- Mã hóa dữ liệu nhạy cảm trong cơ sở dữ liệu.
- Không lưu trữ dữ liệu nhạy cảm không cần thiết trên cơ sở dữ liệu.

4. Directory Traversal Attacks

Directory traversal là một dạng tấn công cho phép Hacker truy cập vào các thư mục và tập tin cấm trên máy chủ (Web Server). Nếu như truy cập thành công thì Hacker

có thể xem được các File, Thư mục cấm và có thể thực thi được các câu lệnh trên máy chủ. Đa số các máy chủ mắc lỗi này đều không kiểm đầu vào dữ liệu được gửi từ phía máy khách hàng. Dạng tấn công này còn có tên gọi khác như Dot-Dot_Slash, Directory Climbing, Path Traversal và Backtracking.

Cách phát hiện và ngăn chặn:

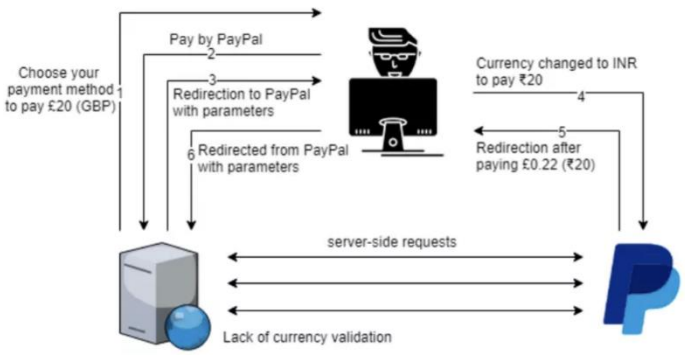
- Cách tốt nhất để kiểm tra liệu trang web hay ứng dụng web có tồn tại lỗ hổng Directory Traversal là sử dụng trình quét lỗ hổng web. Nó sẽ giúp ta quét toàn bộ trang web và tự động kiểm tra lỗ hổng. Sau đó báo cáo và ta có thể dễ dàng sửa chữa.
- Để ngăn chặn lỗ hổ nên đảm bảo rằng ta cài đặt máy chủ web với phần mềm mới nhất, các bản vá có sẵn đã được áp dụng. Thứ hai, cần có bộ lọc cho bất kì dữ liệu đầu vào từ người dùng, đặc biệt các đầu vào có dạng như một đường dẫn.

5. Parameter Manipulation

Loại tấn công bằng cách, thay đổi hoặc thêm bớt các tham số trong yêu cầu được gửi từ người dùng lên máy chủ để khiến các ứng dụng thực hiện mọi việc theo cách mà người dùng thường không thể làm được như bình thường.

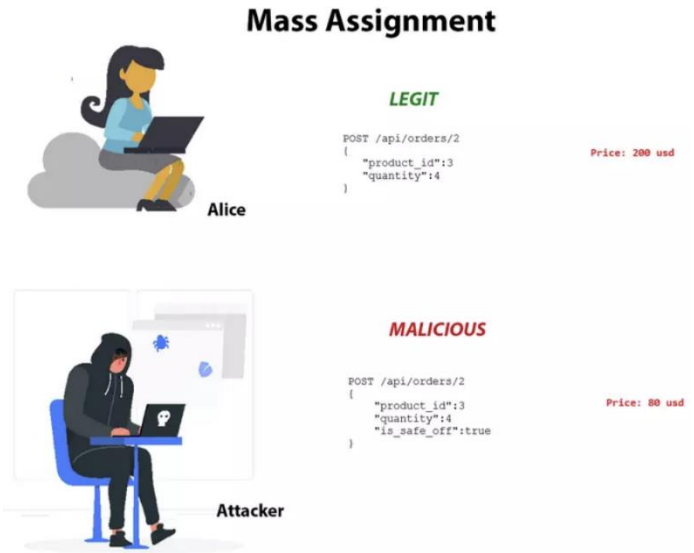
Phân loại:

- Price Manipulation: Thông thường các ứng dụng thanh toán sẽ sử dụng các tham số trong yêu cầu của người dùng gửi lên để xác định được sản phẩm mà người dùng muốn mua (thông qua id của sản phẩm), số lượng sản phẩm họ muốn mua, địa chỉ giao hàng, số điện thoại... Tuy nhiên, giá của sản phẩm là trường mà người dùng sẽ không được nhập. Các ứng dụng web có thể tính giá tiền của đơn hàng bằng cách nhận kèm một hidden param ở trong <form> là giá của sản phẩm hoặc truy vấn giá của sản phẩm từ cơ sở dữ liệu. Với cách làm sử dụng hidden param sẽ dễ bị kẻ tấn công can thiệp và sửa giá sản phẩm bằng các công cụ proxy như BurpSuite để thay đổi giá trị đơn hàng. Còn với cách truy vấn giá từ cơ sở dữ liệu thì kẻ tấn công sẽ không thể tấn công bằng cách trên.
- Currency Manipulation: Lợi dụng lỗ hổng xuất hiện khi người dùng sử dụng nhiều đơn vị tiền tệ khác nhau trong quá trình thanh toán. Ví dụ: người dùng thanh toán £20 (20 bảng anh) cho một trang web và người dùng này sử dụng tùy chọn thanh toán PayPal; kẻ tấn công sẽ sửa yêu cầu được gửi từ trang web đến trang web PayPal, thay đổi tham số tiền tệ từ “GBP” (Bảng Anh) sang “INR” (Rupee Ấn Độ); sau khi hoàn tất giao dịch trên trang web PayPal với 20 Rupee Ấn Độ, trang web đã ủy quyền giao dịch mà không kiểm tra số tiền nhận được. Như vậy, người dùng thanh toán thành công đơn hàng với giá 20 bảng Anh trong khi chỉ mất có £0,22 (20 Rupee) trong tài khoản PayPal.



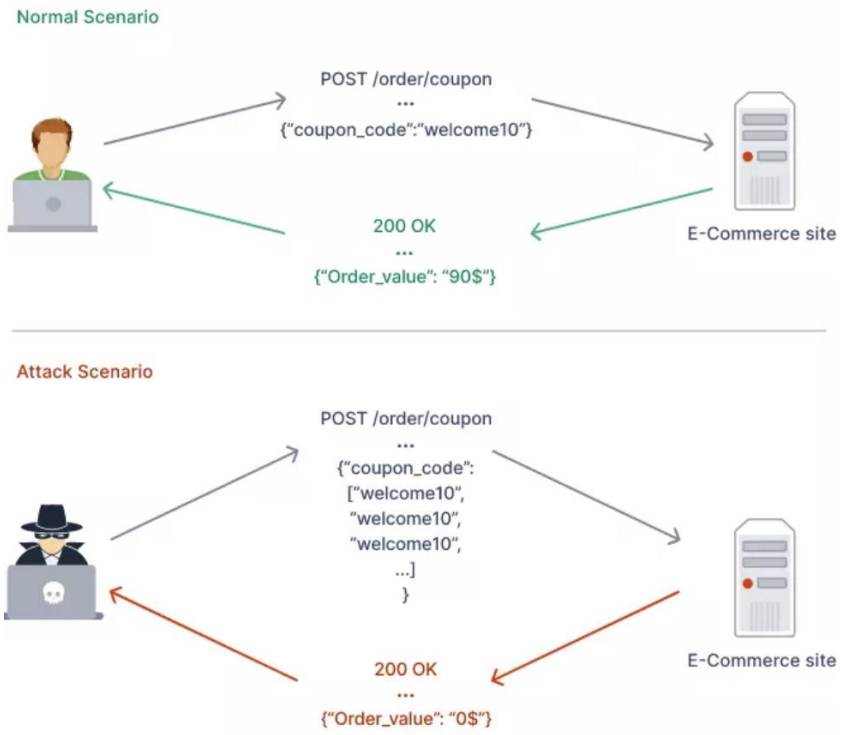
Hình 1: Minh họa tấn công Currency Manipulation

- Quantity Manipulation: Các trang web tính giá cuối cùng dựa trên số lượng mặt hàng đã mua. Vì vậy, hacker có thể thay đổi tham số này để chứa các giá trị nhỏ hoặc âm, nhằm ảnh hưởng đến giá cuối cùng của trang thanh toán. Hacker có thể giảm số lượng để giá trị đơn hàng giảm hoặc sửa thành số âm để phá hoại logic của hệ thống.
- Additional Costs Manipulation: Đôi khi kẻ tấn công có thể chèn thêm các mã giảm giá, khuyến mại vào yêu cầu dù thông thường sản phẩm không được áp dụng khuyến mại. Nếu trên server xử lý không đúng có thể dẫn đến việc kẻ tấn công có thể sử dụng thành công mã giảm giá, khuyến mại để mua hàng với giá trị thấp hơn.
- Mass Assignment, Autobinding, Object Injection: Lỗ hổng xuất hiện khi một ứng dụng chấp nhận các tham số bổ sung khi chúng được đưa vào một yêu cầu. Điều này có thể xảy ra ở một số ngôn ngữ hoặc framework như Ruby on Rails, NodeJS, Spring MVC, ASP NET MVC và PHP; do để thuận tiện cho việc phát triển web, các framework trên cho phép lập trình viên tự động đẩy các tham số thông qua các HTTP yêu cầu vào biến của chương trình hay đối tượng. Kẻ tấn công có thể lợi dụng lỗ hổng để chèn các dữ liệu độc hại là các tham số của chương trình (các tham số này vốn không được cho phép hoặc do các developer không có ý định truyền lên) để từ đó thực hiện các hành vi không mong muốn.



Hình 2: Minh họa tấn công Mass Assignment

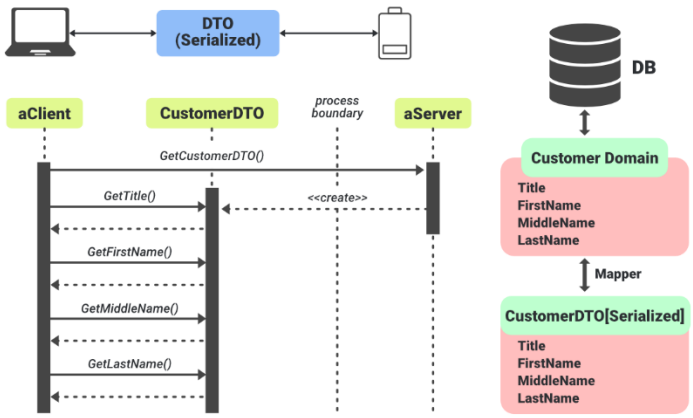
- Repeating an Input Parameter Multiple Times: Kiểu tấn công này rất hiếm khi xảy ra, nhưng việc lặp lại một tham số đầu vào trong một yêu cầu đến ứng dụng hoặc đến cổng thanh toán có thể gây ra các vấn đề logic. Một ví dụ là chúng ta gửi nhiều mã giảm giá trong một yêu cầu để được áp dụng nhiều lần khiến giá sản phẩm giảm hơn bình thường.



Hình 3: Minh họa tấn công Repeating an Input Parameter Multiple Times

Cách ngăn chặn:

- Sử dụng giá sản phẩm bằng cách truy vấn trên cơ sở dữ liệu, không nhận từ phía client, tương tự với các dữ liệu mang tính chất tương tự.
- Luôn luôn kiểm tra yêu cầu được gửi từ phía client, lọc các trường lạ hoặc các trường đáng lẽ không nên có đối với sản phẩm.
- Sử dụng Data Transfer Object (đối tượng vận chuyển dữ liệu).



Hình 4: Minh họa Data Transfer Object

6. SSRF

Server-side Request Forgery (SSRF) – giả mạo yêu cầu phía máy chủ là một lỗ hổng bảo mật mà nó cho phép kẻ tấn công sửa đổi tham số trong yêu cầu gửi đi để khiến máy chủ thực hiện truy xuất đến một miền tùy ý mà đó có thể là các dịch vụ chỉ nằm trong nội bộ như là cơ sở dữ liệu.

Nguyên nhân: là do một số tài nguyên trong một ứng dụng web cần được lấy từ bên ngoài, các yêu cầu phía máy chủ được sử dụng để tìm nạp tài nguyên và đưa nó vào ứng dụng web nhưng lại không kiểm soát chặt chẽ yêu cầu tìm nạp tài nguyên đó, cho phép kẻ tấn công có thể hoàn toàn kiểm soát yêu cầu tìm nạp tài nguyên đến bất kì đâu ngay cả những nơi có chứa dữ liệu nhạy cảm. Trong một vài trường hợp khác, máy chủ cho phép người dùng gửi đến 1 đường dẫn url với mục đích lấy dữ liệu đầu vào do người dùng cung cấp, nhưng do không kiểm soát chặt chẽ đầu vào đó của người dùng dẫn đến những hậu quả như máy chủ bị cài backdoor, RCE, ...

Phân loại:

- SSRF tấn công chính máy chủ: SSRF có thể giả mạo yêu cầu để truy xuất đến các miền khác nhau trong nội bộ hệ thống và nó bao gồm luôn cả chính máy chủ của nó.
- SSRF tấn công các hệ thống back-end khác: tương tự như trên nhưng mà lần này hacker tấn công vào một miền nằm trong sự kiểm soát của máy chủ, khó khăn hơn với việc cần phải tìm chính xác được địa chỉ của miền mà muốn tấn công vào.
- SSRF Blind: tương tự như trên, kẻ tấn công gửi yêu cầu giả mạo và phía máy chủ thực thi nó nhưng thay vì trả lại kết quả như bình thường thì nó lại không trả về bất cứ thứ gì. Để nhận biết được một lỗ hổng SSRF Blind, thông thường chúng ta sẽ thêm vào những payload độc hại một cách "may rủi", nếu gặp may thì hacker thắng sẽ thắng.

Cách ngăn chặn:

- Lọc kĩ đầu vào của mỗi yêu cầu bằng cách sử dụng whitelist (danh sách hợp lệ) thay vì blacklist (danh sách không hợp lệ).
- Whitelist là những gì được phép truy cập còn blacklist là những gì không được phép. Dễ thấy kiến thức hay những câu lệnh là bao la vì vậy các bạn không thể nào chặn được hết các trường hợp, do đó chúng ta nên sử dụng whitelist.

7. XXE

XXE (XML external entity) injection là một lỗ hổng bảo mật web cho phép kẻ tấn công can thiệp vào quá trình xử lý dữ liệu XML của ứng dụng. Nó thường cho phép kẻ tấn công xem các tệp trên hệ thống tệp của máy chủ ứng dụng và tương tác với bất kỳ hệ thống back-end hoặc bên ngoài nào mà chính ứng dụng có thể truy cập. Trong một số trường hợp, kẻ tấn công có thể leo thang cuộc tấn công XXE để xâm phạm máy chủ cơ bản hoặc cơ sở hạ tầng back-end khác, bằng cách lợi dụng lỗ hổng XXE để thực hiện các cuộc tấn công SSRF.

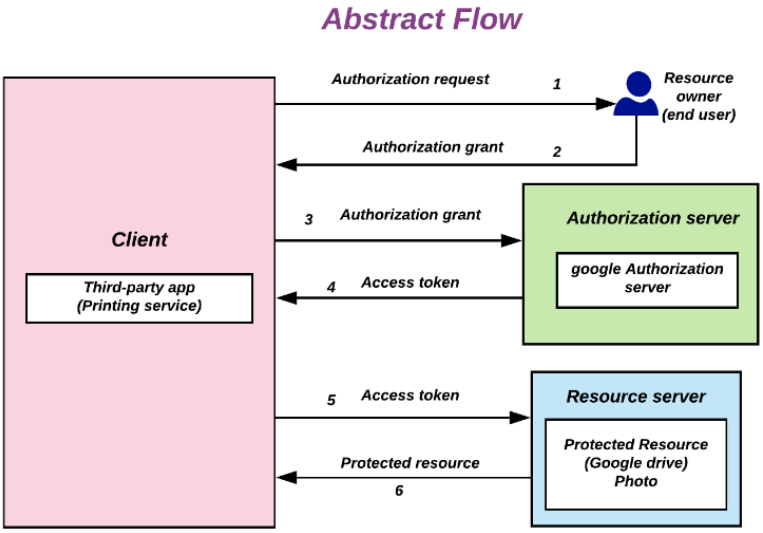
Một số ứng dụng sử dụng định dạng XML để truyền dữ liệu giữa trình duyệt và máy chủ. Các ứng dụng thực hiện việc này hầu như luôn sử dụng thư viện chuẩn hoặc API nền tảng để xử lý dữ liệu XML trên máy chủ. Lỗ hổng XXE phát sinh do đặc tả XML chứa nhiều tính năng nguy hiểm tiềm tàng khác nhau và các trình phân tích cú pháp tiêu chuẩn hỗ trợ các tính năng này ngay cả khi chúng thường không được ứng dụng sử dụng. XXE là một loại thực thể XML tùy chỉnh có các giá trị được xác định được tải từ bên ngoài DTD mà chúng được khai báo. Các thực thể bên ngoài đặc biệt thú vị từ góc độ bảo mật vì chúng cho phép xác định một thực thể dựa trên nội dung của đường dẫn tệp hoặc URL.

Phân loại tấn công:

- Khai thác XXE để lấy tệp: chỉnh sửa phần tử DOCTYPE khai báo một XE chứa đường dẫn đến tệp hoặc chỉnh sửa giá trị dữ liệu trong XML được trả về trong phản hồi của ứng dụng để sử dụng XE đã khai báo.
- Khai thác XXE để thực hiện tấn công SSRF: khai báo một XXE bằng URL mà hacker nhắm vào và sử dụng thực thể đã khai báo trong một giá trị dữ liệu. Nếu hacker có thể sử dụng thực thể đã khai báo trong giá trị dữ liệu được trả về trong phản hồi của ứng dụng thì bạn sẽ có thể xem phản hồi từ URL trong phản hồi của ứng dụng và do đó có được sự tương tác hai chiều với hệ thống back-end. Nếu không, hack chỉ có thể thực hiện các cuộc tấn công Blind SSRF (vẫn có thể gây ra hậu quả nghiêm trọng).
- Khai thác blind XXE lọc ra dữ liệu ngoài luồng: kẻ tấn công lưu trữ một DTD độc hại trên hệ thống mà chúng kiểm soát, sau đó gọi DTD bên ngoài từ bên trong payload XXE trong luồng.
- Khai thác blind XXE để lấy dữ liệu thông quathoong báo lỗi: gây ra lỗi phân tích cú pháp XML và thông báo lỗi gửi về chứa dữ liệu nhạy cảm mà hacker muốn truy xuất. Điều này sẽ có hiệu lực nếu ứng dụng trả về thông báo lỗi trong phản hồi của nó.

8. OAuth

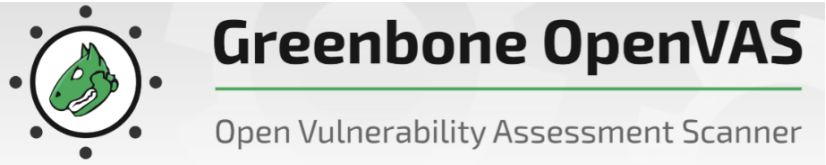
OAuth là một tiêu chuẩn mở cho việc ủy quyền truy cập, thường được sử dụng như một cách để người dùng internet cấp cho các trang web hoặc ứng dụng quyền truy cập vào thông tin của họ trên các các trang web khác nhưng không cung cấp mật khẩu. Cơ chế này được các công ty như Amazon, Google, Meta Platforms, Microsoft và Twitter sử dụng để cho phép người dùng chia sẻ thông tin về tài khoản của họ với các ứng dụng hoặc trang web của bên thứ ba. OAuth có 2 phiên bản là OAuth 1.0 và OAuth 2.0, tuy OAuth 2.0 được sinh do phát hiện lỗi bảo mật nghiêm trọng gây ra cố định phiên trên OAuth 1.0 nhưng OAuth 2.0 cũng đang lộ ra nhiều vấn đề.



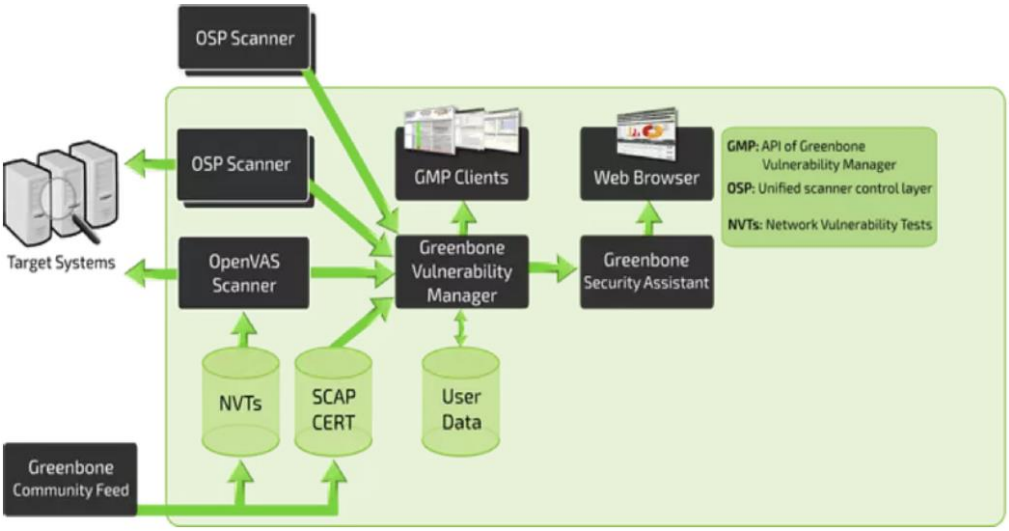
Hình 5: Minh họa cách OAuth 2.0 hoạt động

9. OpenVAS

OpenVAS là thành phần thực thi quét của GVM, một khung phần mềm mã nguồn mở gồm một số dịch vụ và công cụ cung cấp chức năng quét lỗ hổng và quản lý lỗ hổng. Tất cả các sản phẩm GVM đều là phần mềm miễn phí và hầu hết các thành phần đều được cấp phép theo GPL. Các plugin cho GVM được viết bằng NASL.



Hình 6: Logo của OpenVAS



Hình 7: Kiến trúc của OpenVAS

OpenVAS có 3 thành phần chính: GVMd, GSA, OpenVAS Scanner.

- GVMd: là trung tâm dịch vụ, hợp nhất các công cụ quét lỗ hổng đơn giản thành một giải pháp quản lý lỗ hổng đầy đủ. GVMd điều khiển OpenVAS Scanner qua một giao thức nội bộ và cung cấp thêm một giao thức chung OSP để có thể tích hợp các máy quét khác. Bản thân GVMd cũng cung cấp một giao thức dựa trên XML khác, GMP để các thành phần khác có thể gửi những yêu cầu xử lý như tạo người dùng, tạo lịch quét, tạo một mục tiêu quét, tạo một nhiệm vụ để quét mục tiêu, bắt đầu nhiệm vụ quét một mục tiêu,... GVMd cũng kiểm soát cơ sở dữ liệu SQL nơi tất cả dữ liệu kết quả và cấu hình quét được lưu trữ tập trung.
- GSA: là giao diện web của GVM. Nó kết nối với GVMd để cung cấp giao diện cho người dùng với đầy đủ những tính năng của công cụ quản lý lỗ hổng. GSA bao gồm các thành phần:
    - GSA - ứng dụng web được viết bằng React.
    - GSAD – Là HTTP server giao tiếp với GVMd thông qua giao thức GMP.
- OpenVAS Scanner: là một công cụ quét đầy đủ tính năng để thực thi một mẫu thử NVT nhằm mục đích kiểm tra một mục tiêu quét có vi phạm các lỗ hổng bảo mật, chưa cập nhật các bản vá cho hệ thống và các mục đích khác của một công cụ dò quét lỗ hổng. Và hầu hết Openvas Scanner sẽ thực hiện các nhiệm vụ và trả lại kết quả mà GVMd gọi đến.

10. SAST, DAST, IAST và RASP

Quá trình kiểm thử bảo mật là nhằm loại trừ khả năng code bị trục trặc, đảm bảo ứng dụng chạy bình thường và phát hiện lỗ hổng để vá sau khi triển khai. Duy trì kiểm thử từ đầu đến sau cùng, từ đó giảm thiểu thiệt hại cao nhất. Có 4 phương pháp kiểm thử:

- SAST: cho phép phát hiện sớm các lỗi trong quá trình phát triển.
- DAST: kiểm tra các sản phẩm trong quá trình hoạt động và cung cấp phản hồi.
- IAST: kết hợp giữa SAST & DAST, sử dụng thiết bị phần mềm để phân tích các ứng dụng đang chạy.
- RASP: nhận biết được một cuộc tấn công đang xảy ra và thực hiện các biện pháp cần thiết.

SAST Là phương pháp kiểm thử bảo mật được thực hiện trên mã nguồn tĩnh trước khi được biên dịch, không phải trên ứng dụng đang chạy (white box). Người kiểm thử biết thông tin về hệ thống và phần mềm được kiểm thử, bao gồm cả kiến trúc hệ thống, mã nguồn,...

DAST là phương pháp kiểm thử bảo mật mà người kiểm thử sẽ không biết gì về hệ thống (black box). Người kiểm thử sẽ tìm kiếm những lỗ hổng an ninh của một ứng dụng trong trạng thái đang chạy của ứng dụng.

IAST Là phương pháp được phát triển để giải quyết các sai sót trong SAST và DAST thông qua kết hợp hai phương pháp trên. Công cụ IAST thông qua xác định các vấn

đề trong quá trình hoạt động như DAST nhưng cũng chạy trong máy chủ ứng dụng và đánh giá code như SAST.

RASP là bước phát triển so với các công cụ SAST, DAST và IAST. Các công cụ tự bảo vệ ứng dụng trong thời gian chạy tích hợp với các ứng dụng và phân tích lưu lượng cũng như hành vi của người dùng cuối trong thời gian chạy để ngăn chặn các cuộc tấn công.

CHƯƠNG 3: ACUNETIX

Ở chương này, nhóm sẽ trình bày tất cả những gì nhóm tìm hiểu được về Acunetix.

1. Acunetix là gì?

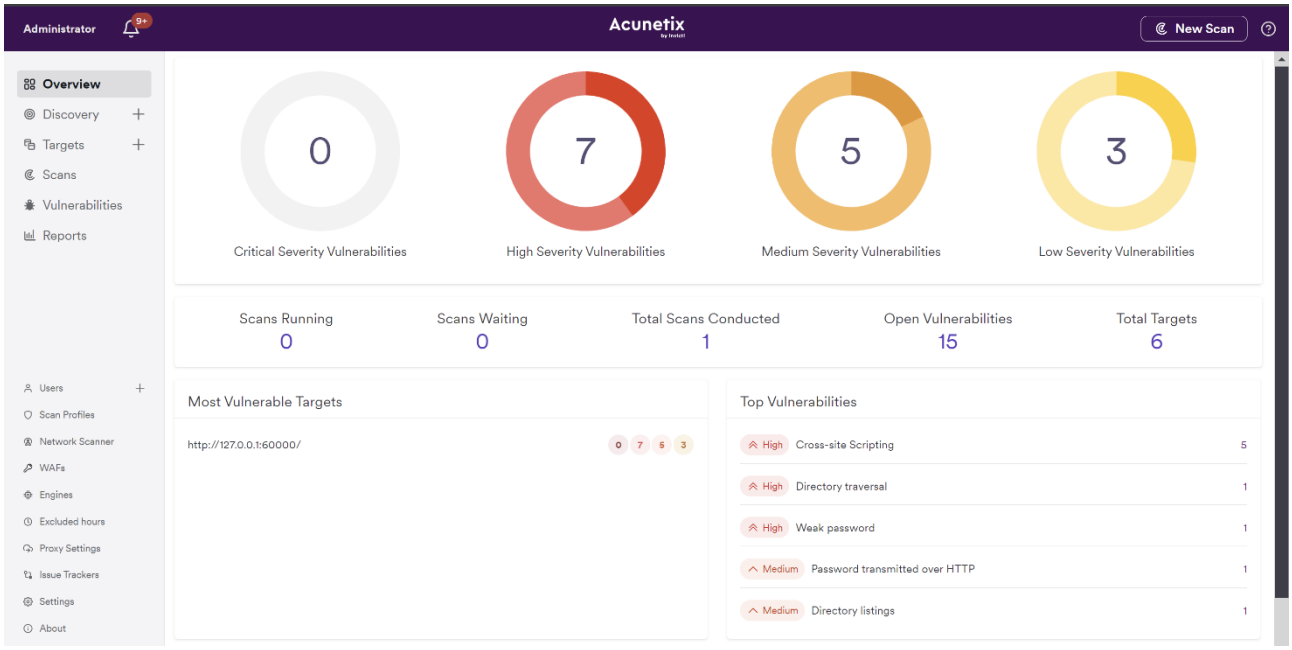
Acunetix là một công cụ kiểm thử bảo mật ứng dụng web tự động. Acunetix cung cấp một giải pháp mạnh mẽ và độc đáo để phân tích các ứng dụng web tùy chỉnh và sẵn có, bao gồm cả những ứng dụng web sử dụng JavaScript, AJAX và Web 2.0. Acunetix có trình thu thập thông tin nâng cao có thể tìm thấy hầu hết mọi tệp. Điều này rất quan trọng vì những thứ không tìm được thì không thể kiểm tra được.

Invicti Security phát triển 2 loại Acunetix là Acunetix và Acunetix 360 hay Acunetix Online. Với Acunetix 360 là Acunetix bản trực tuyến, bản này có 2 bản theo nhu cầu sử dụng là Acunetix 360 On-Demand và Acunetix 360 On-Premises. Với Acunetix thì có 2 bản theo tài chính của khách hàng là Acunetix Standard và Acunetix Premium. Phiên bản mới nhất của Acunetix là Acunetix v24.5.240604185, Acunetix 360 On-Demand v24.5.2 và Acunetix 360 On-Premises v24.5.0.

Acunetix Standard thực chất là bản bị hạn chế đi một số chức năng nên nếu phần sau nhắc đến Acunetix thì đang nhắc đến Acunetix Premium – bản đày đủ chức năng.

2. Các chức năng của Acunetix

Dựa trên giao diện web của Acunetix, nhóm đưa ra các nhóm chức năng: Tổng quan, Khám phá, Mục tiêu, Quét, Lỗ hổng, Báo cáo, Người dùng, Hồ sơ quét, WAFs, Engines, Excluded Hours, Agents, Proxy Settings, Issue Trackers, Cài đặt.



Hình 8: Minh họa giao diện web của Acunetix

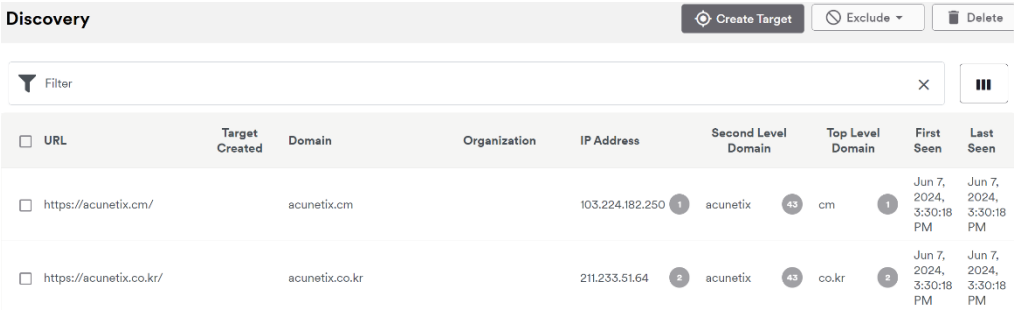
a. *Tổng quan*

Trang Overview (xem Hình 8) cung cấp chế độ xem tóm tắt về số liệu thống kê bảo mật của nội dung web của ta, bao gồm:

- Tổng số lỗ hổng chưa được vá, chia theo mức độ nghiêm trọng.
- Tổng số mục tiêu được xác định.
- Tổng số lần Quét đang chạy; chờ chạy; và hoàn thành.
- Top 5 mục tiêu dễ bị tổn thương nhất.
- Top 5 lỗ hổng được báo cáo nhiều nhất.

b. *Khám phá*

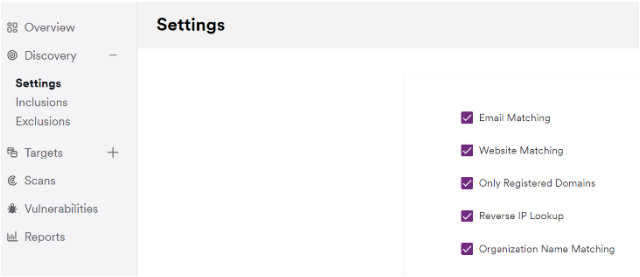
Trang Discovery hiển thị tất cả mục tiêu mà Acunetix khám phá được (các web liên quan "bắt" được trong quá trình quét). Ví dụ quét acunetix.com khám phá được thêm acunetix.cz. Ta có thể lọc, cấu hình danh sách này, cũng như có thể thêm trang web vào danh sách hoặc xóa. Ngoài ra có thể tạo Mục tiêu từ danh sách này để tiến hành Quét.



Hình 9: Minh hoạ trang Discovery trong Acunetix

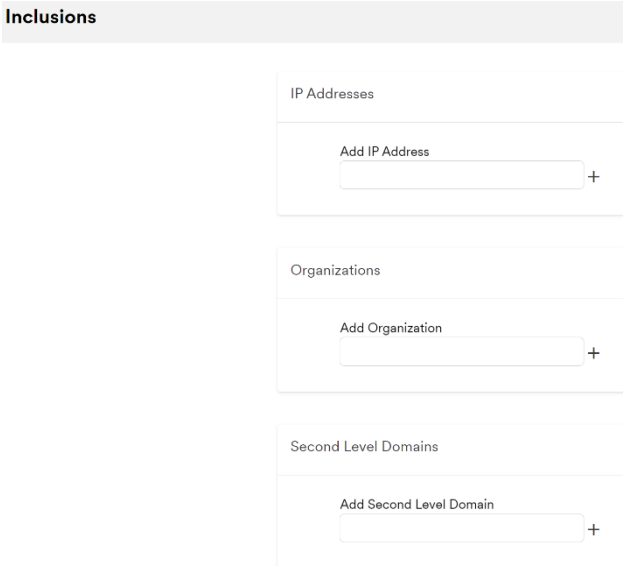
Có thể tùy chỉnh chức năng này ở trang Settings, Inclusions và Exclusions.

- Settings: tùy chỉnh các điều kiện để đưa web bắt được vào danh sách.
    - Enable Risk Scoring: Tính điểm rủi ro bằng AI, giúp xác định sớm các web cần quét ngay hoặc có thể web sau. Chi tiết tại Predictive Risk Scoring.
    - Email Matching: giống email.
    - Website Matching: giống website.
    - Only Registered Domains: miền đã được đăng ký.
    - Reverse IP Lookup: tìm IP dựa trên miền.
    - Organization Name Matching: giống tên tổ chức.



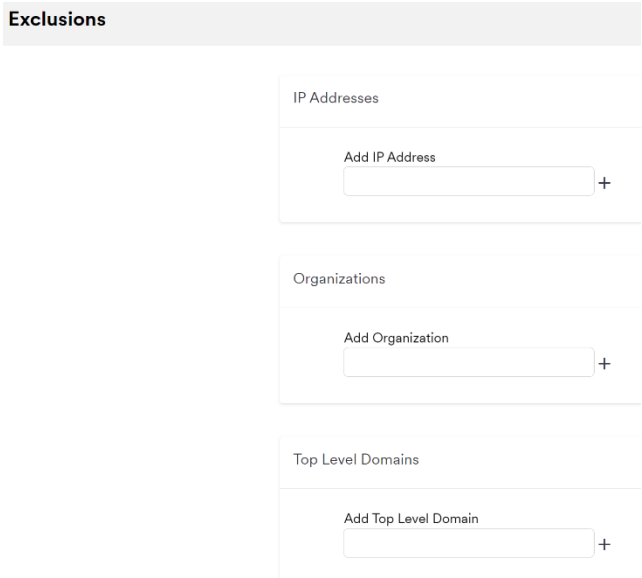
Hình 10: Minh họa Settings của Discovery trong Acunetix

- Inclusions: thêm các điều kiện "bắt" cụ thể hơn.



Hình 11: Minh họa Inclusions của Discovery trong Acunetix

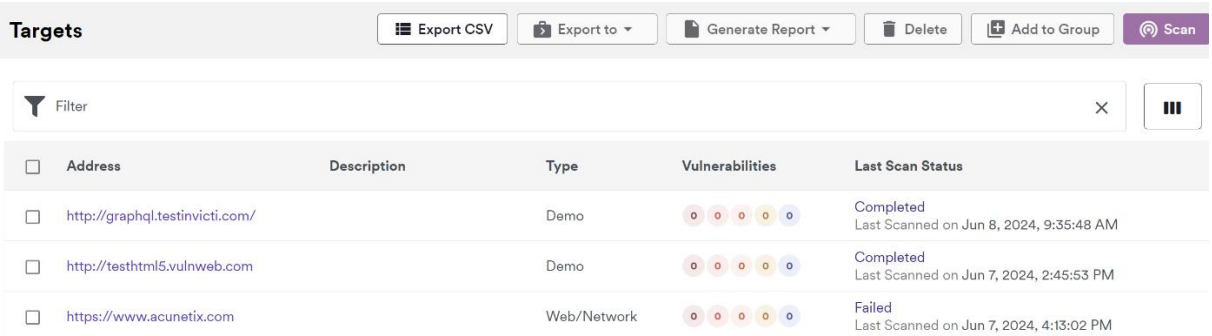
- Exclusions: thêm điều kiện không bắt.



Hình 12: Minh họa Exclusions của Discovery trong Acunetix

c. Mục tiêu

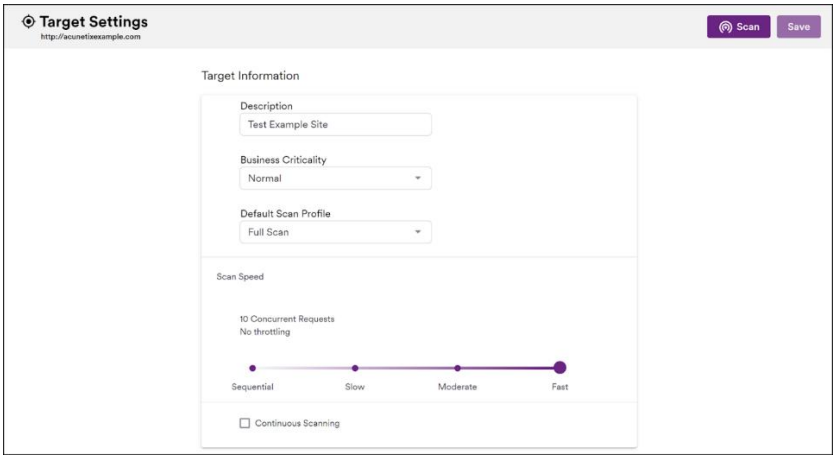
Trang Targets hiển thị danh sách các Mục tiêu, tình trạng bảo mật của các Mục tiêu, lối tắt để tạo báo cáo và quét. Ta có thể thêm hoặc xóa các Mục tiêu.



Hình 13: Minh họa trang Targets của Acunetix

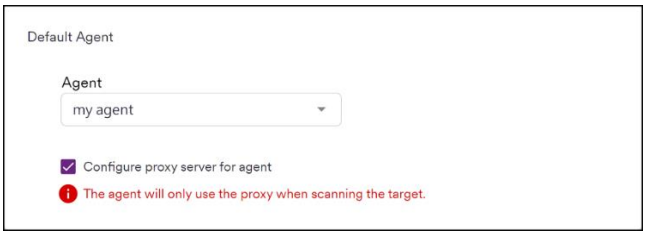
Các thuộc tính của Mục tiêu cần quan tâm khi thêm Mục tiêu mới:

- Description: Mô tả.
- Business Criticality: Ta có thể chỉ định một mức độ quan trọng trong kinh doanh (Low, Normal, High, Critical) cho mục tiêu, mặc định là Normal. Điều này sẽ cung cấp cho ta một thuộc tính để lọc các lượt quét và lỗ hổng, cho phép ta tập trung vào các mục quan trọng hơn.
- Default Scan Profile: Mỗi khi ta bắt đầu quét trên một mục tiêu, ta có thể chỉ định cấu hình quét để sử dụng (Full Scan, High Risk Vulnebilities, Cross-site Scripting Vulnerabilities, SQL Injection Vulnerabilities, Weak Passwords, Crawl Only, Malware Scan), với cấu hình quét mặc định là Full Scan. Giải nghĩa các lựa chọn:
    - High Risk Vulnebilities: Chỉ báo cáo các lỗ hổng có rủi ro cao.
    - Cross-site Scripting Vulnerabilities: Chỉ báo cáo các lỗ hổng XSS.
    - SQL Injection Vulnerabilities: Chỉ báo cáo các lỗ hổng SQL Injection.
    - Weak Passwords: Chỉ báo cáo các lỗ hổng mật khẩu yếu.
    - Crawl Only: Chỉ thu thập thông tin, "vẽ" bản đồ trang web.
    - Malware Scan: Chỉ quét phần mềm độc hại, cần có phần mềm Anti-virus.
- Scan Speed: Mục tiêu của ta có thể bị ảnh hưởng tiêu cực bởi quá trình quét tốc độ cao hoặc cường độ cao (yêu cầu đồng thời) hoặc có thể kích hoạt các cơ chế bảo vệ làm mất hiệu lực kết quả quét của ta (ví dụ: bị chặn bởi IPS). Các lực chọn tốc độ quét:
    - Fast (default): 10 yêu cầu đồng thời, không điều tiết độ trễ.
    - Moderate: 5 yêu cầu đồng thời, gửi yêu cầu 20 mili giây một lần.
    - Slow: 2 yêu cầu đồng thời, gửi yêu cầu cứ sau 50 mili giây.
    - Sequential: 1 yêu cầu đồng thời, không điều tiết độ trễ.
- Continuous Scanning: Quét liên tục hay quét theo lịch. Sau khi chọn và lưu lại, các lỗ hổng của mục tiêu sẽ được tự động cập nhật và có thể xem ở trang Vulnerabilities. Thông báo về các lỗ hổng mới phát hiện sẽ được gửi qua email và các "vùng thông báo" khác như hệ thống theo dõi vấn đề (issue tracker).

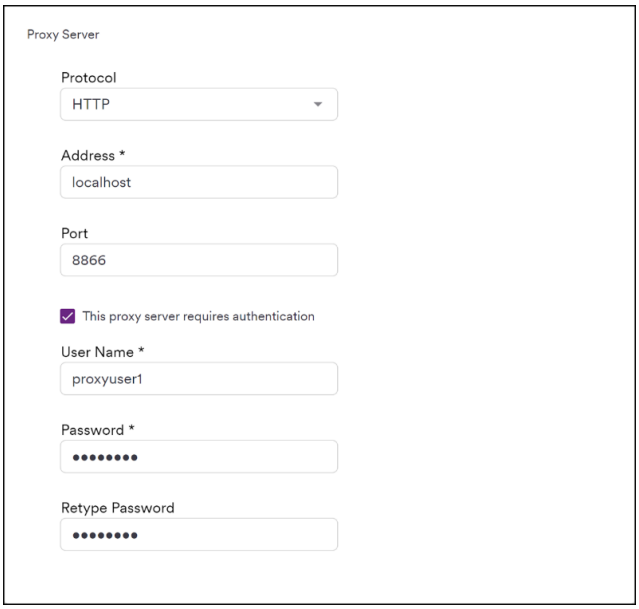


Hình 14: Minh họa 5 thuộc tính đầu của Mục tiêu trong Acunetix

- Default Agent: Đây là agent được sử dụng bởi mục tiêu. Agent mặc định cho tất cả các mục tiêu mới trên Acunetix Online là Cloud Agent. Cloud Agent được quản lý bởi Invicti và chúng có thể truy cập bất kỳ trang web nào có thể truy cập công khai trên internet. Nếu ta đã thiết lập bất kỳ agent nội bộ nào, thì những agent này có thể được chọn thông qua danh sách agent trong phần Default Agent. Thuộc tính này chỉ khả dụng cho Acunetix 360.
- Configure proxy server for agent: cấu hình proxy server cho agent, chỉ khả dụng với Acunetix 360.

