TRƯỜNG ĐẠI HỌC SƯ PHẠM THÀNH PHỐ HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

----- ☙ 🕮 ❧ -----

ĐỒ ÁN MÔN HỌC

ĐỀ TÀI: SECURITY TEST TOOL NETSPAKER

Giáo viên hướng dẫn: TS. Trần Sơn Hải

Nhóm sinh viên thực hiện:

Huỳnh Thị Yến Khoa	MSSV: 46.01.104.087
Võ Thị Hồng Diễm	MSSV: 46.01.104.027
Nguyễn lê Phú Hưng	MSSV: 46.01.104.060
Huỳnh Đăng Phong	MSSV: 46.01.104.037

Thành Phố Hồ Chí Minh, ngày 18 tháng 5 năm 2021

TRƯỜNG ĐẠI HỌC SƯ PHẠM THÀNH PHỐ HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

----- ☙ 🕮 ❧ -----

ĐỒ ÁN MÔN HỌC

ĐỀ TÀI: SECURITY TEST TOOL NETSPAKER

Giáo viên hướng dẫn: TS. Trần Sơn Hải

LỜI CẢM ƠN

Đầu tiên, chúng em xin gửi lời cảm ơn sâu sắc đến Trường Đại học Sư Phạm TP Hồ Chí Minh đã đưa bộ môn *Kiểm thử phần mềm nâng cao* vào chương trình giảng dạy. Đặc biệt, chúng em xin bày tỏ lòng biết ơn sâu sắc đến giảng viên bộ môn - Thầy Trần Sơn Hải. Chính thầy là người đã tận tình dạy dỗ và truyền đạt những kiến thức quý báu cho chúng em trong suốt học kỳ vừa qua. Trong thời gian tham dự lớp học của thầy Trần Sơn Hải, chúng em đã được tiếp cận với nhiều kiến thức bổ ích và rất cần thiết cho quá trình học tập, làm việc sau này của chúng em. Bộ môn *Kiểm thử phần mềm nâng cao* là một môn học thú vị và vô cùng bổ ích. Tuy nhiên, những kiến thức và kỹ năng về môn học này của chúng em vẫn còn nhiều hạn chế. Do đó, bài làm của chúng em khó tránh khỏi những sai sót. Kính mong thầy Trần Sơn Hải xem xét và góp ý giúp bài nhóm của chúng em được hoàn thiện hơn. Chúng em xin chân thành cảm ơn!

TP Hồ Chí Minh, tháng 05/2023

Sinh Viên

Nguyễn Lê Phú Hưng

Huỳnh Thị Yến Khoa

Võ Thị Hồng Diễm

Huỳnh Đăng Phong

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ BIỂU ĐỒ

MỞ ĐẦU

Ngày nay, với sự phát triển mạnh mẽ của Internet, ngày càng nhiều tổ chức cá nhân sử dụng thông tin của mình để giới thiệu, quảng bá cũng như thực hiện các giao dịch trực tuyến ngày càng nhiều. Không ít kẻ xấu đã lợi dụng những lỗ hổng trên trang web để đánh cắp thông tin người dùng, đem đến nhiều hệ quả khác nhau. Tình trạng an toàn thông tin mạng trên toàn thế giới đang đối mặt với nhiều thách thức và nguy cơ từ các hoạt động tấn công mạng ngày càng tinh vi phức tạp. Những lỗi có mặt ở trên các web hầu hết là do có người cố tình phá hoại nhằm mục đích xấu.

Vì vậy những công cụ phát hiện lỗ hỏng bảo mật được ra đời cho phép ta thực hiện kiểm tra lỗi trước khi đưa sản phẩm đến người dùng cuối và fix lại những lỗ hổng đó để bảo mật an toàn thông tin trên mạng cho người dùng. Chính vì vậy nhóm em đã tìm hiểu và chọn đề tài" Tìm hiểu công cụ kiểm thử Netspaker". Mục tiêu mà đồ án chúng em hướng đến là tìm hiểu, nghiên cứu sử dụng netspaker để tìm ra các lỗ hỏng bảo mật và các giải pháp để đưa ra phương án tốt nhất cho hệ thống mạng của các nhà phát triển.

Đồ án gồm 3 chương:

Chương 1: Tổng quan về bảo mật mạng

Chương 2: Tổng quan về Netspaker

Chương 3: Cài đặt và thực nghiệm

Chương 4: Kết luận

CHƯƠNG I: TỔNG QUAN VỀ BẢO MẬT MẠNG

1. Các khái niệm cơ bản về bảo mật

Bảo mật mạng là tập hợp các công cụ, chính sách, khái niệm về bảo mật, hướng dẫn, phương pháp quản lý rủi ro, phản ứng, đào tạo, diễn tập, thiết bị và công nghệ có thể được dùng để bảo vệ hệ thống mạng và tài ản (Theo như tiêu chuẩn của Liên minh Viện thông tin Quốc tế (ITU)).

Bảo mật thông tin là bảo vệ thông tin dữ liệu cá nhân, tổ chức nhằm tránh khỏi sự" đánh cắp, ăn cắp" bởi những kẻ xấu hoặc tin tặc. An ninh thông tin cũng như sự bảo mật an toàn thông tin nói chung. Việc bảo mật tốt những dữ liệu và thông tin sẽ tránh những rủi ro không đáng có cho chính cá nhân và doanh nghiệp của bạn.

Vấn đề an toàn và bảo mật thông tin phải đảm bảo những yếu tố chủ yếu sau:

– Tính bảo mật: Đảm bảo thông tin đó là duy nhất, những người muốn tiếp cận phải được phân quyền truy cập.

– Tính toàn vẹn. Bảo vệ sự hoàn chỉnh toàn diện cho hệ thống thông tin.

– Tính chính xác. Thông tin đưa ra phải chính xác, đầy đủ, không được sai lệch hay không được vi phạm bản quyền nội dung.

– Tính sẵn sàng. Việc ***bảo mật thông tin*** luôn phải sẵn sàng, có thể thực hiện bất cứ đâu, bất cứ khi nào.

2. Các loại lỗ hỗng bảo mật

Lỗ hỏng bảo mật là một điểm yếu có thể bị khai thác bởi một tác nhân xấu để thực hiện một cuộc tấn công mạng nhằm mục đích thực hiện các hành vi phi pháp lên hệ thống mục tiêu. Lỗ hổng của hệ thống thông tin rất đa dạng và có thể do nhiều nguyên nhân khác nhau, có thể phát sinh từ những yếu tố về kỹ thuật, cũng có thể do các yếu tố về tổ chức và quản lý như: thiếu kinh nghiệm hoặc khiếm khuyết trong các biện

pháp bảo vệ thông tin. Do vậy, có khá nhiều phương pháp phân loại lỗ hổng của hệ thống thông tin.

Lỡ hỏng bảo mật có thể phân loại theo nhiều cách khác nhau. Tuy nhiên phân loại chung nhất có thể chia làm ba loại chính:

Lỗ hỏng phân quyền: Lỗ hỏng phân quyền là lỗ hỏng liên quan đến việc kiểm soát quyền truy cập và phân quyền trong hệ thống. Những lỗ hỏng này cho phép kẻ tấn công có thể xâm nhập vào hệ thống và truy cập vào các thông tin hoặc chức năng mà họ không được phép sử dụng.

Lỗ hỏng xác thực và phiên: Lỗ hỏng xác thực và phiên liên quan đến việc kiểm soát quá trình đăng nhập và xác thực trong hệ thống. Những lỗ hỏng này cho phép kẻ tấn công đánh cắp thông tin đăng nhập của người dùng hoặc sử dụng các phiên đăng nhập đã được xác thực để truy cập vào hệ thống một cách trái phép.

3. Một số phương thức tấn công mạng

Tấn công mạng (cyber attack) là cuộc tấn công trái phép đối với các tài sản digital bên trong mạng của 1 tổ chức do tội phạm mạng (hacker) thực hiện bằng cách sử dụng một hoặc nhiều máy tính chống lại một hoặc nhiều máy tính hoặc mạng. Một cuộc tấn công mạng có thể vô hiệu hóa máy tính, đánh cắp dữ liệu nhằm đặt được các mục tiêu khác nhau mang đến nhiều nguy hiểm và các mối đe dọa vô cùng lớn.

Cụm từ "Tấn công mạng" có 2 nghĩa hiểu:

Hiểu theo cách tích cực (positive way): Tấn công mạng (penetrationtesting) là phương pháp Hacker mũ trắng xâm nhập vào một hệ thống mạng, thiết bị, website để tìm ra những lỗ hổng, các nguy cơ tấn công nhằm bảo vệ cá nhân hoặc tổ chức.

Hiểu theo cách tiêu cực (Negative way): Tấn công mạng (networkattack) là hình thức, kỹ thuật Hacker mũ đen tấn công vào một hệ thống để thay đổi đối tượng hoặc tống tiền.

Các đối tượng phổ biến bị tấn công mạng là các cá nhân, doanh nghiệp tư nhân và tổ chức chính phủ hoặc phi chính phủ. Các hacker sẽ tiếp cận nhưng đối tượng này qua mạng nội bộ như máy tính hay thiết bị điện tử, hoặc tiếp cận qua con người nhờ các

thiết bị di động, mạng social và các ứng dụng phần mềm nhằm đe dọa, làm ảnh hưởng tới đời sống, tinh thần của cá nhân hoặc đe dọa đến các thông tin nội bộ làm ảnh hưởng đến hiệu quả hoạt động của doanh nghiệp.

Có 6 hình thức điển hình mà hacker sử dụng để tấn công, tìm ra lỗ hổng đó là:

3.1 Tấn công bằng phần mềm độc hại (malware)

Đây là một trong những hình thức tấn công mạng điển hình nhất những năm gần đây. Các phần mềm đọc hại này bao gồm: spyware (phần mềm gián điệp), ransomeware (mã độc tống tiền), virus và worm (phần mềm độc hại có khả năng lây lan với tốc độ chóng mặt). Thông thường, các tin tặc sẽ tiến hành tấn công người dùng qua các lỗ hổng bảo mật hoặc lừa người dùng click vào một đường link hoặc email để cài đặt phần mềm độc hại vào thiết bị nhằm xâm nhập và tấn công hệ thống.

Một khi đã được cài đặt thành công, thì malware sẽ gây ra những hậu quả nghiêm trọng sau:

- Chặn người dùng truy cập vào hệ thống mạng và các file hoặc folder nhất định.
- Theo dõi hành động của người dùng và đánh cắp dữ liệu.
- Cài đặt thêm các phần mềm độc hại khác vào máy tính người dùng.
- Phá hoại phần cứng, phần mềm làm hệ thống bị ngưng trệ, không thể hoạt động.