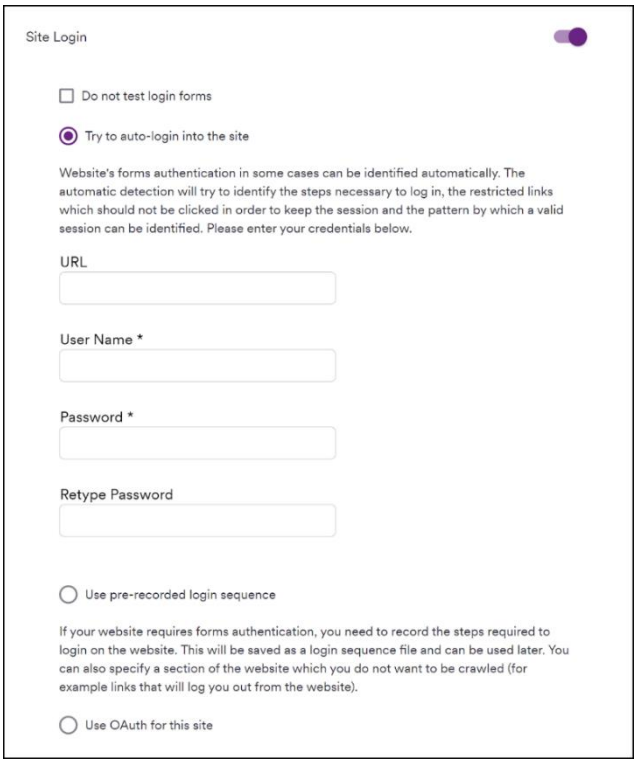


Hình 15: Minh họa thuộc tính Default Agent, Configure proxy server for agent của Mục tiêu trong Acunetix



Hình 16: Minh họa cấu hình Proxy Server cho Agent trong Acunetix

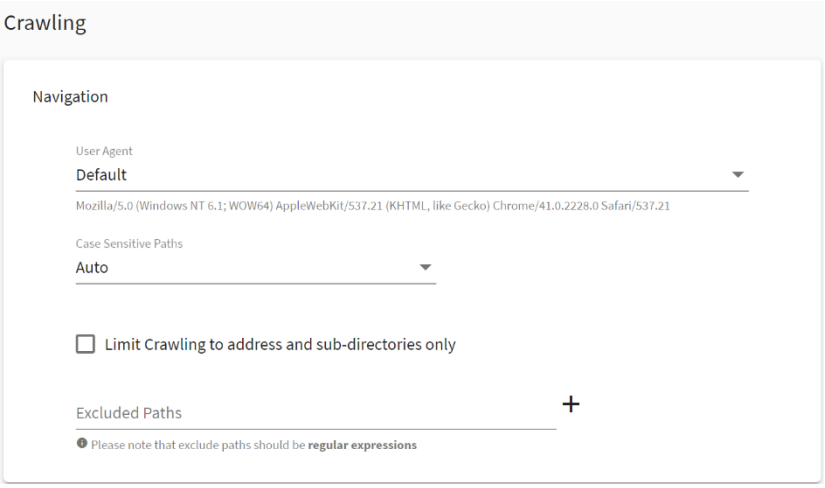
- Site Login: Phần này chứa các tùy chọn để cho phép Acunetix quét các khu vực bị hạn chế trong ứng dụng web. Điều này có thể đạt được bằng cách cung cấp tên người dùng và mật khẩu để Acunetix tự động đăng nhập vào các khu vực hạn chế của ứng dụng web hoặc thông qua việc sử dụng "trình tự đăng nhập được ghi trước" hoặc cơ chế xác thực OAuth2. Chi tiết hơn tại Site Login.



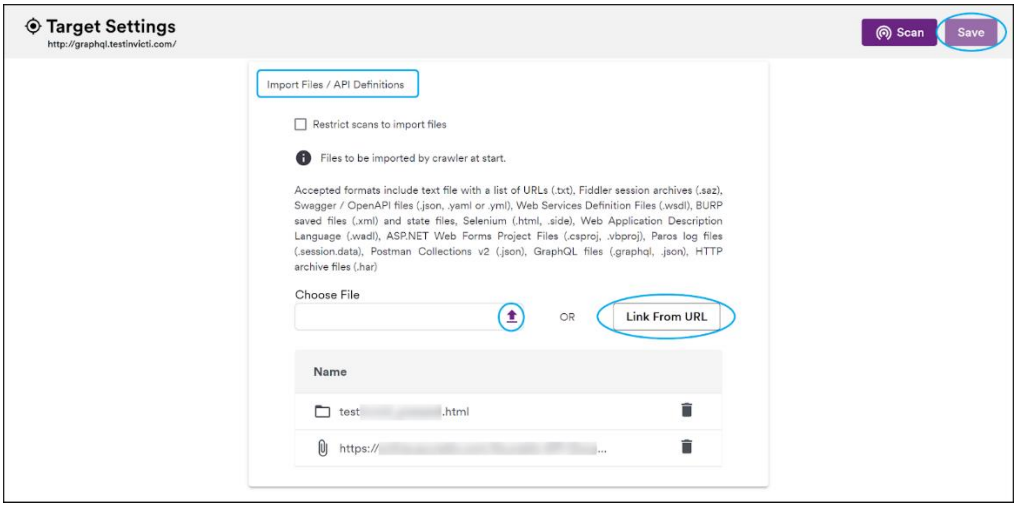
Hình 17: Minh họa thuộc tính Site Login của Mục tiêu trong Acunetix

- Business Logic Recorder: Nhiều ứng dụng web sử dụng các biểu mẫu "mở rộng động", nhiều bước hoặc nhiều trang. Nghĩa là biểu mẫu "giai đoạn đầu tiên" được hiển thị cho người dùng và khi người dùng nhập thông tin vào "giai đoạn đầu tiên" này, thông tin được cung cấp sẽ xác định biểu mẫu sẽ thay đổi như thế nào trong "giai đoạn" tiếp theo. Business Logic Recorder cho phép ta tạo một chuỗi hành động để Acunetix scanner tuân theo để nó có thể điều hướng chính xác các biểu mẫu nhiều phần (nhiều giai đoạn).
- SSH Credentials: Nếu ứng dụng web mục tiêu của ta yêu cầu thông tin đăng nhập SSH để Acunetix scanner truy cập vào ứng dụng đó, ta có thể cung cấp những thông tin này dưới dạng khóa riêng hoặc bằng cách thêm tên người dùng và mật khẩu vào.
- AcuSensor: Khi quét mục tiêu có sử dụng AcuSensor. Chỉ thực sự có tác dụng nếu mục tiêu thực có cài AcuSensor.
- Crawling: Cấu hình các tùy chọn thu thập thông tin:
    - User-Agent String: giá trị của trường User-Agent trong gói HTTP Request.
    - Case Sensitive Paths: Mặc định là "Auto", tự động kiểm tra xem mục tiêu có sử dụng case-sensitive (phân biệt chữ hoa, chữ thường) URL hay không. Hoặc chỉ định có ("Yes"), không ("No").

- Limit Crawling to address and sub-directories only: Chỉ quét địa chỉ và thư mục con, dùng để giới hạn phạm vi quét các phần của ứng dụng web.
- Excluded Paths: Các đường dẫn mà scanner sẽ không quét.
- Adding paths via Import Files / API Definitions: Ta có thể thêm đường dẫn đến mục tiêu của mình thông qua "nhập" tệp hoặc "định nghĩa" API để hướng dẫn trình thu thập thông tin. Điều này rất hữu ích khi có những phần của trang web không được liên kết với mục tiêu chính. Bằng cách chỉ định đường dẫn để trình thu thập thông tin thêm vào quá trình quét, ta có thể đảm bảo rằng mọi trang và thư mục không được liên kết đều được quét. Tìm hiểu thêm tại đây.

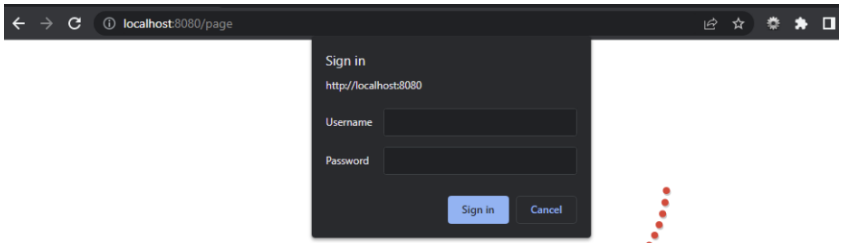


Hình 18: Minh họa thuộc tính Crawling của Mục tiêu trong Acunetix

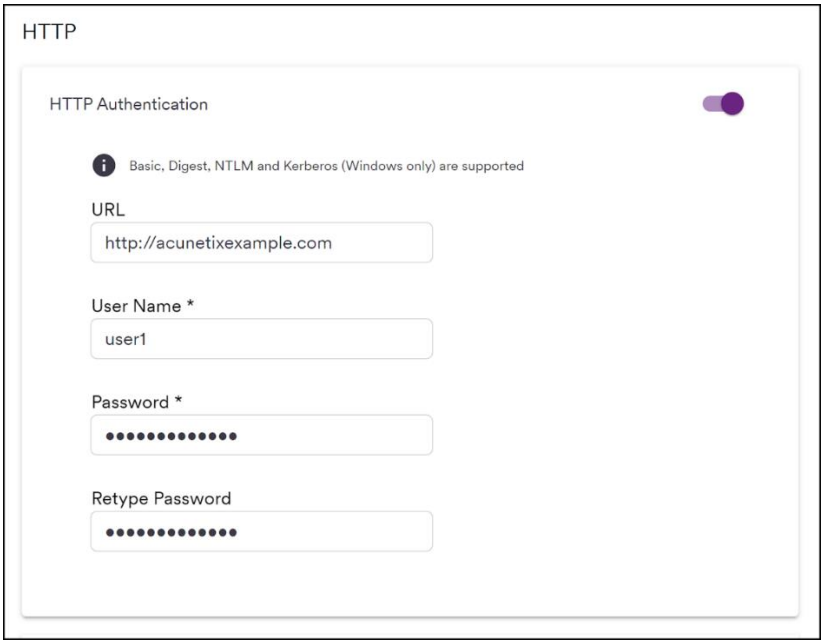


Hình 19: Minh họa Import Files / API Definitions của Crawling của Mục tiêu trong Acunetix

- HTTP: Cấu hình các tùy chỉnh HTTP:
  - HTTP Authentication: Web server có thể yêu cầu người dùng tự xác thực, hiển thị cho người dùng hộp thoại để điền tên người dùng và mật khẩu. Thông tin này được gửi đến web server trong "Authorization: Basic" header.

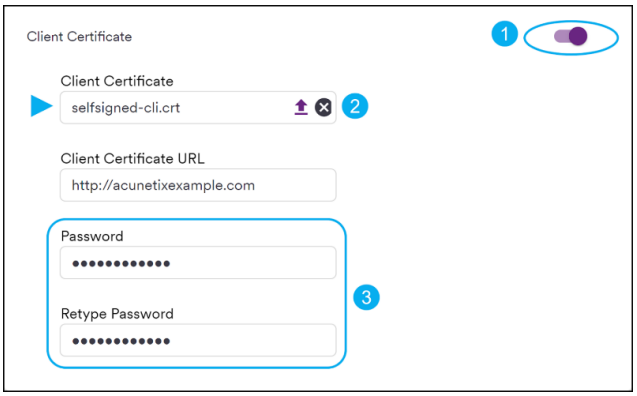


Hình 20: Minh họa web server yêu cầu xác thực



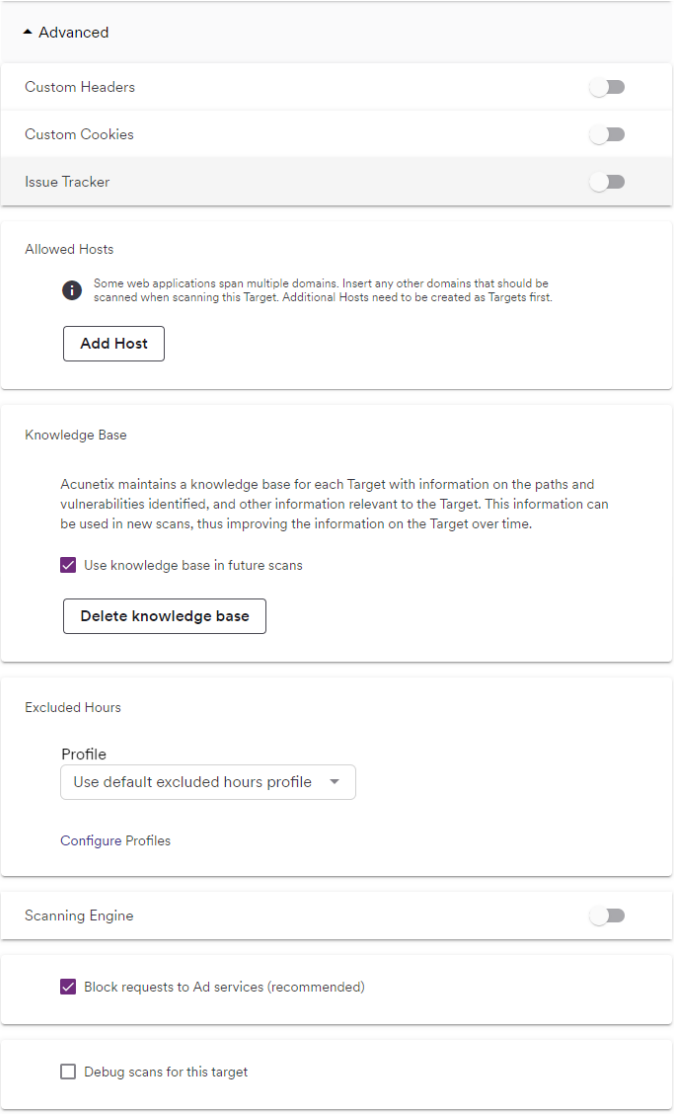
Hình 21: Minh họa HTTP Authentication của HTTP của Mục tiêu trong Acunetix

- Client Certificates: Nếu web server của mục tiêu yêu cầu xác thực ứng dụng khách (trình duyệt) thông qua chứng chỉ, ta có thể cấu hình Mục tiêu của mình để sử dụng tệp chứng chỉ khách.



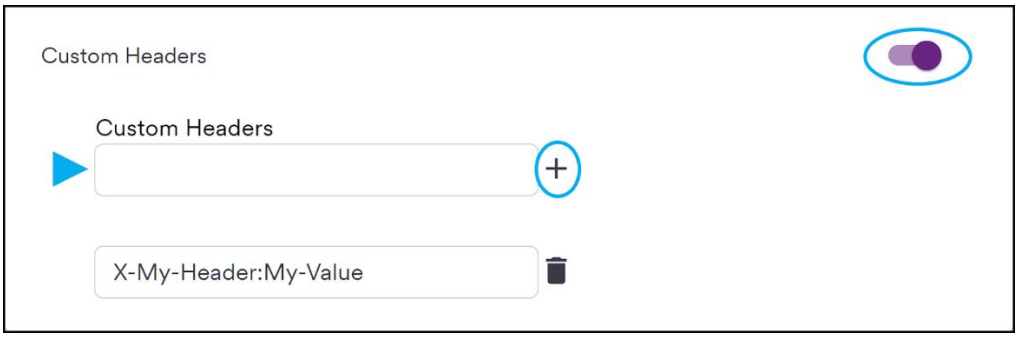
Hình 22: Minh họa các bước thêm Client Certificates của HTTP của Mục tiêu trong Acunetix

- Advanced Options: Các tùy chọn nâng cao:



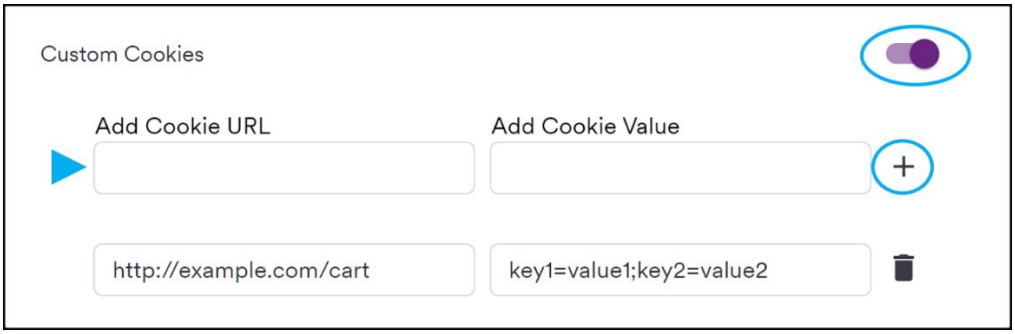
Hình 23: Minh họa thuộc tính Advanced Options của Mục tiêu trong Acunetix

- Custom Headers: Mục tiêu có thể sẽ thay đổi phản hồi với header tùy chỉnh. Ví dụ: Bài tập 6 bài thực hành 1 của môn này, thêm trường X-Host thì web phản hồi khác so với trước.



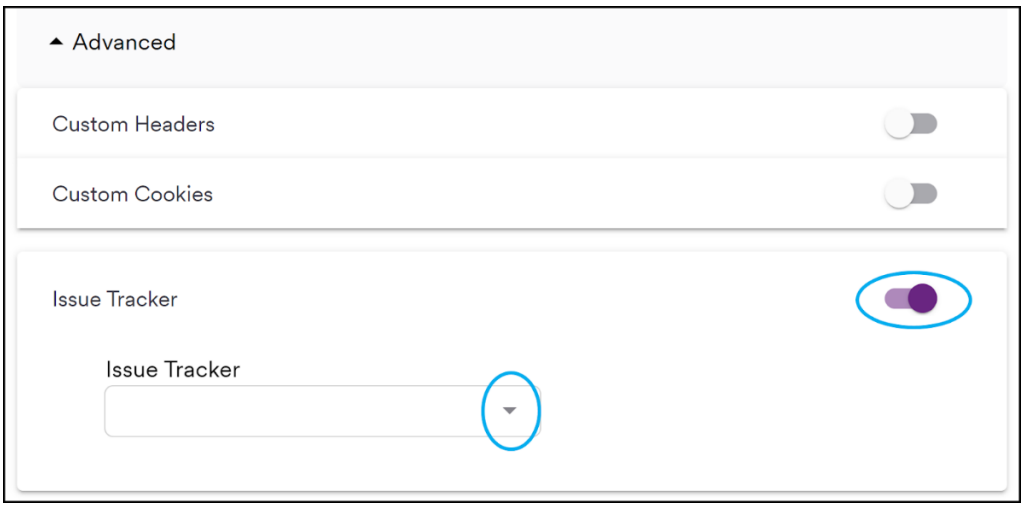
Hình 24: Minh họa Custom Headers của Advanced Options của Mục tiêu trong Acunetix

- Custom Cookies: thêm cookie tùy chỉnh cho các yêu cầu gửi tới mục tiêu.



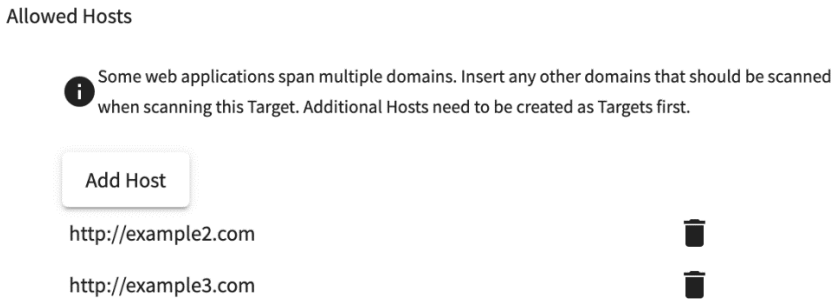
Hình 25: Minh họa Custom Cookies của Advanced Options của Mục tiêu trong Acunetix

- Issue Tracker Integration: Tích hợp issue tracker đã được thêm ở trang Issue Trackers. Có thể gửi báo cáo các lỗ hổng về issue tracker được tích hợp.



Hình 26: Minh họa Issue Tracker của Advanced Options của Mục tiêu trong Acunetix

- Allowed Hosts: Mục tiêu của ta có thể bắt đầu ở một tên miền nhưng trải rộng trên nhiều tên miền. Ta có thể sử dụng tùy chọn này để cho phép trình thu thập thông tin và scanner đi theo các liên kết trong ứng dụng web của ta trên nhiều miền, miễn là mỗi miền trong số nhiều miền đó đã được cầu hình thành Mục tiêu hoặc có trong danh sách Allowed Hosts.



Hình 27: Minh họa Allowed Hosts của Advanced Options của Mục tiêu trong Acunetix

d. Quét

Ở trang Scans, ta có thể xem kết quả, thêm, xóa và dừng các lần quét. Ngoài ra, có các lối tắt để tạo báo cáo cho các lần quét đã hoàn thành.

Cách để thêm một lần quét:

Bước 1: Click New Scan.

Hình 28: Minh họa bước 1 cách thêm lần quét mới trong Acunetix

Bước 2: Chọn các Mục tiêu để quét.

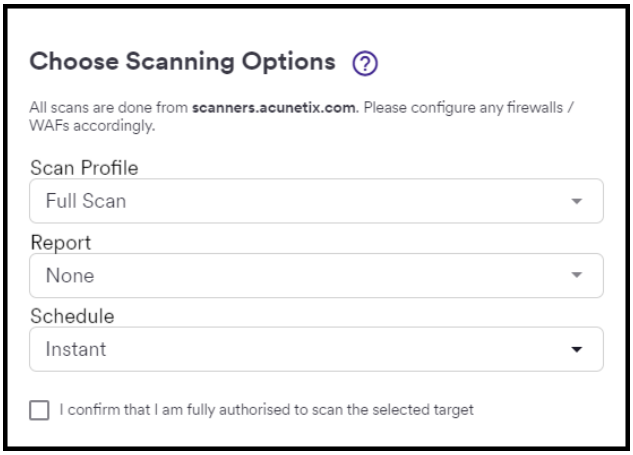
Hình 29: Minh họa bước 2 cách thêm lần quét mới trong Acunetix

Bước 3: Click Scan.

Hình 30: Minh họa bước 3 cách thêm lần quét mới trong Acunetix

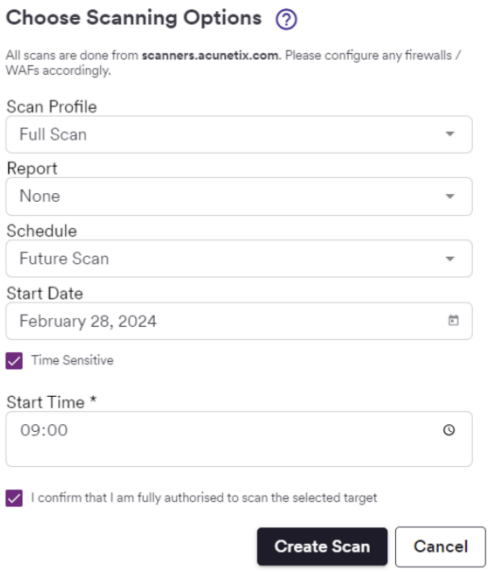
Bước 4: Cấu hình lần quét. Scan Profile giống với Default Scan được viết ở mục 3.2.c; Report là loại báo cáo sẽ xuất sau khi quét xong; Schedule là lập lịch cho lần quét này.

- Các kiểu lập lịch quét:
  - Instant scan: quét ngay bây giờ.



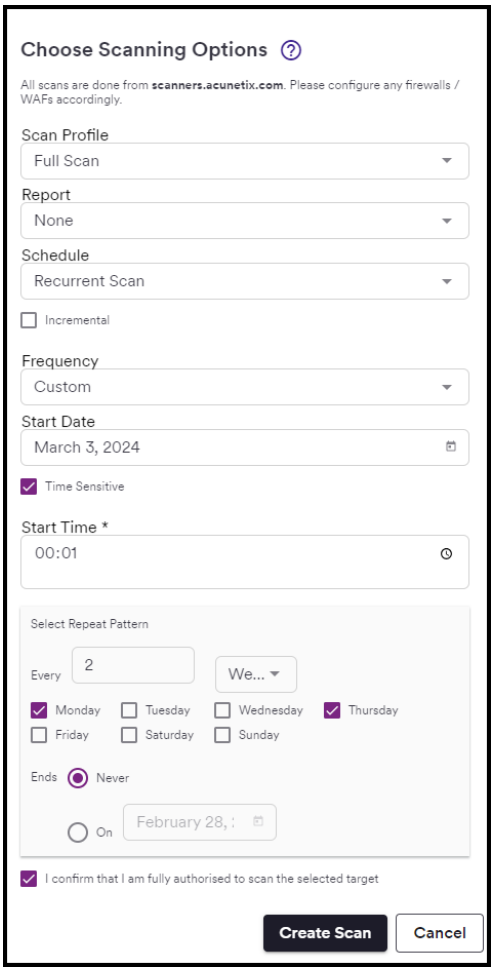
Hình 31: Minh họa Instant scan khi cấu hình lần quét trong Acunetix

- Future scan: Quét vào 1 ngày giờ cụ thể trong tương lai.



Hình 32: Minh họa Future scan khi cấu hình lần quét trong Acunetix

- Recurrent scan: thiết lập 1 chu kỳ quét (hàng ngày, hàng tuần, ...) và bắt đầu vào ngày giờ cụ thể. Chọn Incremental scan để chỉ quét có chọn lọc các trang mới được phát hiện hoặc sửa đổi.

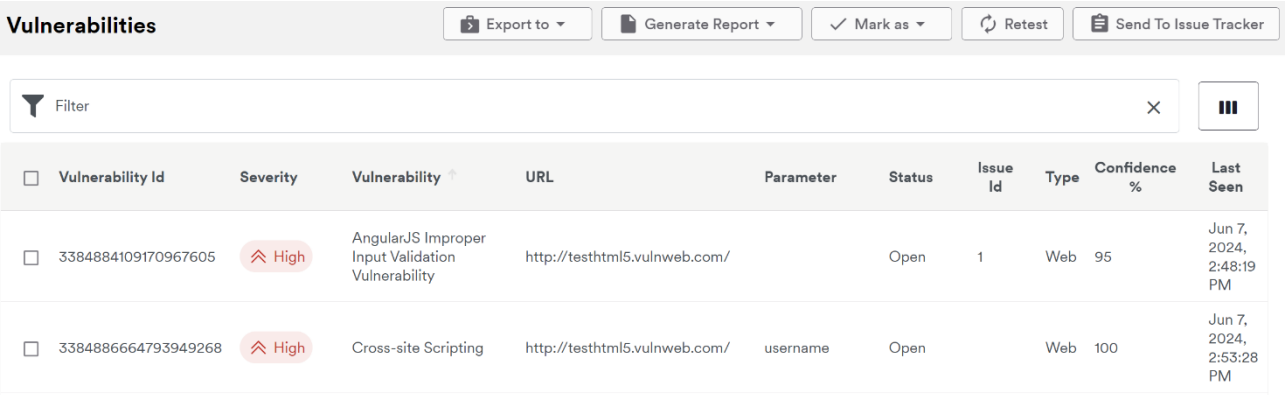


Hình 33: Minh họa Recurrent scan

Bước 5: Chọn "I confirm that I am fully authorised to scan the selected target checkbox" và click "Create Scan".

e. Lỗ hổng

Ở trang Vulnerabilities, ta có thể xem tất cả các Lỗ hổng tìm được.



Hình 34: Minh họa trang Vulnerabilities trong Acunetix

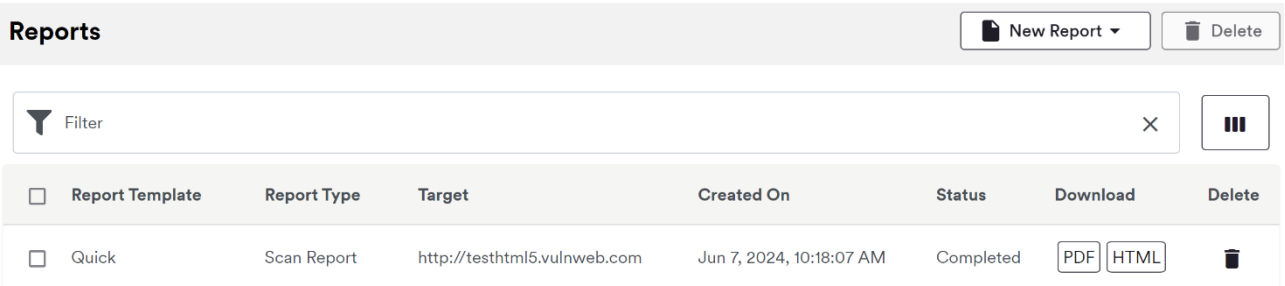
Các thuộc tính của Lỗ hổng:

- Severity: Mức độ nghiêm trọng của Lỗ hổng, gồm các mức Critical, High, Medium, Low, Informational.
    - Critical: Kẻ tấn công hoàn toàn có thể xâm phạm tính bảo mật, tính toàn vẹn hoặc tính khả dụng của hệ thống mục tiêu mà không cần quyền truy cập chuyên biệt, sự tương tác của người dùng hoặc các trường hợp nằm ngoài tầm kiểm soát của kẻ tấn công. Rất có khả năng cho phép kể tấn công "di chuyển ngang" và "leo thang tấn công" sang các hệ thống khác trên mạng nội bộ của ứng dụng có lỗ hổng.
    - High: Kẻ tấn công rất có thể xâm phạm tính bảo mật, tính toàn vẹn hoặc tính khả dụng của hệ thống mục tiêu. Một số quyền truy cập chuyên dụng, tương tác của người dùng hoặc các trường hợp nằm ngoài tầm kiểm soát của kẻ tấn công có thể không cần thiết để cuộc tấn công thành công. Rất có khả năng cho phép kể tấn công "di chuyển ngang" và "leo thang tấn công" sang các hệ thống khác trên mạng nội bộ của ứng dụng có lỗ hổng.
    - Medium: Kẻ tấn công có thể xâm phạm một phần tính bảo mật, tính toàn vẹn hoặc tính khả dụng của hệ thống mục tiêu. Quyền truy cập chuyên biệt, tương tác của người dùng hoặc các trường hợp nằm ngoài tầm kiểm soát của kẻ tấn công có thể cần thiết để cuộc tấn công thành công. Rất có thể được sử dụng cùng với các lỗ hổng khác để "leo thang" một cuộc tấn công.
    - Low: Kẻ tấn công có phạm vi hạn chế trong việc xâm phạm tính bảo mật, tính toàn vẹn hoặc tính khả dụng của hệ thống mục tiêu. Cần có quyền truy cập chuyên biệt, tương tác của người dùng hoặc các trường hợp nằm ngoài tầm kiểm soát của kẻ tấn công để cuộc tấn công thành công. Cần được sử dụng kết hợp với các lỗ hổng khác để "leo thang" một cuộc tấn công.

    - Info: Kẻ tấn công có thể lấy được thông tin về trang web. Đây không nhất thiết là một lỗ hổng, nhưng bất kỳ thông tin nào mà kẻ tấn công có được cũng có thể được sử dụng để thực hiện một cuộc tấn công chính xác hơn vào một ngày nào đó. Khuyến nghị hạn chế tối đa việc tiết lộ thông tin.
- Vulnerability: Tên của Lỗ hổng được xác định bởi Acunetix.
- URL: URL nơi lỗ hổng được tìm thấy.
- Parameter: Tham số mà Acunetix sử dụng để tìm thấy lỗ hổng.
- Status: Trạng thái của lỗ hổng, có thể là Open, Fixed, Ignored, Rediscovered, False Positive hoặc Not Open.
- Confidence: Mức độ tin cậy, cho thấy mức độ chắc chắn của Acunetix đối với lỗ hổng mà nó đã tìm thấy. Ý nghĩa của một số mức độ tin cậy:
    - 100%: Acunetix tự tin 100% rằng lỗ hổng này tồn tại. Những lỗ hổng như vậy có thể được chuyển trực tiếp đến nhóm lập trình hoặc quản trị để khắc phục.
    - 95%: Acunetix khá chắc chắn rằng lỗ hổng này tồn tại, tuy nhiên, do tính chất của lỗ hổng nên Acunetix không thể xác nhận đầy đủ sự tồn tại của nó. Những lỗ hổng này thường có thể được chuyển tiếp đến các lập trình viên nhưng trước tiên có thể yêu cầu kiểm tra thủ công.
    - 80%: Do cách phát hiện các lỗ hổng này nên chúng dễ bị dương tính giả hơn. Chúng yêu cầu xác minh thủ công trước khi được chuyển đến nhóm lập trình để sửa chữa.
- Last Seen: Ngày giờ mà Acunetix tìm thấy Lỗ hổng.
- Vulnerability Id: Số nhận dạng được Acunetix cấp cho một Lỗ hổng.
- Issue Id: Số định danh vấn đề mà ta đã gửi Issue Tracker, chẳng hạn như Jira, ...
- Type: Loại quét (Web hoặc Network) đã xác định được lỗ hổng.

f. Báo cáo

Ở trang Reports, ta có thể xem các Báo cáo được tạo cho các lần quét đã hoàn thành hoặc ta có thể xóa, tải Báo cáo về.



Hình 35: Minh họa trang Reports trong Acunetix

Các loại báo cáo:

- Standard Reports:
    - Affected Items Report: hiển thị các tệp và vị trí nơi các lỗ hổng đã được phát hiện trong quá trình quét. Báo cáo cho thấy mức độ nghiêm trọng của lỗ

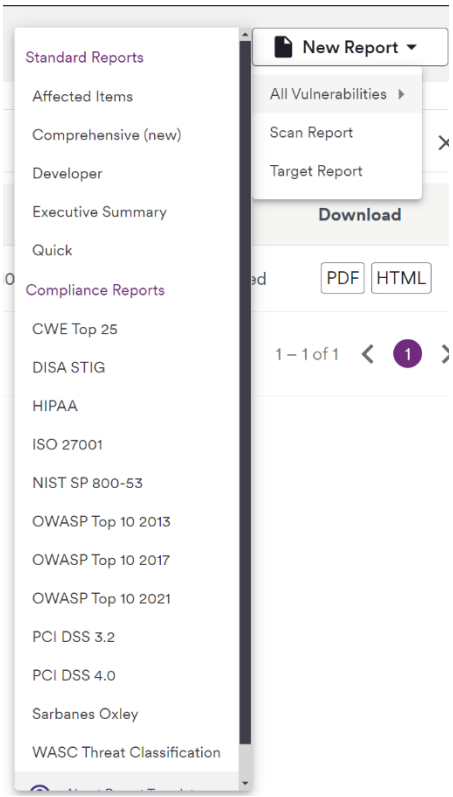
hổng được phát hiện, cùng với các chi tiết khác về cách lỗ hổng đã được phát hiện.

  - Developer Report: dành cho các lập trình viên cần làm việc trên trang web để giải quyết các lỗ hổng được phát hiện bởi Acunetix. Báo cáo cung cấp thông tin về các tệp có thời gian phản hồi dài, danh sách các liên kết bên ngoài, địa chỉ email, tập lệnh khách và máy chủ bên ngoài, cùng với các ví dụ khắc phục và đề xuất phương pháp tốt nhất để khắc phục các lỗ hổng.
  - Comprehensive Report: lấy các thông tin có sẵn trong Developer Report và trình bày một cách ngắn gọn hơn, thêm phần biểu đồ với dữ liệu thống kê. Đối với mỗi lỗ hổng, mỗi yêu cầu HTTP đến được mục tiêu được kèm theo phản hồi HTTP nhận được.
  - Executive Summary Report: tóm tắt các lỗ hổng được phát hiện trong một trang web và đưa ra một cái nhìn tổng quan rõ ràng về mức độ nghiêm trọng của các lỗ hổng được tìm thấy trong trang web.
  - Quick Report: cung cấp danh sách chi tiết tất cả các lỗ hổng được phát hiện trong quá trình quét.

- Comparing Scans: giúp ta so sánh hai lần quét trên cùng một Mục tiêu, làm nổi bật sự khác biệt giữa các lần quét. Tùy chọn này chỉ khả dụng khi 2 lần quét cho cùng một Mục tiêu được chọn.
- Compliance Reports:
  - CWE Top 25 Most Dangerous Software Weaknesses: Báo cáo này hiển thị danh sách các lỗ hổng đã được phát hiện trên trang web của ta, được liệt kê trong CWE Top 25 Most Dangerous Software Weaknesses. Những lỗi này thường dễ phát hiện, khai thác và nguy hiểm vì chúng thường sẽ cho phép kẻ tấn công chiếm quyền điều khiển trang web hoặc đánh cắp dữ liệu. Ta có thể tìm thêm thông tin tại http://cwe.mitre.org/top25/ .
  - The Health Insurance Portability and Accountability Act (HIPAA): Một phần của HIPAA Act định nghĩa các chính sách, thủ tục và nguyên tắc để duy trì quyền riêng tư và bảo mật của các thông tin sức khỏe cá nhân. Báo cáo này tìm ra các lỗ hổng có thể vi phạm các chính sách này. Các lỗ hổng này được nhóm theo các phần như được định nghĩa trong HIPAA Act.
  - International Standard – ISO 27001: là một phần của bộ tiêu chuẩn ISO / IEC 27000, chính thức chỉ định một hệ thống quản lý nhằm đưa bảo mật thông tin dưới sự kiểm soát quản lý 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: đề cập đến các biện pháp kiểm soát bảo mật được khuyến nghị dành cho "Federal Information Systems and Organizations". Các lỗ hổng được tìm thấy trong quá trình quét được nhóm theo danh mục như được định nghĩa trong ấn phẩm.
  - OWASP Top 10 2017: Open Web Application Security Project (OWASP) là một dự án bảo mật web do cộng đồng quốc tế của các tập đoàn, các tổ chức giáo dục và các nhà nghiên cứu bảo mật dẫn đầu. OWASP nổi tiếng với hoạt động bảo mật web, đặc biệt thông qua danh sách 10 rủi ro bảo mật web

hàng đầu cần tránh. Báo cáo này cho thấy lỗ hổng nào được phát hiện nằm trong 10 lỗ hổng hàng đầu của OWASP.

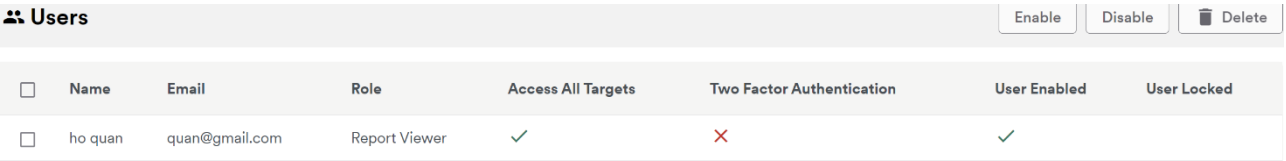
- Payment Card Industry (PCI) standards: Payment Card Industry Data Security Standard (PCI DSS) là một tiêu chuẩn bảo mật thông tin, áp dụng cho các tổ chức xử lý thông tin chủ thẻ tín dụng. Báo cáo này xác định các lỗ hổng có thể vi phạm các phần của tiêu chuẩn và nhóm các lỗ hổng theo điều vi phạm. Báo cáo PCI DSS 4.0 là phiên bản mới nhất. Các báo cáo cho phiên bản trước, PCI DSS 3.2, cũng vẫn có hiệu lực cho đến cuối tháng 3 năm 2024.
- Sarbanes Oxley Act: được ban hành nhằm ngăn chặn các hoạt động tài chính gian lận của các tập đoàn và ban lãnh đạo cấp cao. Báo cáo này liệt kê các lỗ hổng được phát hiện trong quá trình quét và có thể dẫn đến vi phạm các phần của Đạo luật.
- DISA STIG Web Security: Security Technical Implementation Guide (STIG) là hướng dẫn cấu hình cho phần mềm và phần cứng máy tính do Defense Information System Agency (DISA) - một bộ phận của Bộ Quốc phòng Hoa Kỳ định nghĩa. Báo cáo này xác định các lỗ hổng vi phạm các phần của STIG và nhóm các lỗ hổng theo các phần vi phạm trong hướng dẫn STIG.
- Web Application Security Consortium (WASC) Threat Classification: WASC là một tổ chức phi lợi nhuận bao gồm một nhóm chuyên gia bảo mật quốc tế, đã tạo ra một 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 ta bằng hệ thống phân loại mối đe dọa WASC.



Hình 36: Minh họa các loại báo cáo trong Acunetix

g. *Người dùng*

Ở trang Users, ta có thể xem các người dùng khác ngoài Administrator, những người này có thể truy cập Acunetix bằng tài khoản của mình do Admin thêm, thường là một nhóm người cùng 1 dự án. Nếu là Admin thì có thể thêm người dùng và tùy chỉnh các cài đặt bảo mật với người dùng.



Hình 37: Minh họa trang Users trong Acunetix

Các thuộc tính cần quan tâm khi thêm người dùng:

- Tên người dùng.
- Role: vai trò.

	Default Roles				
Chức năng	**System Administrator**	**Platform Administrator**	**AppSec Admin**	**AppSec User**	**Report Viewer**
Mục tiêu	Toàn quyền	Toàn quyền	Toàn quyền	Chỉ đọc	Chỉ đọc
Nhóm mục tiêu	Toàn quyền	Toàn quyền	Chỉ đọc	Chỉ đọc	Chỉ đọc
Hồ sơ quét	Toàn quyền	Toàn quyền	Chỉ đọc	Chỉ đọc	Chỉ đọc
Issue Tracker	Toàn quyền	Toàn quyền	Toàn quyền	Chỉ đọc	Chỉ đọc
Lỗ hổng	Toàn quyền	Toàn quyền	Toàn quyền	Toàn quyền	Chỉ đọc
Quét	Toàn quyền	Toàn quyền	Toàn quyền	Toàn quyền	Chỉ đọc
Báo cáo	Toàn quyền	Toàn quyền	Toàn quyền	Toàn quyền	Toàn quyền
Cài đặt hệ thống	Toàn quyền	Không	Không	Không	Không
WAF	Toàn quyền	Toàn quyền	Toàn quyền	Chỉ đọc	Chỉ đọc
Engines (chỉ khả dụng cho Acunetix	Toàn quyền	Chỉ đọc	Không	Không	Không

360 On-Premises)					
Khám phá	Toàn quyền	Toàn quyền	Toàn quyền	Không	Không
Excluded Hours	Toàn quyền	Toàn quyền	Chỉ đọc	Chỉ đọc	Chỉ đọc

Bảng 1: Bảng phân quyền các vai trò đối với các chức năng

h. Hồ sơ quét

Ở trang Scan Profiles, ta có thể xem các Hồ sơ quét và có thể thêm các Hồ sơ quét mới.

Hình 38: Minh họa trang Scan Profiles trong Acunetix

Hồ sơ quét là một tập hợp các các thử nghiệm được cấu hình sẵn để kiểm tra ứng dụng web của ta để tìm lỗ hổng. Khi khởi chạy quét, ta chọn một Hồ sơ quét để chạy lên Mục tiêu. Một loạt các Hồ sơ quét được thêm theo mặc định, với mặc định này được thiết kế để dựa trên các yêu cầu từ các chuyên gia bảo mật ứng dụng. Ta có thể sử dụng cấu hình quét mặc định hoặc tùy chỉnh dựa trên nhu cầu của mình bằng cách tạo Hồ sơ quét tùy chỉnh cho phù hợp với yêu cầu cụ thể của ta. Một Mục tiêu có thể được quét nhiều lần bằng cách sử dụng nhiều Hồ sơ quét khác nhau.

Các Hồ sơ quét mặc định:

- Critical / High Risk: Chỉ kiểm tra các lỗ hổng web nguy hiểm nhất, chẳng hạn như Cross-site Scripting, SQL Injection, File Inclusion, ...
- Critical / High / Medium Risk: Chỉ kiểm tra các lỗ hổng web khiến trang web có nguy cơ bị tấn công nghiêm trọng và cao cũng như rủi ro trung bình về cấu hình sai máy chủ và lỗi mã hóa trang web.
- Cross-site Scripting: Chỉ kiểm tra các lỗ hổng XSS.
- SQL Injection: Chỉ kiểm tra các lỗ hổng SQL Injection.
- Weak Passwords: Hồ sơ quét này xác định các biểu mẫu nhận tên người dùng và mật khẩu. Nó sẽ tấn công các biểu mẫu này để xác định các lỗ hổng.

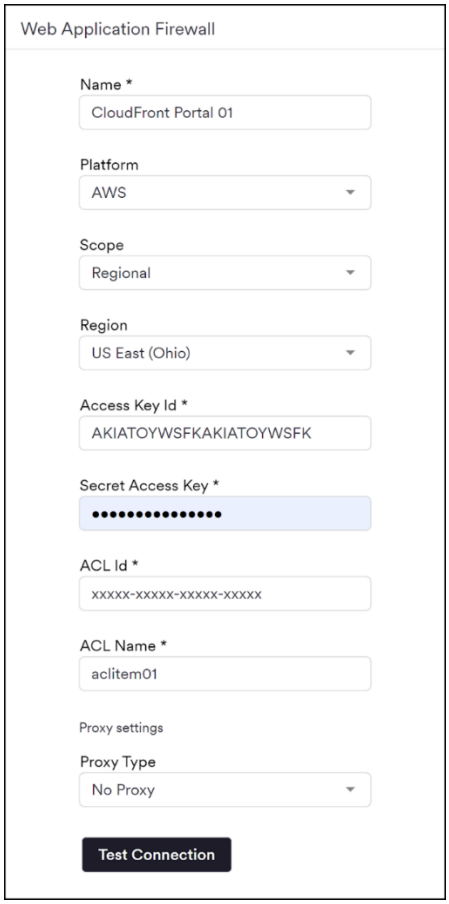
- Crawl Only: Chỉ thu thập dữ liệu trang web và xây dựng cấu trúc của trang web mà không chạy bất kỳ kiểm tra lỗ hổng nào.
- Full Web and Network Scan: Hồ sơ này bao gồm tất cả các bước kiểm tra lỗ hổng web mà Acunetix hỗ trợ và tất cả các bước kiểm tra bảo mật mạng mà Acunetix hỗ trợ thông qua công cụ OpenVAS.
- OWASP Top 10: Chỉ kiểm tra các rủi ro bảo mật nghiêm trọng nhất đối với các ứng dụng web theo quy định của OWASP Top 10.
- Network Scan: Sử dụng công cụ OpenVAS bên trong mạng của ta để quét các dịch vụ mạng không sẵn sàng với bên ngoài nhưng vẫn có thể gặp phải các mối đe dọa nội bộ.
- PCI checks: Xác định các lỗ hổng không tuân thủ các tiêu chuẩn bảo mật dữ liệu của PCI.
- Sans Top 25: Chỉ kiểm tra 25 lỗi phần mềm nguy hiểm nhất trong danh sách CWE.
- Full Scan: Khởi chạy quét bằng cách sử dụng tất cả các thử nghiệm có sẵn trong Acunetix. Hồ sơ này cung cấp phạm vi bảo hiểm toàn diện nhất về các lỗ hổng.

i. WAFs

Ở trang WAFs, ta có thể xem các WAF (Tường lửa ứng dụng web) đã cấu hình và thêm các luật mới cho tường lửa. Ta có thể sử dụng kết quả quét Acunetix để cấu hình WAF của mình nhằm giảm thiểu các lỗ hổng được phát hiện. Acunetix có chức năng tích hợp sẵn để tạo tệp cho một số sản phẩm WAF, cũng như các định dạng chung hơn như CSV và XML.

Ở trang Scans, ta có thể xuất kết quả quét đến các WAF bằng tính năng Export to. Các định dạng có thể xuất:

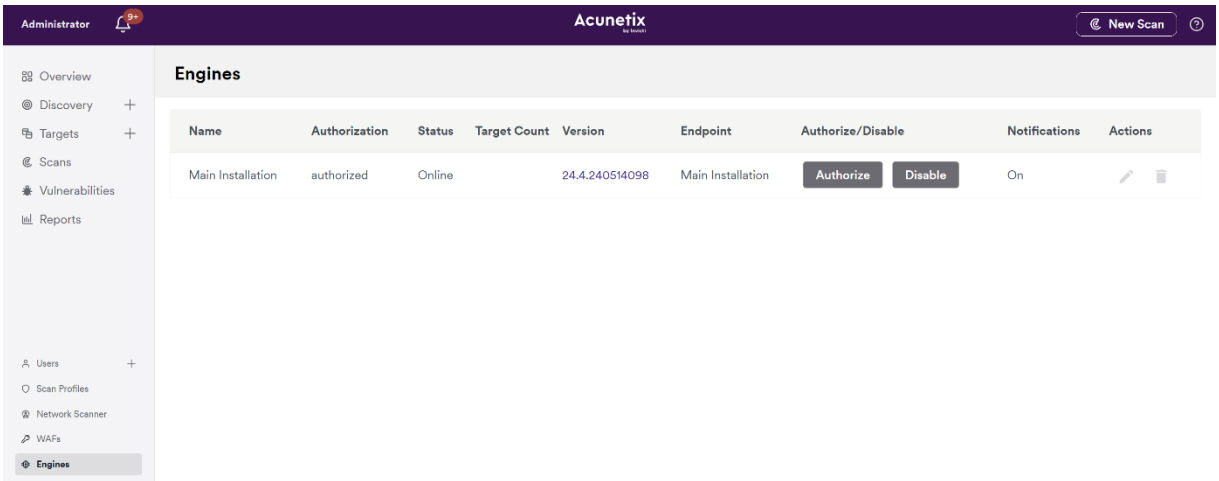
- Citrix Web App Firewall: tìm hiểu thêm cách đưa tệp xuất ra vào Citrix Web App Firewall tại đây.
- F5 Big-IP ASM (Application Security Manager): tìm hiểu thêm cách đưa tệp xuất ra vào F5 BIG-IP ASM tại đây.
- Fortinet Fortiweb: tìm hiểu thêm cách đưa tệp xuất ra vào Fortinet Fortiweb tại đây.
- Imperva SecureSphere WAF: tìm hiểu thêm cách đưa tệp xuất ra vào SecureSphere tại đây.
- Amazon AWS Web Application Firewall: chuyển kết quả trực tiếp đến API của AWS Web Application Firewall của Amazon. Trong trường hợp này, để tích hợp API của chúng vào ta cần cấu hình WAF trong Acunetix.



Hình 39: Minh họa cấu hình WAF trong Acunetix

j. Engines

Chỉ khả dụng với Acunetix Premium và Acunetix 360. Ngoài Scan Engines chính ra thì ta có thể thêm Engines cho Acunetix. Việc thêm Engines giúp Acunetix có thể thực nhiều lần Scan trên nhiều Mục tiêu cùng lúc. Cách để cài chế độ Multi-Engine cho Acunetix: https://www.acunetix.com/support/docs/how-to-install-acunetix-multi-engine/

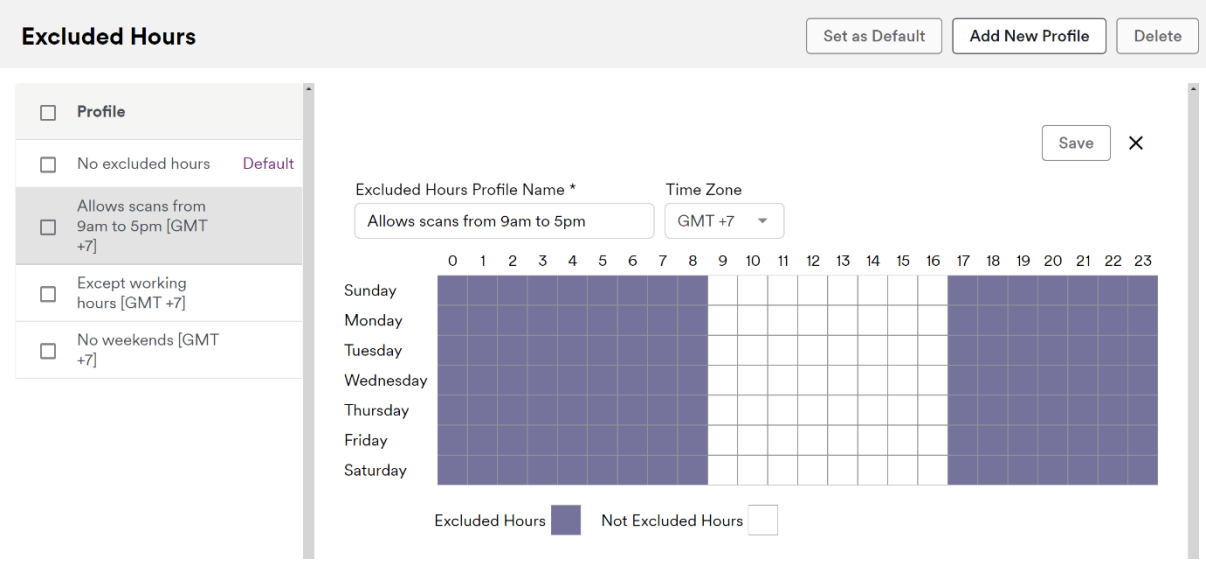


Hình 40: Giao diện Engines của Acunetix

k. Excluded Hours

Ở trang Excluded Hours, ta có thể xem các hồ sơ về khung giờ mà scanner sẽ không tự quét Mục tiêu. Ngoài ra, ta có thể thêm, xóa và chỉnh sửa các hồ sơ này hoặc đặt 1 hồ sơ làm mặc định cho các lần quét theo lịch. Các thông tin cần quan tâm khi cấu hình một hồ sơ:

- Excluded Hours Profile Name: tên hồ sơ.
- Time Zone: Múi giờ.
- Bảng thời gian: các cột là giờ trong ngày và các hàng là thứ trong tuần.



Hình 41: Minh họa cấu hình Excluded Hours Profile trong Acunetix

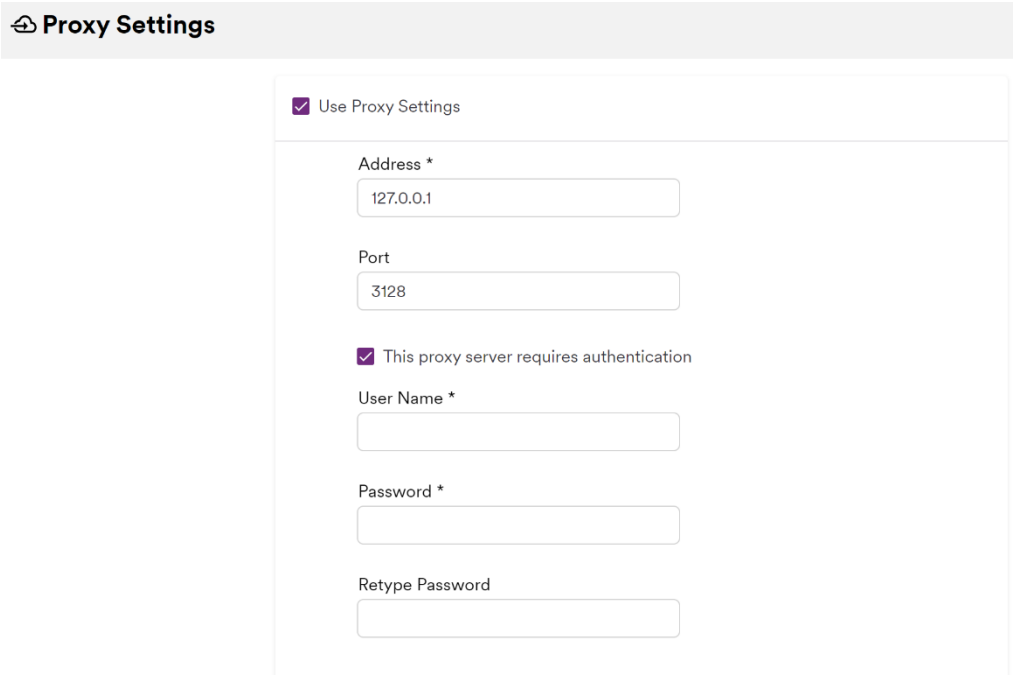
l. Agents

Chỉ khả dụng với Acunetix 360, ở trang Agents, ta có thể cài đặt và quản lý các Agent nội bộ. Gắn các Agent nội bộ cho các Mục tiêu nội bộ giúp ta có thể quét các ứng dụng quét không thể tiếp cận qua internet. Chức năng này dùng để hỗ trợ quét nội bộ, tìm hiểu thêm tại https://www.acunetix.com/support/docs/internal-site-scanning/ .

m. Proxy Settings

Ở trang này, ta có thể kết nối Acunetix tới 1 máy chủ Proxy cụ thể, thường sử dụng khi cần quét các web chỉ có thể tiếp cận thông qua 1 máy chủ Proxy riêng, tuy chỉnh, đặc biệt. Các thông cần cung cấp:

- Address: Địa chỉ máy chủ, thường là địa chỉ IP.
- Port: Cổng chạy dịch vụ Proxy, có thể là 3128 đối với Squid Proxy.
- Các thông tin chứng thực trong trường hợp máy chủ Proxy yêu cầu chứng thực.



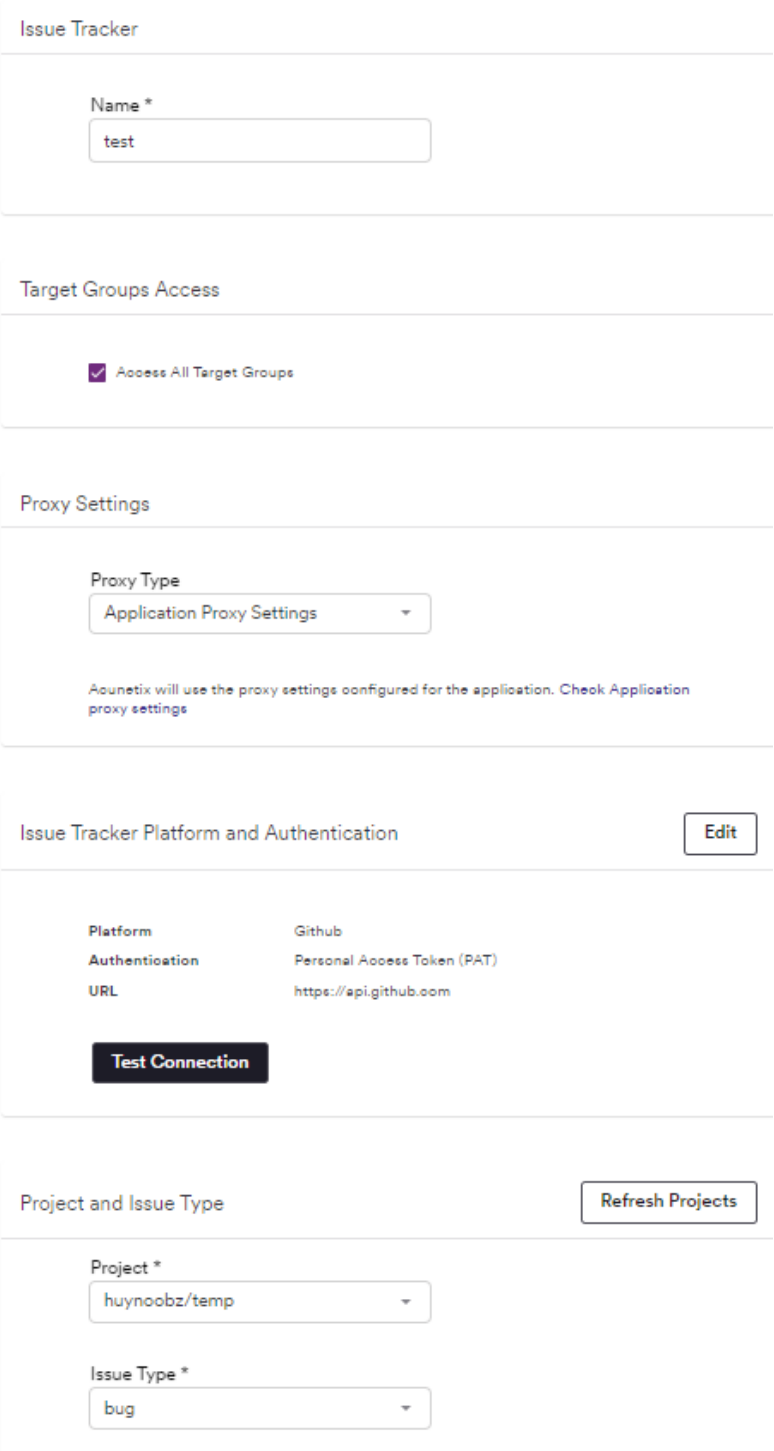
Hình 42: Minh họa cấu hình Proxy Settings trong Acunetix

n. Issue Trackers

Ở trang Issue Trackers, ta có thể xem các Issue Trackers và thêm Issue Trackers mới. Các trường cần quan tâm khi cấu hình Issue Tracker:

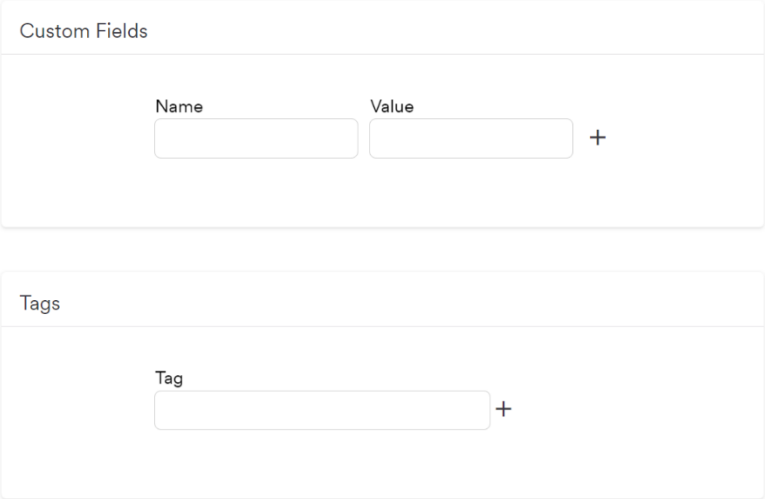
- Name: Tên Issue Tracker.
- Target Groups Access: Nhóm Mục tiêu mà Issue Tracker này được phép tiếp cận.
- Proxy Settings: Máy chủ Proxy mà Acunetix sẽ dùng khi gửi báo cáo vấn đề đến Issue Tracker.
- Issue Tracker Platform and Authentication: Nền tảng và các thông tin chứng thực để kết nối với nền tảng.
    - Các platform: Azure DevOps (trước gọi là Team Foundation Server (TFS)), Azure DevOps Services, BugZilla, Github, Gitlab, JIRA, Mantis.
    - URL: Đường dẫn tới API nhận thông tin chứng thực. Ví dụ với Github là https://api.github.com .
    - Các phương thức xác thực:
        - Azure DevOps: Username or Email/Password.
        - Azure DevOps Services: Token.
        - BugZilla: Token.
        - Github: PAT (Token), HTTP Basic (đã lỗi thời).
        - Gitlab: PAT, Impersonation tokens.
        - JIRA: HTTP Basic Token (Username or Email/Token), Oauth (Consumer key/Private key), HTTP Basic (đã lỗi thời), Cookie (đã lỗi thời).
        - Mantis: Token.

- Project and Issue Type: Tên dự án trên nền tảng sẽ nhận báo cáo và loại vấn đề mà báo cáo được chỉ định.



Hình 43: Minh họa cấu hình Issue Tracker trong Acunetix

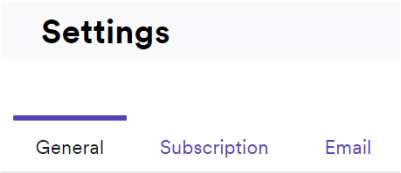
- Custom Fields: Có thể thêm các trường tùy chỉnh được gán giá trị. Chỉ các nền tảng sau có trường này: Azure DevOps, Azure DevOps Services, BugZilla, JIRA, Mantis. Với Mantis thì có thêm trường Tags.



Hình 44: Minh họa trường Custom Fields và Tags trong việc cấu hình Issue Tracker trong Acunetix

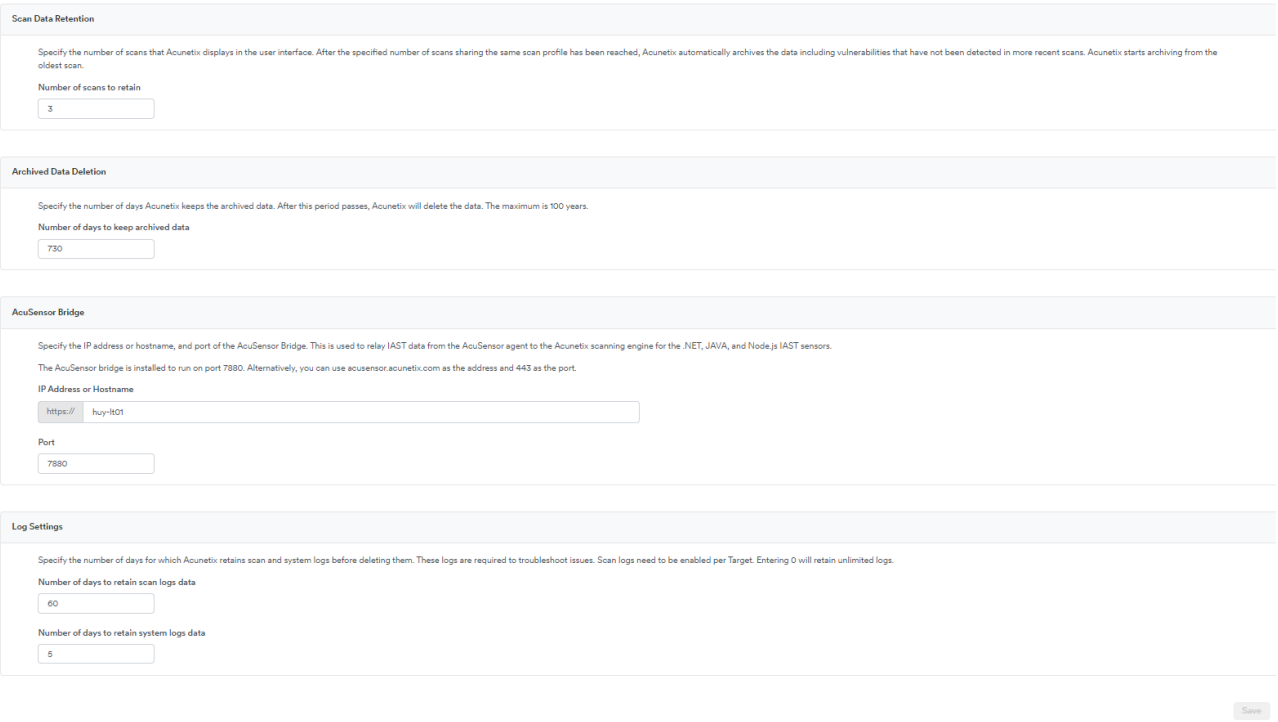
o. *Cài đặt*

Ta có thể xem và tùy chỉnh các cài đặt ở trang Settings:



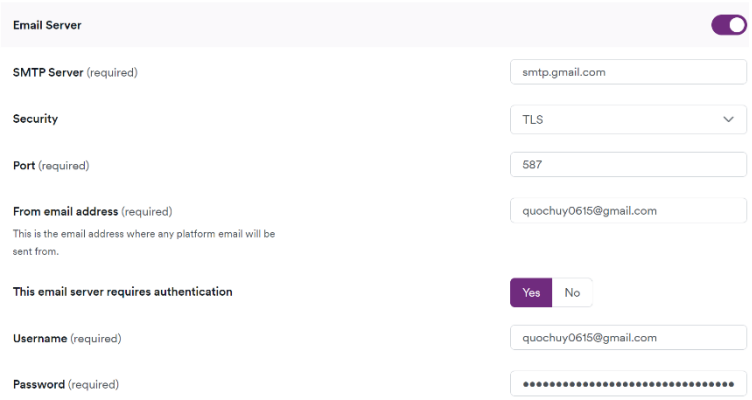
Hình 45: Minh họa trang Settings trong Acunetix

- General: Các cài đặt chung.
    - Scan Data Retention: Số lần quét mà Acunetix hiển thị trên giao diện. Sau khi đạt đến số lần quét được chỉ định chia sẻ cùng một Hồ sơ quét, Acunetix sẽ tự động lưu trữ dữ liệu bao gồm các lỗ hổng chưa được phát hiện trong các lần quét gần đây hơn. Acunetix bắt đầu lưu trữ từ lần quét cũ nhất.
    - Archived Data Deletion: Chỉ định số ngày Acunetix lưu trữ dữ liệu. Sau khi khoảng thời gian này trôi qua, Acunetix sẽ xóa dữ liệu. Tối đa là 100 năm.
    - AcuSensor Bridge: Chỉ định địa chỉ IP hoặc tên máy chủ và cổng của AcuSensor Bridge. Dùng để chuyển tiếp dữ liệu IAST từ AcuSensor agent đến công cụ quét Acunetix cho các cảm biến IAST .NET, JAVA và Node.js. AcuSensor Bridge được cài đặt để chạy trên cổng 7880. Ngoài ra, ta có thể sử dụng acusensor.acunetix.com làm địa chỉ và 443 làm cổng.
    - Log Settings: Chỉ định số ngày mà Acunetix giữ lại bản ghi hệ thống và quét trước khi xóa chúng. Những nhật ký này được yêu cầu để khắc phục sự cố. Nhật ký quét cần phải được bật cho mỗi Mục tiêu. Nhập 0 sẽ giữ lại nhật ký không giới hạn.



Hình 46: Minh họa các cài đặt chung của Acunetix

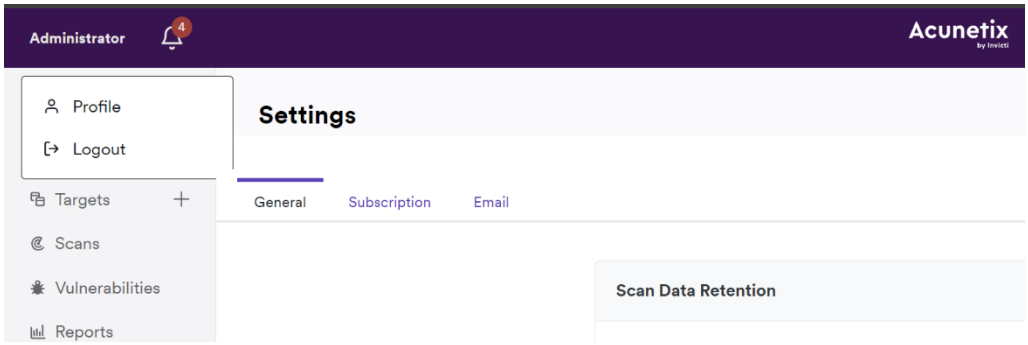
- Subscription: chứa thông tin chứng chỉ.
- Email: cấu hình một máy SMTP để gửi email khi cần thông báo. Thường là máy chủ SMTP riêng, nội bộ.
    - SMTP Server: Địa chỉ máy chủ SMTP.
    - Security: Giao thức bảo mật: None, Auto, SSL, TLS.
    - Port: cổng, mặc định là 587 nếu dùng TLS, 465 nếu dùng SSL.
    - From email address: Địa chỉ email dùng để gửi mail.
    - This email server requires authentication: thêm thông tin chứng thực nếu cần.



Hình 47: Minh họa cấu hình SMTP server trong Acunetix

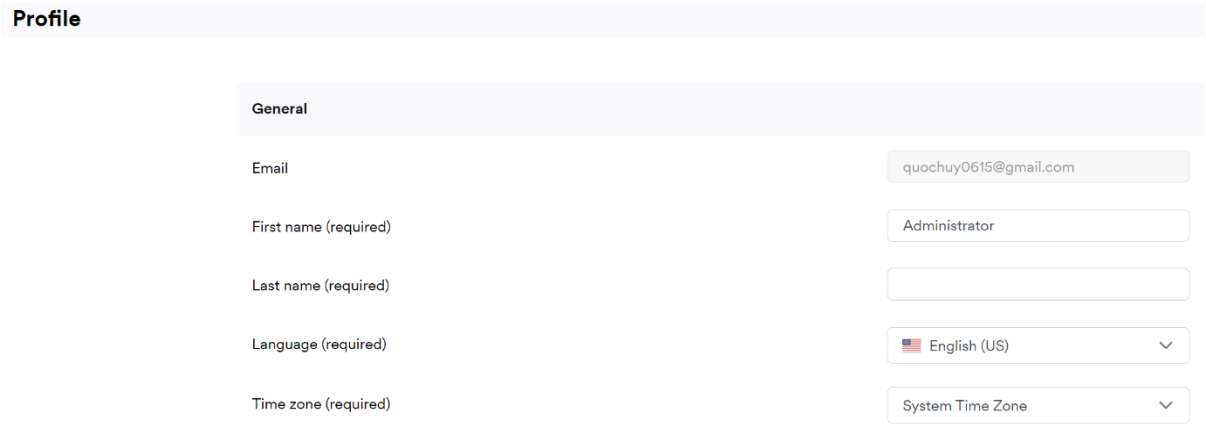
Có thể xem thông tin phiên bản của Acunetix và kiểm tra cập nhật ở trang About.

Xem thông tin và các cài đặt khác ở trang Profile:



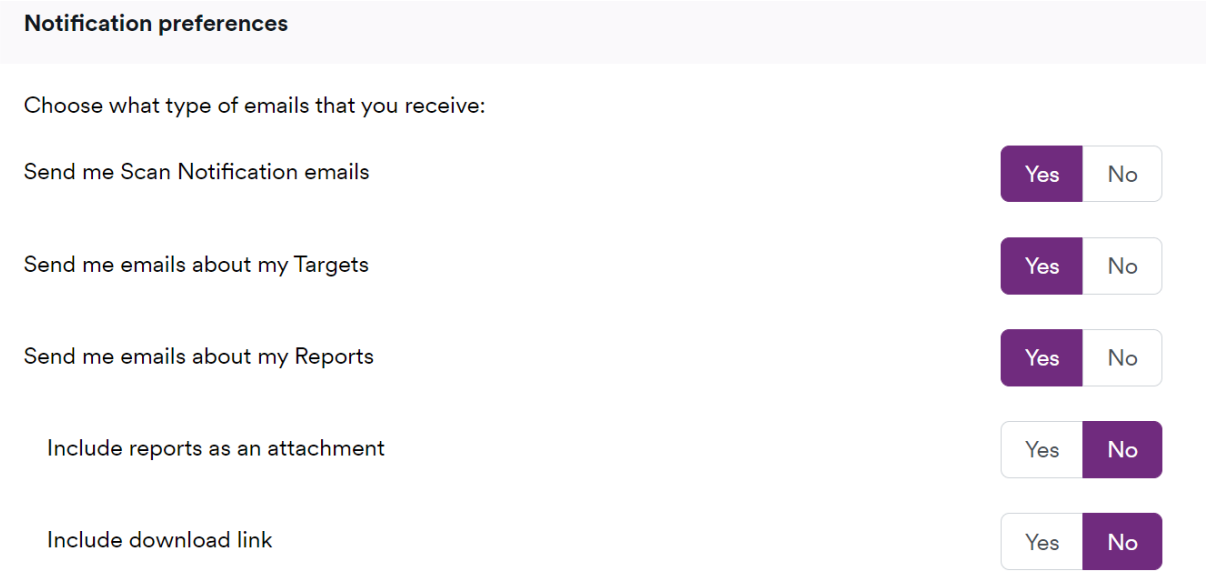
Hình 48: Vị trí để truy cập Profile

- General: Các thông tin và cài đặt chung: Email, tên, ngôn ngữ, múi giờ.



Hình 49: Minh họa General của Profile trong Acunetix

- Notification preferences: Các cài đặt liên quan đến các thông báo.

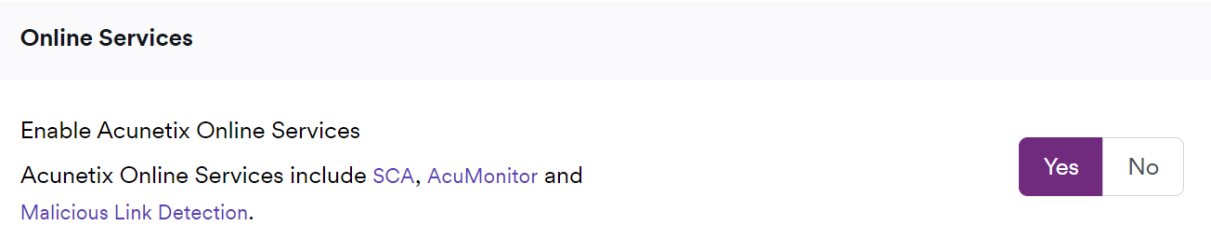


Hình 50: Minh họa cài đặt thông báo của Profile trong Acunetix

- Security: Các cài đặt bảo mật cho tài khoản.

Hình 51: Minh họa các cài đặt bảo mật của Profile trong Acunetix

- Online Services: Có sử dụng các dịch vụ trực tuyến như SCA, AcuMonitor, Malicious Link Detection, ... hay không.



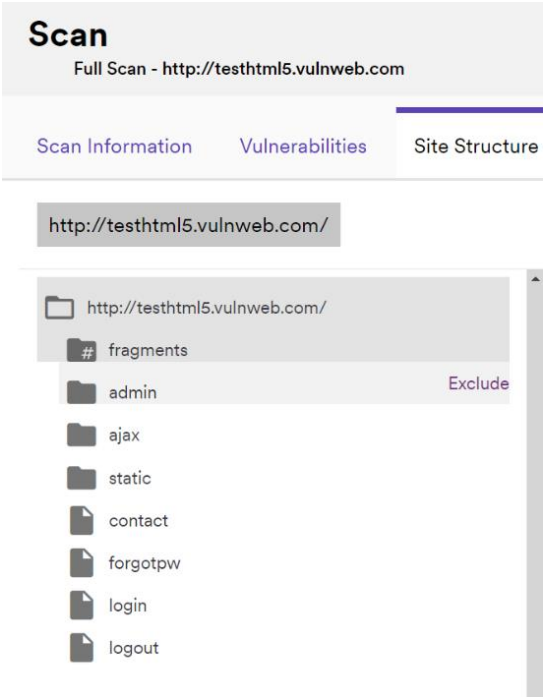
Hình 52: Minh họa Online Services của Profile trong Acunetix

- API Key: Khóa API, dùng để tích hợp với ứng dụng khác.

Hình 53: Minh họa API Key của Profile trong Acunetix

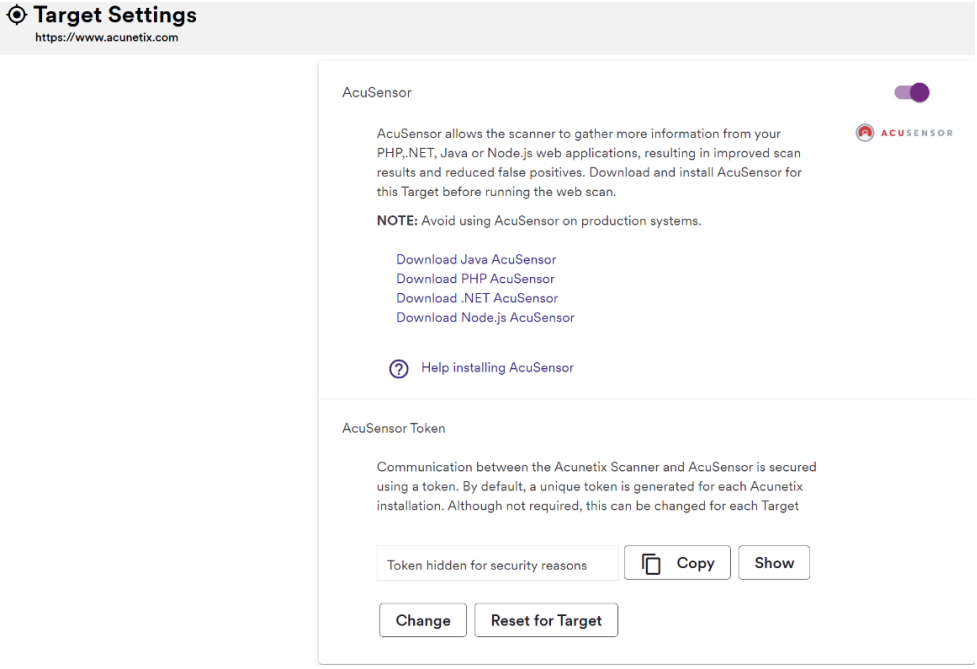
3. Một lần quét của Acunetix hoạt động thế nào?

Đầu tiên là giai đoạn thu thập thông tin, Acunetix sử dụng Acunetix DeepScan để phân tích toàn bộ trang web bằng cách đi theo tất cả các liên kết trên trang web, bao gồm các liên kết được tạo động bằng JavaScript và các liên kết được tìm thấy trong robots.txt và sitemap.xml (nếu có). Kết quả là một bản đồ của trang web mà Acunetix sẽ sử dụng để khởi chạy các cuộc kiểm tra có mục tiêu đối với từng phần của trang web.



Hình 54: Minh họa bản đồ của trang web được tạo bởi Acunetix khi quét

Nếu lần quét này có sử dụng Acunetix AcuSensor Technology thì AcuSensor sẽ truy xuất danh sách tất cả các tệp có trong thư mục ứng dụng web và thêm các tệp mà trình thu thập thông tin không tìm thấy vào đầu ra của trình thu thập thông tin. Các tệp như vậy thường không được trình thu thập thông tin phát hiện vì chúng không thể truy cập được từ máy chủ web hoặc không được liên kết qua trang web. AcuSensor cũng phân tích các tệp không thể truy cập được từ internet, chẳng hạn như web.config.



Hình 55: Minh họa quét có dùng AcuSensor của Acunetix

Sau quá trình thu thập thông tin, máy quét sẽ tự động khởi chạy một loạt các cuộc kiểm thử lỗ hổng trên mỗi trang được tìm thấy, về bản chất là mô phỏng tin tặc. Acunetix cũng phân tích từng trang để tìm những vị trí có thể nhập dữ liệu và sau đó thử tất cả các kết hợp đầu vào khác nhau. Đây là Giai đoạn quét tự động. Nếu AcuSensor được sử dụng thì một loạt các biện pháp kiểm tra lỗ hổng bảo mật bổ sung sẽ được triển khai đối với trang web. Thông tin thêm về AcuSensor được cung cấp trong phần sau.

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

Filter

Severity	Vulnerability	URL	Parameter	Status	Confidence %
Critical	Command Injection	http://graphql.testinvicti.com/graphql	variables.createFunnyPicturetext	Open	100
Critical	Local File Inclusion	http://graphql.testinvicti.com/graphql	variables.getWebsiteSeoScoreurl	Open	100
Critical	Server-Side Request Forgery	http://graphql.testinvicti.com/graphql	variables.getWebsiteSeoScoreurl	Open	100
Critical	Server-Side Template Injection	http://graphql.testinvicti.com/graphql	variables.getWebsiteOfferbrandName	Open	95
High	Cross-site Scripting via Remote File Inclusion	http://graphql.testinvicti.com/graphql	variables.getWebsiteSeoScoreurl	Open	100
Medium	GraphiQL Explorer/Playground Enabled	http://graphql.testinvicti.com/		Open	95
Medium	GraphQL Alias Overloading Allowed: Potential Denial of Service Vulnerability	http://graphql.testinvicti.com/		Open	95

Hình 56: Minh họa kết quả quét của Acunetix

Các lỗ hổng được tìm thấy sẽ được hiển thị trong tab "Vulnerabilities". Mỗi cảnh báo về lỗ hổng bảo mật chứa thông tin về lỗ hổng như dữ liệu POST được sử dụng, mục bị ảnh hưởng, phản hồi HTTP của máy chủ, ... Nếu AcuSensor được sử dụng thì các chi tiết như số dòng mã nguồn, dấu vết ngăn xếp (stack trace) hoặc truy vấn SQL bị ảnh hưởng dẫn đến lỗ hổng sẽ được liệt kê. Các khuyến nghị về cách khắc phục lỗ hổng cũng sẽ được hiển thị.

Có thể tạo các báo cáo dựa trên kết quả quét. Các định dạng báo cáo đã viết ở mục 3.2.f của báo cáo.

4. Acunetix AcuSensor Technology

AcuSensor là công nghệ độc nhất của Acunetix cho phép ta tìm thấy nhiều lỗ hổng hơn các Máy quét ứng dụng web khác, đồng thời tạo ra ít kết quả dương tính giả hơn. Acunetix AcuSensor chỉ ra chính xác vị trí có lỗ hổng trong mã của ta và báo cáo thêm thông tin gỡ lỗi.

Độ chính xác tăng lên, tính sẵn sàng cho các ứng dụng web PHP, .NET và JAVA, đạt được bằng cách kết hợp các kỹ thuật quét "hộp đen" (black box) với phản hồi từ các cảm biến (AcuSensor) được đặt bên trong mã nguồn. Kĩ thuật quét "hộp đen" thì không thể biết ứng dụng phản ứng như thế nào khi bị tấn công và trình phân tích mã nguồn thì không thể hiểu ứng dụng sẽ hoạt động như thế nào khi bị tấn công. Công

nghệ AcuSensor kết hợp cả hai kỹ thuật trên để đạt được kết quả tốt hơn đáng kể so với việc sử dụng trình phân tích mã nguồn và quét "hộp đen" một cách riêng biệt.

AcuSensor có thể được cài trong mã nguồn .NET, PHP và JAVA một cách minh bạch (transparently). AcuSensor có thể được cài vào các mã assembly đã biên dịch (pre-compiled assembly) của .NET và JAVA ngay cả khi chúng được ký, do đó, không cần mã nguồn .NET hoặc JAVA, cũng như trình biên dịch (hoặc bất kỳ phụ thuộc nào khác). Trong trường hợp các ứng dụng web PHP thì mã nguồn luôn sẵn sàng. Đến nay, Acunetix là giải pháp bảo mật lỗ hổng web duy nhất triển khai công nghệ này.

Lợi ích của việc sử dụng AcuSensor:

- Cho phép ta xác định vị trí và khắc phục lỗ hổng nhanh hơn nhờ khả năng cung cấp thêm thông tin về lỗ hổng, chẳng hạn như số dòng mã nguồn, dấu vết ngăn xếp, truy vấn SQL bị ảnh hưởng, …
- Giảm đáng kể các kết quả dương tính giả khi quét một trang web vì nó đã hiểu rõ hơn các hành vi của ứng dụng web mục tiêu.
- Có thể cảnh báo ta về các vấn đề cấu hình có thể dẫn đến "misconfiguration" hoặc làm lộ thông tin nhạy cảm. Ví dụ, nếu "custom errors" được bật trong .NET, điều này có thể làm lộ các chi tiết ứng dụng nhạy cảm cho người dùng độc hại.
- Tư vấn cho ta cách bảo mật các tùy chỉnh của web server tốt hơn, ví dụ: nếu "write access" được bật trên web server.
- Phát hiện nhiều lỗ hổng SQL injection hơn. Các lỗ hổng SQL injection trước đây chỉ có thể được tìm thấy nếu lỗi cơ sở dữ liệu (ví dụ: khi thực thi câu truy vấn không hợp lệ) được báo cáo, trong khi bây giờ mã nguồn có thể được phân tích để cải thiện khả năng phát hiện.
- Khả năng phát hiện các lỗ hổng SQL injection trong tất cả các câu lệnh SQL, bao gồm cả trong câu lệnh SQL INSERT. Nếu chỉ sử dụng kỹ thuật quét "hộp đen" thì không thể phát hiện được các lỗ hổng SQL injection như vậy. Điều này làm tăng đáng kể khả năng Acunetix tìm ra các lỗ hổng.
- Khi quét có sử dụng AcuSensor để thu thập thông tin từ phía back-end sẽ hiển thị được tất cả các tệp có thể truy cập được thông qua web server tới trình quét; ngay cả khi những tệp này không được kết nối thông qua ứng dụng front-end. Điều này đảm bảo phạm vi bao phủ 100% của ứng dụng và cảnh báo người dùng về bất kỳ tệp backdoor nào có thể đã được kẻ tấn công tải lên với mục đích xấu.
- Công nghệ AcuSensor có thể chặn tất cả đầu vào của ứng dụng web và xây dựng danh sách toàn diện với tất cả đầu vào khả thi có trên trang web và kiểm tra chúng.
- Khả năng kiểm tra các lỗ hổng trong quá trình tạo và xóa một tập tin bất kỳ. Ví dụ: thông qua một tập lệnh có lỗ hổng, người dùng độc hại có thể tạo một tệp trong thư mục ứng dụng web và thực thi nó để lấy đặc quyền hoặc xóa các tệp ứng dụng web nhạy cảm.

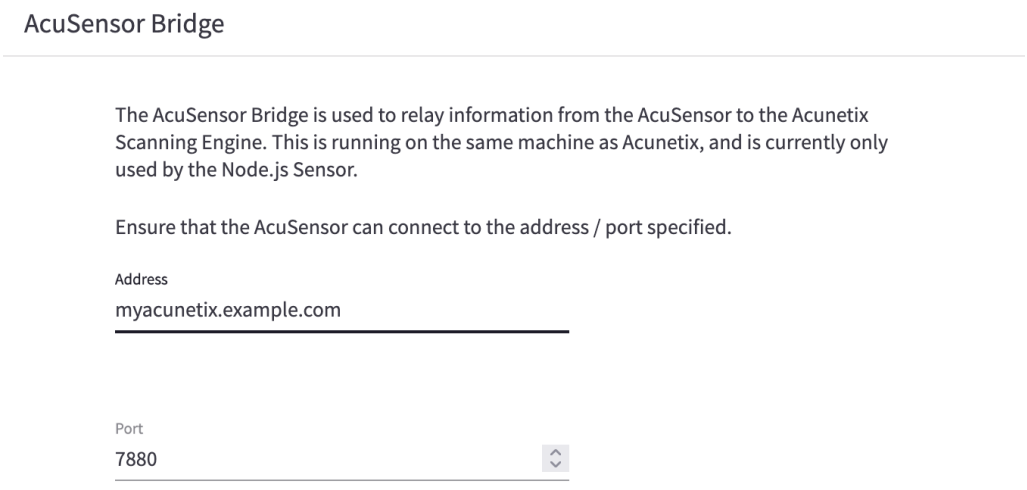
Cách triển khai AcuSensor với các nên tảng công nghệ ứng dụng web có thể tìm hiểu thêm tại đây.

5. AcuSensor Bridge

AcuSensor Bridge là một thành phần quan trọng đối với IAST trong Acunetix. Chức năng chính của nó là tạo điều kiện thuận lợi cho việc chuyển tiếp các tin nhắn "ngoài băng tần" giữa công cụ quét Acunetix và cảm biến IAST. AcuSensor Bridge được sử dụng bởi AcuSensors Java, .NET và Node.js. Còn PHP IAST AcuSensor có thể giao tiếp trực tiếp với scanner.

Trước khi triển khai AcuSensor, điều quan trọng là phải chú ý đến địa chỉ (tên máy chủ hoặc IP) và số cổng được cấu hình cho AcuSensor Bridge. Cảm biến IAST sẽ gửi dữ liệu đến địa chỉ/cổng đã định cấu hình. Đảm bảo rằng địa chỉ đã cấu hình có thể được phan giải bởi máy chủ đang chạy ứng dụng web và không có hạn chế nào ngăn cản cảm biến IAST gửi dữ liệu đến AcuSensor Bridge. Điều này có nghĩa là nếu không triển khai Acunetix trên một máy có địa chỉ IP công khai thì chỉ có thể áp dụng quét có AcuSensor với các ứng dụng web nội bộ.

Theo mặc định, AcuSensor Bridge lắng nghe dữ liệu AcuSensor đến trên cổng 7880. Tên máy chủ được AcuSensor triển khai sử dụng tương ứng với tên máy chủ được cấu hình trong quá trình cài đặt Acunetix ban đầu.



Hình 57: Minh họa cấu hình AcuSensor Bridge trong Acunetix

6. Network Vulnerability Scanning

Bản Acunetix Premium cung cấp thêm các chức năng liên quan đến kiểm toán trang web, trong đó có chức năng "Network Vulnerability Scanning". Acunetix Premium sẽ yêu cầu phiên bản trực tuyến của Acunetix thực thi một cuộc kiểm toán an ninh mạng với server đang vận hành (hosting) trang web. Lần quét này sẽ xác định bất kỳ dịch vụ nào đang chạy trên server bằng cách thực hiện "quét cổng". Acunetix sau đó sẽ báo cáo thông tin về hệ điều hành và các phần mềm đang vận hành các dịch vụ mà lần quét này phát hiện. Quá trình này có thể kiểm tra xem liệu có Trojan đang ẩn trên server hay không.