Hình 3.1: minh họa phương thức tấn công bằng phần mềm độc hại

3.2 Tấn công giả mạo (phishing)

Phishing là hình thức tấn công mạng bằng cách tin tặc giả mạo thành một tổ chức hoặc cá nhân uy tín để lấy lòng tin của người dùng và yêu cầu họ cung cấp thông tin cá nhân cho chúng nhằm đánh cắp các dữ liệu nhạy cảm như tài khoản ngân hàng, thẻ tín dụng, ...

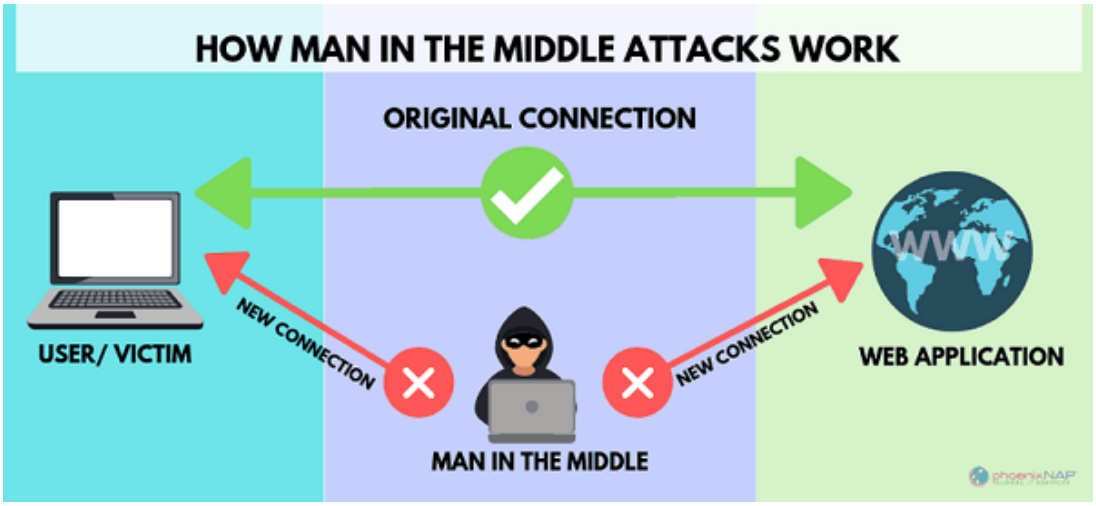
Các cuộc tấn công giả mạo này thường được thực hiện qua tin nhắn SMS hoặc email. Cụ thể là, các Hacker sẽ giả mạo là ngân hàng, ví điện tử, website giao dịch trực tuyến hoặc các công ty thẻ tín dụng uy tín với các thông điệp vô dùng khẩn thiết để người dùng click vào một đường link do tin tặc tạo ra. Khi click vào đường link đó, người dùng sẽ được chuyển đến 1 website giả mạo yêu cầu người dùng đăng nhập, lừa người dùng chia sẻ các thông tin cá nhân như: tài khoản, mật khẩu đăng nhập, mật khẩu giao dịch, thẻ tín dụng và các thông tin quan trọng khác. Khi đó, tin tặc sẽ dễ dàng có được thông tin cá nhân và dữ liệu nhạy cảm của người dùng.

Mục đích của hình thức tấn công này là đánh cắp các dữ liệu quan trọng như thông tin ngân hàng, thẻ tín dụng, mật khẩu của người dùng. Đôi khi, phishing là một công đoạn trong một cuộc tấn công malware bằng cách tấn công phishing để lừa người dùng cài đặt phần mềm độc hại vào thiết bị.

Hình 3.2: minh họa phương thức tấn công giả mạo

3.3 Tấn công trung gian (man – in the – middle – attack)

Tấn công trung gian (MitM), hay còn gọi là tân công nghe lén, là hình thức tin tặc xen vào giữa phiên giao dịch hay giao tiếp giữa 2 đối tượng. Một khi xâm nhập thành công, chúng có thể theo dõi được mọi hành vi của người dùng, đánh cắp được toàn bộ dữ liệu trong giao dịch đó. Hình thức tấn công này dễ xảy ra khi nạn nhân truy cập vào một mạng wifi không an toàn.



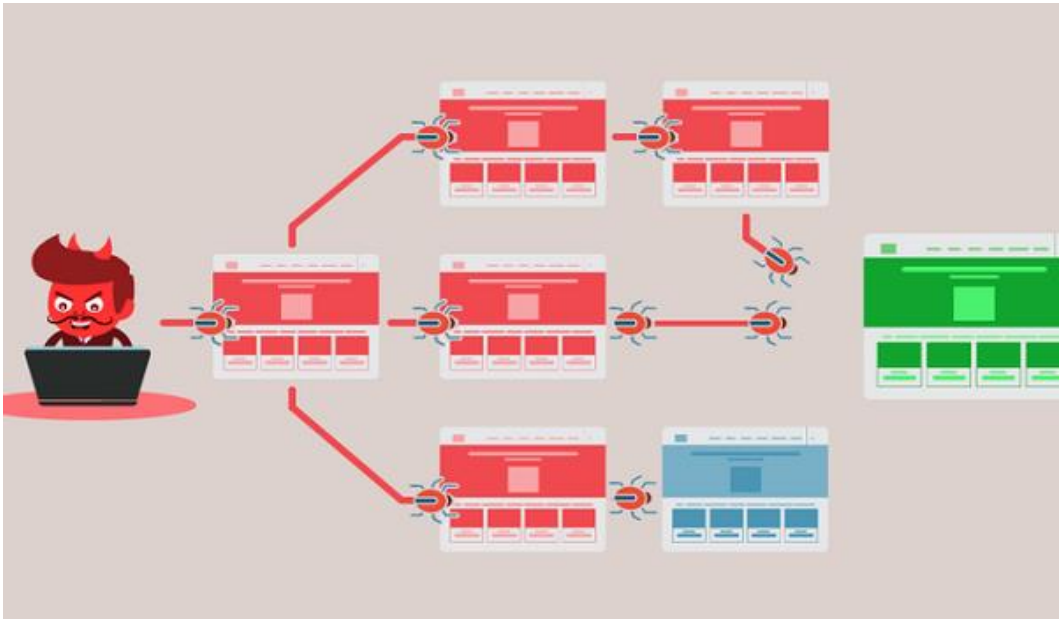
Hình 3.3: minh họa tấn công phương thức tấn công trung gian

3.4 Tấn công từ chối dịch vụ (DoS & DDoS)

DoS (Denial of Service) là hình thức tấn công mà hacker đánh sập tạm thời một hệ thống máy chủ hoặc mạng nội bộ bằng cách tạo ra một lượng Trafic/Request khổng lồ ở cùng một thời điểm làm cho hệ thống bị quá tải khiến người dùng không thể truy cập vào dịch vụ trong khoảng thời gian mà cuộc tấn công DoS diễn ra.

Bên cạnh đó, DoS cũng có một hình thức biến thể đó là DDoS (Distributed Denial of Service). Đây là hình thức tấn công mạng mà tin tặc sử dụng một mạng lưới các máy tính để tấn công người dùng tuy nhiên điều đặc biệt ở hình thức tấn công này là chính các máy tính thuộc mạng lưới máy tính này cũng không biết bản thân đang bị lợi dụng trở thành công cụ tấn công.

Một số hình thức tấn công DDoS như: tấn công gây nghẽn mạng (UDP Flood và Ping Flood), tấn công SYN flood (TCP), tấn công khuếch đại DNS.

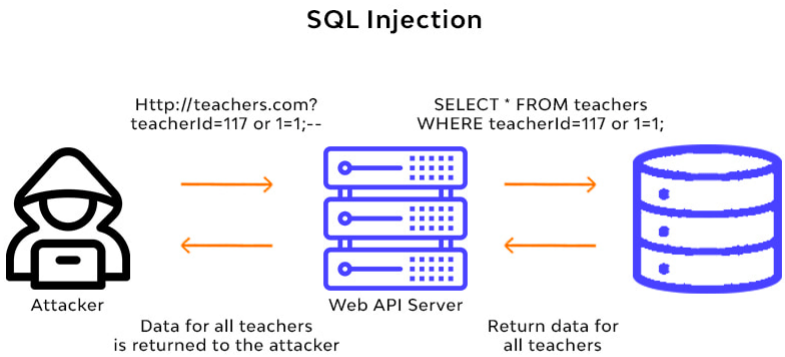


Hình 3.4: minh họa phương thức tấn công từ chối dịch vụ

3.5 Tấn công cơ sở dữ liệu (SQL Injection)

Tấn công cơ sở dữ liệu là hình thức tấn công mà để đánh cắp những tài liệu quan trọng, hacker sẽ chèn một đoạn mã độc hại vào server sửa dụng ngôn ngữ SQL.

Hậu quả lớn nhất của hình thức tấn công này chính là làm lộ dữ liệu trong database - một điều đặc biệt tối kị vì chúng sẽ làm ảnh hưởng vô cùng nặng nề đến uy tín của các doanh nghiệp bị hại bởi sẽ khiến khách hàng mất niềm tin vào doanh nghiệp, họ sẽ ngừng sử dụng dịch vụ của doanh nghiệp đó và chuyển sang sử dụng dịch vụ của bên khác. Điều đó sẽ dẫn đến việc doanh số giảm sút, đây là hậu quả đầu tiên mà doanh nghiệp phải gánh chịu.



Hình 3.5: minh họa phương thức tấn công cơ sở dữ liệu

3.6 khai thác lỗ hổng Zero Day (Zero Day Attack)

Lỗ hổng Zero Day là (0-day Vulnerability) thực chất là những lỗ hổng của phần mềm hoặc phần cứng mà chưa được các nhà phát triển phần mềm biết tới. Chúng tồn tại trong nhiều môi trường khác nhau như Website, Mobile Apps, hệ thống mạng doanh nghiệp, phần mềm- phần cứng máy tính, thiết bị IoT, cloud, ... Thông thường khi phát hiện ra lỗ hổng này, bên cung cấp sản phẩm sẽ tung ra bản vá bảo mật cho lỗ hổng để người dùng được bảo mật tốt hơn. Vì vậy chưa có bản vá chính thức cho lỗ hổng 0-day. Có thể nói, các vụ tấn công Zero Day xảy ra một cách bất ngờ mà các nhà phát triển phần mềm không thể dự liệu trước. Đó là lí do Zero Day được coi là những lỗ hổng cực kì nguy hiểm, gây thiệt hại vô cùng nghiêm trọng cho doanh nghiệp và người dùng. Một khi được công bố rộng rãi ra công chúng, 0-day sẽ trở thành lỗ hổng n-day.