Network Vulnerability Scanning đánh giá tính bảo mật của các giao thức phổ biến như FTP, DNS, SMTP, IMAP, POP3, SSH, SNMP và Telnet. Ngoài việc kiểm tra mật khẩu yếu hoặc mật khẩu mặc định, Acunetix cũng sẽ kiểm tra "misconfiguration" trong các dịch vụ được phát hiện mà có thể dẫn đến các vi phạm bảo mật. Acunetix cũng sẽ kiểm tra các server khác đang chạy trên máy xem liệu có dùng các giao thức bị lỗi thời. Tất cả những điều trên sẽ dẫn đến một hệ thống không an toàn, thứ mà sẽ cho phép kẻ xâm nhập phá hủy trang web và danh tiếng của ta.

Acunetix Online còn tích hợp trình quét mạng OpenVAS phổ biến để kiểm tra hơn 50.000 lỗ hổng mạng. Trong quá trình quét mạng, Acunetix sử dụng nhiều kỹ thuật dò cổng và OS fingerprinting khác nhau để xác định một số lượng lớn thiết bị, hệ điều hành và các sản phẩm máy chủ. Sau đó, nhiều biện pháp kiểm tra bảo mật sẽ được triển khai đối với các sản phẩm được xác định đang chạy trên máy chủ được quét, cho phép ta phát hiện tất cả các lỗ hổng tồn tại trên máy chủ ngoại vi của mình.

7. Cách cài đặt Acunetix

Ở đây là cách cài đặt Acunetix bản quyền phiên bản mới nhất.

a. Yêu cầu hệ thống để cài đặt Acunetix

Trong đồ án này, ngoài tìm hiểu hiểu về Acunetix, nhóm còn phải tìm một bản Acunetix chi phí thấp để triển khai các kịch bản nên những gì trình bày sau đây là về phiên bản Acunetix mới nhất – Acunetix v24.5.240604185 ra mắt 05/01/2024. Còn về phiên bản Acunetix mà nhóm sử dụng để thực nghiệm sẽ được nói ở phần sau.

Các hệ điều hành hỗ trợ	- Microsoft Windows 10 hoặc Windows Server 2016 R2 hoặc mới hơn - Ubuntu Desktop/Server 18.0.4 LTS hoặc cao hơn - Suse Linux Enterprise Server 15 - Kali Linux các phiên bản 2019.1 hoặc mới hơn - CentOS 8 hoặc CentOS Stream Server hoặc Workstation (với SELinux bị tắt) - RedHat 8 hoặc 9 (với SELinux bị tắt) - Oracle Linux 8 (với SELinux bị tắt)
Yêu cầu phần cứng	- CPU: bộ xử lý 64-bit - RAM: tối thiểu 2 GB - Bộ nhớ: ít nhất 1 GB trống
Trình duyệt hỗ trợ	Các bản mới nhất của các trình duyệt sau: - Firefox - Chrome - Edge - Safari
Các yêu cầu truy cập	Máy vận hành Acunetix phải truy cập được erp.acunetix.com

Bảng 2: Yêu cầu hệ thống của Acunetix v24.5

b. Cài đặt trên Windows

Bước 1: Tải phiên bản mới nhất của Acunetix cho Windows về máy, nới tải sẽ được cấp sau khi ta mua chứng chỉ.

Bước 2: Chạy tệp cài đặt để bắt đầu cài đặt thông qua "Acunetix installation wizard". Trong quá trình cài đặt, cung cấp thông tin chứng thực cho tài khoản admin. Người dùng sẽ dùng tài khoản này để truy cập và cấu hình Acunetix. Trong quá trình cài đặt, cấu hình cách truy cập Acunetix Web UI và có cho phép truy cập UI từ xa hay không. Sau khi cài đặt hoàn tất nhấn "Finish" và thử truy cập Acunetix.

c. Cài đặt trên Linux

Bước 1: Cài các thư viện cần thiết:

- Ubuntu: sudo apt-get install libxdamage1 libgtk-3-0 libasound2 libnss3 libxss1 libx11-xcb1 libxcb-dri3-0 libgbm1 libdrm2 libxshmfence1 libxmlsec1-openssl bzip2
- Suse Linux Enterprise Server: sudo zypper install libXdamage1 libgtk-3-0 libasound2 mozilla-nss libX11-xcb1 libXss1 libxmlsec1-openssl1 libgbm.so.1
- Red Hat Enterprise Linux 8 or CentOS 8 or CentOS Stream: sudo yum install libX11 libX11-devel gtk3 nss libXScrnSaver alsa-lib bzip2 mesa-libgbm libxshmfence xmlsec1-openssl

Bước 2: Tắt SeLinux trên CentOS 8, CentOS Stream, RedHat 8 hoặc Oracle Linux. Đổi dòng "SELINUX=enabled" trong tệp /etc/selinux/config thành "SELINUX=disabled", rồi khởi động lại máy.

Bước 3: Tải Acunetix bản mới nhất cho Linux, nơi tải được cung cấp sau khi mua chứng chỉ.

Bước 4: Cấp quyền thực thi cho tệp acunetix_*.sh. Ví dụ: chmod +x acunetix_13.0.200205121_x64.sh

Bước 5: Thực thi tệp với quyền quản trị để bắt đầu cài đặt. Ví dụ: sudo ./acunetix_13.0.200205121_x64.sh

Bước 6: Trong quá trình cài đặt, cung cấp hostname sẽ được sử dụng để truy cập Acunetix UI và cung cấp thông tin chứng thực cho tài khoản admin. Tài khoản này sẽ được dùng để truy cập Acunetix. Hoàn tất cài đặt và thử truy cập Web UI của Acunetix.

d. Kích hoạt Acunetix

Đăng nhập vào Acunetix thông qua web UI, mặc định web UI của Acunetix sẽ chạy trên https://localhost:3443.

Sau khi đăng nhập thành công, người dùng sẽ được chuyển hướng đến trang "Subscription" để thêm khóa của chứng chỉ đã mua và tiến hành kích hoạt Acunetix.

e. Các cấu hình khác trong quá trình cài đặt Acunetix

- AcuSensor: Để biết thông tin về cách định cấu hình cài đặt cho AcuSensor Bridge và thông tin mạng mà Acunetix sẽ sử dụng dữ liệu AcuSensor sắp tới.
- Language: Trên trang "User Profile", ta có thể chọn từ một trong các ngôn ngữ có sẵn cho giao diện web.
- Timezone: Nếu ta muốn Acunetix trình bày thông tin ngày tháng theo Múi giờ khác với múi giờ của hệ điều hành, ta có thể chọn múi giờ mong muốn từ trang "User Profile".
- AcuMonitor Service: Ta cũng có thể chọn đăng ký cài đặt của mình với dịch vụ AcuMonitor. AcuMonitor được sử dụng để phát hiện một số loại lỗ hổng nhất định, chẳng hạn như Blind XSS, SSRF, XXE và các lỗ hổng khác, thứ mà chỉ có thể được phát hiện bằng cách sử dụng dịch vụ trung gian.

f. Thêm các công nghệ quét bổ sung

Ta có thể thêm các công cụ quét bổ sung để tăng hiệu quả đánh giá mục tiêu.

- AcuSensor: Nếu ta cần quét các ứng dụng web .NET, Java hoặc PHP, ta nên cài đặt Acunetix AcuSensor trên ứng dụng web của mình để cải thiện việc phát hiện các lỗ hổng, lấy dòng trong mã nguồn nơi có lỗ hổng và giảm kết quả dương tính giả. Chi tiết cách cài đặt AcuSensor sẽ được viết ở phần sau.
- Network Scanning (OpenVAS): Acunetix On-Premises có thể cấu hình sử dụng OpenVAS nhằm thực hiện quét mạng đối với các mục tiêu. Hướng dẫn trên trang chính chủ: Installing Network Scanning (OpenVAS)
- Malware Scanning: Acunetix có thể hoạt động kết hợp với các công cụ chống vi-rút để kiểm tra phần mềm độc hại trên trang web của ta. Công cụ mặc định được sử dụng là dịch vụ Windows Defender AntiVirus, với ClamAV là một giải pháp thay thế khả thi. Chi tiết cài đặt và thực hiện Malware Scanning sẽ được viết ở phần sau.

8. Acunetix 360 là gì?

Acunetix 360 là trình quét bảo mật ứng dụng web trực tuyến tự động, cho phép ta quét các trang web, ứng dụng web và dịch vụ web cũng như xác định các lỗi bảo mật. Acunetix 360 có thể quét tất cả các loại ứng dụng web, bất kể nền tảng hoặc ngôn ngữ mà chúng được xây dựng.

Acunetix 360 là trình quét bảo mật ứng dụng web trực tuyến duy nhất tự động khai thác các lỗ hổng đã xác định theo cách "chỉ đọc"(read-only) và an toàn để xác nhận các vấn đề được tìm thấy. Nó cũng đưa ra các bằng chứng về lỗ hổng để ta không cần lãng phí thời gian xác minh nó theo cách thủ công. Ví dụ: trong trường hợp lỗ hổng

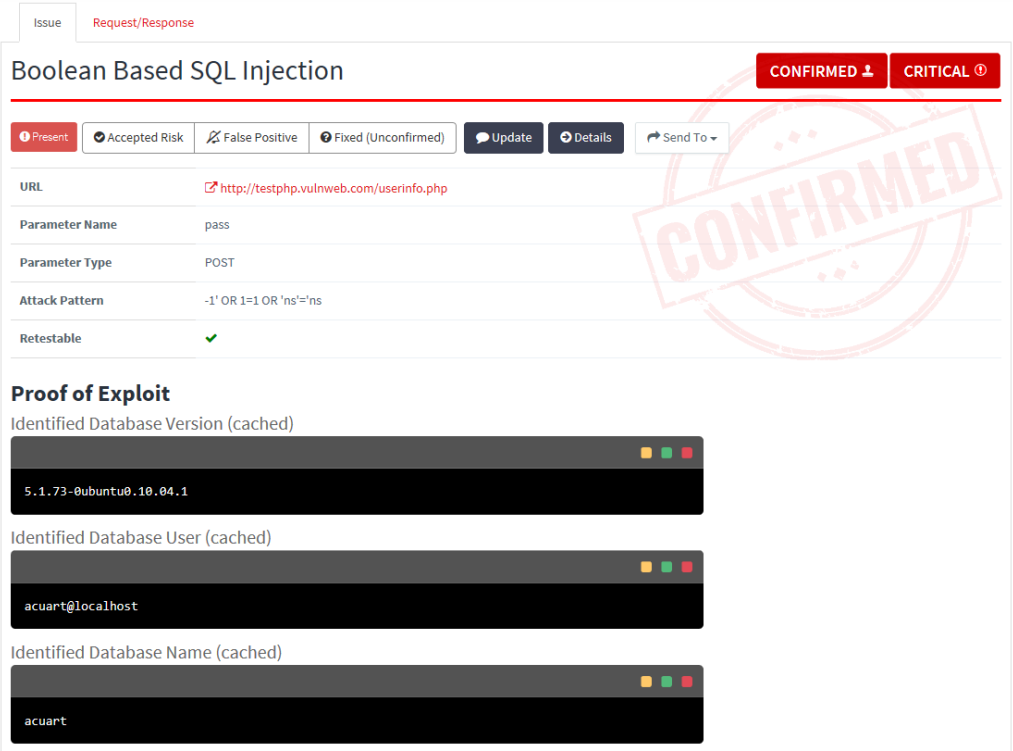
SQL Inejection được phát hiện, nó sẽ hiển thị tên cơ sở dữ liệu làm bằng chứng về lỗ hổng.

Các chức năng mà Acunetix có thì Acunetix 360 cũng có, ngoài ra có các chức năng mà chỉ Acunetix 360 có, đã được ghi rõ ở mục "Các chức năng của Acunetix".

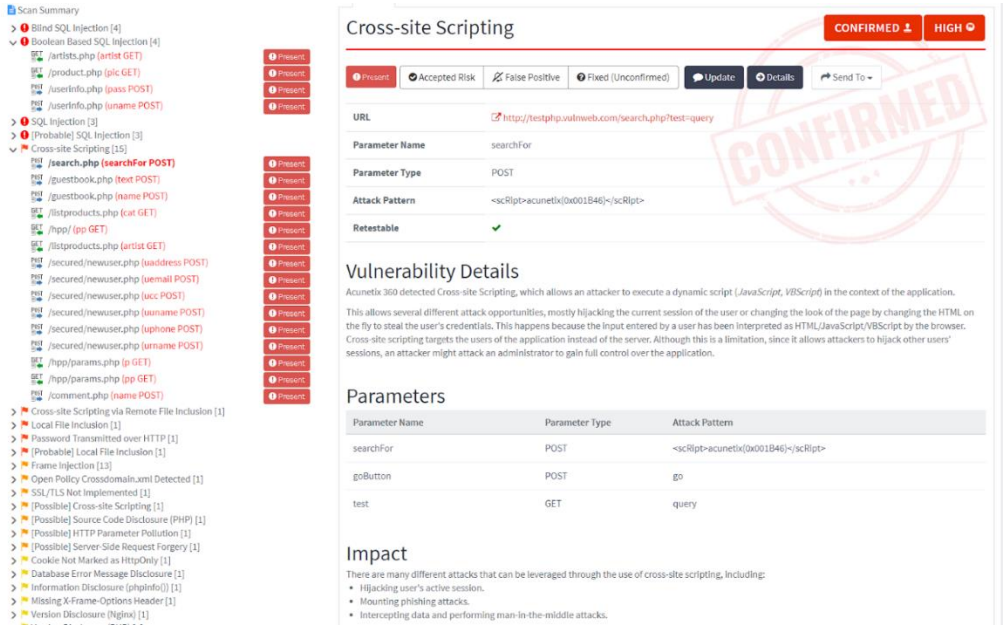
Điểm nổi bật	**Mô tả**
Độ chính xác cao	Acunetix 360 tạo ra những lần quét bảo mật ứng dụng web có độ chính xác cao, với các lỗ hổng đã được xác thực thì chứng minh rằng chúng không phải là kết quả dương tính giả.
Bằng chứng khai thác (POE)	Công nghệ của Invicti Security chủ động và tự động xác minh các lỗ hổng được phát hiện, xác nhận rằng chúng là thật chứ không phải giả, bằng cách khai thác chúng theo cách "chỉ đọc" và an toàn. Tùy thuộc vào loại lỗ hổng, Acunetix 360 sẽ tạo bằng chứng. Tuy nhiên, một số lỗ hổng cho phép ta khai thác chúng theo cách thủ công hoặc tạo POC. Nó hoàn toàn an toàn. Ví dụ: khi khai thác lỗ hổng SQL injection và tạo bằng chứng khai thác lỗ hổng đó, máy quét sẽ chỉ cố đọc dữ liệu từ cơ sở dữ liệu chứ không ghi hoặc xóa dữ liệu khỏi cơ sở dữ liệu. POE được sử dụng để báo cáo rằng dữ liệu có thể bị trích xuất từ mục tiêu một khi lỗ hổng bị khai thác, thể hiện tác động mà lỗ hổng bị khai thác có thể gây ra và chứng minh rằng đó không phải là kết quả dương tính giả. Acunetix 360 có thể tạo bằng chứng khi xác định được các loại lỗ hổng sau: - SQL Injection - Boolean SQL Injection - Blind SQL Injection - Command Injection - Local File Inclusion (LFI) - Remote File Inclusion (RFI) - Remote Code Evaluation - Remote Code Execution thông qua LFI Nếu Acunetix 360 không thể tự động chứng minh lỗ hổng tồn tại, ta sẽ được thông báo để có thể kiểm tra kỹ các phát hiện của nó.
Proof of Concept	Acunetix 360 xác định các lỗ hổng rồi khai thác chúng một cách an toàn trong quá trình quét lỗ hổng trên web. POC là cách khai thác thực tế, chứng minh rằng lỗ hổng này tồn tại. Không cần xác minh lỗ hổng một cách thủ công. Và nó rất hữu ích nếu ta cần tái hiện lỗ hổng cho lập trình viên.
Chính sách quét	Acunetix 360 cho phép ta sử dụng Chính sách quét để xác định và chỉ định loại, phạm vi và mục tiêu quét theo nhu cầu của ta.

Tích hợp	Acunetix 360 tích hợp với nhiều phần mềm và công cụ cho phép ta kết nối với SDLC hiện có của mình, bao gồm hệ thống quản lý lỗ hổng, hệ thống theo dõi sự cố, hệ thống CI, nhà cung cấp dịch vụ đăng nhập một lần, hệ thống nhắn tin nhóm và tường lửa ứng dụng web.

Bảng 3: Bảng liệt kê các điểm nổi bật của Acunetix 360



Hình 58: Minh họa bằng chứng khai thác lỗ hổng SQL Injection của Acunetix 360



Hình 59: Minh họa báo cáo lỗ hổng XSS của Acunetix 360 với URL là thứ dùng để khai thác lỗ hổng

Acunetix 360 có 2 phiên bản là Acunetix 360 Online hay Acunetix 360 On-Demand và Acunetix 360 On-Premises. Acunetix 360 Online là bản Acunetix 360 trực tuyến công khai ai cũng có thể tiếp cận và có một số hạn chế do nhà sản xuất đặt ra, có thể truy cập qua đường dẫn: https://online.acunetix360.com/ . Acunetix 360 On-Premises là bản Acunetix 360 bán cho khách hàng để họ tùy ý triển khai, phiên bản này không bị hạn chế như bản On-Demand để khách hàng có thể tùy chỉnh và mở rộng theo ý muốn.

Menu (In nghiêng là menu con)	**Acunetix 360 On-Demand**	**Acunetix 360 On-Premises**
Discovery	Có	Có
Trang webs	Có	Có
Scans	Có	Có
Scheduled Scans	Có	Có
Reporting	Có	Có
Issues	Có	Có
Technologies	Có	Có
Policies	Có	Có
Notifications	Có	Có
Integrations	Có	Có
Team	Có	Có
Activity	Có	Có
Agents	Có	Có
Settings	Có	Có
General	Có	Có
Security	Không	Có
Database	Không	Có
Email	Không	Có
SMS	Không	Có
Service Credentials	Không	Có
Cloud Provider	Không	Có
Authentication Verifier	Có	Có
Licensing	Không	Có
Single Sign-On	Có	Có

IP Restrictions	Có	Có

Bảng 4: Bảng so sánh menu giữa Acunetix 360 On-Demand và On-Premises

Điểm so sánh	Acunetix Standard	Acunetix Premium	Acunetix 360
Trình thu thập thông tin DeepScan	Có	Có	Có
AcuSensor	Có	Có	Có
AcuMonitor	Có	Có	Có
Continuous Scanning	Không	Có	Có
Kiểm soát truy cập theo vai trò	Không	Có	Có
Compliance Reports	Không	Có	Có
Issue Tracke và khả năng tích hợp SDLC	Không	Có	Có
Chế độ Multi-Engine	Không	Có	Có
Khám phá tài nguyên web	Có	Có	Có
Cho phép tùy chỉnh Workflows	Không	Không	Có
Đã phát hiện hơn 7000 lỗ hổng web	Có	Có	Có
Đã quét hơn 50000 lỗ hổng mạng	Không	Có	Không

Bảng 5: Bảng so sánh sơ bộ Acunetix Standard, Premium và 360

Chi tiết so sánh tại đây.

9. Một vài thông tin về Acunetix 360 On-Premises

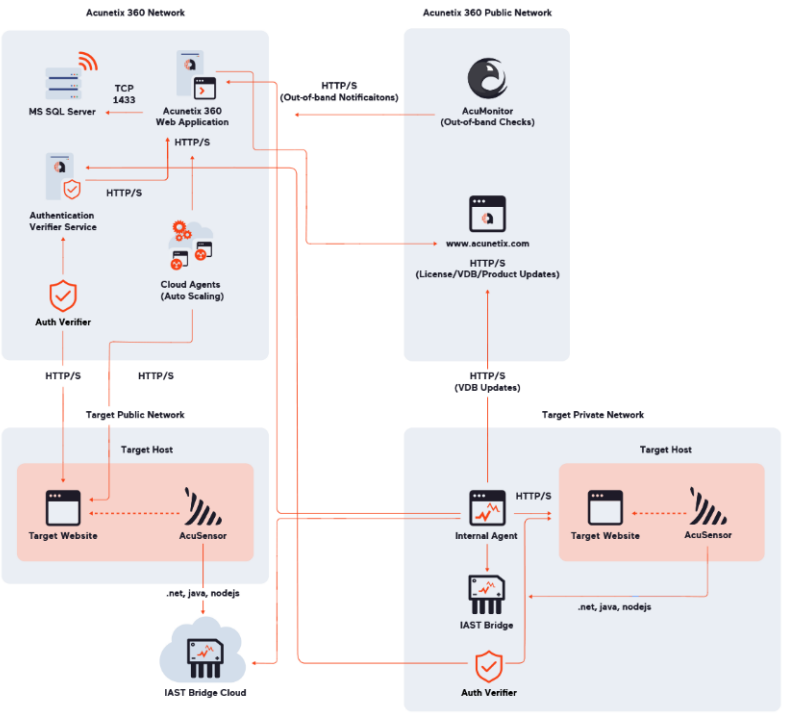
Với Acunetix 360 On-Premises ta có thể:

- Quét bất kỳ ứng dụng web nội bộ nào mà không cần cho phép truy cập thông qua tường lửa của công ty.
- Không cần kết nối internet.
- Có thể được triển khai dễ dàng trên AWS, Microsoft Azure, Google Cloud hoặc bất kỳ nền tảng đám mây nào khác. Do đó, ta không cần phải tự mua và bảo trì phần cứng và nếu không cần khả năng mở rộng theo yêu cầu, ta có thể sử dụng máy vật lý hoặc máy ảo.

- Nếu doanh nghiệp của ta phải tuân thủ các yêu cầu và chính sách tuân thủ quy định nghiêm ngặt hoặc ta lo ngại về việc dữ liệu của mình được lưu trữ trên máy chủ của Invicti Security, nhưng ta vẫn cần các chức năng của Acunetix 360 thì phiên bản On-Premises có thể được cài đặt trên máy chủ của riêng ta, được quản lý bởi nhóm của ta.

Acunetix 360 On-Premises gồm 5 thành phần chính:

- Application Server: Là máy chủ cung cấp giao diện web cho phép quản trị hiệu quả và tự động hóa quét. Đây là ứng dụng mà người dùng sẽ thấy và sử dụng thông qua giao diện người dùng của Acunetix 360.
- Agent: Đây là một ứng dụng dịch vụ thực thi quét và thông báo cho Application Server Acunetix 360 về kết quả. Một Agent duy nhất chỉ có thể chạy một lần quét tại một thời điểm. Nếu ta muốn chạy nhiều lần quét cùng một lúc, ta sẽ cần cài đặt nhiều Agent hơn.
- Authentication Verifier Agent: Đây là một ứng dụng dịch vụ giúp kiểm tra cấu hình xác thực đăng nhập dựa trên biểu mẫu. Đây là một thành phần tùy chọn. Nếu ta cần quét các trang web yêu cầu xác thực biểu mẫu, ta cần cài đặt nó.
- Authentication Verifier Service: Đây là một ứng dụng dịch vụ thiết lập giao tiếp giữa Authentication Verifier Agent và Acunetix 360 Application Server. Đây là một thành phần tùy chọn. Nếu ta cần quét các trang web yêu cầu xác thực biểu mẫu, ta cần cài đặt nó.
- Acunetix 360 Bridge: Đây là một ứng dụng dịch vụ được sử dụng để chuyển tiếp thông tin từ AcuSensor Agent đến Agent quét. Đây là một thành phần tùy chọn. Nếu ta đang sử dụng AcuSensor cho Java, .NET và Node.js, ta cần cài đặt cầu nối này.



Hình 60: Sơ đồ kiến trúc của Acuntix 360 On-Premises

10. Cách cài đặt Acunetix 360 On-Premises

a. Yêu cầu hệ thống cho Acunetix 360 Application Server

Yêu cầu phần mềm	- Windows Server 2016 trở lên (khuyến nghị Windows Server 2019 trở lên) - Vai trò máy chủ web (IIS) nên được cài đặt trên máy chủ - IIS 10 - .NET Framework 4.8
Yêu cầu phần cứng	Tối thiểu: CPU 2 nhân, RAM 4GB, dung lượng đĩa trống 5 GB - Với phần cứng như trên thì có thể sử dụng giao diện Acunetix 360 và quét một vài trang web đơn giản. Có thể gặp vấn đề hiệu suất. Khuyến nghị: CPU 2 nhân, RAM 16 GB, Dung lượng ổ đĩa trống 20 GB - Phần cứng như thế này là tốt. Nâng cao: CPU 4 nhân, RAM 32 GB, Dung lượng ổ đĩa trống 50 GB - Nếu ta có nhiều người dùng, trang web nâng cao và muốn chạy nhiều lượt quét cùng lúc thì cần phần cứng như này.
Yêu cầu truy cập	- Thông tin xác thực RDP và quyền truy cập với tư cách là Quản trị viên - Có thể được cài đặt bởi Kỹ sư Acunetix (hoặc người dùng) bằng trình cài đặt được cung cấp

Bảng 6: Yêu cầu hệ thống cho Acunetix 360 Application Server

b. Yêu cầu hệ thống cho Acunetix 360 Agent

Yêu cầu phần mềm	- Windows Server 2016 trở lên (khuyên dùng Windows Server 2019 trở lên) - .NET 6
Yêu cầu phần cứng	- Bộ xử lý tối thiểu 1,4 GHz (khuyên dùng 2 GHz hoặc nhanh hơn) - Khuyến nghị RAM 4 GB trở lên - Dung lượng đĩa trống 10 GB cho mỗi Agent nội bộ
Yêu cầu về mạng	- Agent cần có khả năng truy cập vào cổng HTTP(S) (443/80) của Acunetix 360 Application Server
Yêu cầu truy cập	- Việc cài đặt Agent yêu cầu quyền Quản trị viên - Đảm bảo rằng các nhóm sau không có quyền sửa đổi hoặc ghi đè tệp thực thi dịch vụ và các nhóm này không có toàn quyền kiểm soát đối với bất kỳ thư mục nào chứa tệp thực

	thi dịch vụ: *Everyone, Users, Domain Users, Authenticated Users*

Bảng 7: Yêu cầu hệ thống cho Acunetix 360 Agent

c. *Yêu cầu hệ thống với Authentication Verifier Service và Authentication Verifier Agent*

Yêu cầu phần mềm	- Windows Server 2016 trở lên (khuyên dùng Windows Server 2019 trở lên) - .NET 6
Yêu cầu phần cứng	- Bộ xử lý tối thiểu 1,4 GHz (khuyên dùng 2 GHz hoặc nhanh hơn) - Tối thiểu 1GB RAM (khuyến nghị RAM 4 GB trở lên) - Dung lượng đĩa trống tối thiểu 2 GB (khuyên dùng 5 GB trở lên)
Yêu cầu về mạng	- Authentication Verifier Agent cần có khả năng truy cập vào cổng HTTP(S) của Authentication Verifier Service (Cổng mặc định: 5000). - Người dùng doanh nghiệp có thể truy cập công khai vào Invicti Authentication Verifier Service Hub (Cổng mặc định: 5000). - Authentication Verifier Service cần có khả năng truy cập vào cổng HTTP(S) (443/80) của Acunetix 360 Application Server
Yêu cầu truy cập	- Việc cài đặt Authentication Verifier Agent và Authentication Verifier Service yêu cầu quyền của Quản trị viên - Đảm bảo rằng các nhóm sau không có quyền sửa đổi hoặc ghi đè tệp thực thi dịch vụ và các nhóm này không có toàn quyền kiểm soát đối với bất kỳ thư mục nào chứa tệp thực thi dịch vụ: *Everyone, Users, Domain Users, Authenticated Users*

Bảng 8: Yêu cầu hệ thống với Authentication Verifier Service và Authentication Verifier Agent

d. *Yêu cầu hệ thống cho Acunetix 360 Bridge*

Yêu cầu phần mềm	- Windows Server 2016 trở lên (khuyên dùng Windows Server 2019 trở lên)
Yêu cầu phần cứng	- Bộ xử lý tối thiểu 1,4 GHz (khuyên dùng 2 GHz hoặc nhanh hơn) - Khuyến nghị RAM 4 GB trở lên

Yêu cầu về mạng	- Acusensor Bridge Service cần có khả năng lắng nghe trên cổng HTTP(S) (7880) của Acunetix 360 Application Server
Yêu cầu truy cập	- Việc cài đặt Acunetix 360 Bridge yêu cầu quyền Quản trị viên - Đảm bảo rằng các nhóm sau không có quyền sửa đổi hoặc ghi đè tệp thực thi dịch vụ và các nhóm này không có toàn quyền kiểm soát đối với bất kỳ thư mục nào chứa tệp thực thi dịch vụ: *Everyone*, *Users*, *Domain Users*, *Authenticated Users*

Bảng 9: Yêu cầu hệ thống cho Acunetix 360 Bridge

e. Yêu cầu hệ thống với Database Server

Yêu cầu phần mềm	- Windows Server 2016 trở lên (khuyên dùng Windows Server 2019 trở lên)
Yêu cầu phần cứng	- Tương tự Application Server
Yêu cầu về mạng	- Acunetix 360 Application Server phải truy cập được vào Database Server này bằng cổng liên quan (1433 theo mặc định) hoặc nằm trên cùng một máy chủ
Yêu cầu truy cập	- Đăng nhập cơ sở dữ liệu SQL Server với vai trò db_owner - Tên của cơ sở dữ liệu SQL Server trống - Trường Database Collation phải được cấu hình là không phân biệt chữ hoa chữ thường

Bảng 10: Yêu cầu hệ thống với Database Server

f. Tóm tắt các bước cài đặt

Tóm tắt các bước như sau:

Bước 1: Tải tệp Acunetix360.zip được gửi qua mail (có sau khi mua).

Bước 2: Giải nén và chạy tệp WebAppSetup.exe để bắt đầu cài đặt Acunetix 360 Application Server và Authentication Verifier Service.

Bước 3: Sau khi cài xong Acunetix 360 Application Server và Authentication Verifier Service, chạy tệp AgentSetup.exe để bắt đầu cài đặt Acunetix 360 Agent.

Bước 4: Sau khi cài xong Acunetix 360 Agent, chạy tệp AuthVerifierSetup.exe để bắt đầu cài Acunetix 360 Authentication Verifier Agent.

Bước 5: Sau khi cài xong Acunetix 360 Authentication Verifier Agent, chạy tệp IASTBridgeSetup.exe để bắt đầu cài Acunetix 360 Bridge.

Bước 6: Sau khi cài xong Acunetix 360 Bridge thì coi như có đủ 5 thành phần chính cảu Acunetix 360, tiếp theo là các cài đặt mợ rộng như thêm máy chủ Proxy, cài thêm nhiều Agent, bảo mật cho Acunetix 360, …

Chi tiết cài đặt Acunetix 360 On-Premises xem tại đây.

11. Acunetix Manual Tools là gì?

Acunetix Manual Tools (AMT) không phải là ứng dụng kiểm thử ứng dụng web tự động mà là một bộ công cụ kiểm thử xâm nhập thủ công miễn phí được cấp bởi Invicti. Tải xuống tại đây: https://www.acunetix.com/vulnerability-scanner/free-manual-pen-testing-tools/ .

Những công cụ này không phải là một phần của sản phẩm Acunetix. Acunetix Manual Tools gồm 8 mô-đun: HTTP Editor, Subdomain Scanner, Target Finder, Blind SQL Injector, HTTP Fuzzer, Authentication Tester, Web Services Editor và HTTP Sniffer. Acunetix Manual Tools là miễn phí dành cho mục đích sử dụng cá nhân và thương mại nhưng chúng không phải là một dự án nguồn mở. Hiện tại, chúng chỉ có sẵn cho hệ điều hành Microsoft Windows. Các công cụ chỉ sử dụng giao diện đồ họa và không hỗ trợ dùng lệnh. Người kiểm thử xâm nhập có thể sử dụng bộ công cụ này cùng với các công cụ khác như Metasploit exploitation framework, OWASP Zed Attack Proxy (ZAP), w3af audit framework, Wireshark, ... để mở rộng kiến thức của họ về một vấn đề bảo mật cụ thể được phát hiện bởi trình quét lỗ hổng web tự động hoặc để tìm các lỗ hổng bảo mật nâng cao mà trình quét tự động không thể phát hiện được. Sự kết hợp giữa các công cụ tự động và thủ công là giải pháp tốt nhất cho một khung kiểm thử bảo mật ứng dụng web. Trình quét tự động tiết kiệm rất nhiều thời gian trong khi các công cụ thủ công cho phép người kiểm thử xâm nhập khám phá sâu hơn.

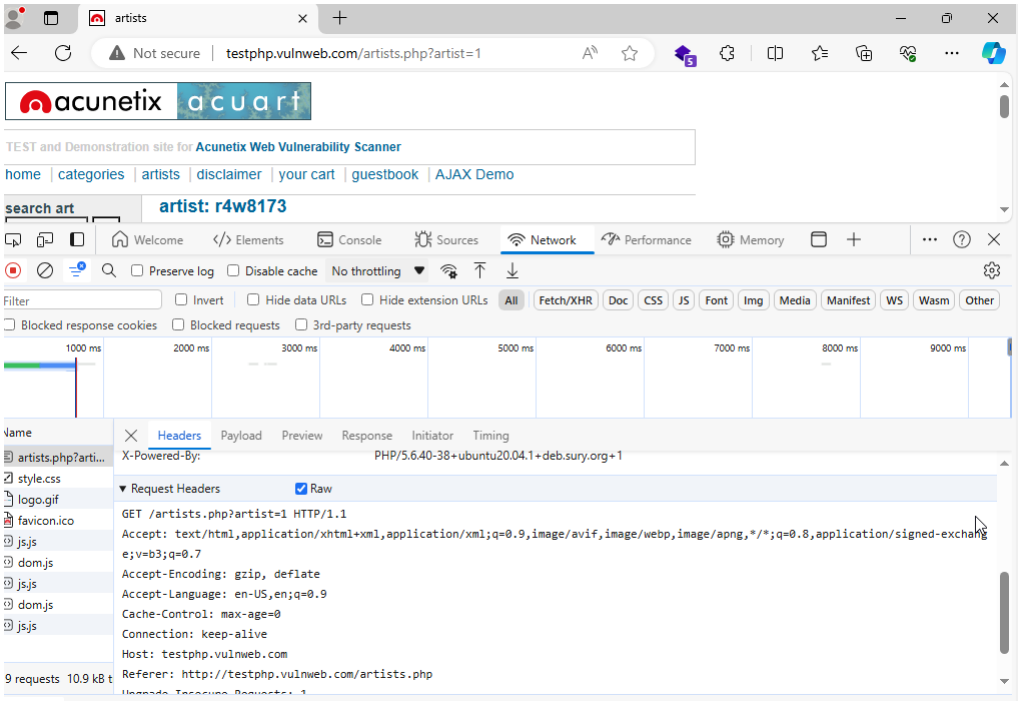
12. Các tính năng của Acunextix Manual Tools

a. HTTP Editor

HTTP Editor là Mô đun hỗ trợ soạn thảo và gửi HTTP Requets và nhận Reponse cho Request được gửi.

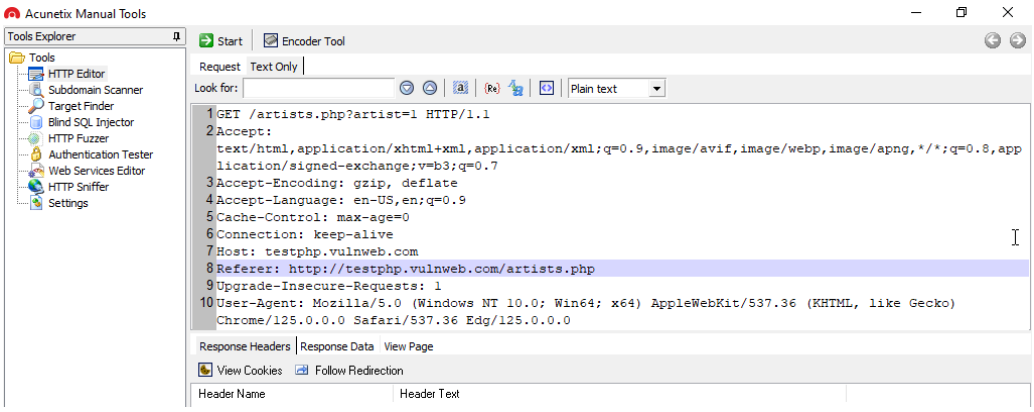
Nhóm thử nghiệm tính năng này như sau:

- Nhóm thử nghiệm chức năng này với trang web “http://testphp.vulnweb.com”.
- Em truy cập trang web với url http://testphp.vulnweb.com/artist.php?artist=1 và thực hiện bắt gói tin http request bằng “Dev tool” của Microsoft Edge.



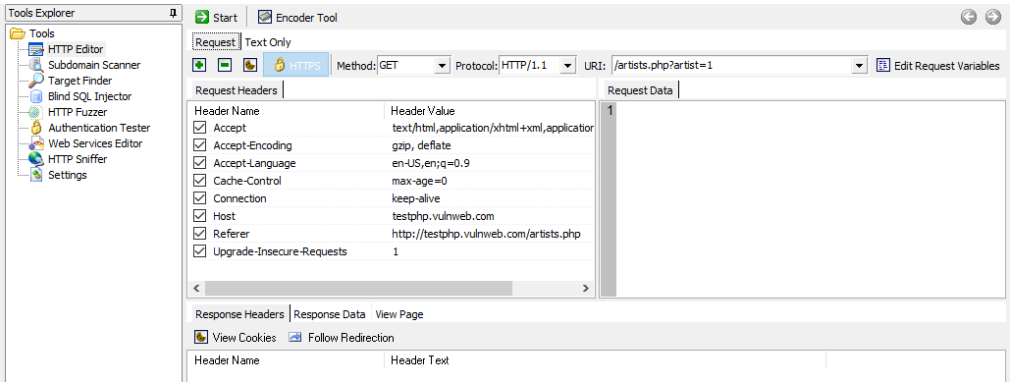
Hình 61: Xem Request header bằng Dev Tool

- Copy đoạn GET request bên trên vào HTTP Editor của AMT.



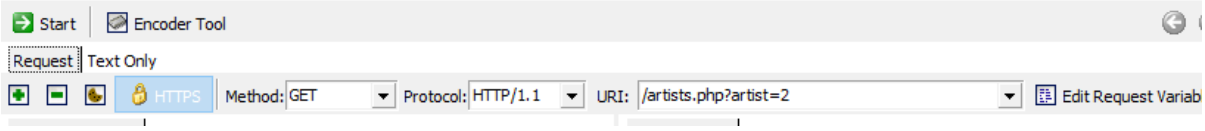
Hình 62: Giao diện HTTP Editor của AMT

- Bên trên là dạng raw của GET request được xem bằng cách chọn "text only", ta có thể xem dạng "request" của gói tin bằng cách chọn "request".



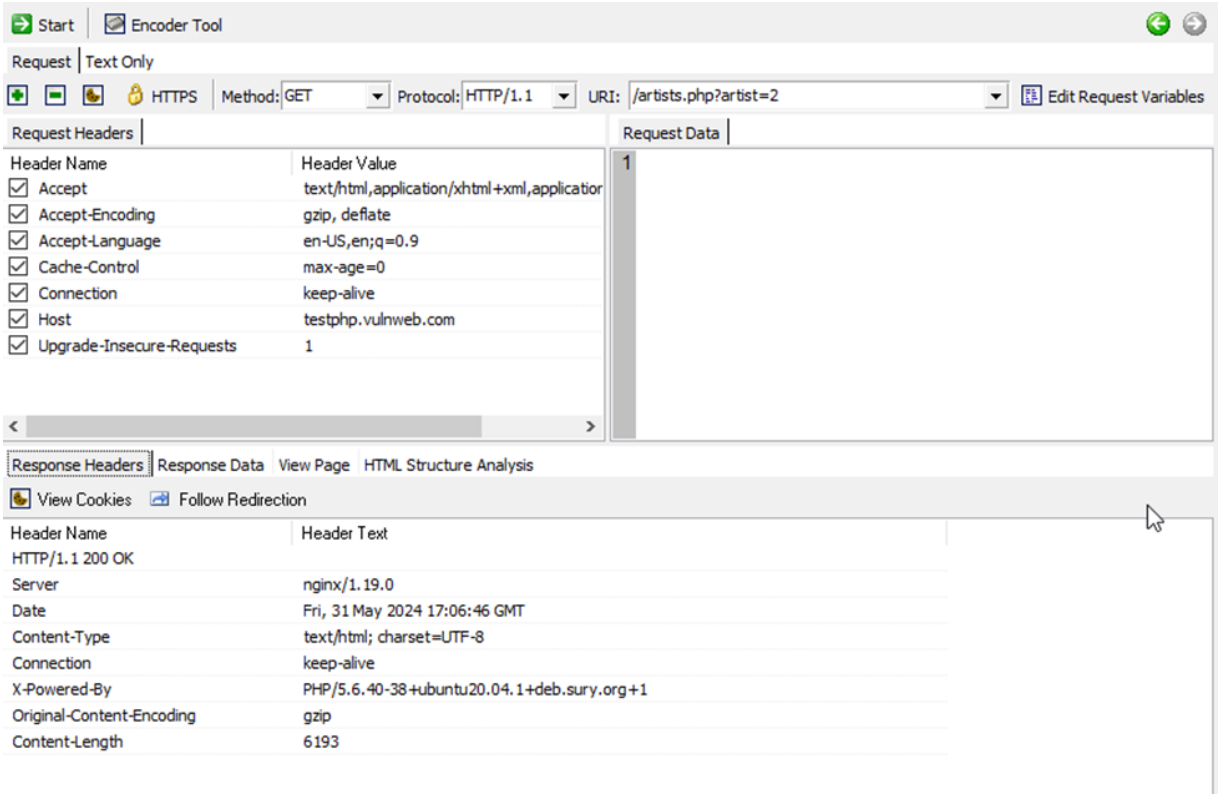
Hình 63: Tab Request của HTTP Editor

- Dạng "request" thể hiện rõ trường thuộc tính và giá trị tương ứng của thuộc tính đó.
- Sau đó, HTTP Editor cho phép chỉnh sửa các trường và giá trị trên và gửi đi theo mục đích của chúng ta, thử thay đổi trường URI để tìm kiếm tài nguyên có artist=2.



Hình 64: Chỉnh sửa các trường và giá trị của Request bằng HTTP Editor

- Ta có thể sửa như trên hoặc vào "Text Only" để thay đổi. Sau đó, gửi gói tin đi bằng cách nhấn "Start" và có kết quả sau.



Hình 65: Kết quả sau khi gửi Request được chỉnh sửa bởi HTTP Editor

- Ngoài "GET request, Acunetix còn có thể chỉnh sửa và gửi các gói tin "HEAD", "POST".

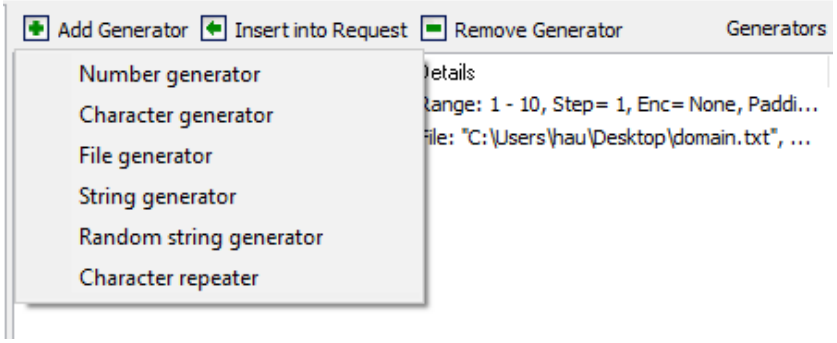
b. HTTP Fuzzer

HTTP Fuzzer là mô đun hỗ trợ tạo ra các cuộc Brute-force attacker bằng cách thêm một placeholder vào Request form cho trước và gửi liên tục Request đó với placeholder thay đổi giá trị mỗi lần gửi.

Nhóm thử nghiệm như sau:

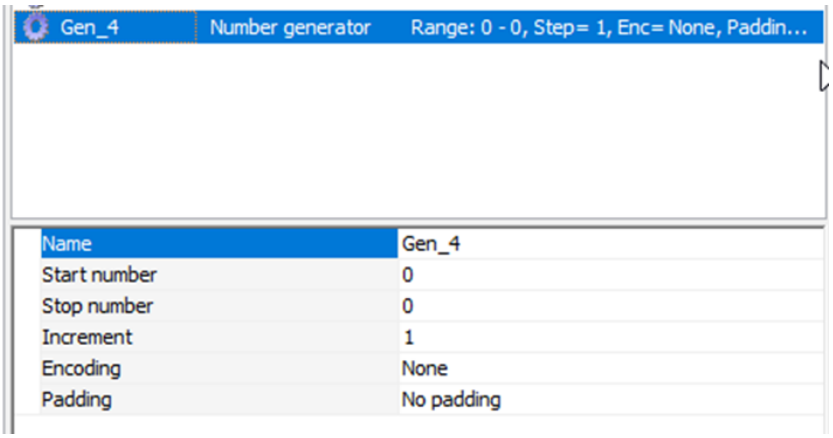
- Nhóm thử nghiệm chức năng với trang web "http://testphp.vulnweb.com"

- Để thực hiện Fuzzing trang web, AMT cung cấp chức năng Generator bằng chọn "Add Generator". Có nhiều loại Generator như number, string, character, random … để tìm nhiều tài nguyên khác nhau có trong web lưu theo dạng id số hoặc chuỗi, kí tự …



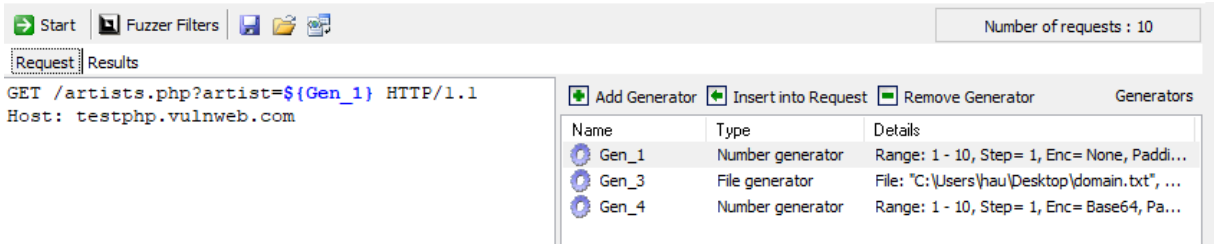
Hình 66: Generator của AMT

- Nếu chọn, "Number generator", ta có thể bắt đầu tìm tài nguyên từ "Start number" cho đến "Stop number", và tăng theo "Increment" đơn vị. Ta có thể chỉnh sửa các tham số này theo ý muốn.