Hình 3.6: minh họa phương thức Lỗ hổng Zero Day

4. Các giải pháp và công cụ hỗ trợ bảo mật mạng

Với việc Internet và con người đang gần nhau, việc mà mỗi tổ chức, cá nhân cần làm là cần có những giải pháp và những công cụ để đảm bảo an toàn cho việc bảo mật thông tin. Sau đây sẽ là những giải pháp và một số công cụ hữu ích.

4.1 các giải pháp bảo mật mạng

Trong thời đại ngày nay có rất nhiều phương pháp bảo mật an ninh mạng. Nhiều công ty lớn đã đưa ra nhưng giải pháp, công cụ, … để có thể bảo mật thông tin, chống đánh cắp dữ liệu, xâm nhập tài nguyên mạng, …

Dưới đây là nhưng giải pháp có chất lượng uy tín hàng đầu, được các chuyên gia trên toàn thế giới khuyên dùng.

- Giải pháp tường lửa:

Lợi ích: bảo vệ cổng hệ thống (gateway), ngăn chặn các rủi ro từ môi trường internet.

Tính năng:

- Lọc web
- Chống xâm nhập (IPS)
- Chống DdoS
- Chống virus, spam
- Lọc các cổng dịch vụ
- Giám sát ứng dụng và người dùng

- Giải pháp chống xâm nhập và chống tấn công từ chối dịch vụ(DDoS)

Lợi ích: thiết bị chuyên dụng ngăn chặn hình thức tấn công DDoS.

Tính năng:

- Ngăn chặn các hình thức xâm nhập
- SSL offload
- Chống tấn công DdoS

- Giải pháp mã hóa và bảo mật đường truyền

Lợi ích: giải pháp chuyên dụng bảo vệ kết nối giữa các site trong cùng một hệ thống, đặc biệt phù hợp với các doanh nghiệp có nhiều chi nhánh và yêu cầu bảo mật cao trên đường truyền.

Tính năng:

- Mã hóa từ mức layer 2 (theo mô hình OSI), hỗ trợ các giao thức Ethernet, Fibre Channel/FICON và SDH/SONET từ 20Mbps đến10Gbps
- Mã hóa cuộc gọi/ voice
- Mã hóa đường truyền fax

- Giải pháp giám sát và phân tích mã độc

Lợi ích: xác định các loại mã độc đang hiện hữu trên hệ thống, tích hợp các giải pháp mức gateway ngăn chặn mã độc xâm hại trên hệ thống

Tính năng:

- Phát hiện và chống lại APTs và các tấn công có mục tiêu Zero-daymalware và các khai thác lỗ hổng trên document
- Các hành vi tấn công mạng
- Email threats (phishing, spear-phishing): Bots, Trojans, Worms, Key Loggers and Crime ware
- Giám sát thời gian thực, phân tích sâu dựa trên giao diện điều khiển trực quan
- Giám sát tập trung vào các nguy cơ có mức độ nghiêm trọng cao và các đối tượng có giá trị
- Cung cấp các thông tin về an ninh hệ thống, và đưa ra các biện pháp khắc phục

4.2 Các công cụ hỗ trợ

CyStack Web Security

CyStack Web Security là công cụ quét lỗ hổng website, web server miễn phí được phát triển bởi CyStack. Hệ thống được tích hợp những công nghệ mới nhất về Plugins & Web fuzzing. Giúp cho việc kiểm tra bảo mật website và server trở nên dễ dàng. Phần mềm hoạt động hoàn toàn online và miễn phí.

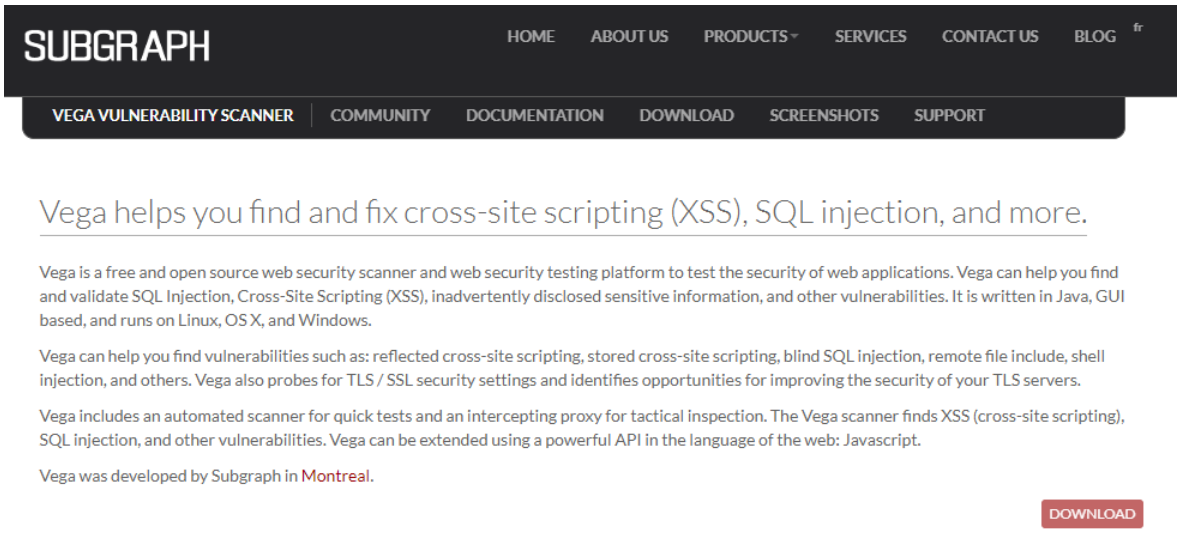
Ưu điểm:

- Quét lỗ hổng bảo mật cho website và cả server
- Sử dụng chung công nghệ với phần mềm Premium (trả phí) của CyStack là Cloud Security.
- Cơ sở dữ liệu được cập nhật thường xuyên, giúp bảo vệ website khỏi những rủi ro mới nhất
- Hoạt động online, không cần cài đặt
- Dễ sử dụng

Nhược điểm:

- Giới hạn 2 lượt quét miễn phí/ngày

Các bước sử dụng: Nhập website > Xác minh chủ sở hữu > Nhập email và đợi kết quả trả về khi quét xong.



Hình 4.1 phần mềm CyStack Web Security

Vega giúp tìm và khắc phục lỗ hổng XSS, SQLi.

Vega là một phần mềm scan lỗ hổng website trên nền Java hỗ trợ Windows, Linux và OS X. Công cụ miễn phí và mã nguồn mở này cho phép bạn tìm và sửa lỗi chèn SQL, XSS và rò rỉ thông tin nhạy cảm.

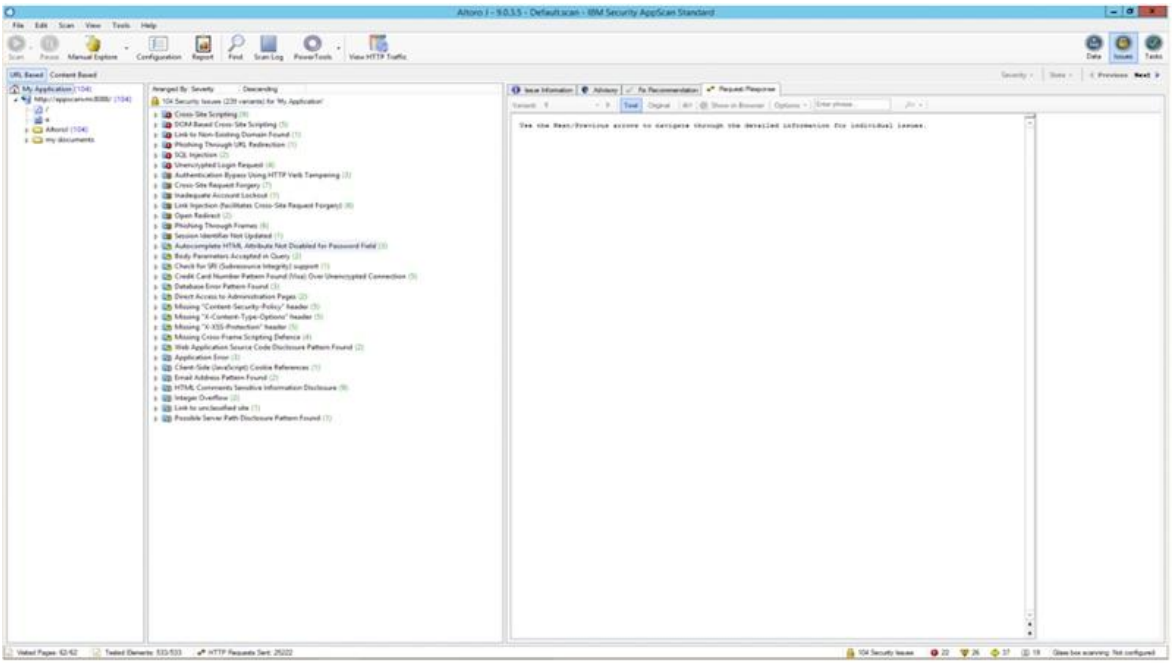
Các tính năng & ưu điểm:

- Crawl và quét lỗ hổng tự động
- Proxy trung gian
- Hỗ trợ module API JavaScript
- Chia sẻ cơ sở dữ liệu
- Phân tích nội dung

Nhược điểm:

- Không có tiếng Việt
- Không thể sử dụng online.
- Công cụ khó sử dụng, chỉ phù hợp với các kĩ thuật viên có kiến thức bảo mật.

IBM Security AppScan Standard



Hình 4.2: phần mềm IBM Security AppScan Standard

Một trong những phần mềm scan lỗ hổng website được tin dùng nhất là IBM Security AppScan, được phát hành bởi IBM – tập đoàn về máy tính có tuổi đời lớn nhất thế giới. Security AppScan có 2 phiên bản: Standard (dành cho doanh nghiệp vừa và nhỏ) & Enterprise (dành cho các tập đoàn lớn).

Các chức năng chính:

- Cung cấp kiến thức về bảo mật ứng dụng web
- Scan ứng dụng web & mobile app để tìm lỗ hổng
- Test Whitebox và blackbox
- Đề xuất phương án khắc phục
- Xuất báo cáo riêng theo đặc trưng từng ngành

Ưu điểm:

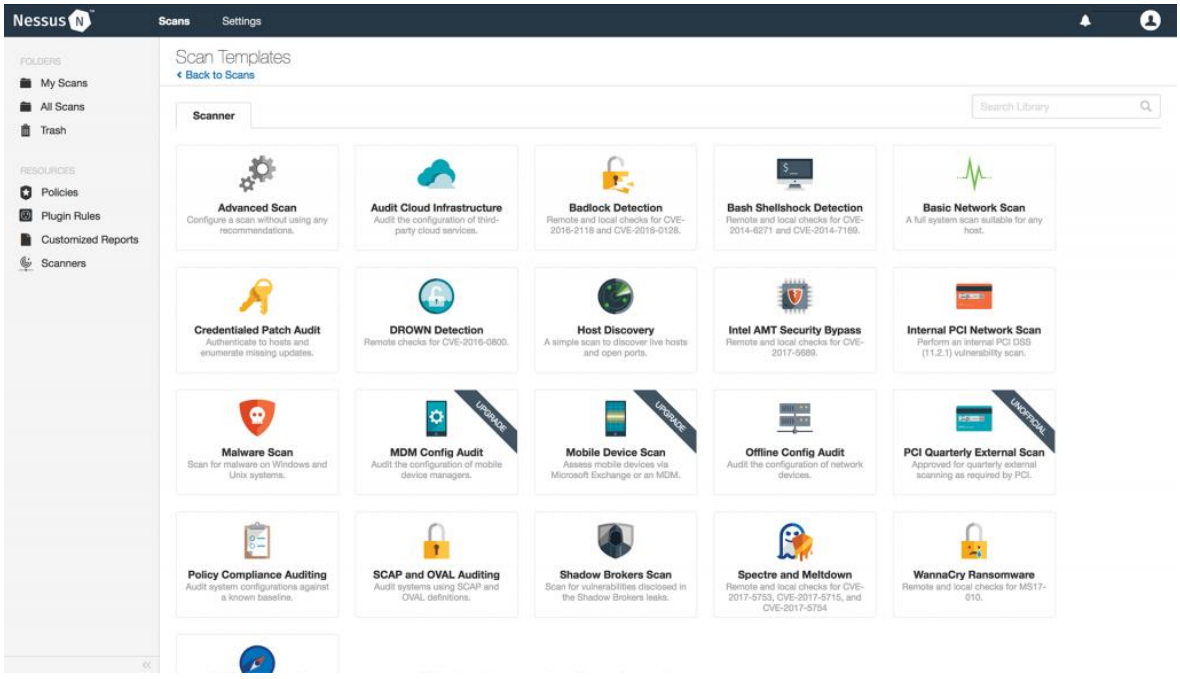
- Dùng thử miễn phí
- Giao diện tối giản, trình bày khoa học
- Cung cấp kiến thức cần thiết cho người dùng (miễn phí)
- Phát hiện được nhiều loại lỗ hổng khác nhau như: Cross-site scripting, SQL Injection, Command Injection, Path Traversal, etc.

- Xuất báo cáo đặc trưng theo từng ngành cụ thể
- Hỗ trợ 24/7

Nhược điểm:

- Thủ tục download và sử dụng phần mềm tương đối phức tạp và tốn thời gian, do luật liên bang về xuất khẩu phần mềm ngặt nghèo của Mỹ.
- Không hỗ trợ tiếng Việt. Dù dịch vụ khách hàng của IBM phục vụ 24/7 nhưng rào cản ngôn ngữ vẫn gây trở ngại phần nào cho người dùng Việt.
- Chỉ hỗ trợ HĐH Windows.
- Giá cao. Khởi điểm từ 11,000 USD/năm đối với bản Standard và 33,400 USD/năm đối với phiên bản Enterprise.

Nessus Pro

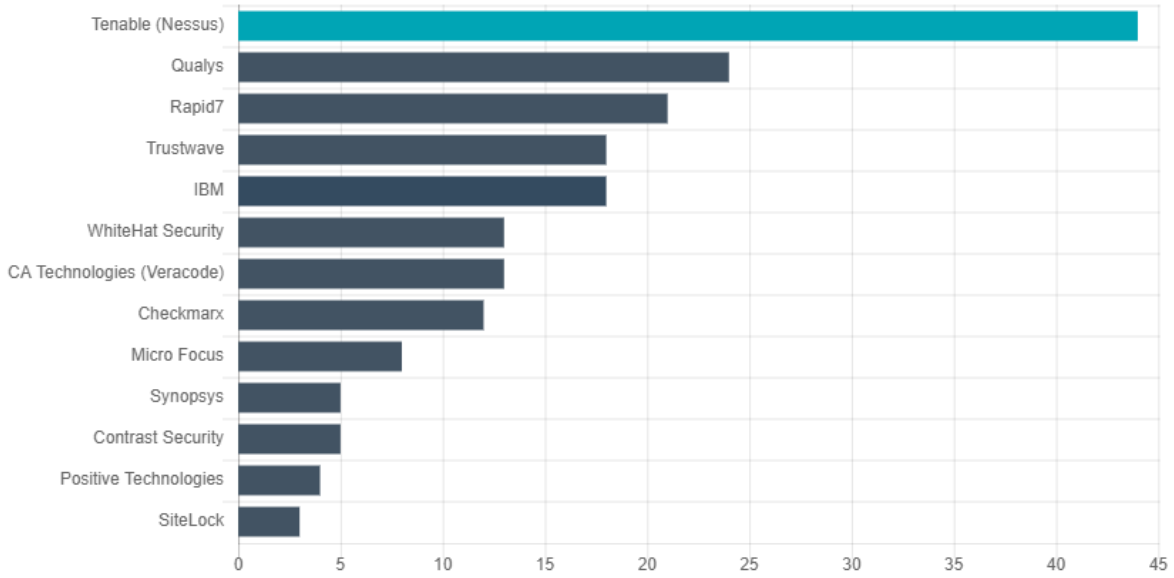


Hình 4.3: phần mềm Nessus Pro

Các tính năng của Nessus Pr

Nessus Pro được phát triển bởi Tenable – công ty bảo mật có bề dày lịch sử và đã phục vụ hơn 50% các tập đoàn thuộc danh sách Fortune 500, bao gồm Microsoft, Amazon, PayPal, Starbucks, và cả IBM. Nessus Pro được Gartner bình chọn là phần

mềm bảo mật được yêu thích nhất thế giới (Tháng 3, 2019) với lượng khách hàng cực khủng lên tới 27,000 doanh nghiệp trên toàn cầu.



Hình 4.4: Đánh giá độ hiệu quả của các phần mềm bảo mật

Nguồn: Tenable

Tính năng chính của Nessus Pro:

- Phát hiện các lỗ hổng Website theo tiêu chuẩn OWASP & đưa ra biện pháp khắc phục.
- Phát hiện điểm yếu trên Mobile app Android, iOS, Window phone; các thiệt bị IoT: máy tin, switch, router, …
- Hỗ trợ kiểm tra bản vá hệ điều hành, trình duyệt web, phần mềm
- Cung cấp tiện ích plugin hỗ trợ người dùng tối đa.
- Tự động quét theo lịch cố định
- Phát hiện phần mềm độc hại, malware

Ưu điểm:

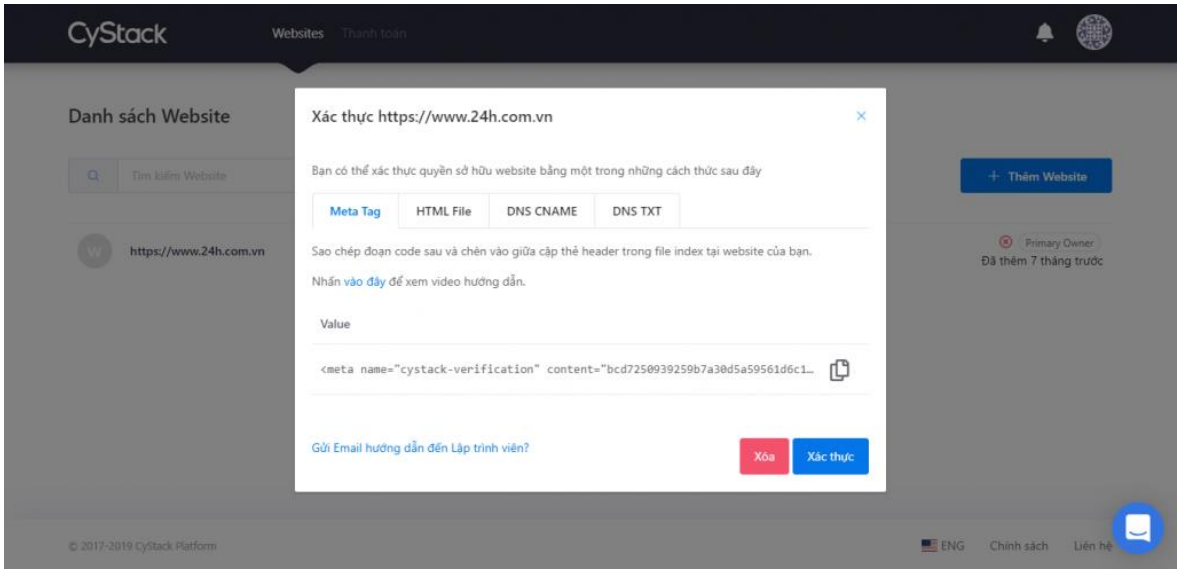
- Dùng được cho cả hệ thống vận hành, các thiết bị IoT và ứng dụng (web, mobile app)
- Giao diện trực quan, khoa học
- Nhiều plugin hỗ trợ, cập nhật thường xuyên
- Hỗ trợ HĐH Windows, Linux, Mac

- Giá từ 2190 USD/năm

Nhược điểm:

- Không hỗ trợ tiếng Việt
- Phần mềm rất nặng, chiếm lượng lớn tài nguyên hệ thống

CyStack Web Security (Premium)



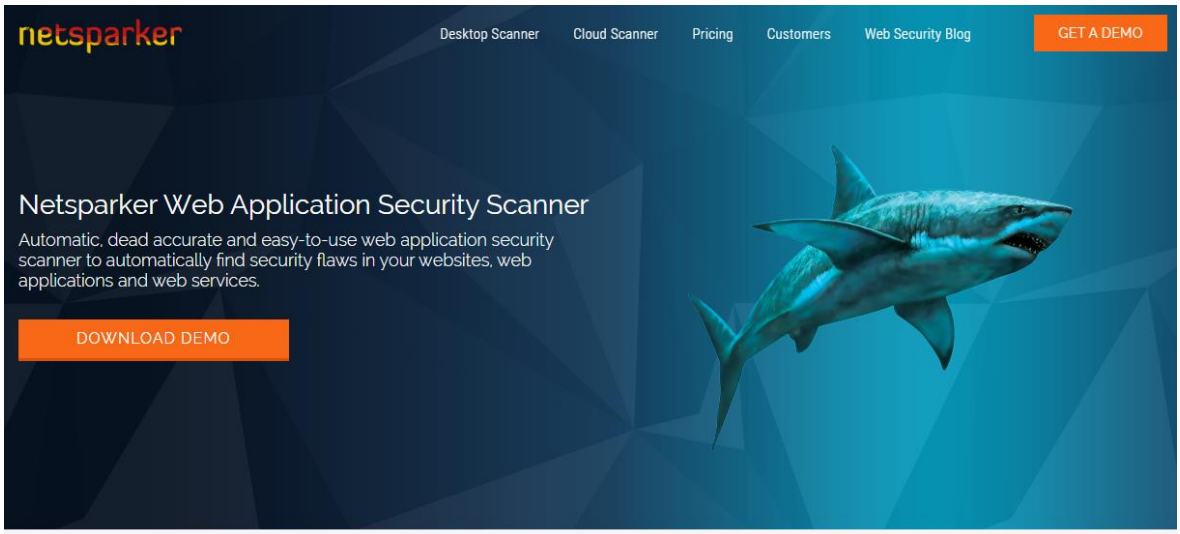
Hình 4.5: phần mềm CyStack Web Security (Premium)

CyStack Web Security là phần mềm giúp bảo vệ website, máy chủ, và các dịch vụ đám mây. Phần mềm được phát triển bởi CyStack Security – một trong những công ty tiên phong tại Việt Nam trong lĩnh vực an ninh mạng & cung cấp các giải pháp an toàn thông tin cho doanh nghiệp. Sản phẩm tích hợp những ưu điểm như công nghệ Fuzzing tương tự Nesus Pro, là một SaaS chạy trên môi trường đám mây, và có giá cả phù hợp với các doanh nghiệp Việt.