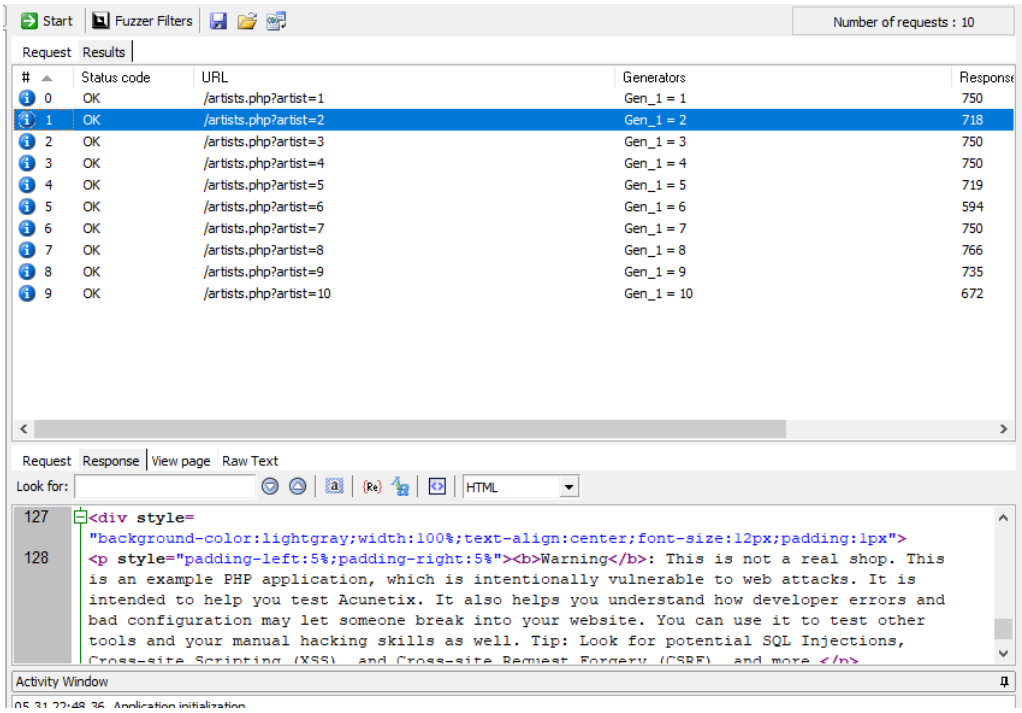


Hình 67: Number generator của AMT

- Các generator này sẽ được tạo sẵn và dùng như một template, có thể được dùng chung cho các trang web khác nhau. Để có thể sử dụng một generator cho một trang web nào đó, ta chọn "Insert into Request". Bên cạnh đó, nếu muốn xóa một generator nào đó không cần thiết nữa, ta chọn generator đó và chọn "Remove Generator".
- Để tìm thông tin về các artist trong trang web http://testphp.vulnweb.com, ta thực hiện thêm "Number generator" và có "Start number =1", "Stop number = 10", "Increment=1". Tiếp theo, chọn "Insert Into Request" và chọn "Start".



Hình 68: Tìm thông tin về các artist trong trang web mục tiêu với HTTP Fuzzer của AMT

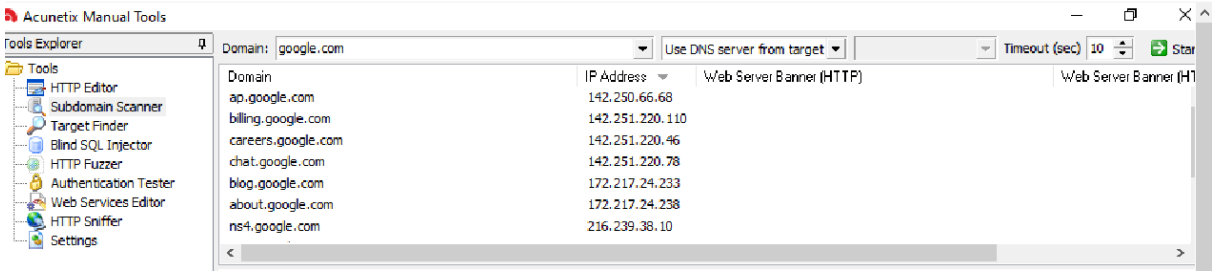


Hình 69: Kết quả của việc tìm kiếm bằng HTTP Fuzzer của AMT

c. *Subdomain Scanner*

Subdomain Scanner là mô đun hỗ trợ quét tên miền con của tên miền chính cho trước.

Nhóm thử sử dụng "Subdomain Scanner" để quét các subdomain của "google.com": Nhập tên miền > Start.

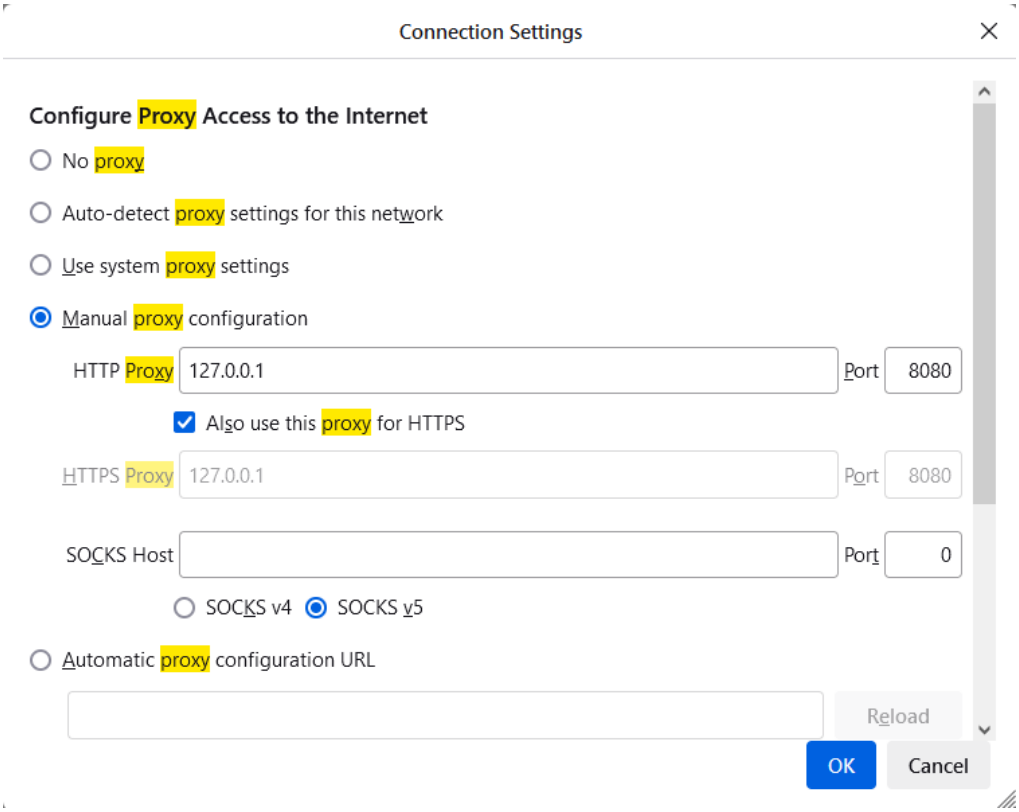


Hình 70: Kết quả quét subdomain của "google.com"

d. *HTTP Sniffer*

HTTP Sniffer là mô đun có thể đóng vai như một Proxy server và có thể can thiệp vào các gói HTTP Request và HTTP Reponse.

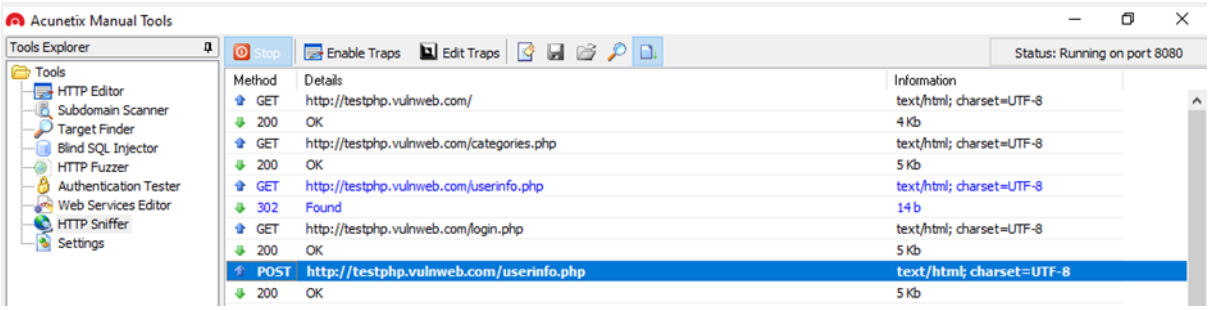
Để thử nghiệm tính năng này, ta cần cấu hình proxy cho trình duyệt, ở đây nhóm dùng Firefox:



Hình 71: Cấu hình Proxy cho trình duyệt Firefox

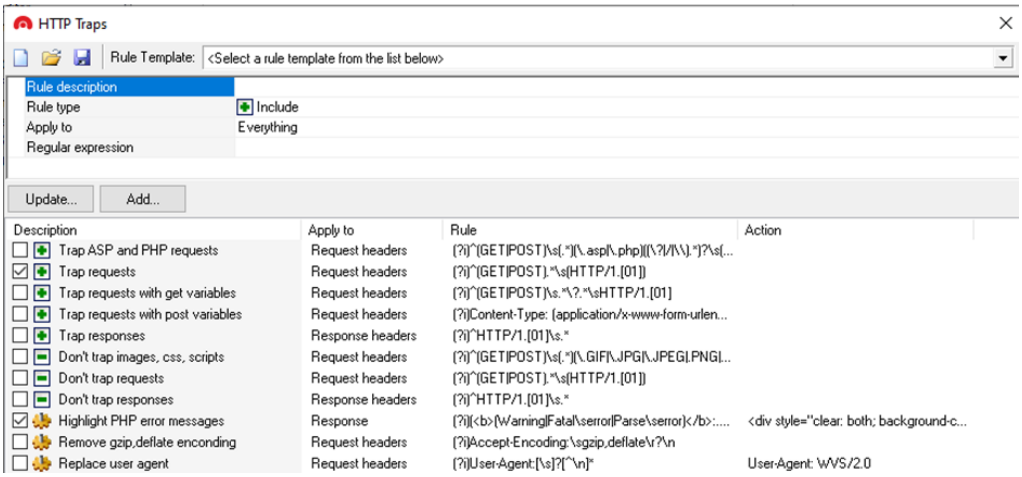
Sau khi cấu hình proxy, mở công cụ AMT, chọn "HTTP Sniffer", chọn "Start". Công cụ sẽ thực hiện lắng nghe trên cổng 8080 của proxy. Nhóm bắt đầu thử nghiệm tính năng như sau:

- Mở trình duyệt FireFox và truy cập trang web "http://testphp.vulnweb.com". Thực hiện một số tương tác với trang web như click vào 'artists', 'categories', 'your profile' sau đó login.
- Trên giao diện của AMT, ta có thể thấy các yêu cầu GET, POST cùng với các phản hồi đã được lưu lại.



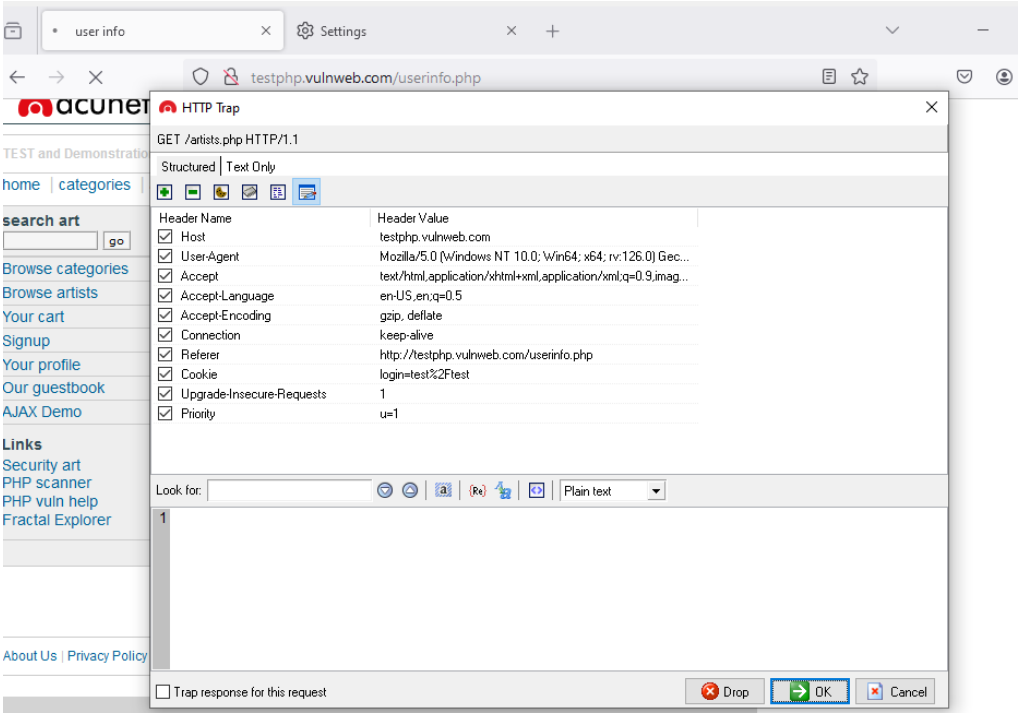
Hình 72: Các request được HTTP Sniffer của AMT ghi lại

- Bên cạnh chức năng sniff các yêu cầu, phản hồi trên trang web mục tiêu, HTTP Sniffer còn có thể chặn gói tin theo mẫu (pattern) bằng "Enable Traps" và "Edit Traps". Đầu tiên, cần thiết lập và chọn mẫu để Acunetix có thể dựa vào đó để chặn gói tin nếu trùng khớp với mẫu, chọn "Edit Traps".



Hình 73: Giao diện Edit Traps của HTTP Sniffer của AMT

- Sau đó, ta chọn một mẫu có sẵn, ở đây ta chọn mẫu thứ 2. Mẫu này có rule (pattern) dùng để chặn các gói tin GET, POST với phiên bản HTTP 1.0 hoặc 1.1. Sau đó, chọn "Enable Traps" để kích hoạt việc chặn gói tin. Quay lại trang web "testphp.vulnweb.com", thực hiện chọn "artists".



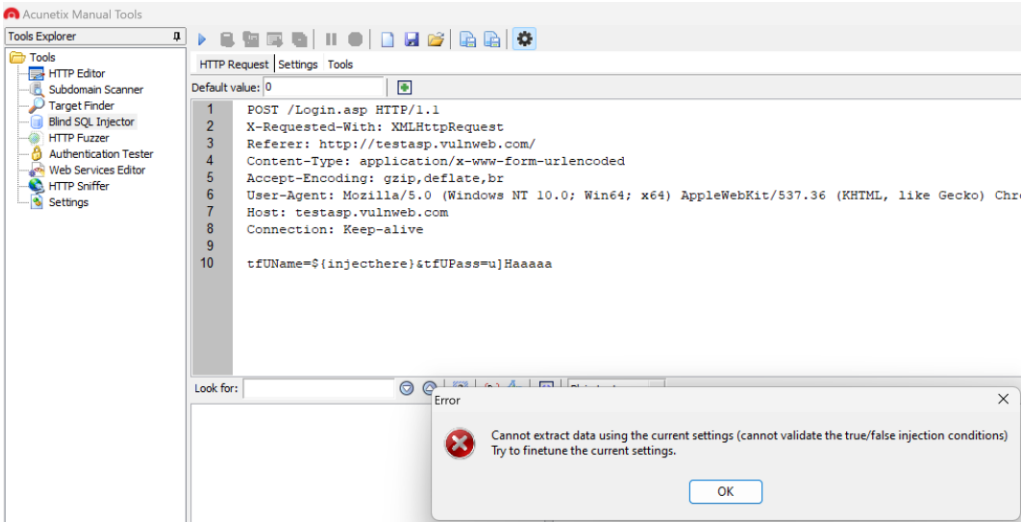
Hình 74: Mẫu yêu cầu sẽ bị chặn bởi HTTP Sniffer của AMT

- Yêu cầu GET bị chặn sẽ khiến trang web luôn trong trạng thái đang xử lý. AMT cho phép "Drop" gói tin bị chặn này, hoặc chỉnh sửa các thành phần trong gói và nhấn "OK" để tiếp tục quá trình chuyển gói tin.

e. *Blind SQL Injector*

Blind SQL Injector là mô đun hỗ trợ tạo ra các cuộc tấn công Blind SQL Injector bằng cách gửi hàng loạt các gói chứa payload tấn công nhằm vào lỗ hổng SQL injection mà không cần thông tin về cơ sở dữ liệu của mục tiêu.

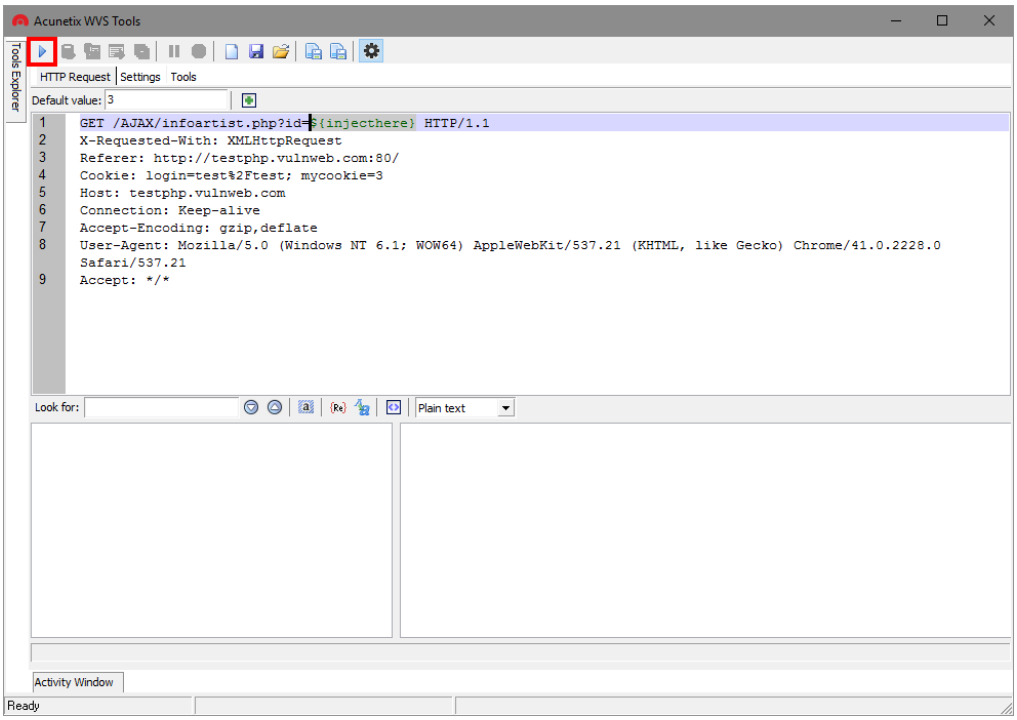
Hiện mô-đun này của AMT đã bị lỗi và nhóm không biết cách sửa cũng như không tìm được cách.



Hình 75: Lỗi không thể trích xuất dữ liệu của Blind SQL Injector của AMT

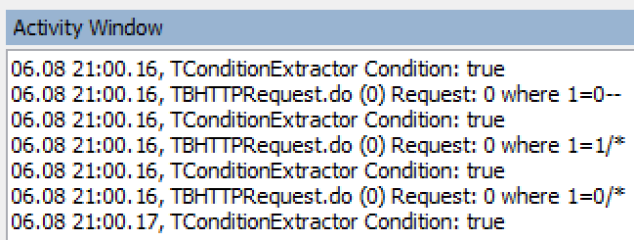
Nếu hoạt động đúng thì mô-đun sẽ hoạt động như sau:

- Nhập Default value, HTTP request và thêm điểm "chèn" để mô-đun tạo các payload tấn công. Rồi click nút hình tam giác để bắt đầu tấn công.



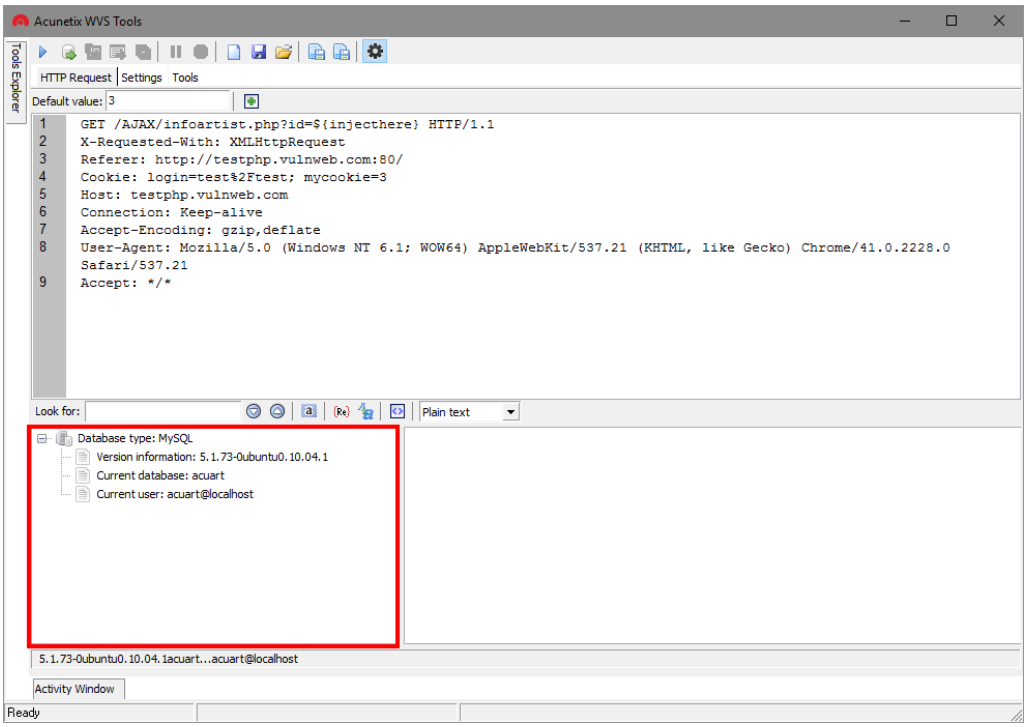
Hình 76: Minh họa các dữ liệu cần cấp cho Blind SQL Injector của AMT và bắt đầu tấn công

- Ví dụ: Default value = 0 thì các chuỗi "chèn" sẽ có tương tự chuỗi mang giá trị true này: "0 where 0=0—" và các chuỗi tương tự sẽ được chèn vào điểm "chèn" tạo thành các payload và gửi tới mục tiêu.



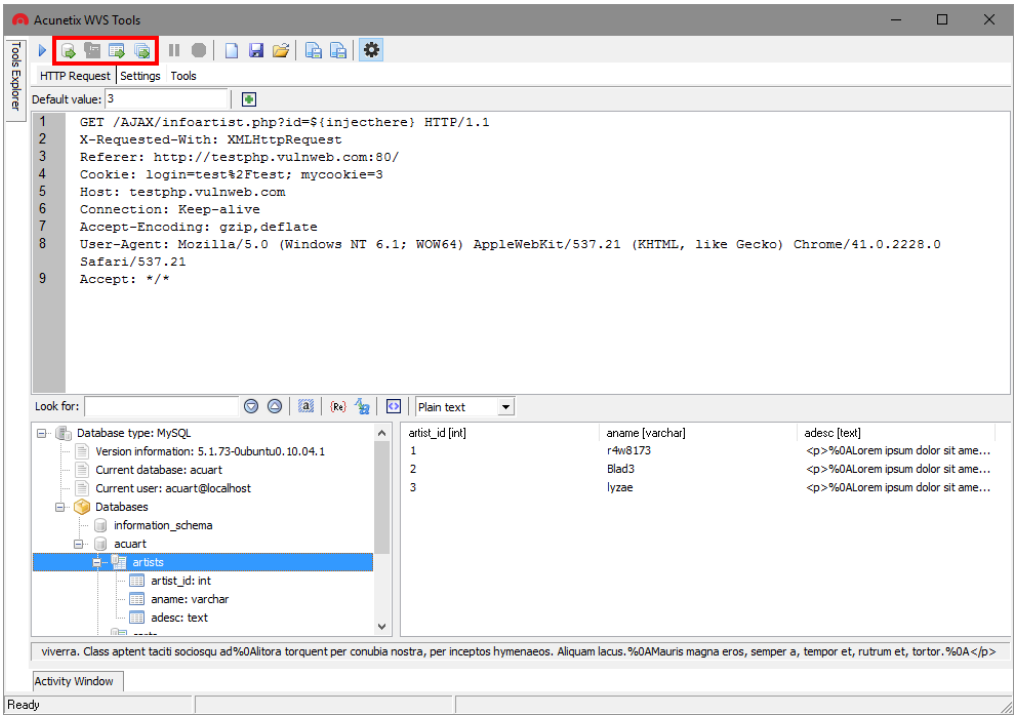
Hình 77: Log ghi lại lịch sử tạo các payload của Blind SQL Injector của AMT

- Các phản hồi từ mục tiêu sẽ được mô-đun trích xuất dữ liệu và phân tích, từ đó đưa ra thông tin, cấu trúc, dữ liệu của cơ sở dữ liệu của mục tiêu.



Hình 78: Blind SQL Injector của AMT đưa ra thông tin về cơ sở dữ liệu của mục tiêu sau khi hoàn thành tấn công

- Có thể dùng data extraction functions trên thanh công cụ để xuất ra database schema và dữ liệu ở các bảng.



Hình 79: Blind SQL Injector của AMT đưa ra dữ liệu của cơ sở dữ liệu của mục tiêu

f. Authentication Tester

Authentication Tester hỗ trợ tạo ra một cuộc Dictionary attack với các đầu vào là:

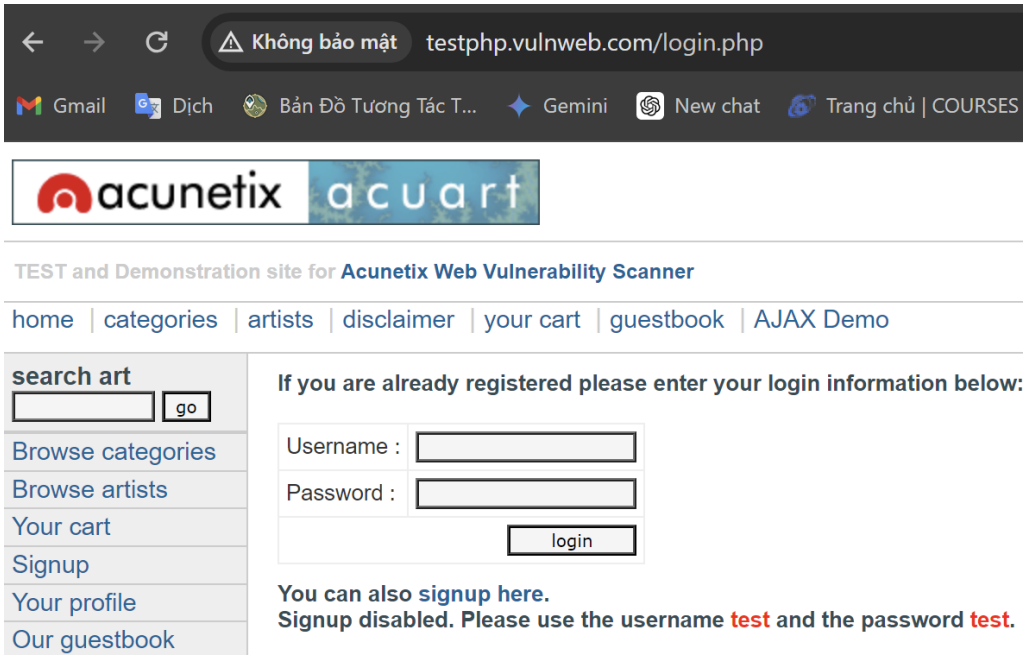
- Target URL to test: đường dẫn đến mục tiêu.
- Authentication method: phương thức xác thực, có 2 lựa chọn HTTP và Web form based.
- Logon has failed if: điều kiện dựa trên phản hồi để xác định username và password vừa gửi đi có đúng hay không; có 3 loại điều kiện:
    - "HTTP status code is" - dựa trên mã trang thái.
    - "Result contains" – Kết quả có chứa chuỗi.
    - "Result match regular expression" – Dùng chuỗi lọc.
- Username dictionary path: đường dẫn tới danh sách username.
- Password dictionary path: đường dẫn tới danh sách password.

Sau khi thêm vào các đầu vào ta có thể bắt đầu bằng cách click "Start".

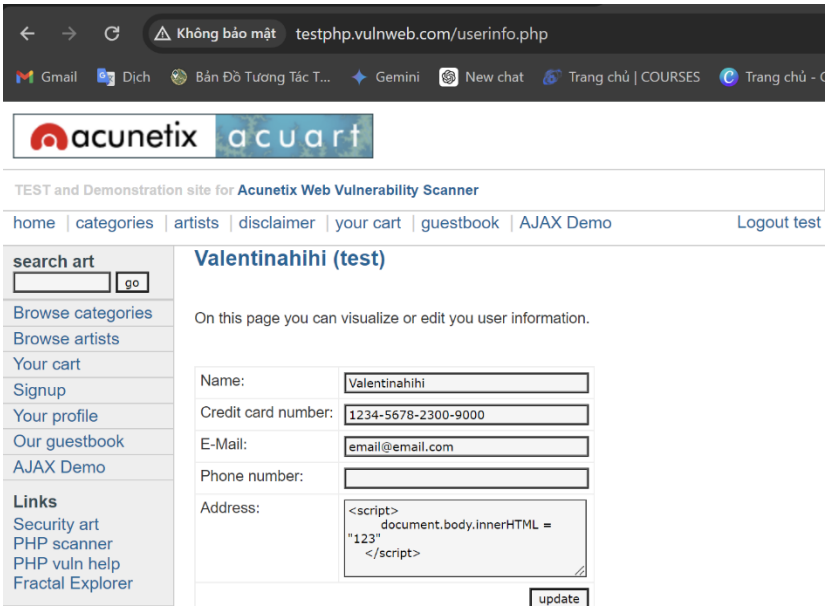
Hình 80: Các đầu vào cho Authentication Tester của AMT

Tuy nhiên mô-đun trước, mô-đun này cũng bị lỗi ở đâu đó. Nhóm thử nghiệm với trang web http://testphp.vulnweb.com/login.php :

- Đăng nhập trang web với tài khoản test: thử trường hợp đúng và sai mật khẩu. Sau khi nhập sai thì giao diện không đổi, giống như tải lại trang.



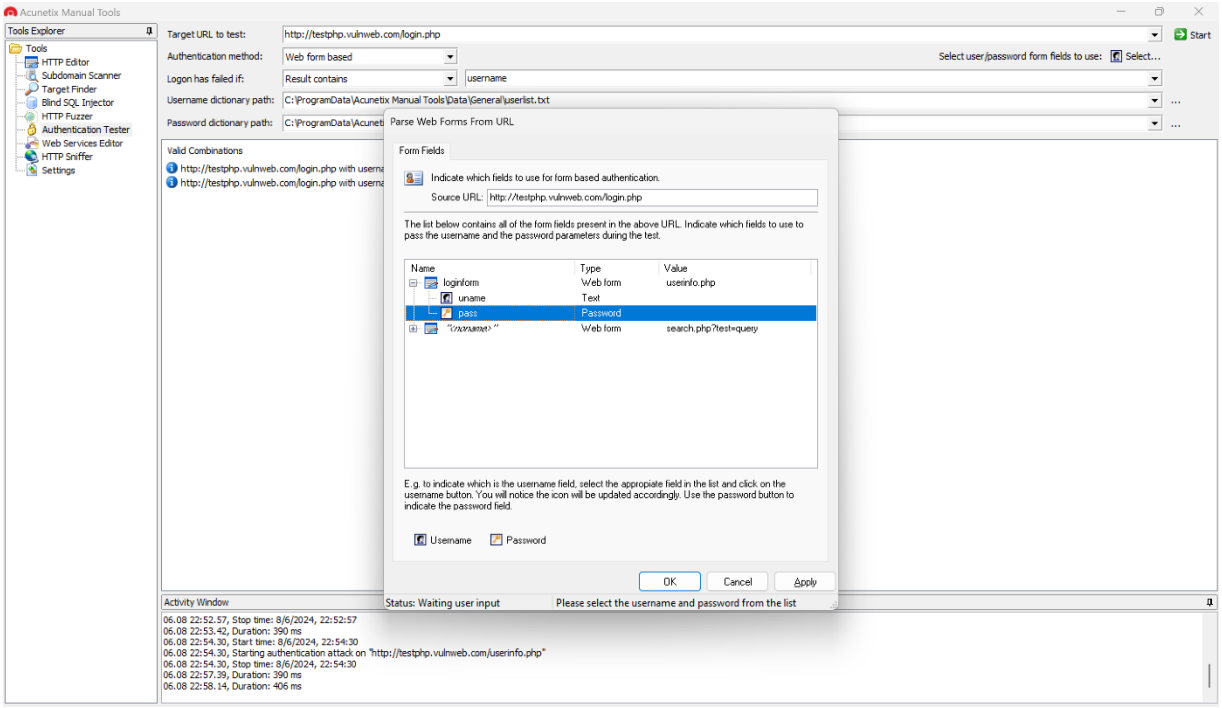
Hình 81: Giao diện web testphp trước khi đăng nhập và khi đăng nhập sai



Hình 82: Giao diện web testphp khi đăng nhập đúng

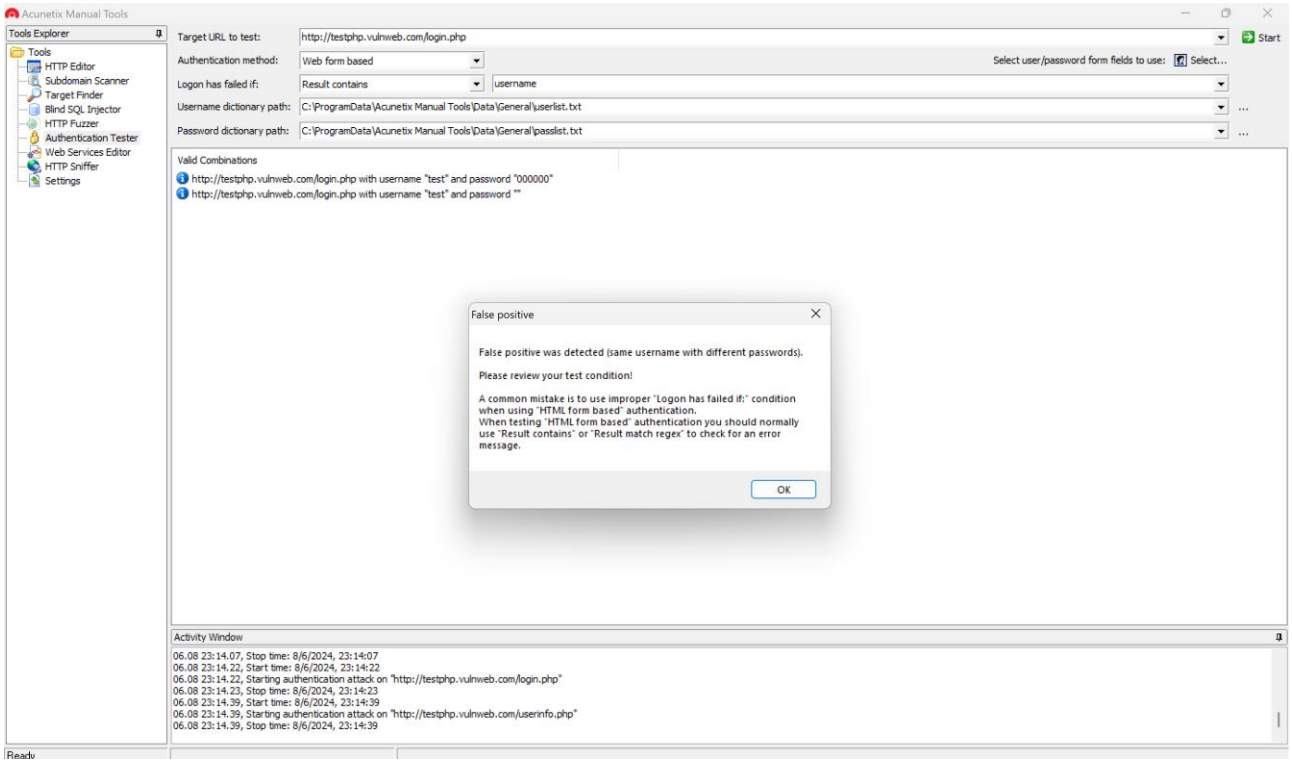
- Các đầu vào cho mô-đun:
  - Target URL to test: http://testphp.vulnweb.com/login.php
  - Authentication method: Web form based
  - Logon has failed if: Result contains: username . Nội dung phản hồi sau khi đăng nhập thành công không có chuỗi "username".
  - Username dictionary path: đường dẫn mặc định.
  - Password dictionary path: đường dẫn mặc định.

- Chọn trường user/password: chỉ định trường nào của form sẽ nhận giá trị sẽ username/password. Đặt trường uname là Username, trường pass là Password.



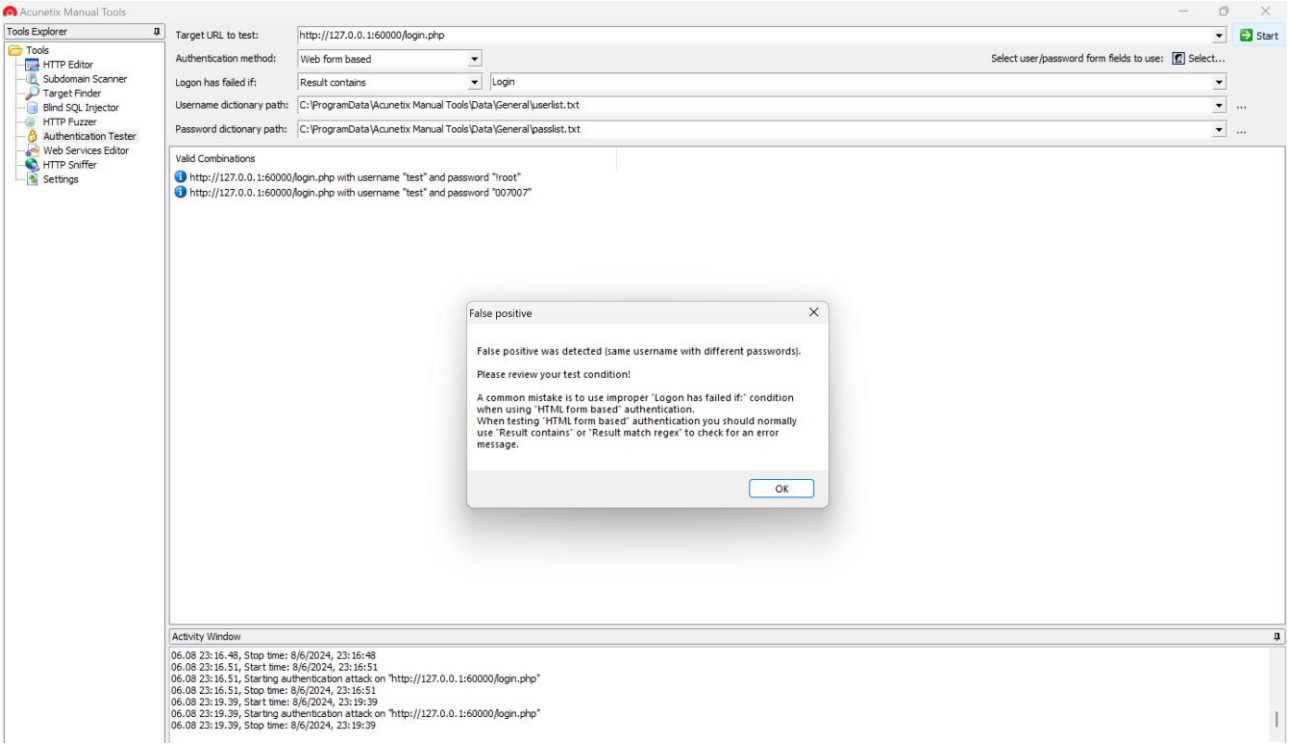
Hình 83: Chọn trường user/password cho phương thức bảo mật Web form based

- Click "Start". Hiện lỗi 1 tài khoản 2 mật khẩu đúng, điều này nghĩa là điều kiện đăng nhập thất bại mà nhóm đặt không có tác dụng. Và có thể thấy mô-đun đã không gửi thông tin đăng nhập tới trang đăng nhập.



Hình 84: Lỗi dương tính giả của Authentication Tester của AMT

- Thử nghiệm nhanh với 1 web nội bộ, lần này không gửi sai đích nhưng vẫn vậy.



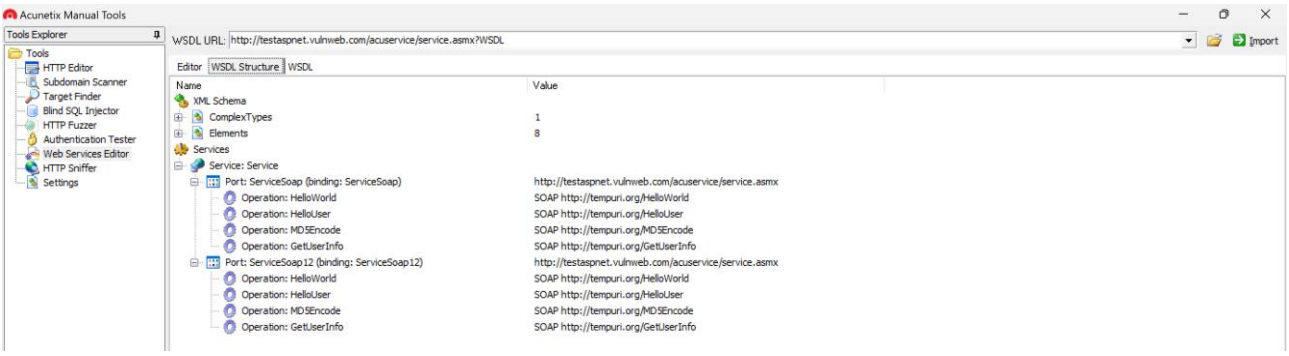
Hình 85: Lỗi dương tính giả của Authentication Tester của AMT (2)

g. Web Services Editor

Web Services Editor cho phép bạn nhập tệp WSDL trực tuyến hoặc cục bộ để phân tích chuyên sâu các yêu cầu và phản hồi WSDL. Trình soạn thảo cũng có tính năng đánh dấu cú pháp cho tất cả các ngôn ngữ, giúp dễ dàng chỉnh sửa các SOAP header và tùy chỉnh các cuộc tấn công thủ công. Việc chỉnh sửa và gửi các thông báo Web Services SOAP rất giống với việc chỉnh sửa các yêu cầu thông thường được gửi qua HTTP Editor.

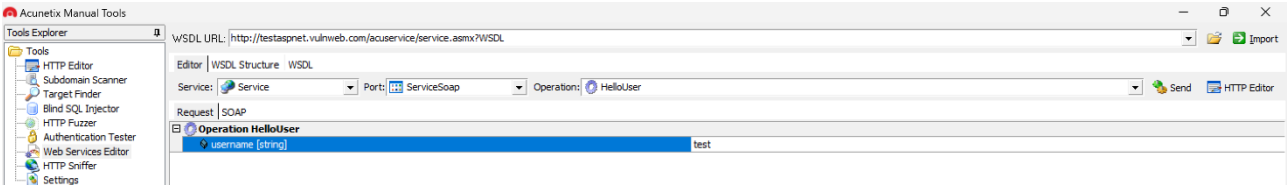
Thử gửi một yêu cầu SOAP đến dịch vụ HelloUser của trang web http://testaspnet.vulnweb.com :

- Phân tích cấu trúc WSDL với Web Services Editor: nhập đường dẫn tới tệp WSDL của trang web mục tiêu vào WSDL URL và click "Import".