Tính năng:

- Scan lỗ hổng bảo mật của website, webserver bằng công nghệ fuzzing.
- Giám sát Uptime 24/7 và cảnh báo sự cố, tình trạng gián đoạn
- Cảnh báo các nguy cơ mất an toàn website.
- Phát hiện sớm tình trạng website bị hack, blacklisted.
- **Cloud Audit**: Kiểm tra an ninh cho hệ thống tài khoản dịch vụ cloud services.

Netsparker



Hình 4.6: phần mềm Netsparker

Phần mềm scan lỗ hổng website này có thể tìm cũng như kiểm thử các lỗ hổng và chỉ báo về các lỗ hổng đã được kiểm thử hoặc kiểm tra cẩn thận. Những mối nguy hiểm như chèn SQL và XSS đều được nhận diện và báo lại với người chủ sở hữu website.

Phiên bản cộng đồng được cung cấp miễn phí cho người dùng Windows. Với người mới bắt đầu, đây là điểm xuất phát lý tưởng để bắt đầu bảo mật cho website.

Nhược điểm:

- Không hỗ trợ Tiếng Việt
- Bạn chỉ có thể download bản DEMO bằng địa chỉ email công ty có dịch vụ G-suite. VD: abc@cystack.net
- Bản DEMO khá hạn chế tính năng.
- Không có hotline hỗ trợ 24/7

CHƯƠNG II: TỔNG QUAN VỀ NETSPARKER

1. Giới thiệu về Netsparker

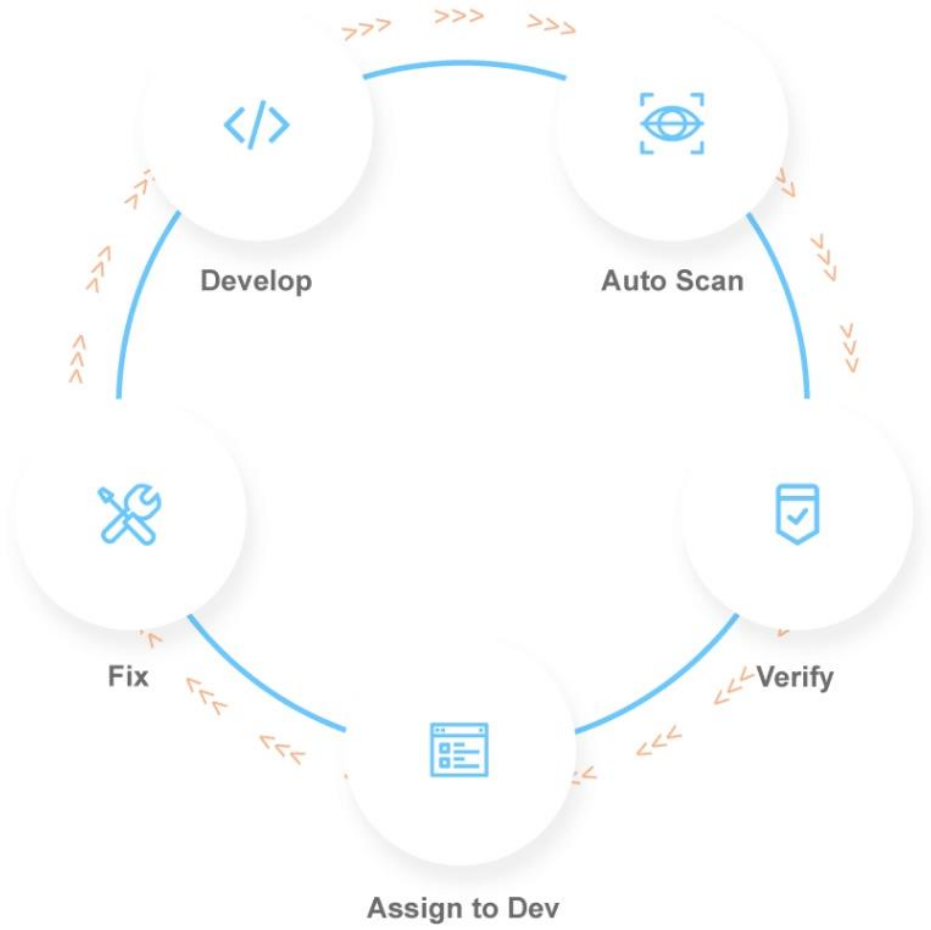
Hình 1.1: Netsparker

Netsparker là một công cụ kiểm thử bảo mật mạng dành cho ứng dụng web. Mục đích của báo cáo này là cung cấp cho độc giả các thông tin chi tiết về công cụ Netsparker, bao gồm tính năng, phương pháp và kỹ thuật sử dụng để kiểm thử bảo mật ứng dụng web.

Các vấn đề mà Netsparker giải quyết là giúp các tổ chức và cá nhân kiểm tra bảo mật của ứng dụng web của họ, phát hiện các lỗ hổng bảo mật và giải quyết chúng trước khi bị tin tặc tấn công và gây thiệt hại cho hệ thống.

Đối tượng sử dụng công cụ này bao gồm các chuyên gia bảo mật, các nhà phát triển web, các nhà quản trị mạng và các tổ chức muốn đảm bảo rằng hệ thống và ứng dụng của họ đang hoạt động một cách an toàn và bảo mật. Báo cáo cũng có thể hữu ích cho các cá nhân hoặc tổ chức mới bắt đầu tìm hiểu về kiểm thử bảo mật và đang tìm kiếm một công cụ đáng tin cậy để sử dụng.

2. Các tính năng chính của Netsparker



Hình 2.1: minh họa các tính năng của Netsparker

+ Phát hiện lỗ hổng bảo mật tự động: Netsparker tự động phát hiện các lỗ hổng bảo mật trong ứng dụng web của bạn, giảm thiểu sự can thiệp của con người và giúp tăng độ chính xác trong quá trình kiểm thử.

+ Hỗ trợ đa nền tảng: Netsparker hỗ trợ kiểm thử trên nhiều nền tảng, bao gồm Windows, Linux và macOS.

+ Tự động xác định các lỗ hổng bảo mật: Netsparker có khả năng xác định các lỗ hổng bảo mật từ các nguồn khác nhau và đưa ra đánh giá về mức độ nghiêm trọng của từng lỗ hổng.

+ Thân thiện với người dùng: Netsparker có giao diện đơn giản và dễ sử dụng, cho phép người dùng kiểm thử bảo mật một cách nhanh chóng và hiệu quả.

Tự động phát hiện các lỗ hổng OWASP Top 10: Netsparker tự động phát hiện các lỗ hổng bảo mật nằm trong danh sách OWASP Top 10, bao gồm XSS, SQL Injection và CSRF.

+Hỗ trợ kiểm thử cho các ứng dụng web động: Netsparker hỗ trợ kiểm thử bảo mật cho các ứng dụng web động, bao gồm các ứng dụng được viết bằng các ngôn ngữ lập trình như PHP, ASP.NET, Ruby on Rails và Node.js.

+ Báo cáo chi tiết và đầy đủ: Netsparker cung cấp báo cáo chi tiết về các lỗ hổng bảo mật đã phát hiện được và đưa ra các đề xuất giải pháp để khắc phục.

3. Cách sử dụng công cụ Netsparker

+Tải xuống và cài đặt Netsparker: Bạn có thể tải xuống phiên bản dùng thử hoặc mua bản quyền của Netsparker trên trang chủ của công cụ. Sau đó, bạn có thể cài đặt phần mềm trên máy tính của mình.

+Tạo một dự án mới: Bạn cần tạo một dự án mới để bắt đầu kiểm thử bảo mật trên ứng dụng web của mình. Bạn cần cung cấp các thông tin về địa chỉ URL của trang web cần kiểm thử và các thông tin khác cần thiết để Netsparker có thể phát hiện các lỗ hổng bảo mật.

+Bắt đầu kiểm thử bảo mật: Sau khi đã tạo dự án, bạn có thể bắt đầu kiểm thử bảo mật bằng cách nhấn vào nút "Scan" trên giao diện của Netsparker. Netsparker sẽ tự động phát hiện các lỗ hổng bảo mật trong ứng dụng web của bạn.

+Xem kết quả kiểm thử: Sau khi quá trình kiểm thử kết thúc, bạn có thể xem kết quả trên giao diện của Netsparker. Netsparker sẽ liệt kê các lỗ hổng bảo mật đã phát hiện được và đưa ra các đề xuất giải pháp để khắc phục.

+Tạo báo cáo: Bạn có thể tạo báo cáo chi tiết về các lỗ hổng bảo mật đã phát hiện được bằng cách sử dụng chức năng "Report" trên giao diện của Netsparker. Bạn có thể tùy chỉnh báo cáo và lưu nó dưới định dạng PDF hoặc HTML để chia sẻ với các thành viên trong đội ngũ phát triển của bạn.

4. Những lổ hổng bảo mật mà Netparker có thể phát hiện được

Hình 4.1: minh họa lỗ hổng bảo mật

+SQL Injection: Netsparker có thể phát hiện các lỗ hổng SQL Injection trên trang web, nơi mà tin tặc có thể chèn mã độc SQL vào trang web của bạn thông qua các biểu mẫu nhập liệu hoặc tham số truy vấn URL.

+XSS (Cross-Site Scripting): Netsparker có thể phát hiện các lỗ hổng XSS, nơi mà tin tặc có thể chèn mã độc JavaScript vào trang web của bạn thông qua các biểu mẫu nhập liệu hoặc các tham số truy vấn URL.

+Lỗ hổng đăng nhập: Netsparker có thể kiểm tra lỗ hổng đăng nhập bằng cách thử các tài khoản đăng nhập giả mạo hoặc thử các mật khẩu yếu.

+Lỗ hổng đường dẫn tệp: Netsparker có thể phát hiện các lỗ hổng đường dẫn tệp, nơi mà tin tặc có thể truy cập các tệp và thư mục trên máy chủ web của bạn thông qua các đường dẫn không được bảo vệ.

+Lỗ hổng xác thực: Netsparker có thể phát hiện các lỗ hổng xác thực, nơi mà tin tặc có thể tìm thấy các thông tin xác thực, chẳng hạn như mã thông báo truy cập hoặc tài khoản đăng nhập của người dùng.

+Lỗ hổng CSRF (Cross-Site Request Forgery): Netsparker có thể phát hiện các lỗ hổng CSRF, nơi mà tin tặc có thể thực hiện các hành động trên trang web của bạn bằng cách lừa đảo người dùng để thực hiện các hành động bất hợp pháp.

+Lỗ hổng điều hướng: Netsparker có thể phát hiện các lỗ hổng điều hướng, nơi mà tin tặc có thể điều hướng người dùng đến các trang web giả mạo hoặc các trang web độc hại.

5. Các phương pháp và kĩ thuật mà Netsparker sử dụng để kiểm thử bảo mật

+Scanner Engine: Netsparker sử dụng một công nghệ quét tự động để tìm kiếm các lỗ hổng bảo mật. Scanner engine này sử dụng một loạt các kỹ thuật quét, bao gồm quét tĩnh và động, để tìm kiếm các lỗ hổng bảo mật trên trang web.

+Fingerprinting: Netsparker sử dụng kỹ thuật fingerprinting để xác định công nghệ và phiên bản của các ứng dụng web được kiểm thử. Các thông tin này được sử dụng để tìm kiếm các lỗ hổng bảo mật cụ thể của các ứng dụng web đó.

+Crawl Engine: Netsparker sử dụng một công nghệ tìm kiếm để tìm kiếm các trang web được kết nối với các trang web chính để kiểm tra các lỗ hổng bảo mật liên quan đến các trang web đó.

+Exploitation: Netsparker sử dụng kỹ thuật exploitation để khai thác các lỗ hổng bảo mật được tìm thấy trong quá trình kiểm thử bảo mật, từ đó xác định mức độ nghiêm trọng của lỗ hổng và đưa ra các giải pháp khắc phục.

+Reporting: Netsparker cung cấp báo cáo chi tiết về các lỗ hổng bảo mật tìm thấy trong quá trình kiểm thử bảo mật, bao gồm mô tả chi tiết, danh sách các yêu cầu HTTP liên quan và các giải pháp khắc phục.

+Integration: Netsparker cung cấp khả năng tích hợp với các công cụ kiểm thử bảo mật khác như Burp Suite, Metasploit và Acunetix.

6. Ưu điểm và nhược điểm của Netsparker

-Ưu điểm:

+Tự động hóa: Netsparker là một công cụ tự động hoàn toàn, giúp giảm thiểu thời gian và chi phí cho các hoạt động kiểm thử bảo mật.

+Quét tĩnh và động: Netsparker sử dụng một loạt các phương pháp quét tĩnh và động để tìm kiếm các lỗ hổng bảo mật, bao gồm quét mã nguồn và kiểm thử động, giúp đảm bảo tính toàn vẹn của ứng dụng web.

+Tích hợp: Netsparker cung cấp khả năng tích hợp với các công cụ khác như Burp Suite, Metasploit và Acunetix.

+Báo cáo chi tiết: Netsparker cung cấp báo cáo chi tiết về các lỗ hổng bảo mật tìm thấy trong quá trình kiểm thử bảo mật, giúp người dùng dễ dàng hiểu được các lỗ hổng và đưa ra giải pháp khắc phục.

+Hỗ trợ nhiều nền tảng: Netsparker hỗ trợ kiểm thử bảo mật trên nhiều nền tảng, bao gồm Windows và Linux.

-Nhược điểm:

+Giá thành cao: Netsparker là một công cụ thương mại, giá thành cao hơn so với các công cụ kiểm thử bảo mật miễn phí hoặc giá rẻ hơn.

+Có thể tạo ra các false positive: Netsparker có thể tạo ra các false positive, do đó, người dùng cần phải xác nhận lại trước khi đưa ra các giải pháp khắc phục.

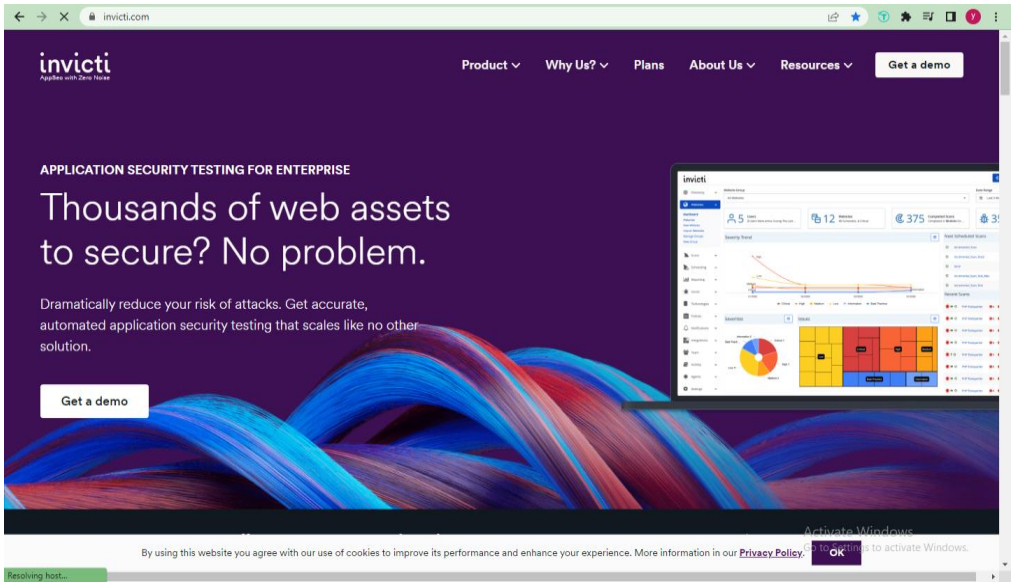
+Không phát hiện được một số lỗ hổng bảo mật: Netsparker không phát hiện được một số lỗ hổng bảo mật đặc biệt như lỗ hổng logic và lỗ hổng bảo mật do thiết kế không an toàn.

CHƯƠNG III: CÀI ĐẶT VÀ THỰC NGHIỆM

1. Cài đặt Netsparker

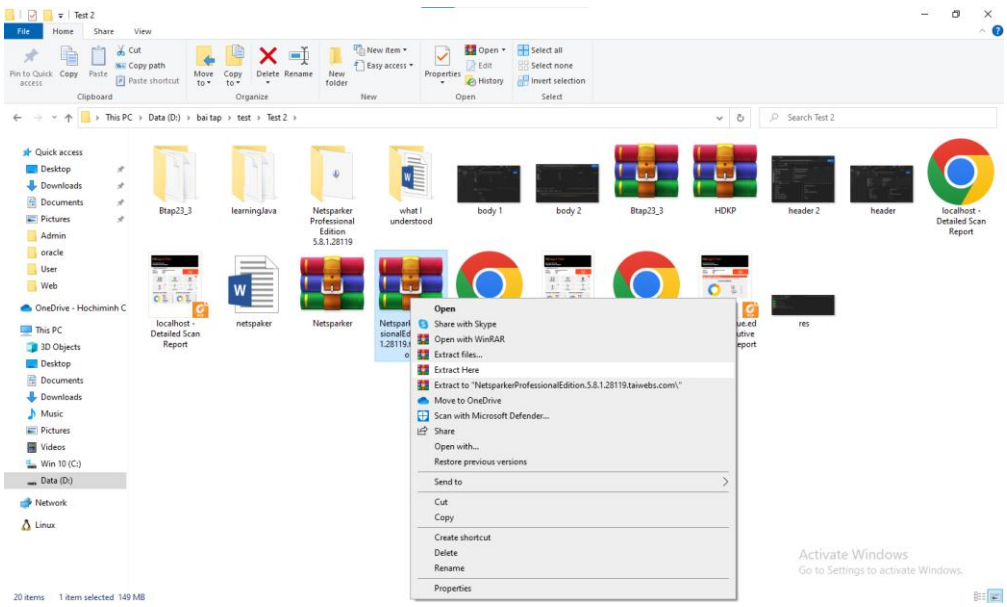
Người dùng có thể download Netsparker tại link

https://taiwebs.com/windows/download-netsparker-professional-edition 4969.html



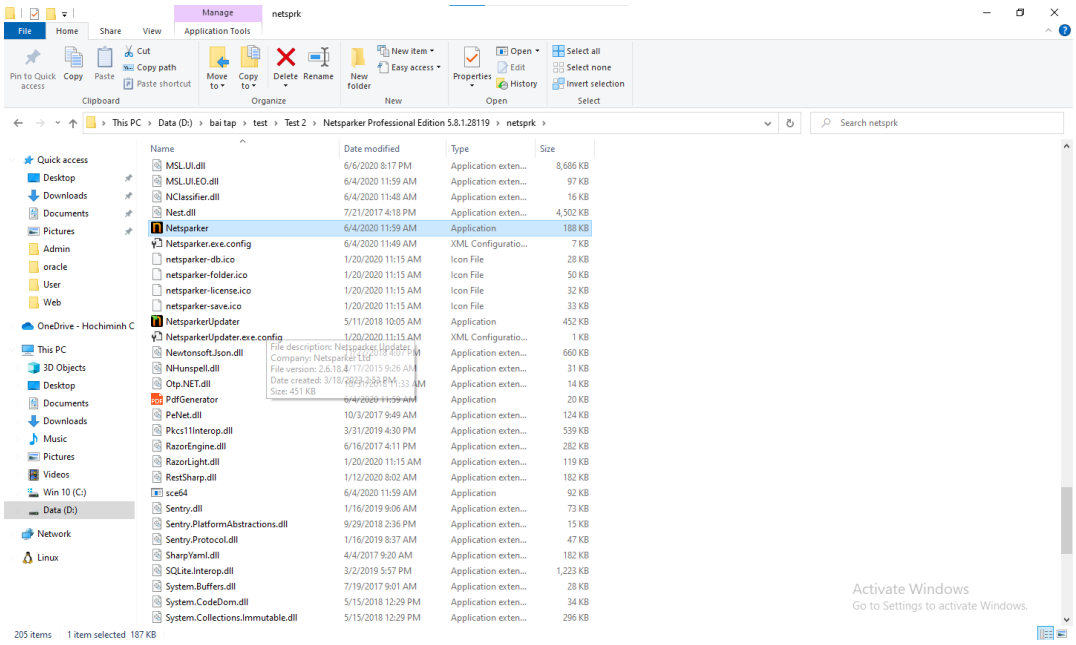
Hình 1.1: trang giới thiệu chính của Netsparker cho đến hiện tại