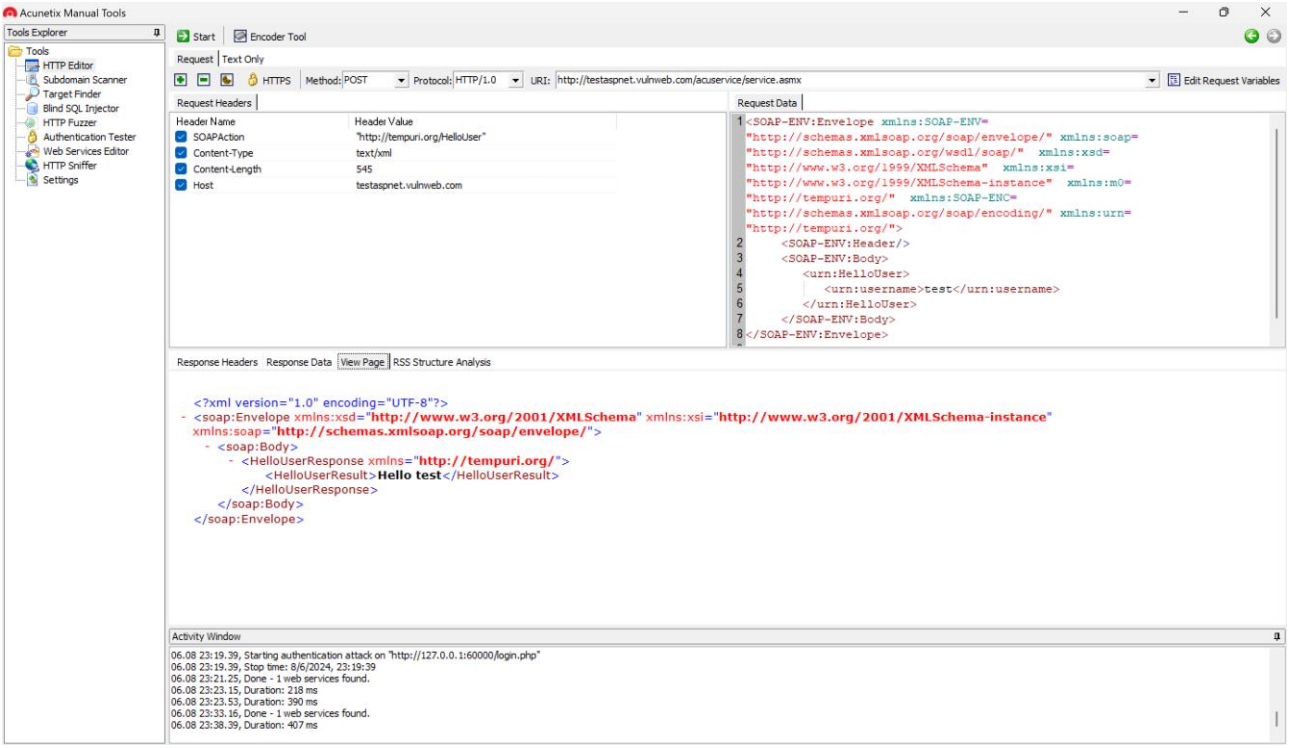
Hình 86: Cấu trúc WSDL của web mục tiêu bởi Web Services Editor của AMT

- Chuyển qua tab Editor để tạo yêu cầu với HelloUser: đổi giá trị Operation thành HelloUser và thêm giá trị cho biến username.



Hình 87: Soạn thảo yêu cầu SOAP tới HelloUser nhờ Web Services Editor của AMT

- Click "HTTP Editor" để chuyển yêu cầu qua mô-đun đó. Click tiếp "Start" và xem phản hồi.



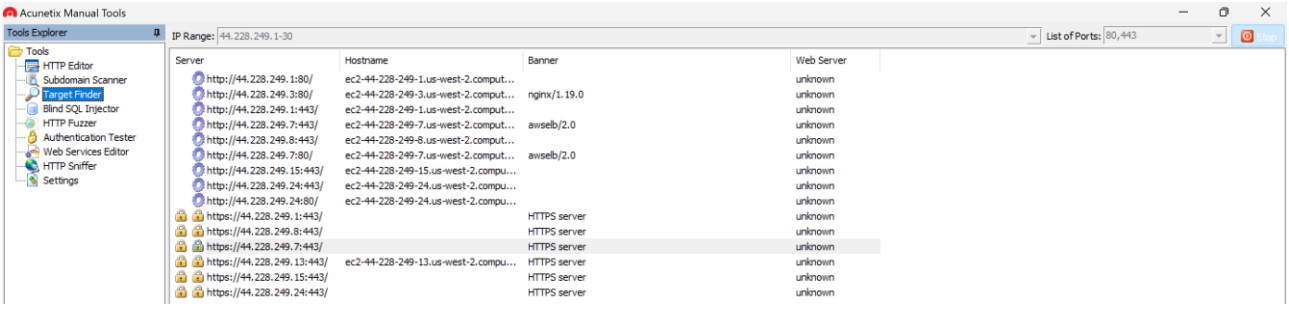
Hình 88: Kết quả yêu cầu SOAP tới dịch vụ HelloWorld nhờ HTTP Editor và Web Services Editor của AMT

h. *Target Finder*

Target Finder dùng để tìm sự tồn tại của các trang web trên một dải IP với các cổng cho trước. Để bắt đầu tìm trang web nhập dải IP vào IP Range và danh sách các port là List of Ports.

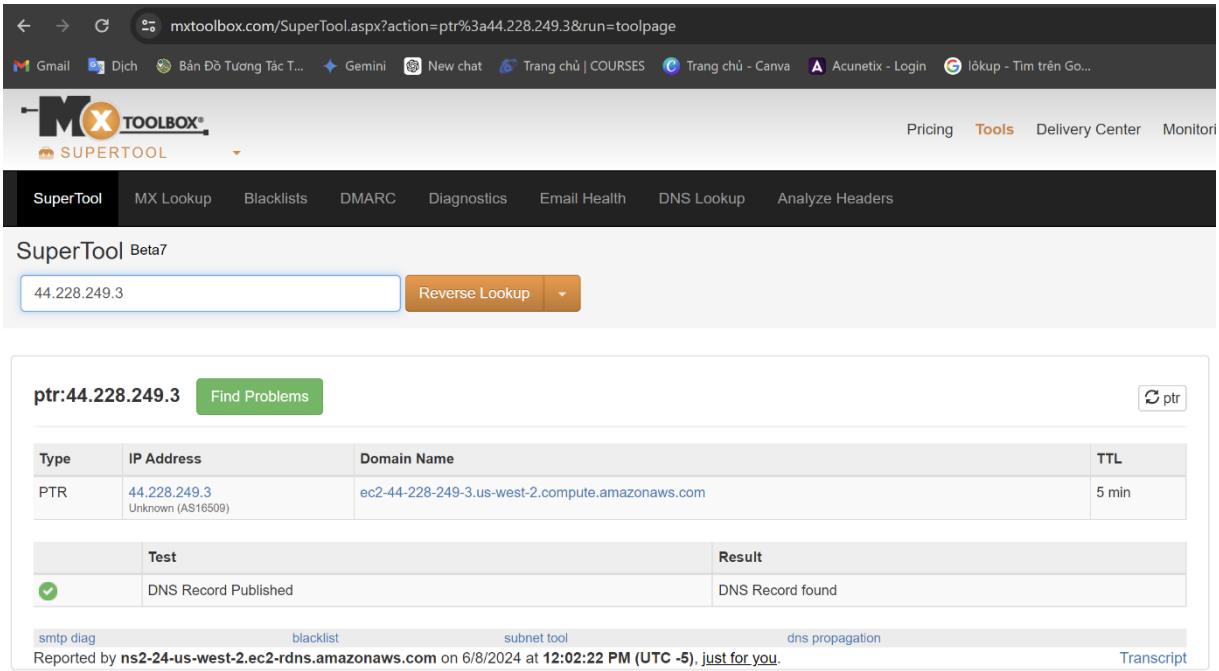
Hình 89: Đầu vào cho Target Finder của AMT

Click "Start". Kết quả trả về là danh sách các URL dẫn đến các trang web và có thể chuyển chúng đến HTTP Editor.



Hình 90: Kết quả quét một dải IP nhờ Target Finder của AMT

Kiểm tra với https://mxtoolbox.com/ReverseLookup.aspx . Kết quả tên miền tìm thấy là chính xác.



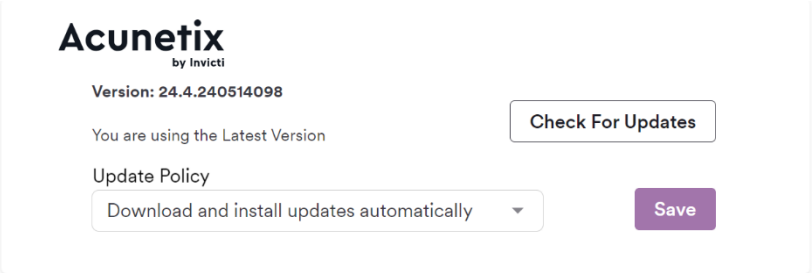
Hình 91: Kết quả tra cứu IP trên https://mxtoolbox.com/ReverseLookup.aspx

13. Phiên bản Acunetix mà nhóm sử dụng

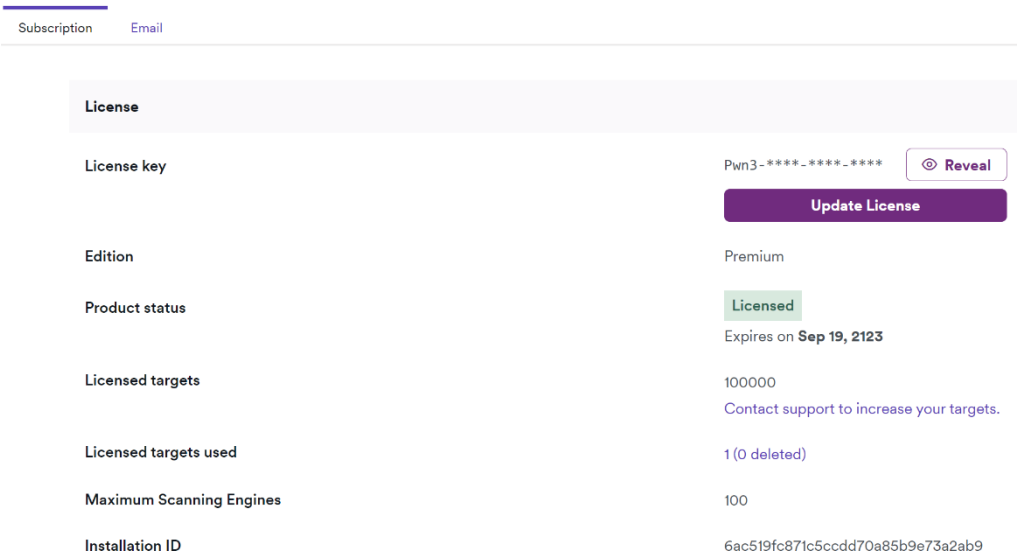
Nhóm sử dụng Acunetix Premium v24.4.240514098 bản CRACK và Acunetix Manual Tools để thực hiện các kịch bản mà nhóm đề ra.

- Về Acunetix Manual Tools đã được viết ở trên.
- Acunetix Premium v24.4.240514098 bản CRACK được lấy từ một diễn đàn chuyên về bảo mật và dịch ngược – CyberArsenal, phiên bản này được cấp bởi một người dùng của diễn đàn nickname "sky" sống đâu đó tại Nga. Trên CyberArsenal có hẳn 2 chủ đề tập trung vào việc crack Acunetix cho hệ điều hành Linux và Windows có sự góp sức của nhiều kỹ sư dịch ngược. Bản CRACK có đầy đủ chức năng của phiên bản 24.4.240514098, chỉ kém bản mới nhất chức năng Predictive Risk Scoring thuộc nhóm chức năng Khám phá (đây là chức năng ra cùng phiên bản mới nhất - 24.5.240604185).

Để không phát tán bản CRACK của Acunetix một cách quá phổ biến mà gây thiệt hại cho phía Invicti nên nhóm quyết định không viết chi tiết cách cài đặt bản CRACK này.



Hình 92: Phiên bản của Acunetix CRACK



Hình 93: License của Acunetix bản CRACK

14. Acunetix hỗ trợ cho một cuộc tấn công

Với khả năng tìm ra các lỗ hổng trên 1 trang web bất kỳ dựa vào các kỹ thuật quét "hộp đen" thì Acunetix hoàn toàn có tiềm năng để hỗ trợ cho một cuộc tấn công web. Việc Acunetix quét trang web sẽ là 1 phần của giai đoạn trinh sát mục tiêu, thậm chí việc dùng Acunetix sẽ rút ngắn thời gian và công sức cho việc trinh sát so với trước. Kết quả quét sẽ có thông tin về lỗ hổng và vị trí của nó, thậm chí còn được đánh giá tình nghiêm trọng, việc này sẽ dúng kẻ tấn công chuẩn bị kịch bản tấn công nhanh hơn, hiệu quả hơn, "chí mạng" hơn.

Ví dụ: Acunetix tìm được một lỗ hổng SQL Injection và chứng minh nó bằng cách khai cho liệt tất cả các dòng. Kẻ tấn công có thể lợi dụng điểm này và đổi lệnh SQL thành xóa dữ liệu.

CHƯƠNG 4: THỰC NGHIỆM

Phần này sẽ viết về các kịch bản nhóm đề ra và thực hiện.

1. Các kịch bản

Kịch bản 1: Thực hiện Quét toàn phần trang web http://testphp.vulnweb.com/

Kịch bản 2: Thực hiện Quét toàn phần ứng dụng web juice-shop với tính năng Site Login.

Kịch bản 3: Sử dụng AMT để giải tìm flag CTF của challenge HTTP – Cookies của Root Me. Link challenge: HTTP – Cookies.

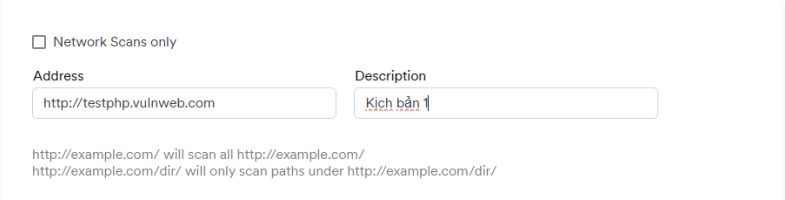
Kịch bản 4: Sử dụng AMT để giải tìm 2 flag CTF của challenge Postbook của ctf.hack101.com.

Kịch bản 5: Cài đặt AcuSensor và quét một trang web nội bộ được xây dựng bằng PHP.

Kịch bản 6: Thử nghiệm tính năng Issue Tracker.

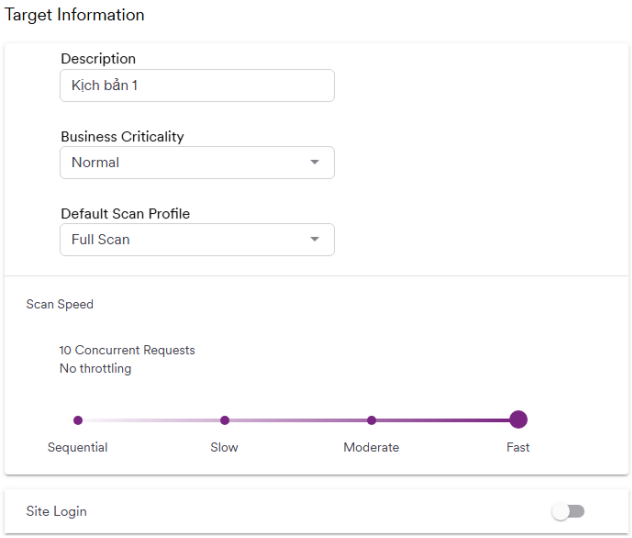
2. Kịch bản 1

Ta tiến hành tạo Mục tiêu, ở trường Address ta nhập url của web.

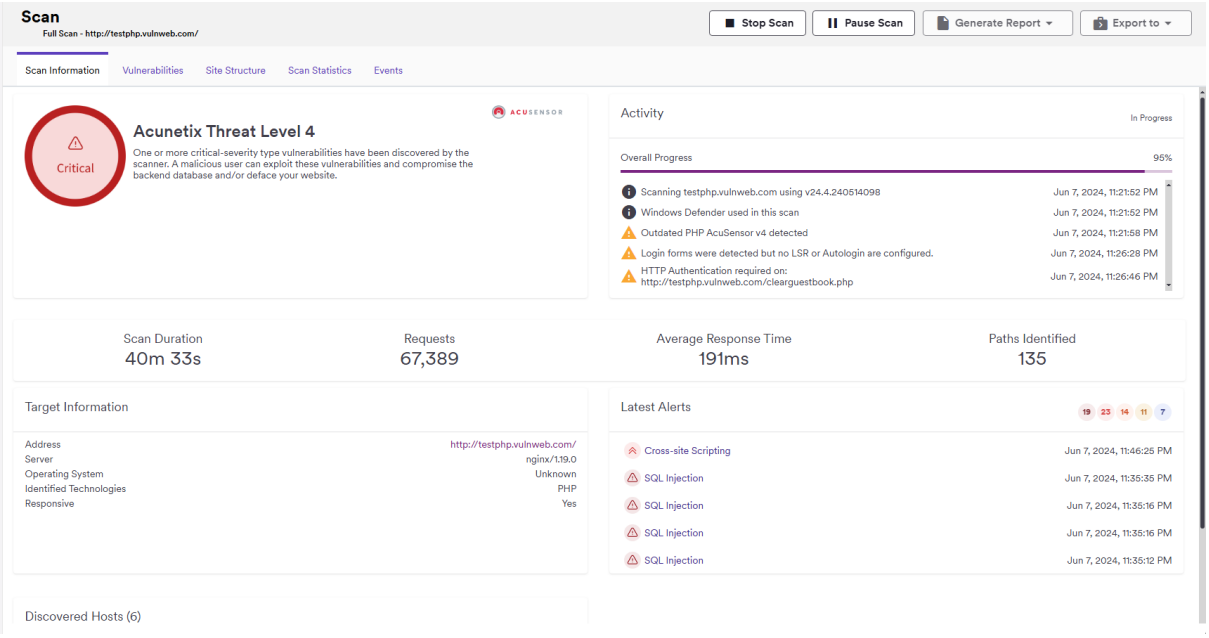


Hình 94: Tạo target http://testphp.vulnweb.com trên Acunetix

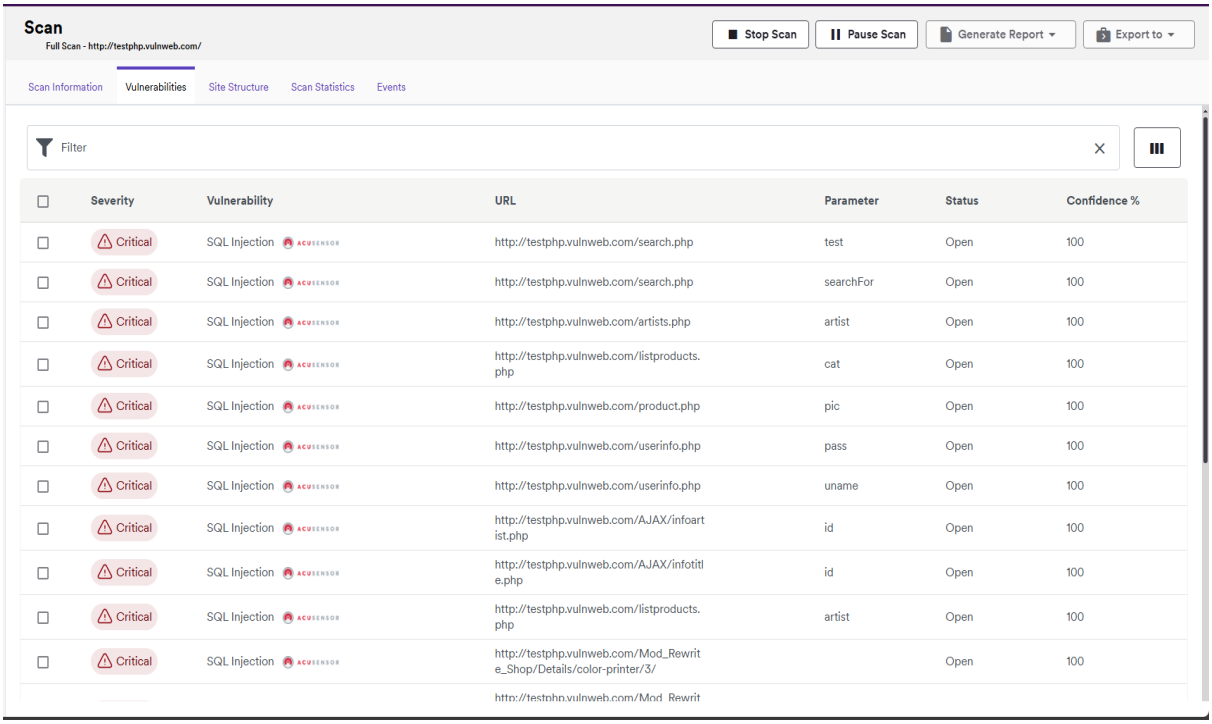
Ta để cấu hình Mục tiêu theo mặc định và tiến hành quét.



Hình 95: Cấu hình Mục tiêu mặc định trên Acunetix

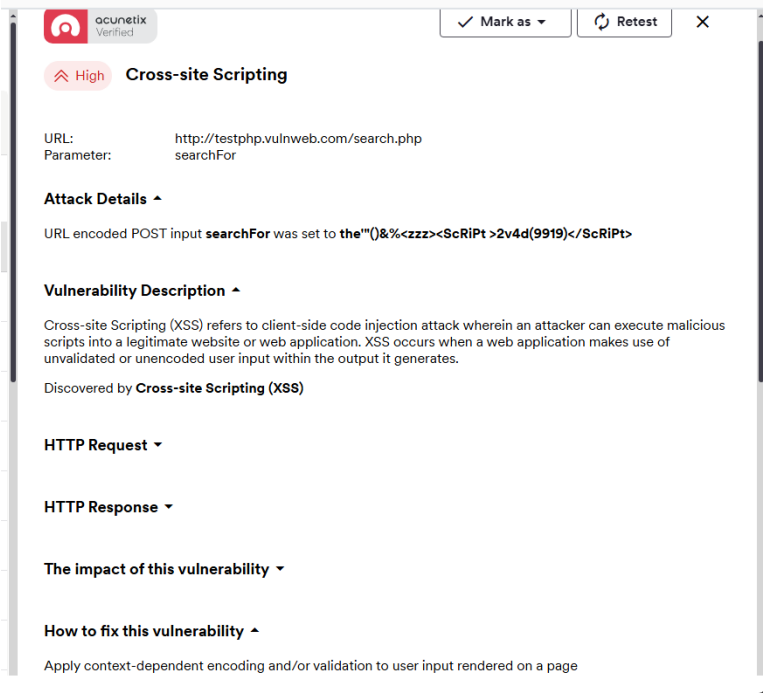


Hình 96: Giao diện Acunetix sau khi bắt đầu quét – Trang thông tin của lần quét này



Hình 97: Danh sách các lỗ hổng quét được của mục tiêu trong lần quét này

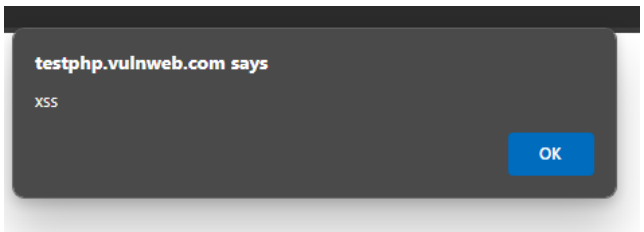
Chọn 1 lỗ hổng trong danh sách, ta sẽ thấy các thông tin về lỗ hổng như yêu cầu dùng để xác minh lỗ hổng, phản hồi từ trang web, khuyến nghị vá lỗi, …



Hình 98: Thông tin của một lỗ hổng trong danh sách lỗ hổng

Thử tiến hành khai thác lỗ hổng, ta nhập vào ô tìm kiếm "search art" chuỗi **()&%<acx><ScRiPt >alert('xss')</ScRiPt>** và ta thành công khai thác XSS.

Hình 99: Nhập chuỗi khai thác vào ô search art



Hình 100: Kết quả khai thác thành công XSS

Nhóm có xuất báo cáo dạng Affected Items cho kịch bản này.

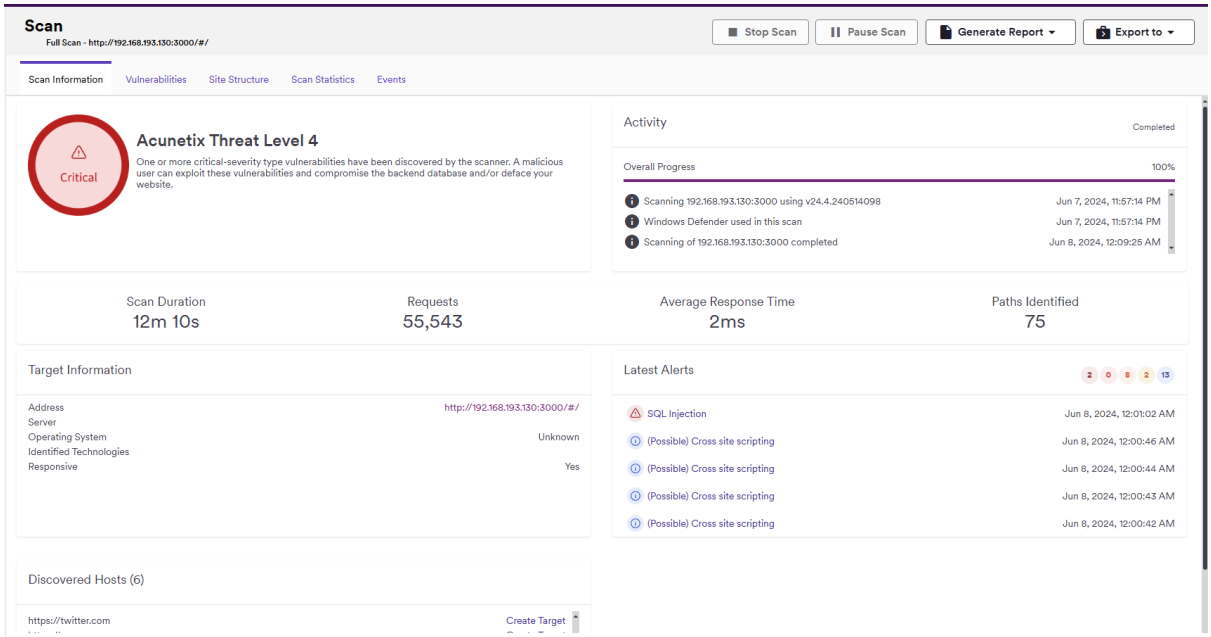
3. Kịch bản 2

Trước khi thực hiện kịch bản, cần cài đặt OWASP Juice Shop trước.

- OWASP Juice Shop là một dự án mã nguồn mở được phát triển bởi OWASP, nhằm cung cấp một môi trường web chứa các lỗi bảo mật phục vụ cho việc nghiên cứu, giáo dục.
- Cách cài đặt đơn giản: Sử dụng docker, chạy 2 lệnh sau:
    - Để tải image về: docker pull bkimminich/juice-shop
    - Để chạy container: docker run --rm -p 3000:3000 bkimminich/juice-shop
- Sau khi chạy container xong thì ta có thể truy cập juice-shop qua đường dẫn: http://localhost:3000/

Khi thực hiện kịch bản này, nhóm thực hiện 2 lần quét để so sánh hiệu quả của việc quét có sử dụng Site Login.

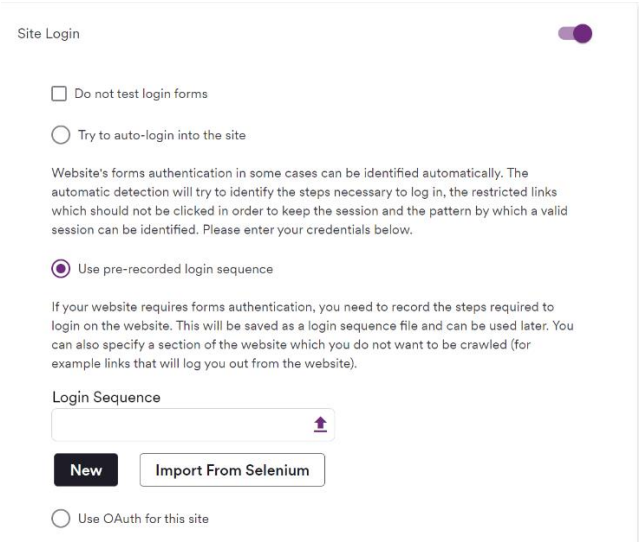
- Lần quét đầu tiên, nhóm không dùng Site Login và tiến hành quét juice shop.



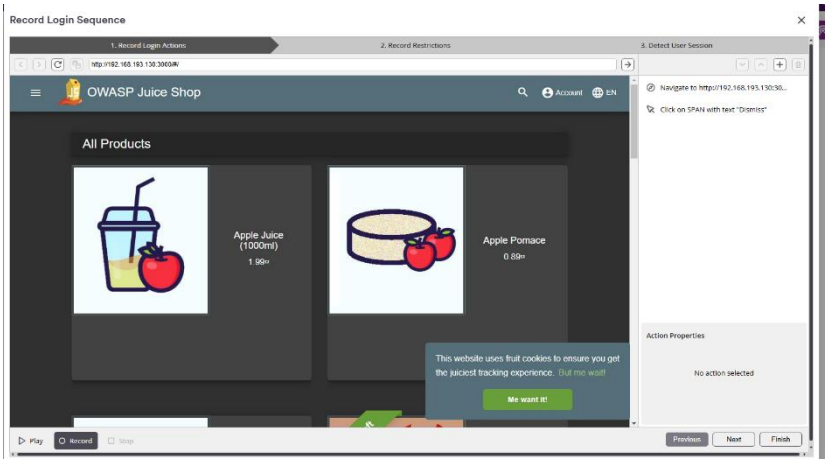
Hình 101: Kết quả quét web juice shop không dùng Site Login trên Acunetix

    - Acunetix không phát hiện được lỗ hổng nào ở mức nghiêm trọng High.

- Lần quét thứ 2, nhóm sử dụng Site Login và tiến hành scan lại. Ở Site login, nhóm dùng "trình tự đăng nhập được ghi trước" (Use pre-recorded login sequence) để đảm bảo Acunetix có thể quét được các vùng cần đăng nhập của juice shop.
    - Ở "Use pre-recorded login sequence" chọn "New" để tiến hành ghi trình tự đăng nhập mới.

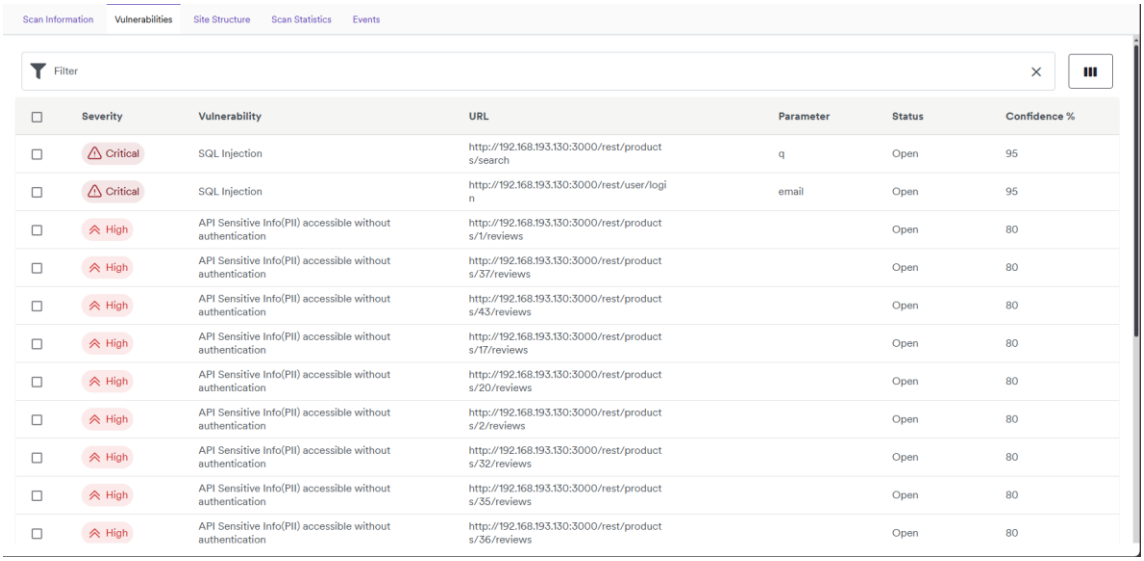


Hình 102: Chọn "New" để tạo trình tự đăng nhập mới cho Site Login trên Acunetix



Hình 103: Ghi lại trình tự đăng nhập cho Site Login trên Acunetix

- Kết quả: Acunetix phát hiện được thêm nhiều lỗ hổng ở mức nghiêm trọng High ở các vùng cần đăng nhập.



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

Filter

Severity	Vulnerability	URL	Parameter	Status	Confidence %
Critical	SQL Injection	http://192.168.193.130:3000/rest/products/search	q	Open	95
Critical	SQL Injection	http://192.168.193.130:3000/rest/user/login	email	Open	95
High	API Sensitive Info(PII) accessible without authentication	http://192.168.193.130:3000/rest/products/1/reviews		Open	80
High	API Sensitive Info(PII) accessible without authentication	http://192.168.193.130:3000/rest/products/37/reviews		Open	80
High	API Sensitive Info(PII) accessible without authentication	http://192.168.193.130:3000/rest/products/43/reviews		Open	80
High	API Sensitive Info(PII) accessible without authentication	http://192.168.193.130:3000/rest/products/17/reviews		Open	80
High	API Sensitive Info(PII) accessible without authentication	http://192.168.193.130:3000/rest/products/20/reviews		Open	80
High	API Sensitive Info(PII) accessible without authentication	http://192.168.193.130:3000/rest/products/2/reviews		Open	80
High	API Sensitive Info(PII) accessible without authentication	http://192.168.193.130:3000/rest/products/32/reviews		Open	80
High	API Sensitive Info(PII) accessible without authentication	http://192.168.193.130:3000/rest/products/35/reviews		Open	80
High	API Sensitive Info(PII) accessible without authentication	http://192.168.193.130:3000/rest/products/36/reviews		Open	80

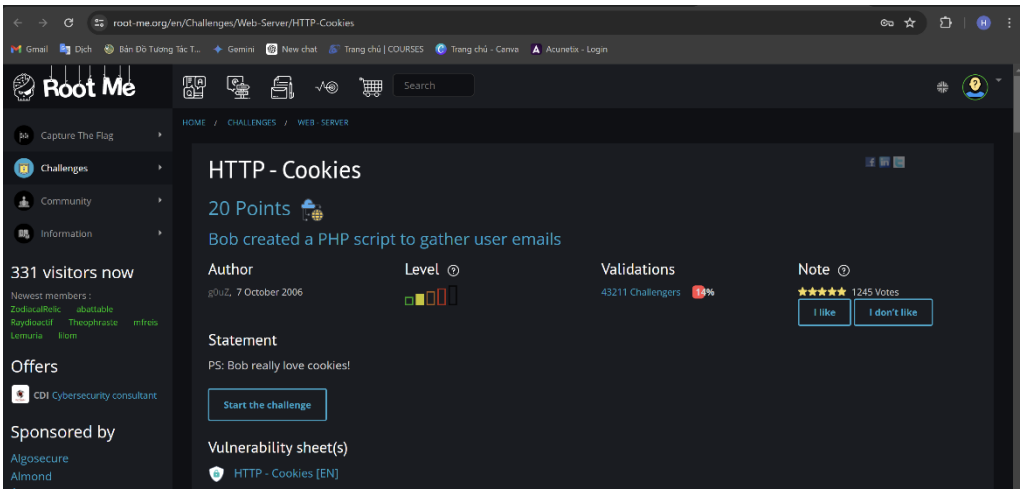
Hình 104: Kết quả quét web juice shop có dùng Site Login trên Acunetix

Target Description	Scan Profile	Schedule	Vulnerabilities
juice-shop with login sequence	Full Scan	Last run on Jun 8, 2024, 12:20:01 PM	2 12 8 3 15
juice-shop	Full Scan	Last run on Jun 7, 2024, 11:57:09 PM	2 0 8 2 13

Hình 105: So sánh tổng quan giữa có và không dùng Site Login để quét juice shop

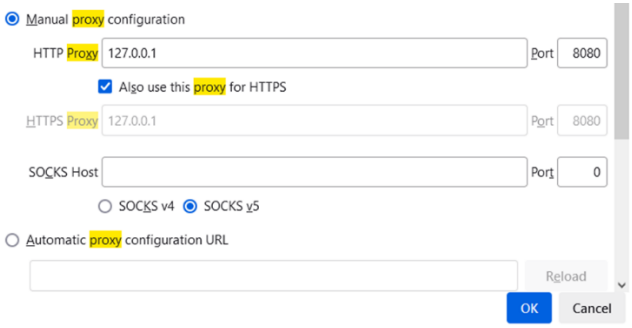
Nhóm có xuất báo cáo so sánh cho 2 lần quét.

4. Kịch bản 3



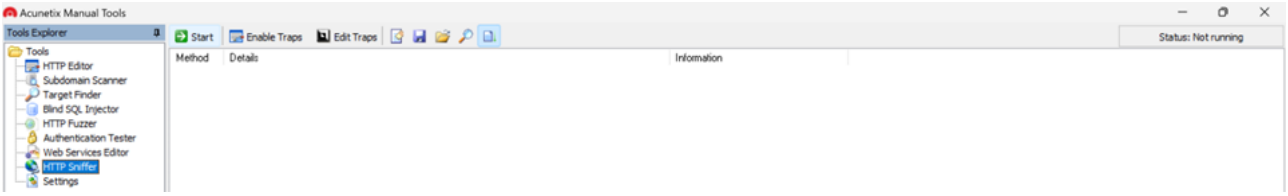
Hình 106: Challenge HTTP – Cookies của Root Me

Thực hiện cấu hình proxy như sau trên trình duyệt để tạo điều kiện cho HTTP Sniffer của AMT làm việc.



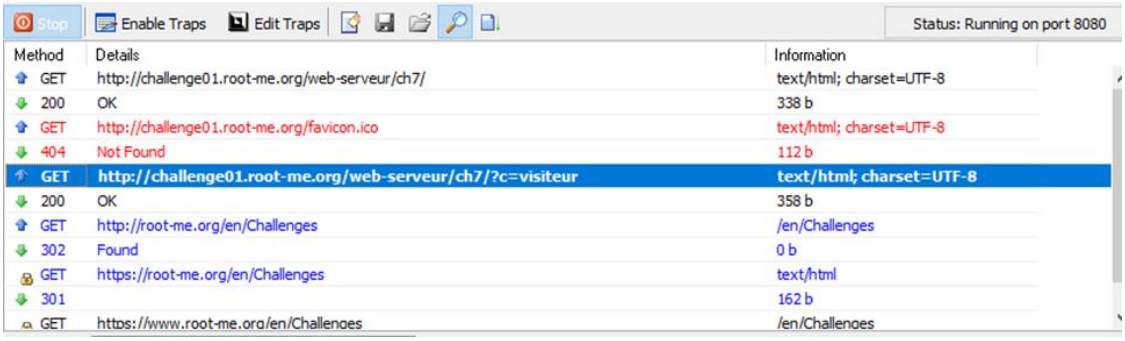
Hình 107: Cấu hình proxy trên trình duyệt

Khởi chạy HTTP Sniffer: click "Start" ở trang HTTP Sniffer của AMT.



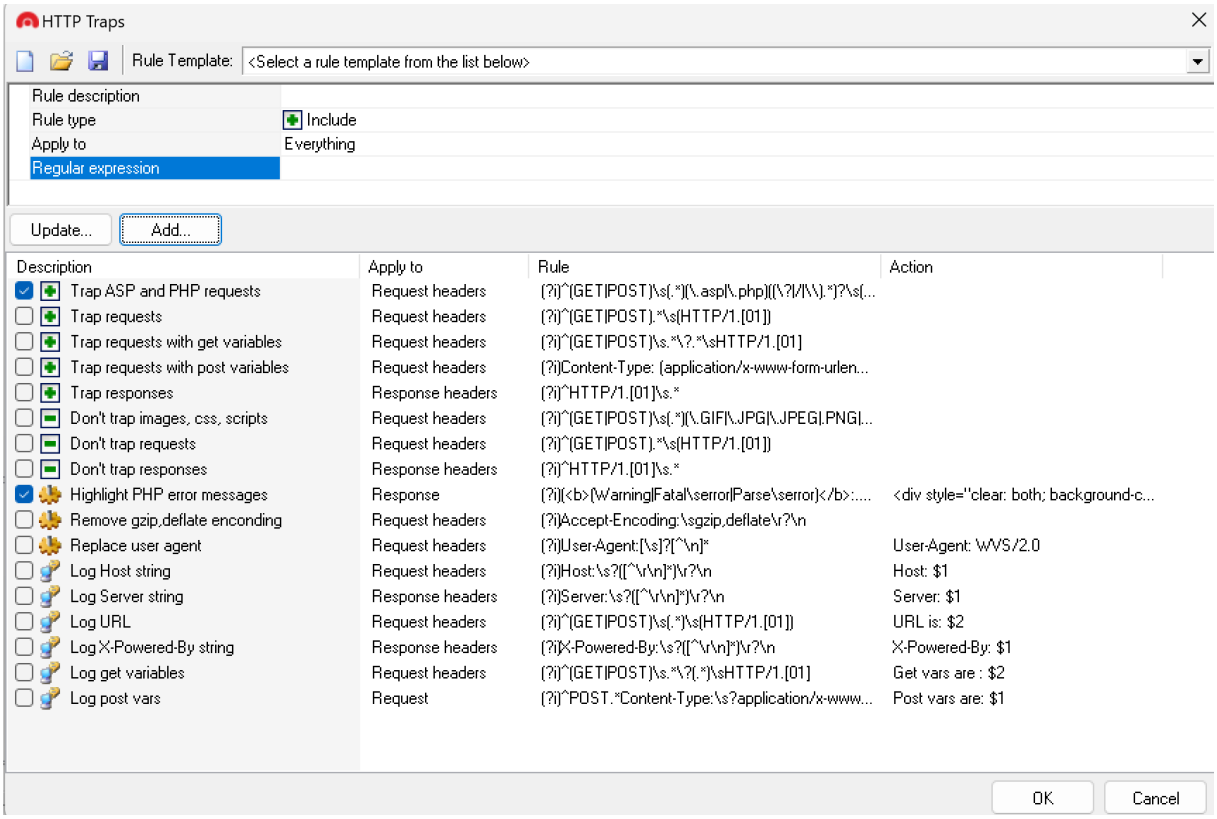
Hình 108: Giao diện trang HTTP Sniffer của AMT

Các gói tin yêu cầu và phản hồi trên trình duyệt sẽ được "đánh hơi" và ghi nhận thành một danh sách.



Hình 109: Danh sách các gói được "đánh hơi" bởi HTTP Sniffer của AMT

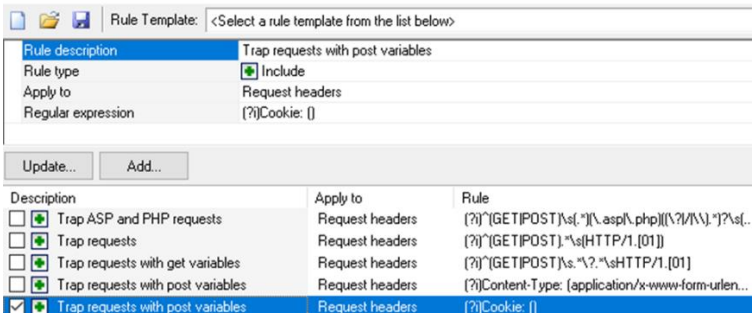
Bên cạnh chức năng theo dõi các gói tin, HTTP Sniffer còn có thể quan sát các gói tin bất thường hoặc có dấu hiện có lỗ hổng bảo mật thì HTTP Sniffer sẽ chặn gói này lại. Trước tiên, cấu hình mẫu các gói được cho là bất thường, vào "Edit Traps". Cửa sổ HTTP Traps vừa hiện lên, hỗ trợ ta thêm, chỉnh sửa các rule. Rule là các điều kiện hay ở đây là các mẫu gói yêu cầu cần chặn.



Hình 110: Cửa sổ HTTP Traps từ trang HTTP Sniffer của AMT

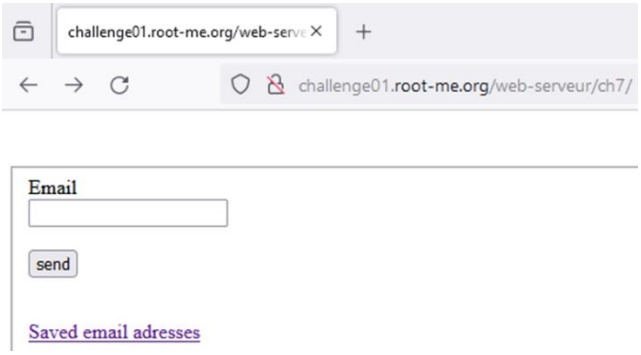
Ở đây, có sẵn một vài rule mặc định để chặn các gói tin theo nhu cầu như các yêu cầu ASP và PHP, các phản hồi với biến GET, ... Để thêm rule ta chọn "Add"; để chỉnh sửa một rule nào đó, ta chọn "Update..". Ngoài ra, để bật rule, ta cần phải click vào ô trống bên trái rule.

Nhóm thực hiện chặn các gói tin POST có bao gồm trường Cookie bằng cách thêm rule.



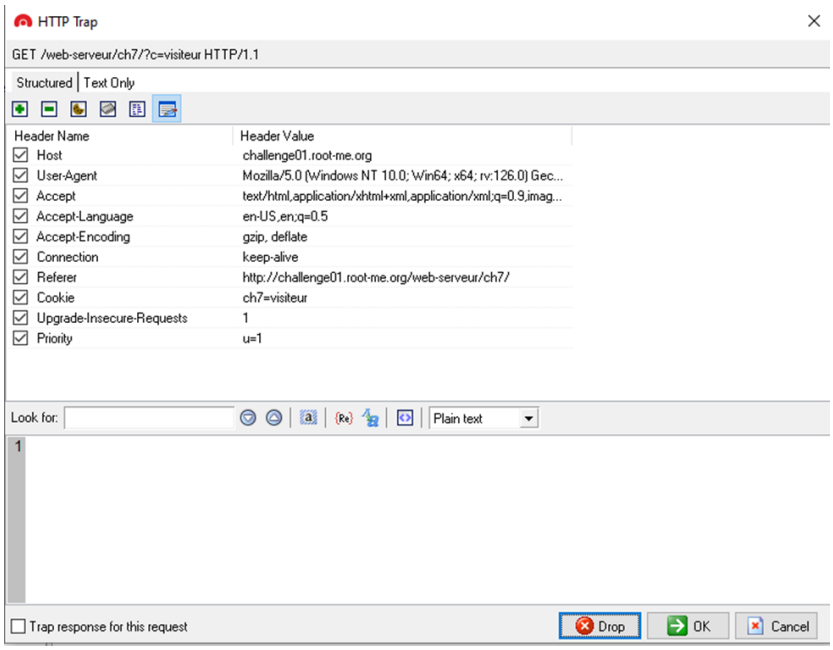
Hình 111: Thêm rule vào HTTP Traps của HTTP Sniffer của AMT

Sau đó, nhóm truy cập trang web chứa challenge HTTP – Cookie của Root Me, click "Start the challenge", ta có thể thấy trang web hiện ra.



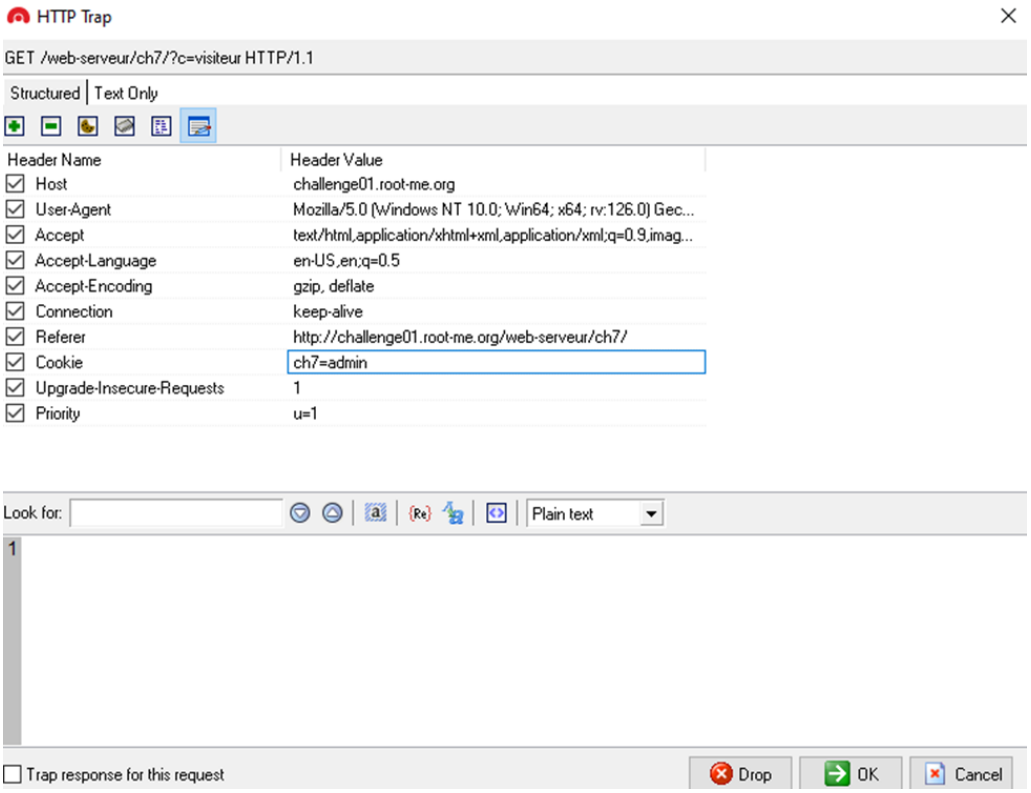
Hình 112: Bắt đầu Challenge HTTP - Cookie

Bắt đầu phân tích challenge với bước đầu là phân tích yêu cầu POST được gửi đi khi click "Saved email adresses". HTTP Sniffer chặn được yêu cầu POST này, yêu cầu này có trường Cookie.



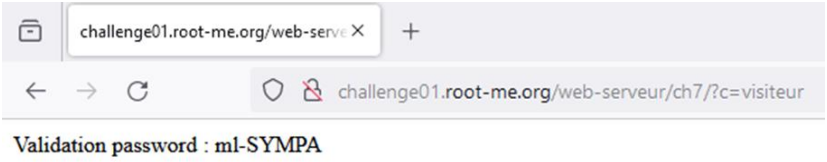
Hình 113: Phân tích yêu cầu POST có trường Cookie được chặn nhò HTTP Traps

Ta có thể click “Drop” để loại bỏ yêu cầu trên, hoặc click “OK” hoặc “Cancel” để chấp nhận chuyển yêu cầu đi hoặc cũng có thể chỉnh sửa nội dung rồi chuyển đi. Nhóm chỉnh sửa trường Cookie “ch7=visiteur” thành “ch7=admin” và click “OK” để chuyển đi.



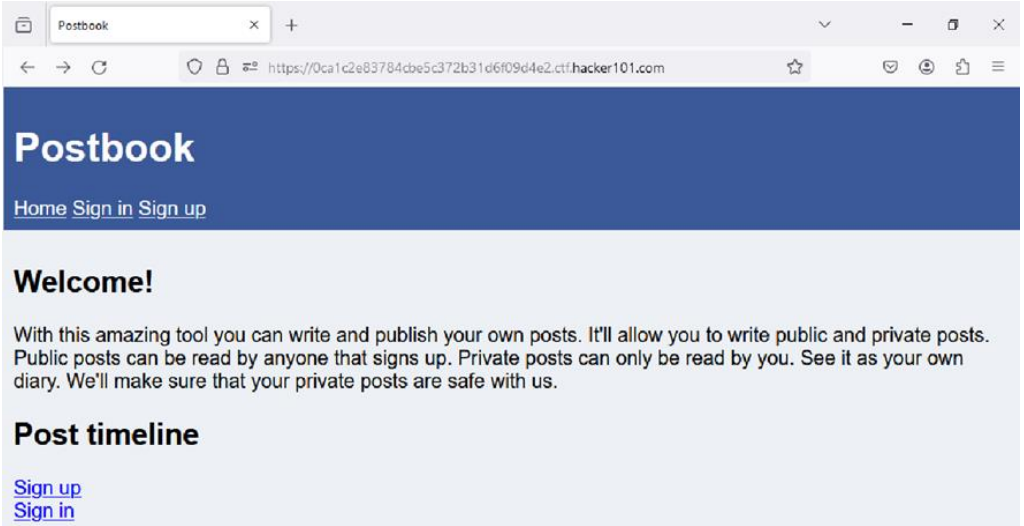
Hình 114: Sửa trường Cookie của yêu cầu bị chặn bởi HTTP Trap của HTTP Sniffer của AMT

Sau khi chuyển yêu cầu, trang web của challenge trên trình duyệt trả về nội dung của flag .



Hình 115: Flag của challeng HTTP – Cookie

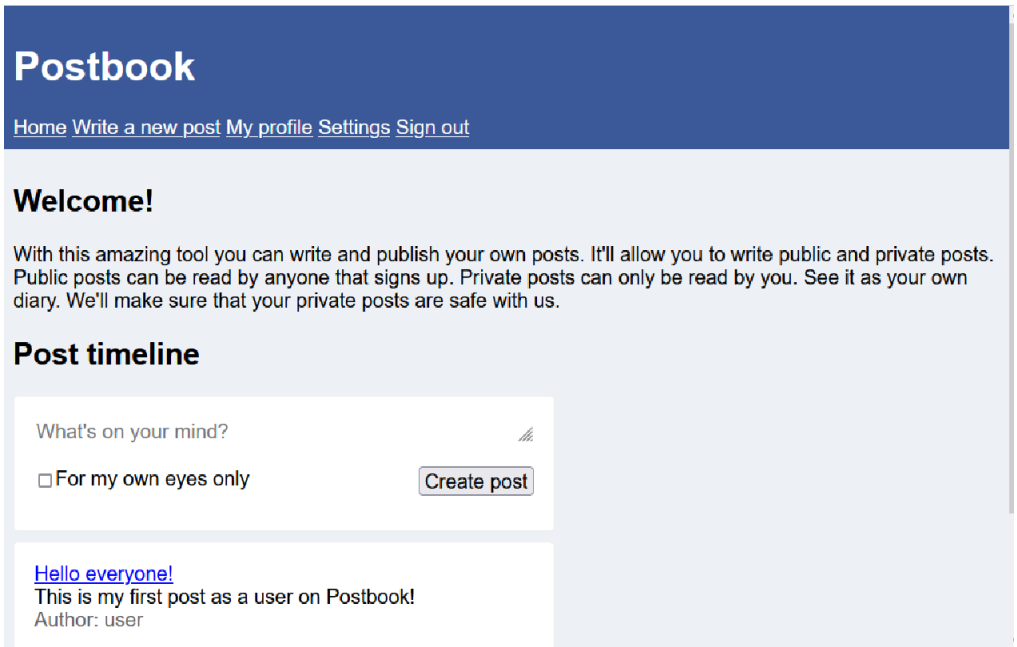
5. Kịch bản 4



Hình 116: Challenge Postbook của Root Me

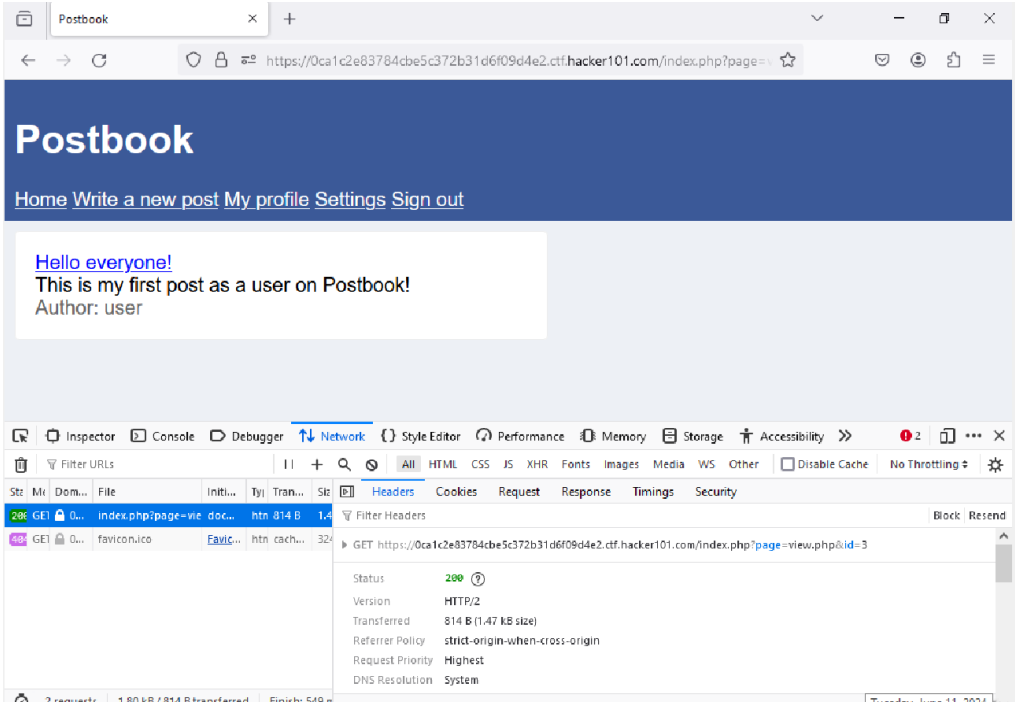
Flag 1:

- Bước 1: Thực hiện đăng ký, đăng nhập.



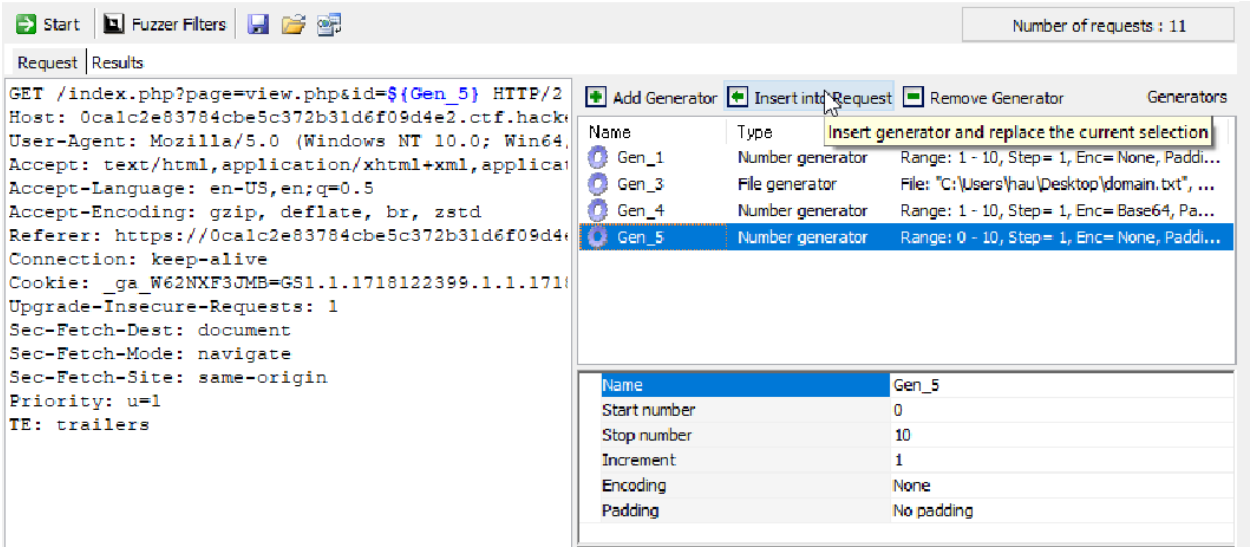
Hình 117: Giao diện của trang web mục tiêu của challenge Postbook sau khi đăng nhập thành công

- Bước 2: Mở "Dev tool" và click vào "Hello everyone" để xem post của người dùng. Sau đó "Dev tool" đã ghi lại được yêu cầu GET có tham số "page=view.php&id=3".



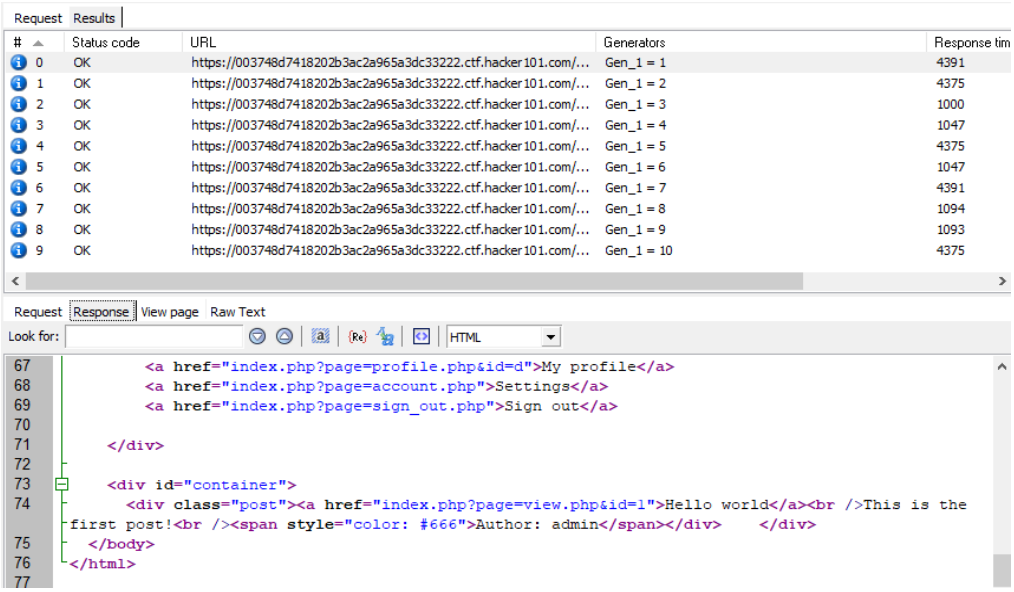
Hình 118: Yêu cầu GET bắt được sau khi click "Hello everyone"

- Bước 3: Copy yêu cầu trên vào mục "Request" của HTTP fuzzer của AMT, thay giá trị 3 của tham số id bằng "$Gen_5" (chọn "Gen_5" > "Insert into Request").



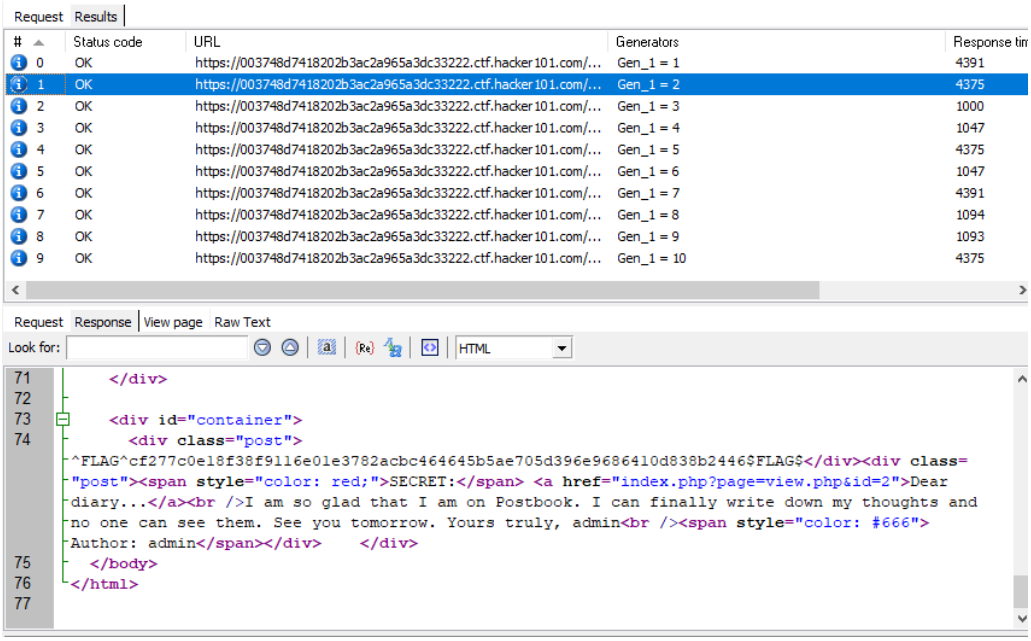
Hình 119: Thêm $(Gen_5) vào yêu cầu GET ở trên trong HTTP fuzzer của AMT

- Bước 4: "Start" để bắt đầu tìm các post có id tăng dần.



Hình 120: Kết quả của HTTP Fuzzer của AMT sau khi Brute-force để tìm các post

- Bước 5: Kiểm tra các post tìm được và phát hiện phản hồi của post có id=2 có chứa flag.

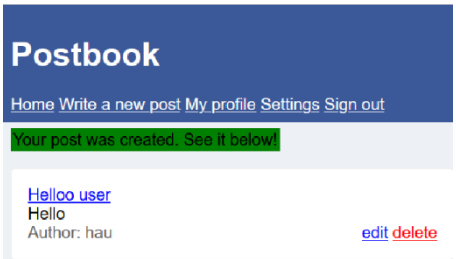


Hình 121: Flag 1 được tìm thấy trong post có id=2

Flag 2:

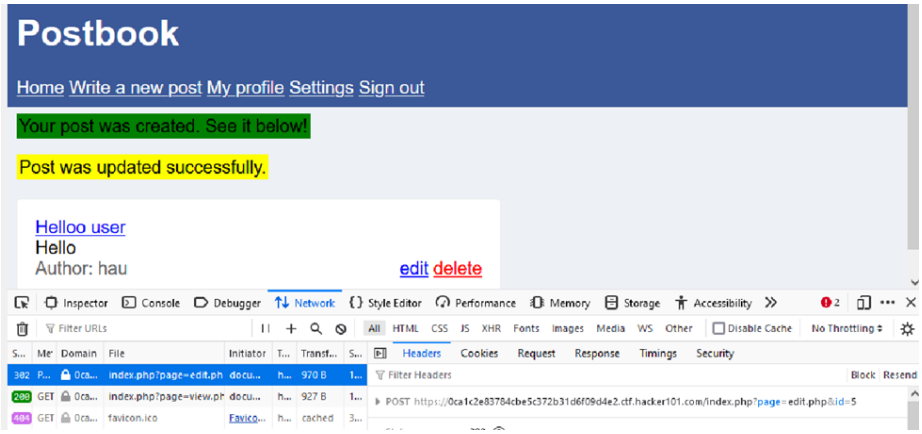
- Bước 1: Chọn “Write a new post” để tạo một post mới với nội dung tùy ý. Sau đó chọn “Create post”.

Hình 122: Tạo post mới trên trang web mục tiêu của challenge Postbook

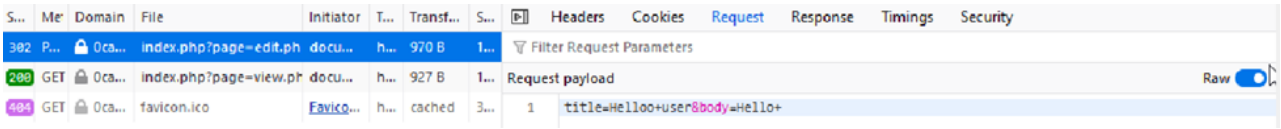


Hình 123: Post được tạo thành công trên trang web mục tiêu của challenge Postbook

- Bước 2: Sau khi tạo một post mới, ta sẽ có thể dùng chức năng "edit". Chức năng này có thể có lỗ hổng (giả sử có thể chỉnh sửa post của người dùng khác) nên ta thực hiện chọn "edit" đồng thời mở "Dev tool". Ta thực hiện chỉnh sửa bài post với nội dung bất kỳ. Khi cập nhật thay đổi của post thì "Dev tool" ghi lại được một yêu cầu POST yêu cầu cập nhật bài post có "id=5" được gửi đến server.

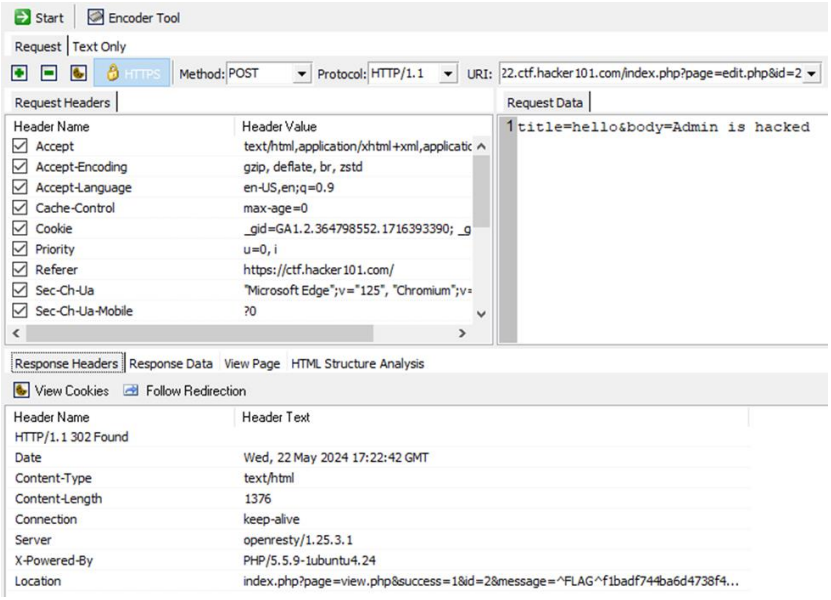


Hình 124: Bắt được gói yêu cầu POST để chỉnh sửa bài post được gửi tới trang web bằng Dev Tool



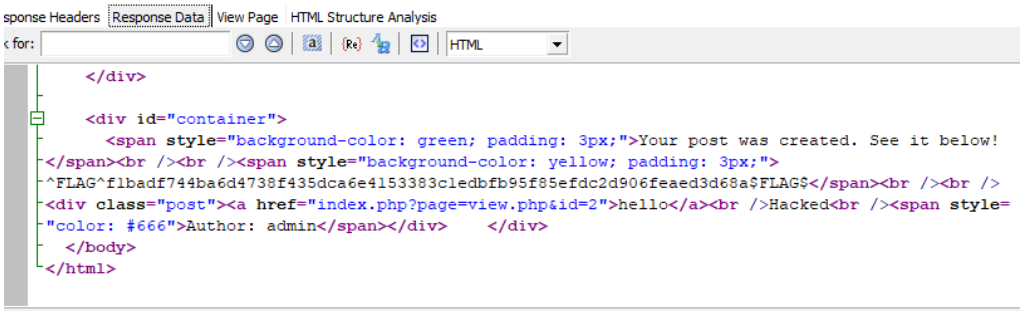
Hình 125: Payload của yêu cầu bắt được

- Bước 3: Để có thể có được flag, ta cần chỉnh sửa bài post ẩn của admin có id=2. Ta copy lại yêu cầu trên vào HTTP editor, sau đó điền url tương tự sau vào trường "URI" https://xx.ctf.hacker101.com/index.php?page=edit.php&id=2 sau đó chọn "Start".



Hình 126: Yêu cầu được chỉnh sửa và phản hồi có chứa flag của nó trong HTTP Editor của AMT

- Bước 4: Do respond trả về là một mã 302, nghĩa là request được redirection đến đường dẫn url khác. Click vào "Follow Redirection" để tạo một request mới cho chuyển hướng và bấm "Start" lần nữa để chuyển hướng đến trang chứa flag.



Hình 127: Trang chứa Flag 2 của challenge

6. Kịch bản 5

Kịch bản được thực hiện trên máy ảo Kali Linux và sử dụng Acunetix v24.1 CRACK.

Các bước thực hiện kịch bản: Xây dựng web PHP > Cài đặt AcuSensor cho web > Tiến hành quét trang web có dùng AcuSensor > Phân tích và vá các lỗ hổng phát hiện nhờ AcuSensor.

- Xây dựng web PHP:

- Bước 1: Tạo mới hoặc sửa đổi tệp index.html trong thư mục /var/www/html như sau:

```
<html>
        <head></head>
        <body>
                <h1>Internal Resources</h1><br><br>
                <a href="catfile.php">Document Library</a>
        </body>
</html>
```

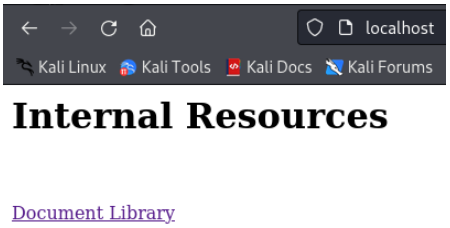
Hình 128: Nội dung index.html sau sửa đổi

- Bước 2: Tạo mới một tệp catfile.php trong thư mục /var/www/html với nội dung sau:

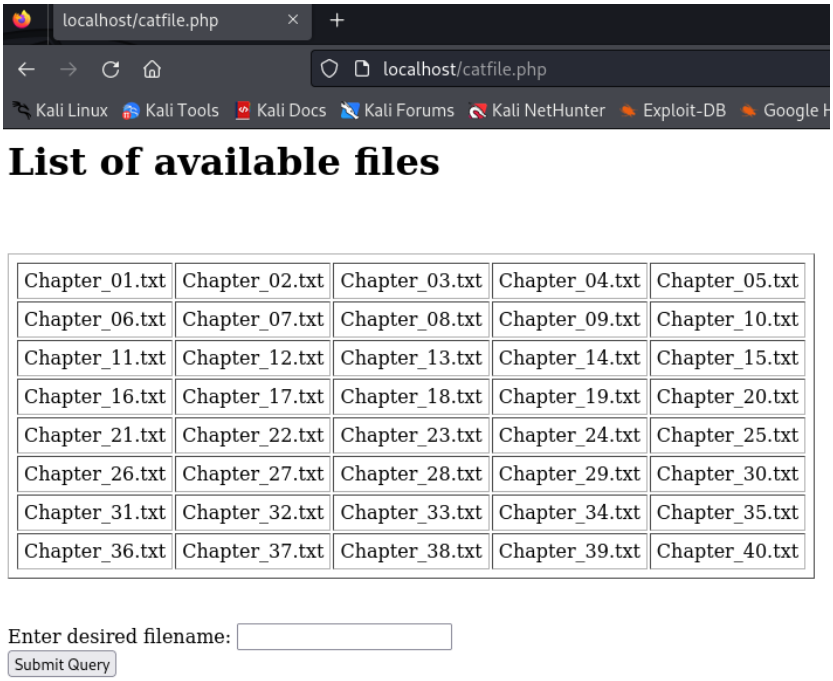
```
<?php
$base_folder = "/var/www/html";
$file=$_POST["filename"];
if (!empty($file)) {
  echo "<h1>This is the content of the file using the file_get_contents instruction</h1><br>";
  $filetext=file_get_contents($base_folder . "/library/" . $file);
  echo $filetext;
}
else {
  $filelist = array_diff(scandir($base_folder . "/library"), array('..','.'));
  $i=1;
  echo "<h1>List of available files</h1><br><br>";
  echo "<table border=\"1\" style=\"padding:5px\">";
  foreach ($filelist as $value) {
    if ($i==1) echo "<tr>";
    echo "<td style=\"padding:5px\">".$value."</td>";
    if ($i==5) {
      echo "</tr>";
      $i=0;
    }
  $i++;
  }
echo "</table><br><br>";
echo "<form action=\"catfile.php\" method=\"post\">";
echo "Enter desired filename: <input type=\"text\" name=\"filename\"><br>";
echo "<input type=\"submit\">";
echo "</form>";
}
?>
```

Hình 129: Nội dung catfile.php

- Bước 3: Trang web đang tạo có thể hiển thị nội dung các tệp dựa vào filename nhận từ phía khách. Tạo các tệp txt mẫu để có đối tượng hiển thị và chạy dịch vụ apache2. Lần lượt chạy các câu lệnh sau:
  - echo $'example contents\n' > /var/www/html/library/Chapter_01.txt
  - tee </var/www/html/library/Chapter_01.txt /var/www/html/library/Chapter_{02..40}.txt >/dev/null
  - sudo systemctl start apache2



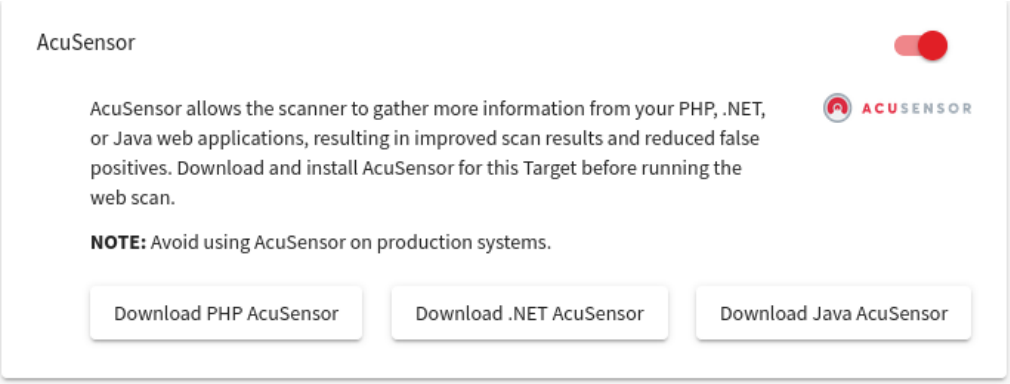
Hình 130: Giao diện web được tạo cho kịch bản 5



Hình 131: Giao diện của catfile.php

- Cài đặt AcuSensor cho trang web:
  - Bước 1: Tạo Mục tiêu trên Acunetix và trong phần cấu hình Mục tiêu bật AcuSensor.

Hình 132: Mục tiêu có địa chỉ là IP của máy Kali Linux



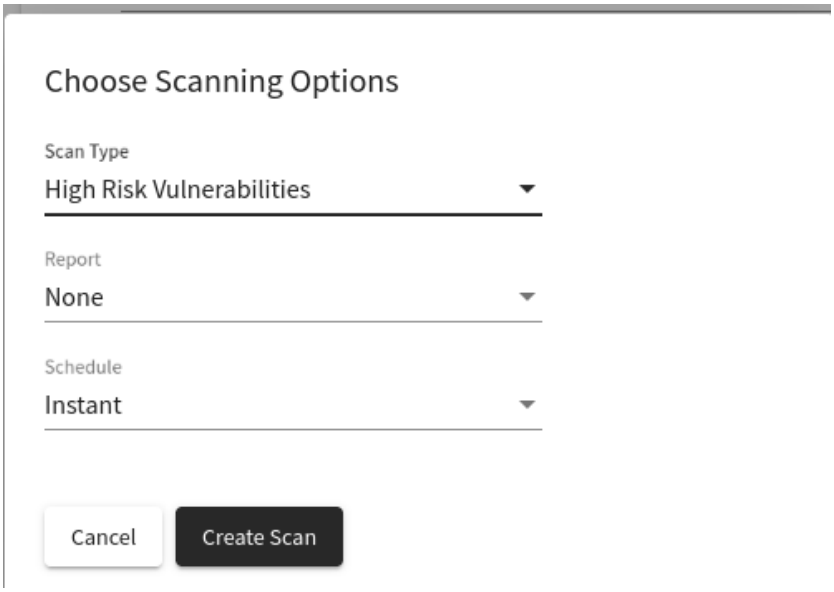
Hình 133: Bật AcuSensor ở phần cấu hình Mục tiêu

  - Bước 2: Sau khi bật AcuSensor, click "Download PHP AcuSensor". Tệp "acu_phpaspect.php" sẽ được tải về. Các trường thông tin khác trong phần cấu hình Mục tiêu giữ nguyên, click "Save".

- Bước 3: Tạo thư mục "acusensor" trong thư mục "/var/www/html/" và chuyển tệp "acu_phpaspect.php" vào.
- Bước 4: Chỉnh sửa tệp php.ini (thường có đường dẫn là /etc/php/8.2/apache2/php.ini) bằng lệnh **sudo nano /etc/php/8.2/apache2/php.ini** . Tìm dòng có chuỗi "allow_prepend_file" và sửa thành "auto_prepend_file = /acusensor/acu_phpaspect.php". Dòng mới này sẽ chạy một tệp PHP trước khi các tệp PHP khác được chạy.
- Bước 5: Khởi động lại dịch vụ Apache2: **sudo systemctl restart apache2**

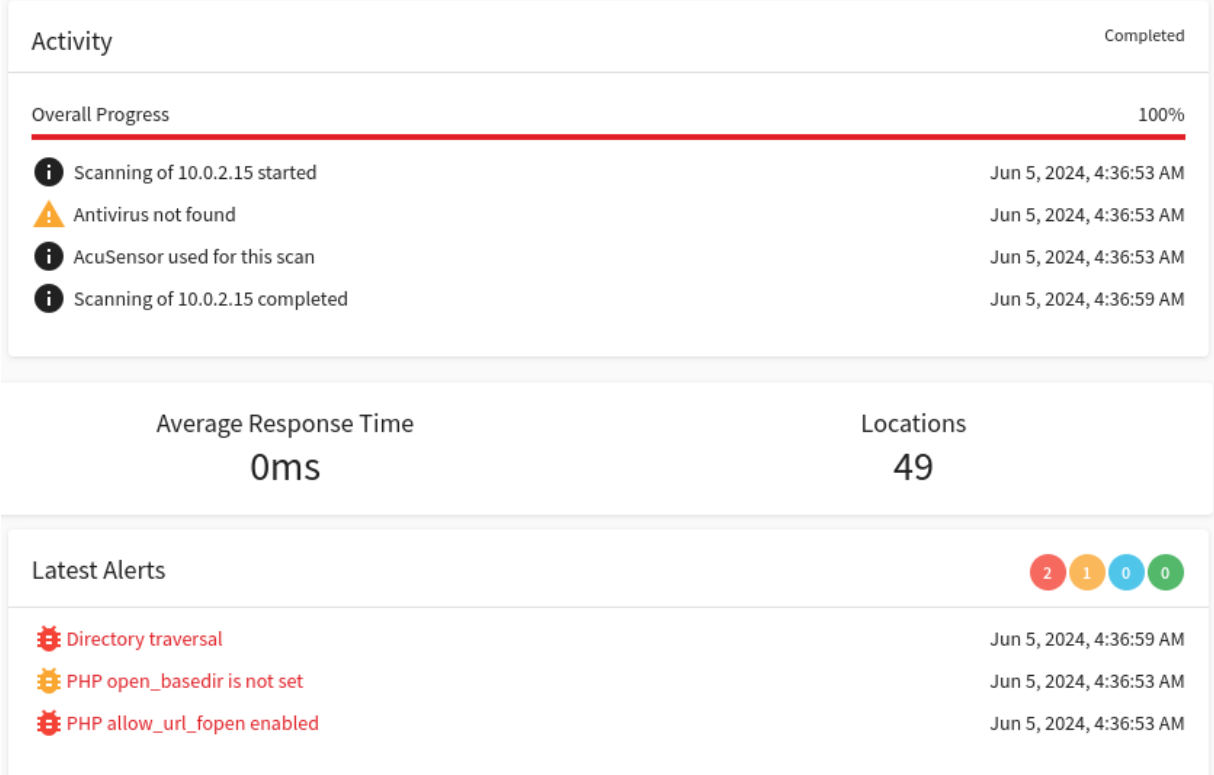
- Tiến hành quét trang web có dùng AcuSensor: Vào "Targets" và tạo lượt quét lỗ hổng có độ nghiêm trọng cao với Mục tiêu đã đã tạo ở trên.

Hình 134: Mục tiêu đã tạo trước đó



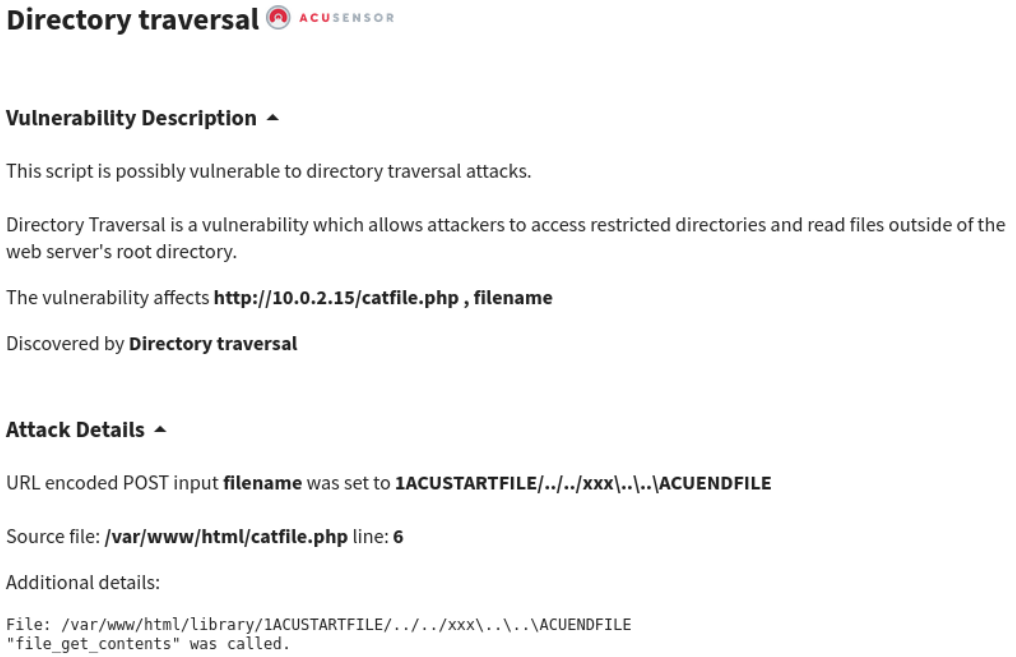
Hình 135: Quét lỗ hổng có mức độ nghiêm trọng cao

- Phân tích và vá các lỗ hổng phát hiện nhờ AcuSensor:



Hình 136: Kết quả quét trang trang web PHP nội bộ bằng Acunetix

- Lỗ hổng Directory traversal:



Directory traversal ACUSENSOR

Vulnerability Description

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

The vulnerability affects **http://10.0.2.15/catfile.php , filename**

Discovered by **Directory traversal**

Attack Details

URL encoded POST input **filename** was set to **1ACUSTARTFILE/../../xxx\..\..\ACUENDFILE**

Source file: **/var/www/html/catfile.php** line: **6**

Additional details:

```
File: /var/www/html/library/1ACUSTARTFILE/../../xxx\..\..\ACUENDFILE
"file_get_contents" was called.
```

Hình 137: Thông tin lỗ hổng Directory traversal quét được nhờ AcuSensor

  - Directory Traversal là một lỗ hổng bảo mật cho phép kẻ tấn công thực hiện truy cập không giới hạn các tệp tin bên ngoài server, từ đó dẫn đến tiết lộ thông tin quan trọng, nhạy cảm.

- "Attack Details" cho biết có lỗ hổng trong tệp "catfile.php" ở dòng 6, hàm **file_get_contents** được gọi.
- Kiểm tra lại trong file "catfile.php" (xem Hình 127) ở dòng 6, **file_get_contents** có nhận một tham số **$file** để tham chiếu đến tệp cần tìm và **$file** nhận giá trị từ tham số **filename** trong yêu cầu POST từ phía khách.
- Acunetix đã xác minh lỗ hổng bằng cách gửi yêu cầu POST với tham số **filename** mang giá trị **1ACUSTARTFILE/../../xxx\..\..\ACUENDFILE** vào trong yêu cầu POST. Trong đó, "../" trong đường dẫn thư mục có nghĩa là trỏ đến thư mục cha.

How to fix this vulnerability ▲

Your script should filter metacharacters from user input.

Hình 138: Khuyến nghị sửa lỗ hổng Directory Traversal của Acunetix

- Để sửa lỗ hổng, cần thực hiện lọc đầu vào có chứa kí tự đặc biệt mà trong ngữ cảnh hiện tại chính là "../".

```
1 <?php
2 $base_folder = "/var/www/html";
3 $file=$_POST["filename"];
4 $file_validated = str_replace ("../","",$file);
5 if (!strcmp($file,$file_validated) == 0){
6         header("Location: /");
7         exit;
8 }
9 if (!empty($file)) {
10   echo "<h1>This is the content of the file using the file_get_contents instruction</h1><br>";
11   $filetext=file_get_contents($base_folder . "/library/" . $file);
12   echo $filetext;
13 }
14 else {
15   $filelist = array_diff(scandir($base_folder . "/library"), array('..','.'));
16   $i=1;
17   echo "<h1>List of available files</h1><br><br>";
18   echo "<table border=\"1\" style=\"padding:5px\">";
19   foreach ($filelist as $value) {
20     if ($i==1) echo "<tr>";
21     echo "<td style=\"padding:5px\">".$value."</td>";
22     if ($i==5) {
23       echo "</tr>";
24       $i=0;
25     }
26   $i++;
27   }
28 echo "</table><br><br>";
29 echo "<form action=\"catfile.php\" method=\"post\">";
30 echo "Enter desired filename: <input type=\"text\" name=\"filename\"><br>";
31 echo "<input type=\"submit\">";
32 echo "</form>";
33 }
```

Hình 139: Tệp catfile.php sau chỉnh sửa để vá lỗ hổng Directory Traversal

- Lỗ hổng PHP allow_url_fopen enabled:

PHP allow_url_fopen enabled ACUSENSOR

Vulnerability Description

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

The vulnerability affects **http://10.0.2.15/**

Discovered by **PHP allow_url_fopen enabled**

Attack Details

Current setting is : **allow_url_fopen =** on

Hình 140: Thông tin lỗ hổng PHP allow_url_fopen enabled quét được nhờ AcuSensor

- Do flag **allow_url_fopen** là một flag trong tệp php.ini nếu được bật, sẽ cho phép máy chủ truy cập các tệp bên ngoài. Điều này có thể dẫn đến lỗ hổng bảo mật cho trang web nếu các máy chủ truy cập phải các tệp độc hại.

How to fix this vulnerability

You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).

php.ini
allow_url_fopen = 'off'

.htaccess
php_flag allow_url_fopen off

Classification

CWE	CWE-16
CVSS	Base Score: **0** - AV:N/AC:L/Au:N/C:N/I:N/A:N Access Vector: Network Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None

Hình 141: Khuyến nghị sửa lỗ hổng PHP allow_url_fopen enabled của Acunetix

- Để sửa lỗ hổng, flag **allow_url_fopen** trong tệp php.ini phải được tắt.