Sau đó tiến hành giải nén tập tin vừa tải:



Hình 1.2: giải nén tập tin Netsparker

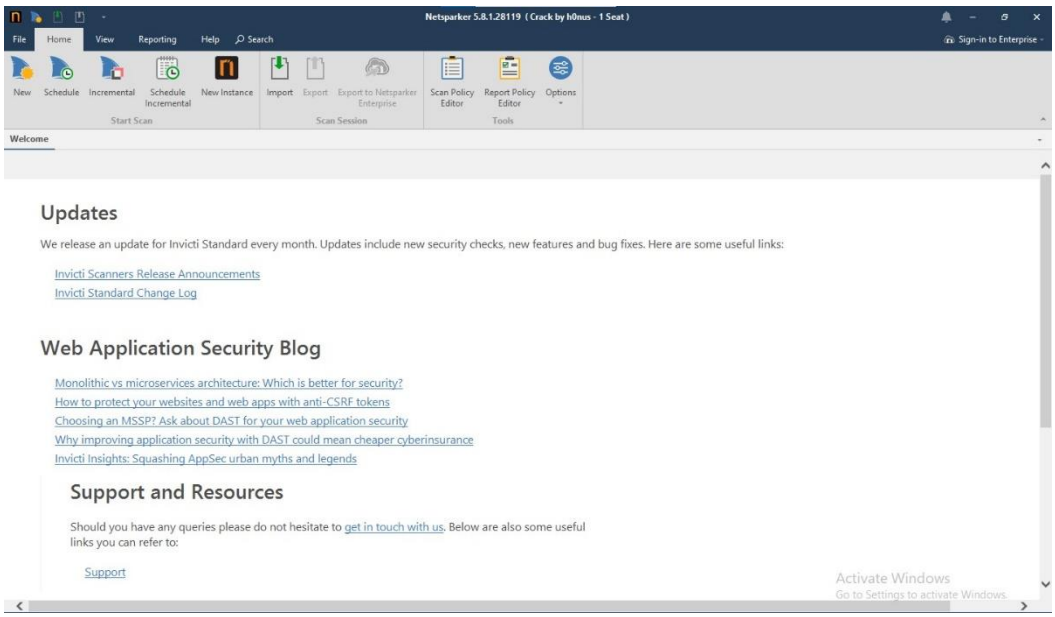
Sau khi giải nén thành công, vào folder đã giải nén tìm file netspaker để mở công cụ lên.



Hình 1.3: mở phần mềm Netsparker

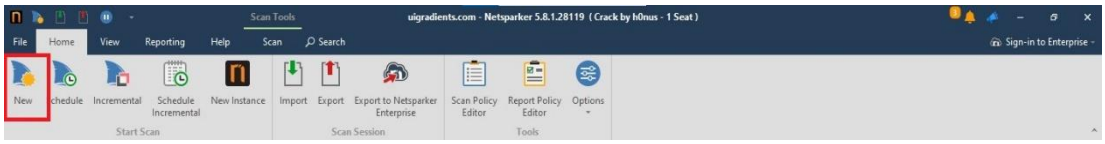
2. Thực nghiệm

Sau khi mở giao diện netspaker lên, tiến hành test một web ngẫu nhiên.



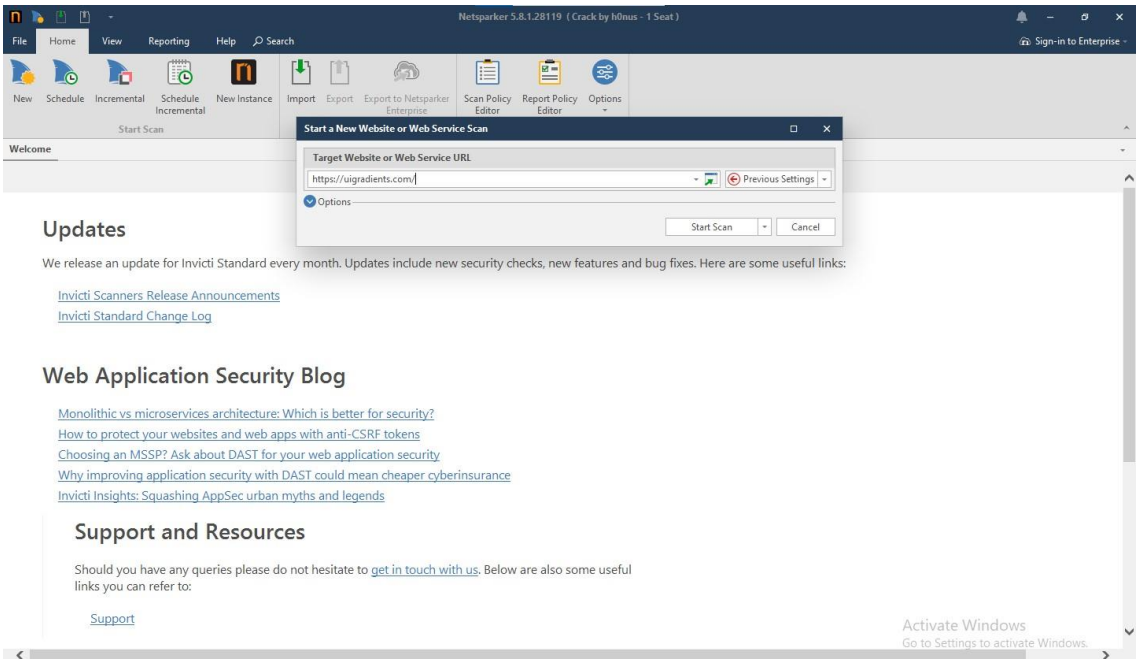
Hình 2.1: giao diện Netsparker

Để test một web ta nhấn vào biểu tượng New trên thanh công cụ của tab Home.

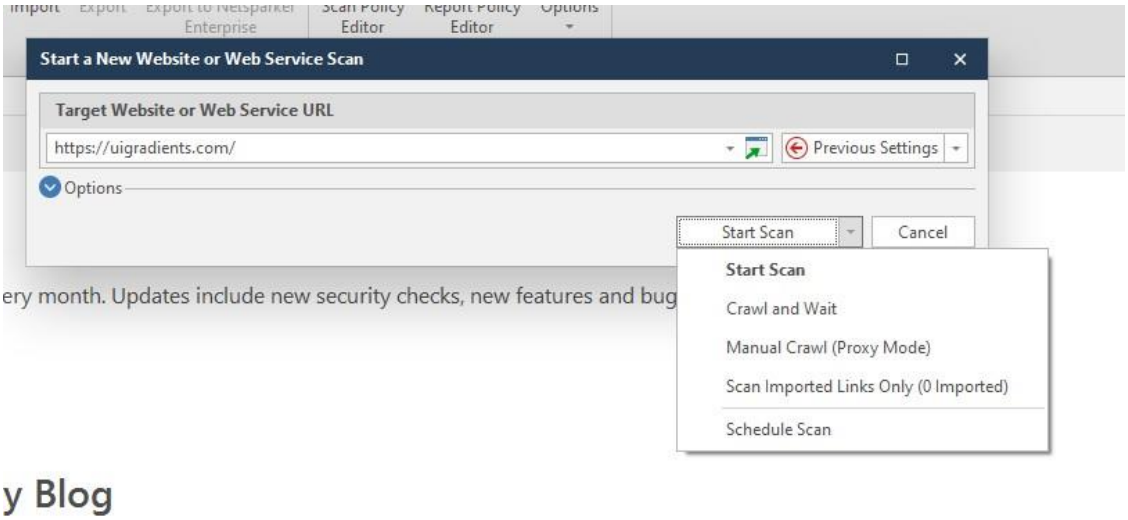


Hình 2.2: Biểu tượng New trên thanh điều hướng

Sau đó hộp thoại Start a New Website or Web Service URL: nhập link web muốn test vào và nhấn Start scan để tiến hành test website.