- Lỗ hổng PHP open_basedir is not set:

PHP open_basedir is not set ACUSENSOR

Vulnerability Description

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

The vulnerability affects **http://10.0.2.15/**

Discovered by **PHP open_basedir is not set**

Attack Details

Current setting is : **open_basedir =**

Hình 142: Thông tin lỗ hổng PHP open_basedir is not set quét được nhờ AcuSensor

- Flag **open_basedir** khi được bật sẽ hạn chế các thư mục mà các trang web PHP được truy cập, từ đó sẽ ngăn các trang web PHP truy cập những thành phần quan trọng trong hệ thống. Ví dụ: khi flag **open_basedir** được cấu hình như thế này **open_basedir = "/var/www/html:/tmp"**, thì các trang web PHP chỉ được phép truy cập vào các tệp trong thư mục **/var/www/html** và **/tmp**

How to fix this vulnerability

You can set open_basedir from php.ini

php.ini
open_basedir = your_application_directory

Hình 143: Khuyến nghị sửa lỗ hổng PHP open_basedir is not set của Acunetix

- Sửa dòng chứa **open_basedir** thành **open_basedir = /var/www** để trang web PHP chỉ có thể truy cập vào các tệp trong thư mục trên.

Sau khi vá lỗ hổng và thực hiện quét lại trang web, có thể thấy không còn phát hiện các lỗ hổng bảo mật trên nữa.

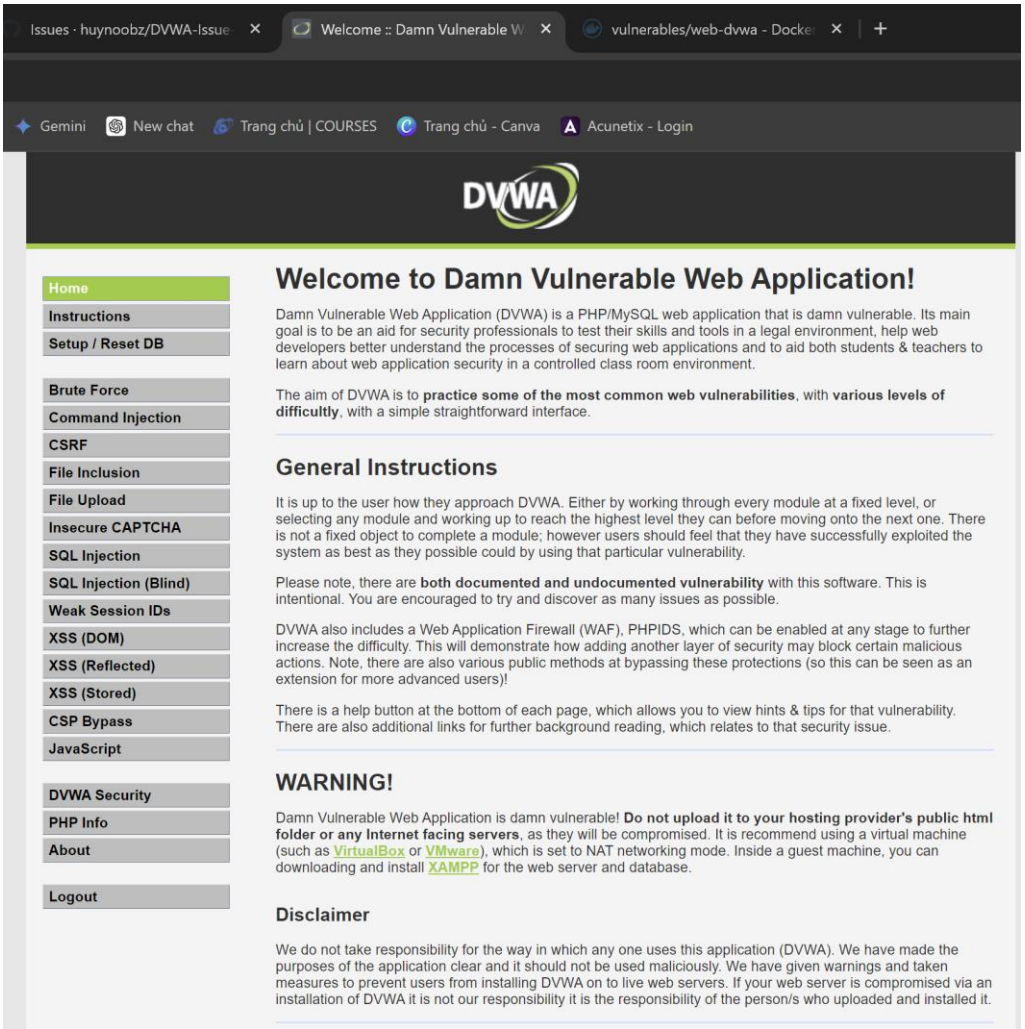
http://10.0.2.15	High Risk Vulnerabilities	Last run on Jun 5, 2024, 6:04:57 AM	0 0 0 0	Completed
http://10.0.2.15	High Risk Vulnerabilities	Last run on Jun 5, 2024, 4:36:48 AM	2 1 0 0	Completed

Hình 144: Tổng quan kết quả quét trước và sau khi vá lỗ hổng

7. Kịch bản 6

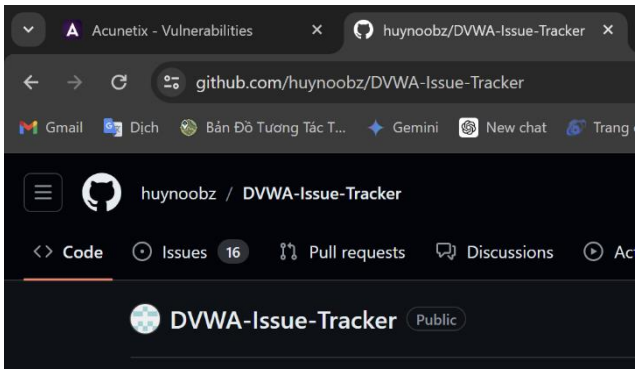
Để thực hiện kịch bản nhóm chuẩn bị trước những thứ sau:

- Web mục tiêu: Sử dụng docker để chạy web DVWA trên cổng 60000.



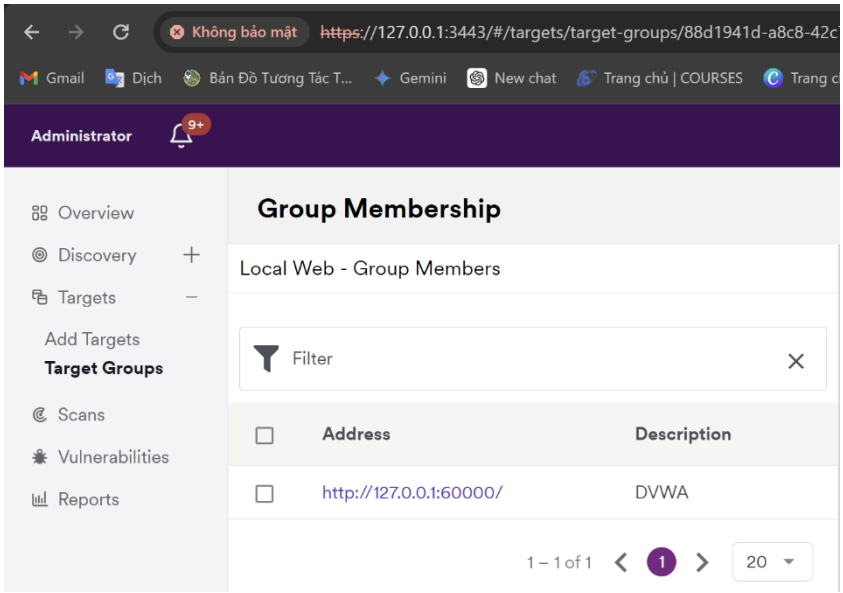
Hình 145: Trang web mục tiêu – DVWA

- Một repository trên Github để lưu trữ các vấn đề (Issue): https://github.com/huynoobz/DVWA-Issue-Tracker



Hình 146: Repository DVWA-Issue-Tracker trên Github để lưu trữ các Issue

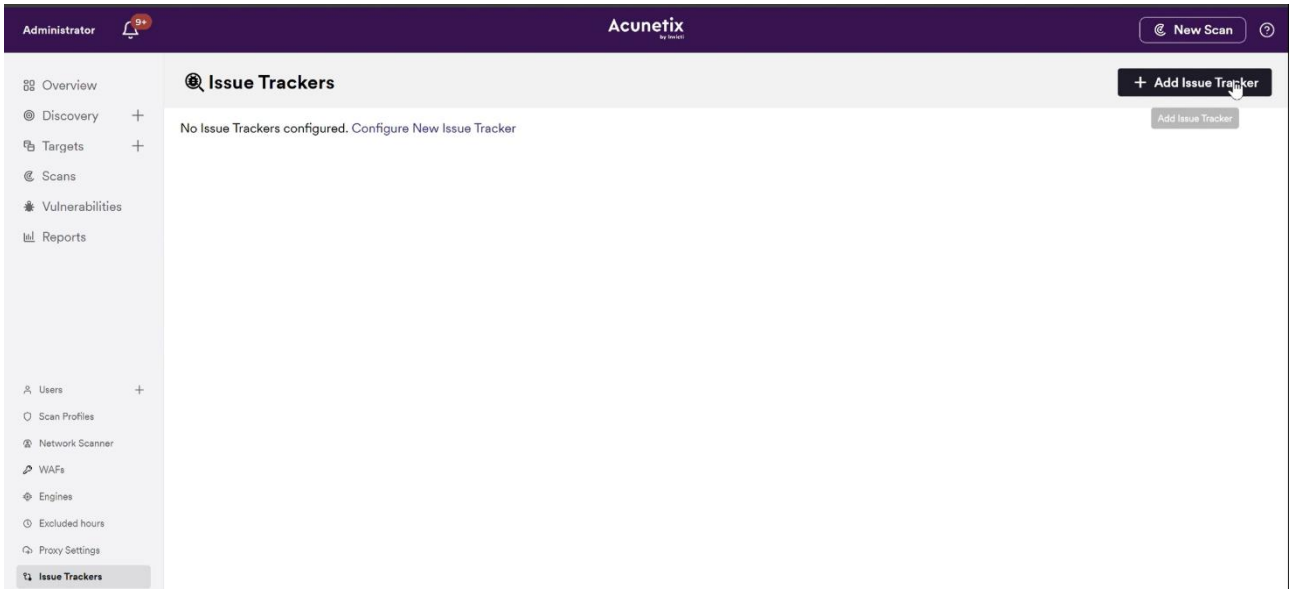
- Mục tiêu nằm trong 1 nhóm mục tiêu trên Acunetix: Ở đây Mục tiêu có địa chỉ http://127.0.0.1:60000 nằm trong nhóm Local Web



Hình 147: Mục tiêu nằm trong nhóm mục tiêu Local Web trên Acunetix

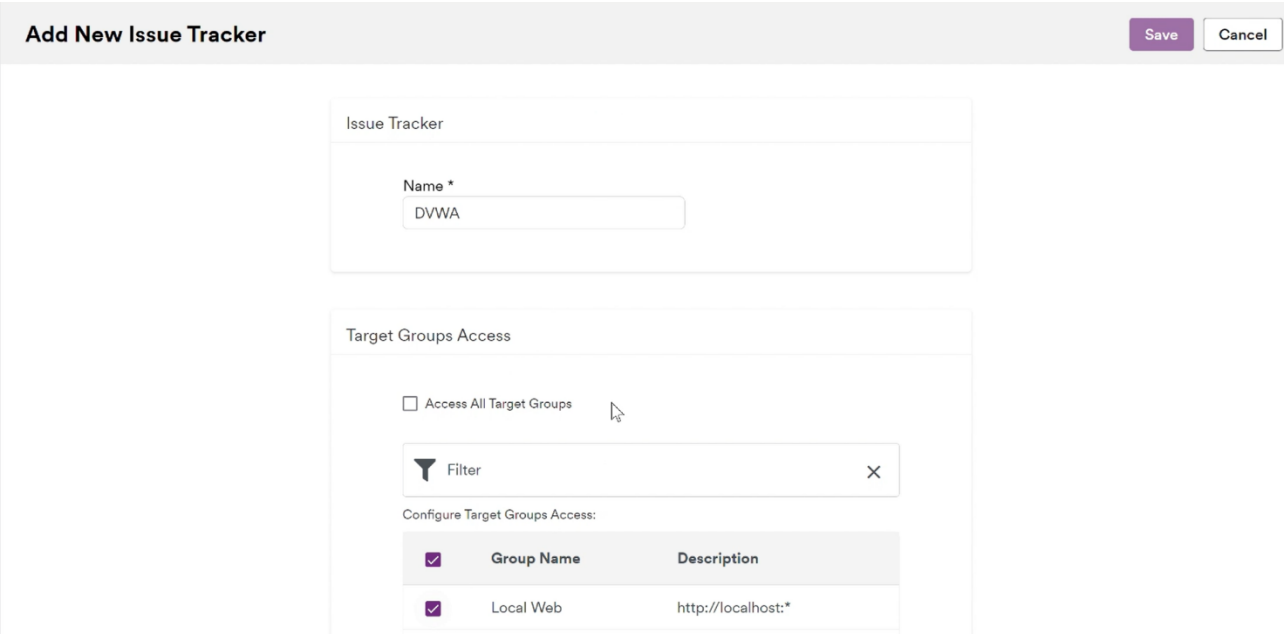
Sau khi chuẩn bị đủ những thứ trên nhóm tiến hành thực hiện kịch bản: Thêm Issue Tracker cho Acunetix > Thêm Issue Tracker vừa thêm cho Mục tiêu > Quét Mục tiêu > Gửi các thông tin lỗ hổng quét được cho Issue Tracker

- Thêm Issue Tracker cho Acunetix:
  - Vào "Issue Trackers" > "Add Isue Tracker"



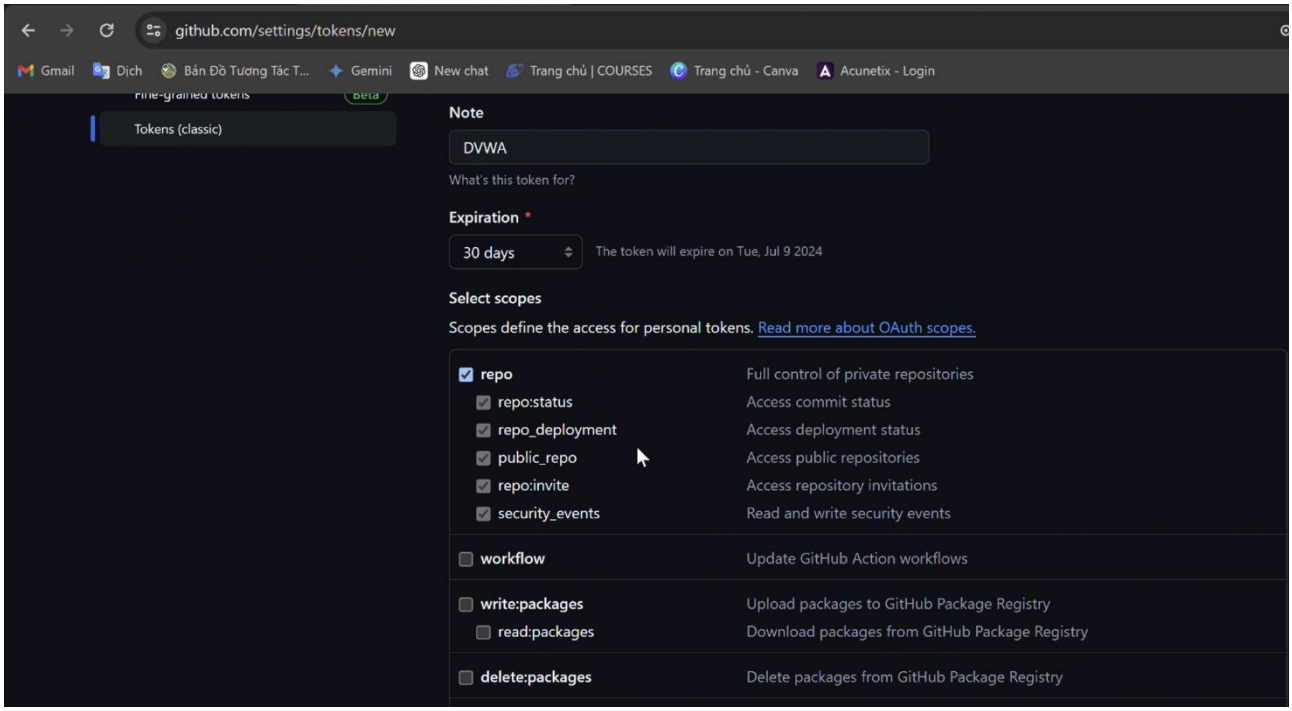
Hình 148: Thêm Issue Tracker cho Acunetix

  - Ở phần cấu hình Issue Tracker, ta thêm tên cho Issu Tracker và chọn nhóm mục tiêu mà Issue Tracker được phép tiếp cận.

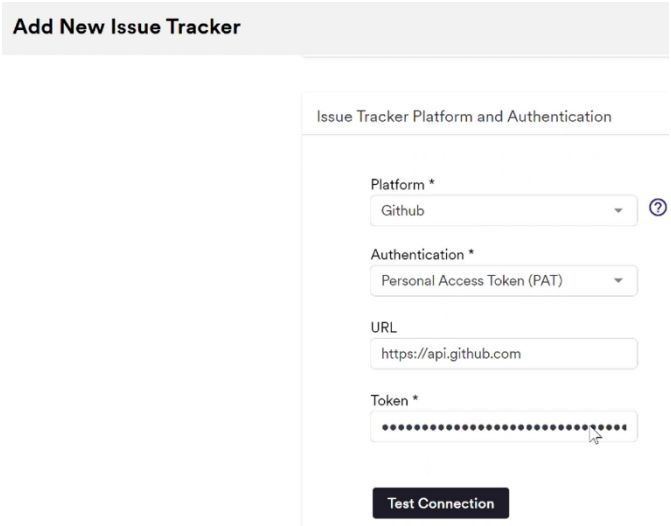


Hình 149: Thêm tên và chọn nhóm mục tiêu cho Issue Tracker

- Ở mục "Issue Tracker Platform and Authentication" của phần cấu hình Issue Tracker, ta tùy chỉnh như sau:
  - Platform: nền tảng sử dụng ở đây là Github
  - Authentication: phương thức xác thực thì dùng PAT
  - URL: đường dẫn đến api nhận thông tin chứng thực, của Github là https://api.github.com
  - Token: lấy từ github.com/settings/tokens, nếu không có thì tạo thêm, lưu ý: token phải có thể truy cập, đọc, viết được trên repository.

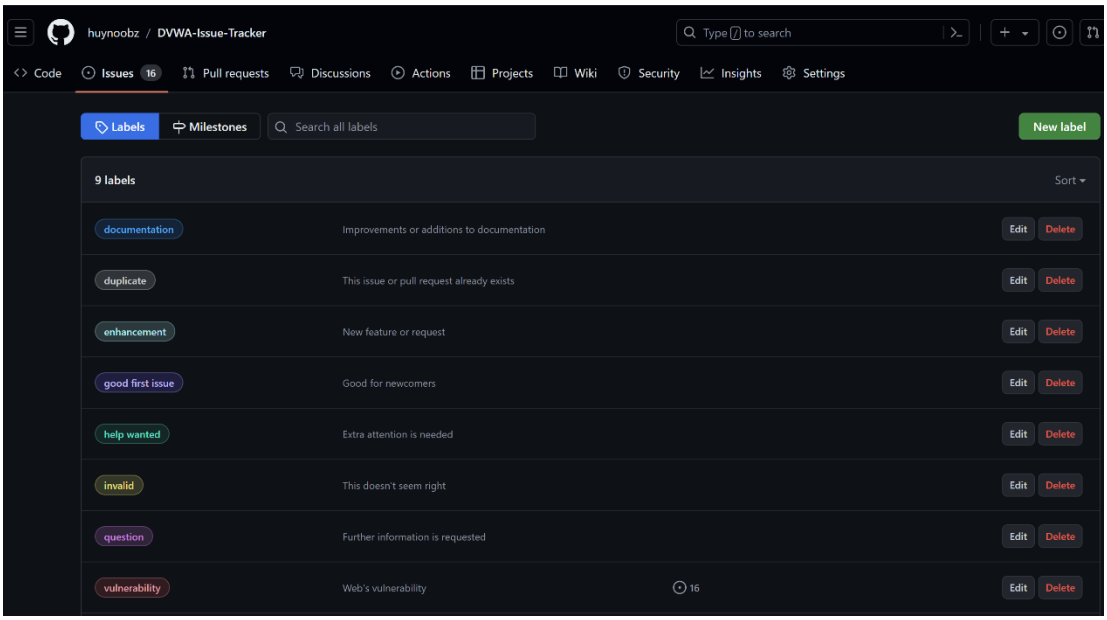


Hình 150: Tạo PAT cho Issue Tracker

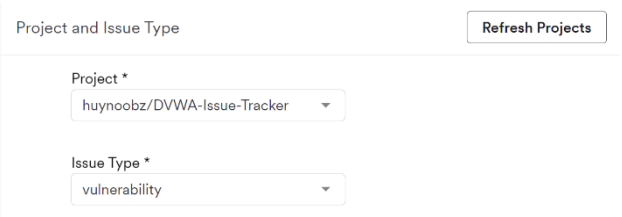


Hình 151: Tùy chỉnh cho "Issue Tracker Platform and Authentication"

- Sau khi tùy chỉnh xong, click "Test Connection" để kiểm tra kết nối. Sau đó sẽ xuất hiện thêm mục "Project and Issue Type". Tiếp tục tùy chỉnh mục này để hoàn thành cấu hình Issue Tracker.
  - Project: chọn dự án hay repository sẽ lưu trữ các vấn đề.
  - Issue Type: tag đính kèm vấn đề mang ý nghĩa là loại vấn đề, với Issue trên Github thì đó là tag Label, ta có thể chỉnh sửa tag Label này trên Github nếu không có loại vấn đề ta muốn.



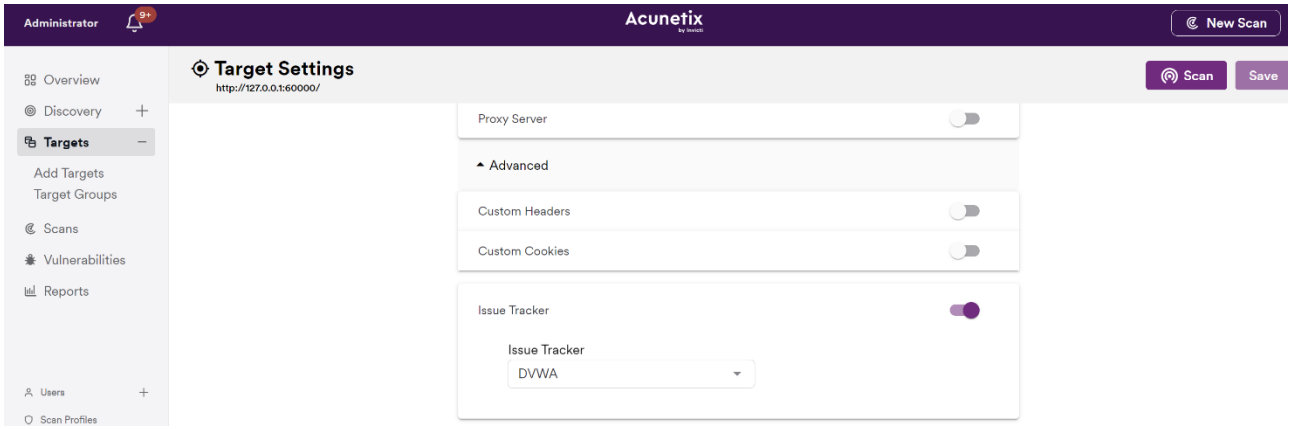
Hình 152: Các tag Label trên Github



Hình 153: Các tùy chỉnh của "Project and Issue Type"

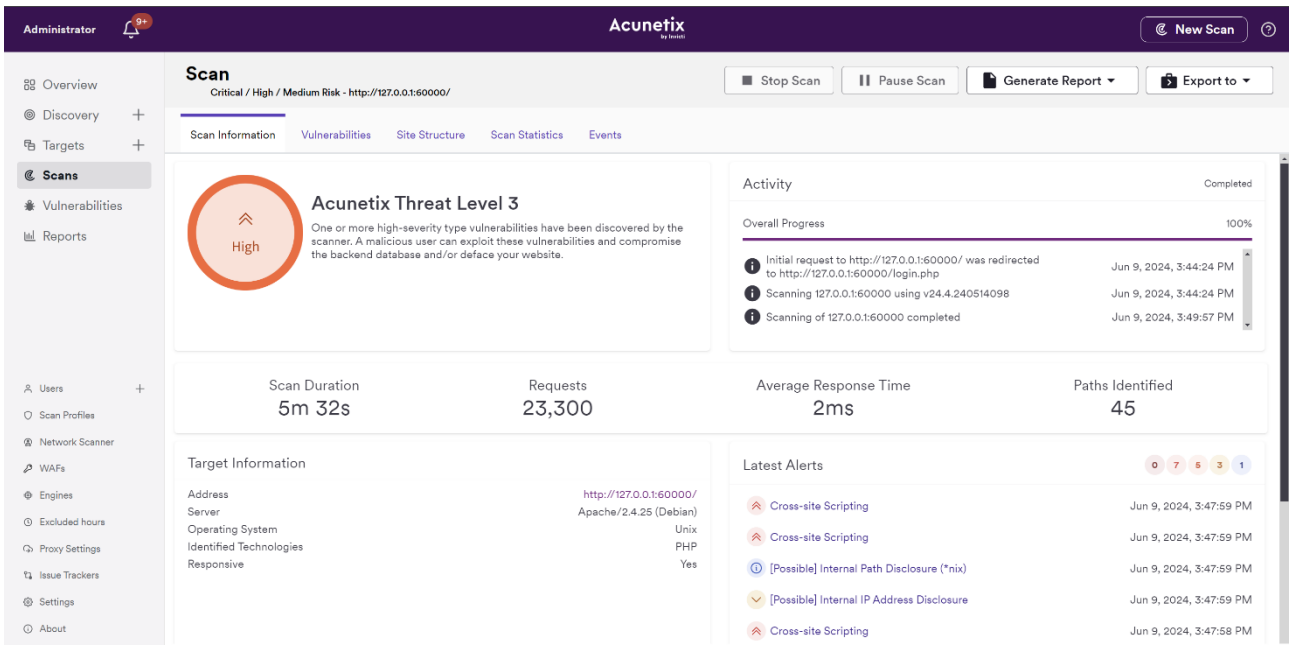
- Click "Save" để hoàn tất cấu hình.

- Thêm Issue Tracker cho mục tiêu: Vào "Targets" để cấu hình mục tiêu. Ở đây nhóm đã cấu hình trước những thứ cần thiết cho mục tiêu (Site Login, Default Scan Profile, ...) nên chỉnh gì thêm. Lướt xuống phần "Advanced", bật Issue Tracker và chọn Issue Tracker vừa thêm và "Save".



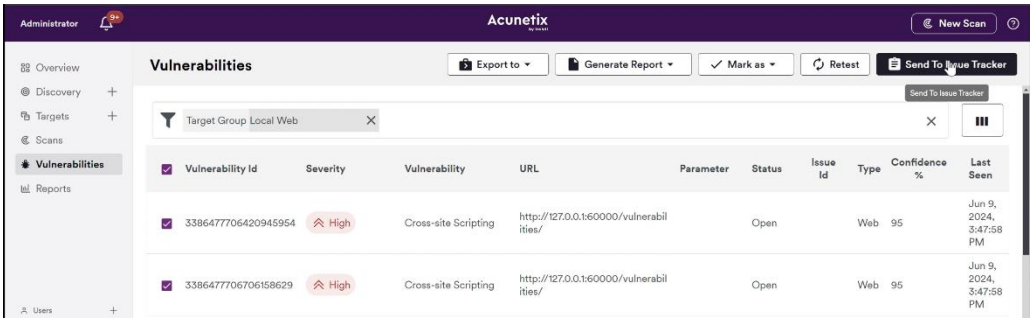
Hình 154: Thêm Issue Tracker cho Mục tiêu trên Acunetix

- Quét Mục tiêu: ta đang ở phần cấu hình Mục tiêu và vừa "Save" các cấu hình, click "Scan" > "Create Scan" để bắt đầu quét ngay lập tức. Cách khác: vào "Scans" > "New Scan" > chọn Mục tiêu > "Scan" > "Create Scan".

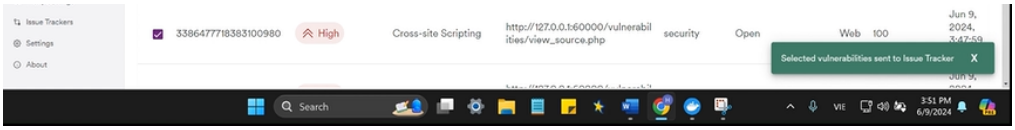


Hình 155: Kết quả quét Mục tiêu của Acunetix

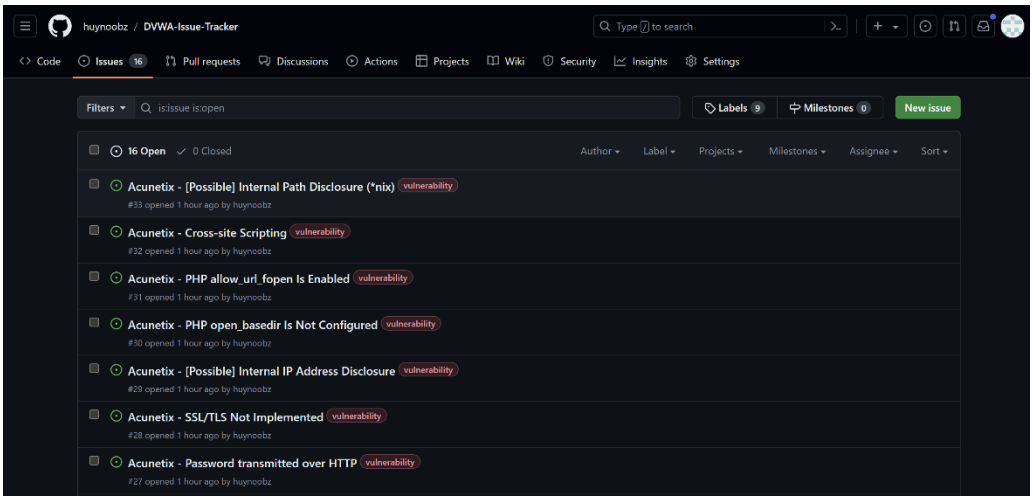
- Gửi các thông tin lỗ hổng quét được cho Issue Tracker: vào “Vulnerabilities” > chọn các lỗ hổng muốn gửi đến Issue Tracker > “Send To Issue Tracker”. Và đợi một lúc, sau khi có thông báo thành công thì có thể kiểm tra bên Github các vấn đề được gửi tới. Lưu ý không thể gửi 1 lỗ hổng 2 lần.



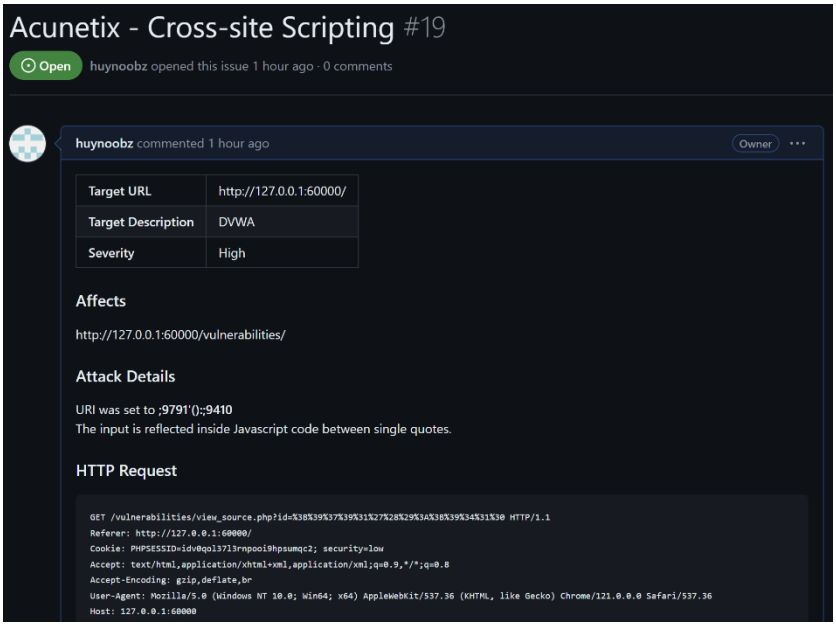
Hình 156: Gửi thông tin lỗ hổng đến Issue Tracker



Hình 157: Thông báo gửi thành công đến Issue Tracker



Hình 158: Repository trên Github nhận được các vấn đề



Hình 159: Một vấn đề được gửi lên Issue Track bởi Acunetix

Với Issue Tracker việc kiểm thử và phối hợp phát triển web sẽ trở nên thuận tiện hơn. Đặt ngữ cảnh mỗi thành viên trong đội phát có 1 Acunetix riêng hoặc có người không có và ở xa nhau thì việc thông báo cho nhau về lỗ hổng hiện có, lỗ hổng mới, lỗ hổng được vá sẽ rất bất tiện, sẽ có trường hợp thông báo trùng lỗ hổng, lỡ lỗ hổng mới, ... Với Issue Tracker việc phát triển trang web sẽ giống như phát triển phần mềm, mọi người trong đội đều có thể tiếp cận với repository trên Github nên không nhất thiết ai cũng phải có Acunetix, đều có thể biết về tình trạng hiện của bảo mật của trang web (các lỗ hổng cũ, lỗ hổng mới), cập nhật các lỗ hổng đã được vá bằng cách "Close Issue", thảo luận với nhau dưới mỗi vấn đề.

Nhóm có quay 1 video demo kịch bản này.

CHƯƠNG 5: KẾT LUẬN VÀ ĐÁNH GIÁ

Ở phần này, nhóm viết các kết luận và đánh giá của nhóm về Acunetix.

1. Kết luận

Acunetix là một công cụ mạnh mẽ và toàn diện trong lĩnh vực kiểm thử bảo mật ứng dụng web, giúp phát hiện và xử lý các lỗ hổng bảo mật một cách hiệu quả. Qua quá trình tìm hiểu, chúng ta thấy rằng Acunetix không chỉ cung cấp khả năng quét tự động mà còn hỗ trợ phân tích thủ công bằng cách cung cấp các bằng chứng khai thác và nhà phát triển cũng cung thêm bộ công cụ thủ công – AMT, ngoài ra còn có thể quét phần mềm độc hại trên máy chủ và quét lỗ hổng trong mạng nội bộ . Với giao diện thân thiện, khả năng báo cáo chi tiết và có thể tích hợp dễ dàng với các nền tảng thứ 3 hỗ trợ thao dõi vấn đề và quý trình DevOps, Acunetix là một lựa chọn hàng đầu cho các doanh nghiệp muốn tăng cường bảo mật cho sản phẩm web của mình.

Công cụ này được phát triển bởi Invicti Security, một công ty hàng đầu trong lĩnh vực bảo mật mạng. Invicti Security đã chứng tỏ sự cam kết của mình đối với việc bảo vệ các ứng dụng web thông qua việc cung cấp các giải pháp bảo mật tiên tiến và hiệu quả. Invicti Security không ngừng cải tiến công nghệ của mình, đưa ra các công nghệ mới để đáp ứng các thách thức bảo mật ngày càng phức tạp, đồng thời cung cấp hỗ trợ và dịch vụ khách hàng chất lượng cao.

Sự kết hợp giữa công nghệ tiên tiến của Acunetix và kinh nghiệm dày dặn của Invicti Security đảm bảo rằng công cụ này không chỉ phù hợp với các chuyên gia bảo mật mà còn với những người mới bắt đầu trong lĩnh vực này. Kết luận, Acunetix là một giải pháp đáng tin cậy và hiệu quả, đóng góp quan trọng vào việc bảo vệ ứng dụng web khỏi các mối đe dọa ngày càng tinh vi trên không gian mạng. Việc sử dụng Acunetix của Invicti Security mang lại sự an tâm và bảo vệ tối ưu cho các doanh nghiệp trong việc bảo vệ dữ liệu và hệ thống của họ.

2. Đánh giá

Điểm mạnh của Acunetix:

- Khả năng quét toàn diện:
    - Acunetix có khả năng quét nhiều loại lỗ hổng bảo mật khác nhau, từ những lỗ hổng phổ biến như SQL Injection và Cross-Site Scripting (XSS) đến các lỗ hổng phức tạp hơn.
    - Có thể quét các ứng dụng web hiện đại sử dụng các công nghệ như HTML5, PHP, JavaScript, ASP, ASP.NET.
    - Không chỉ quét lỗ hổng quét còn có thể quét phần mềm độc hại và lỗ hổng trong mạng nội bộ.

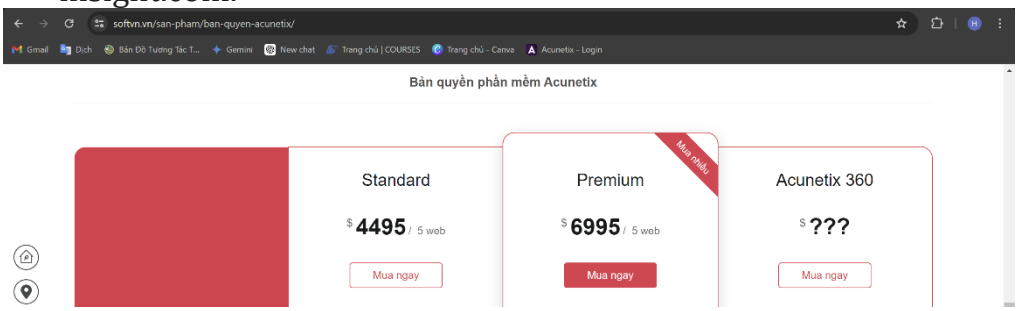
- Tính năng tự động hóa cao:
    - Khả năng quét tự động của Acunetix giúp tiết kiệm thời gian và công sức cho các đội ngũ bảo mật.
    - Công cụ có thể tích hợp các nền tảng theo dõi vấn đề và công cụ SDLC, giúp tự động phát hiện lỗ hổng trong suốt quá trình phát triển web.
- Báo cáo chi tiết:

- Acunetix cung cấp các báo cáo chi tiết và dễ hiểu, giúp các chuyên gia bảo mật dễ dàng nhận diện và khắc phục lỗ hổng.
- Có nhiều kiểu báo cáo để lựa chọn phù hợp với nhu cầu của từng doanh nghiệp.

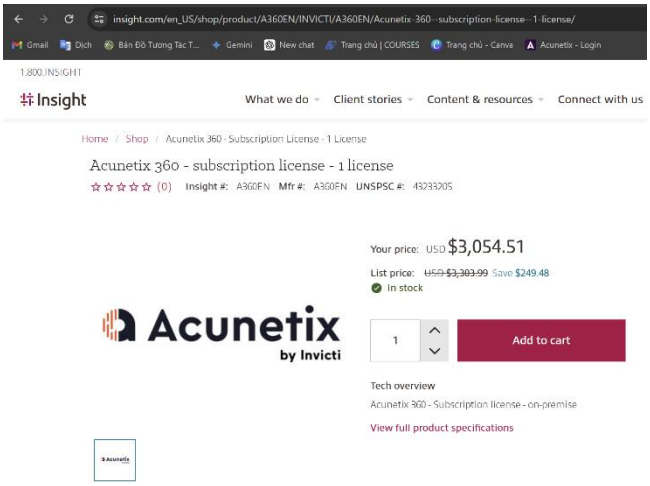
- Giao diện thân thiện và dễ sử dụng:
  - Giao diện của Acunetix được thiết kế thân thiện với người dùng, giúp ngay cả những người mới bắt đầu cũng có thể sử dụng công cụ này một cách hiệu quả.
- Hỗ trợ phân tích thủ công:
  - Acunetix khi quét có cung cấp các bằng chứng khai thác, tác động của lỗ hổng và các khuyến cáo giúp các chuyên viên phân tích thủ công các lỗ hổng nhanh hơn, dễ hơn và vá hiệu quả hơn.

Điểm yếu của Acunetix:

- Chi phí cao:
  - Acunetix là một công cụ cao cấp, và chi phí có thể là một rào cản đối với các doanh nghiệp nhỏ, các cá nhân, các tổ chức phi lợi nhuận.
  - Acunetix Standard có giá trên 110 triệu đồng, Acunetix Premium có giá trên 170 triệu đồng theo softvn.vn, Acunetix 360 giá hơn 70 triệu theo insight.com.



Hình 160: Giá Acunetix theo softvn.vn



Hình 161: Giá Acunetix 360 theo insight.com

TÀI LIỆU THAM KHẢO

Lý thuyết XSS: https://viettelidc.com.vn/tin-tuc/xss-la-gi-cach-kiem-tra-va-ngan-chan

Lý thuyết về Gartner: Gartner

Lý thuyết về SQL Injection: Phân loại và Ngăn chặn

Lý thuyết về Directory Traversal Attacks: DIRECTORY TRAVERSAL ATTACK LÀ GÌ?

Lý thuyết về Parameter Manipulation: Parameter Manipulation

Lý thuyết về SSRF: Tổng quan về lỗ hổng SSRF

Lý thuyết về XXE: XML external entity (XXE) injection

Lý thuyết về OAuth: https://en.wikipedia.org/wiki/OAuth

Lý thuyết về OpenVAS: định nghĩa và kiến trúc

Lý thuyết về SAST, DAST, IAST và RASP: Tìm hiểu về SAST, DAST, IAST và RASP

Giới thiệu về Acunetix: https://www.acunetix.com/support/docs/introduction/

Các chức năng của Acunetix: Features

Nhóm chức năng Mục tiêu: Tagets

Cấu hình một lần Quét: Scans

Quản lý các Lỗ hổng: Managing and prioritizing vulnerabilities

Phân loại mức độ nghiêm trọng Lỗ hổng: Vulnerability classifications

Các loại Báo cáo: https://acunetix.com/support/docs/types-reports/

Thông tin về Hồ sơ quét: What are scan profiles?

Nhóm chức năng WAFs: WAFs

Xuất kết quả quét đến WAFs: Exporting scan results to WAFs

Thông tin các nền tảng Issue Trackers: Configuring Issue Tracker Integration

Phân quyền với các vai trò trong Acunetix: users and roles

Thông tin về AcuSensor Bridge: AcuSensor Bridge

Yêu cầu hệ thống của Acunetix: Minimum system requirements

Thông tin về Acunetix 360: What is Acunetix 360?

So sánh Acunetix 360 On-Demand và Acunetix 360 On-Premises: Online vs On-Premises

Cài đặt Acunetix 360 On-Premises: Acunetix 360 On-Premises

Thông tin về mô-đun Blind SQL Injector của AMT: Acunetix Blind SQL Injector

Thông tin về mô-đun Authentication Tester của AMT: Acunetix Authentication Tester

Thông tin về mô-đun Web Services Editor của AMT: Acunetix Web Services Editor

GIẢI TRÌNH CHỈNH SỬA

STT	Chỉnh sửa	Nội dung chỉnh sửa của nhóm và lý do	Vị trí chỉnh sửa
1	Loại bỏ nội dung cập nhật Acunetix	Xóa bỏ nội dung của mục 3.8 cũ – Cập nhật Acunetix do nôi dung quá đơn giản, không cần thiết.	Trang 58 mới hay trang 57 – 58 cũ
2	Thêm vài dòng định nghĩa cho các mô đun của AMT	Thêm định nghĩa tổng quát về các mô đun của AMT do trước đó không có viết định nghĩa tổng quát cho các mô đun mà đi trực tiếp vào thực nghiệm khiến người đọc khó hình dung được mô đun đó là gì và dùng làm gì?	Trang 67 – 81
3	Sửa lại kịch bản 4	Đổi challenge HTTP – POST của Root Me của kịch bản 4 cũ thành challenge Postbook của ctf.hack101.com do nhóm cho rằng kịch bản 4 cũ quá đơn giản chưa khai thác rõ tính năng của các mô đun của AMT nên đổi thành challenge tương tự như phức tạp hơn một chút.	Trang 83, trang 92 – 96 mới hay trang 92 – 95 cũ.
4	Cập nhật thêm hình ảnh về giao diện của web mục tiêu cho kịch bản 5	Thêm hình 130, 131 mới – giao diện web mục tiêu cho kịch bản 5 do nhóm cho rằng người sẽ là thiếu sót nếu không có hình ảnh về giao diện của web mục tiêu.	Trang 97 – 98 mới hay trang 96 cũ.
5	Một số tinh chỉnh nhỏ khác	Để báo cáo dễ nhìn hơn nhóm thực hiện các thao tác như căn chỉnh, ngắt trang, chỉnh kích thước ảnh sao cho không chừa quá nhiều khoảng trống mỗi trang.	Tất cả các trang.
6	Sửa lại kịch bản 4 của slide thuyết trình	Tương tự với Chỉnh sửa thứ 3 nhưng ở đây là sửa tệp thuyết trình của nhóm.	Trang 36 – 47 mới hay trang 36 – 42 cũ của slide thuyết trình.
7	Một số tinh chỉnh nhỏ khác với slide thuyết trình	Do nhóm không kiểm tra lại khi chuyển đổi từ dự án của Canva qua tệp .pptx nên ở tệp .pptx đã xuất hiện các lỗi thiết kế nên nhóm đã sửa chúng ở bản mới.	Trang 1, trang 29 – 57 mới hay trang 29 – 52 cũ của slide thuyết trình.

Bảng 11: Bảng giải trình chỉnh sửa cho báo cáo cuối cùng