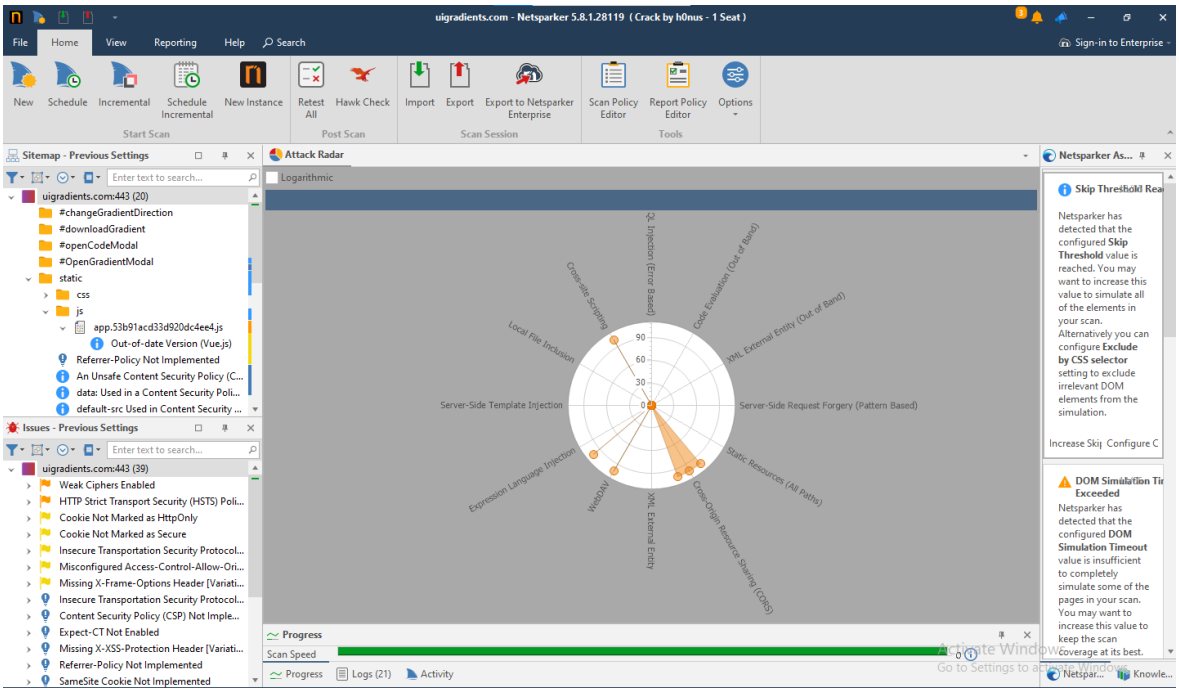
Hình 2.3: Tiến hành test website



Hình 2.4: các kiểu scan

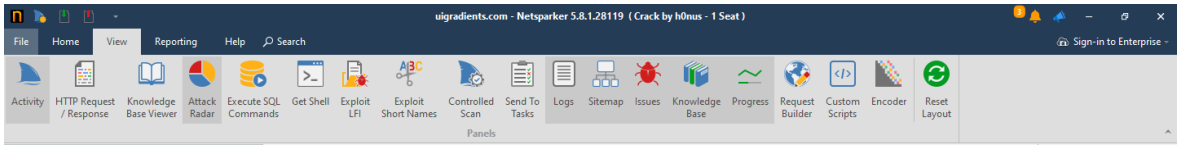
- Start scan: phần mềm tiến hành scan web một cách bình thường và chỉ dừng lại khi scan xong web.
- Crawl and Wait:
- Manual Crawl (Proxy Mode): Netsparker Desktop có tích hợp Proxy cho phép người dùng thu thập dữ liệu mục tiêu theo cách thủ công và quét nó. Manual Crawl là qui trình quét các phần của ứng dụng Web, trong quá trình thu thập thông tin, máy sẽ chỉ quét các URL mà ban cung cấp qua Proxy.
- Scan Imported Links Only: cho phép người dùng thêm các liên kết để xác định các trang web mà bạn muốn quét.
- Schedule Scan: cho phép lên lịch quét trước

Sau khi đã có kết quả test người dùng có thể thấy được trên màn hình các biểu đồ, files, lỗi, … để người dùng biết được Web mình có tính bảo mật cao hay không. Qua đó kiểm soát và khác phục những lỗi đã được xác nhận trên Netsparker.



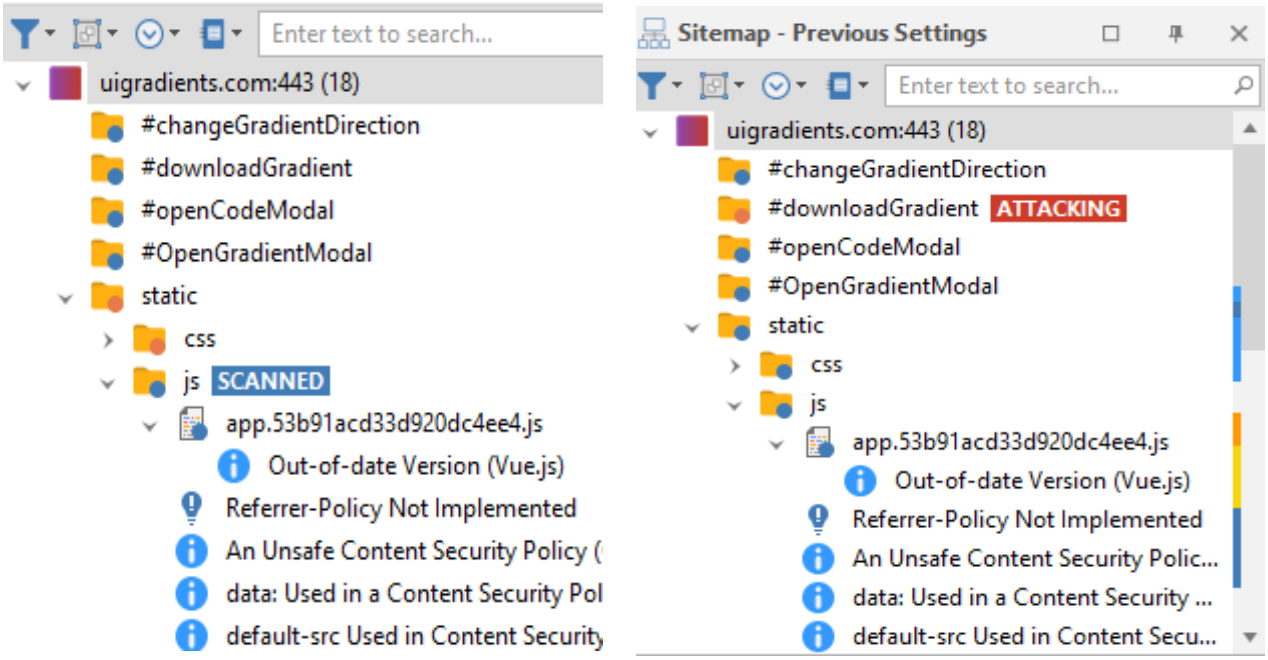
Hình 2.5: kết quả sau khi test xong website

Tại tab View của Netsparker người dùng có thể chọn hiển thị những kết quả test khác nhau như: Activity, logs, Sitemap, Issues, …



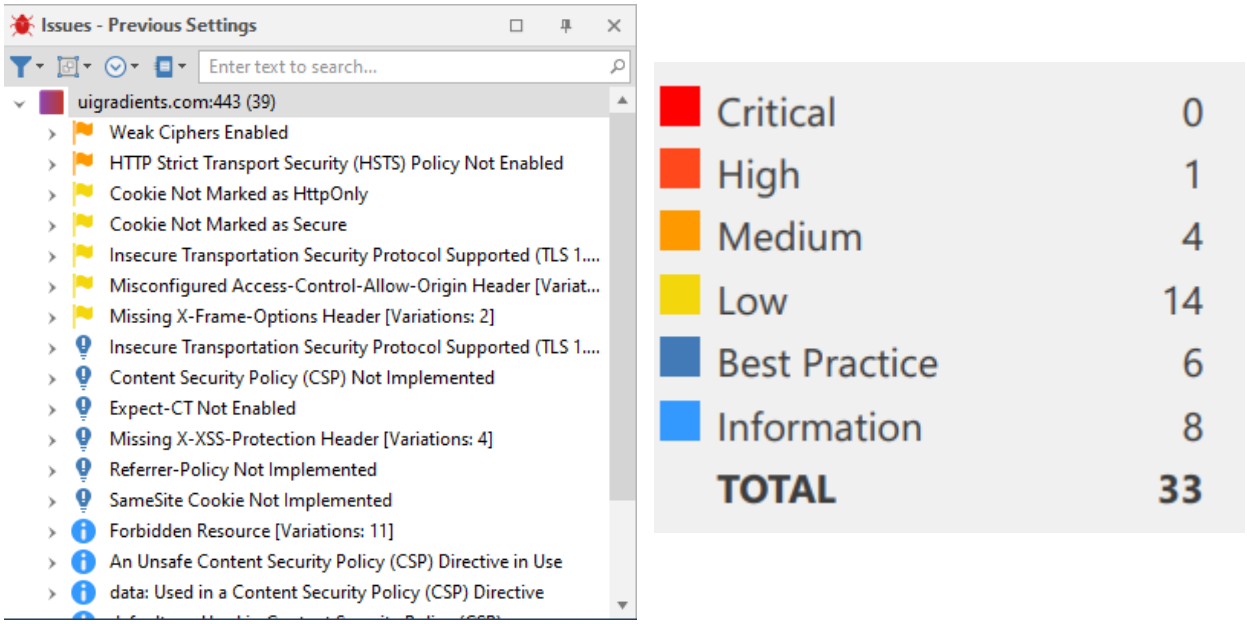
Hình 2.6: Tab View

- Sitemap: khi được chọn Sitemap sẽ xuất hiện ở bên phải của giao diện phần mềm. Sitemap hiển thị danh sách tất cả các thư mục và tệp mà phần mềm đã thu thập thông tin khi tiến hành quét. Khi đang quét, tại tệp đó sẽ hiện trạng thái hoạt đông của từng tệp (Scanned biểu thị tệp đã được quét xong, Attacking cho thấy Netsparker đàng tấn công vào tệp đó để thu thập thông tin).



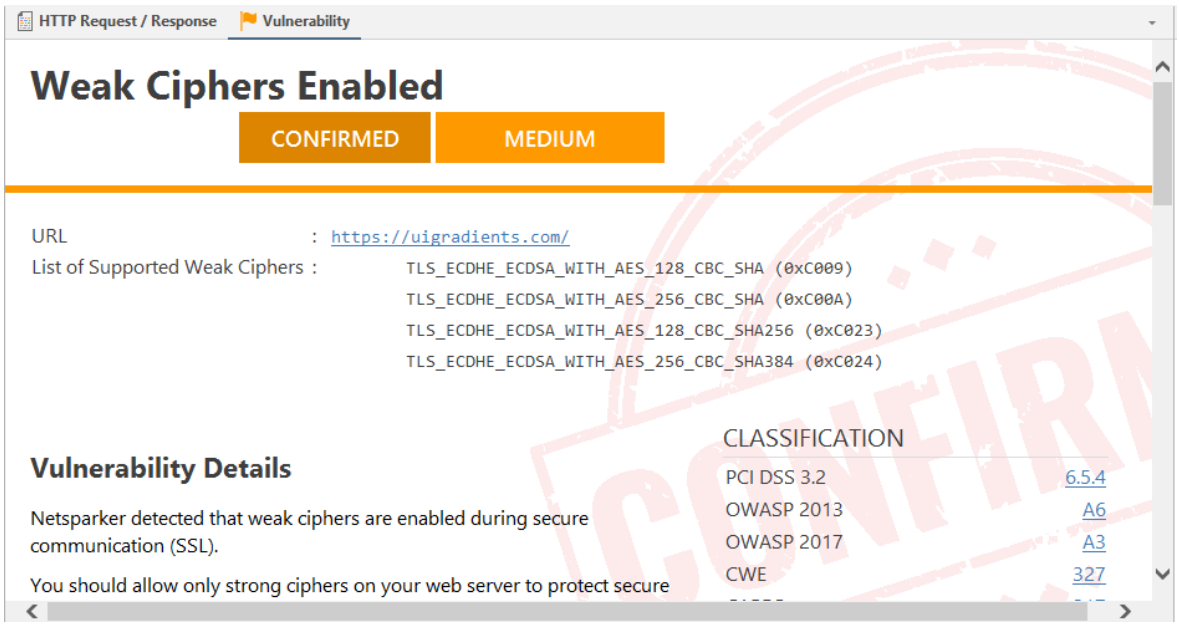
Hình 2.7: Sitemap

- Issues: hiển thị danh sách các lỗi, vấn đề được tìm thấy sau khi quét xong Website. Màu càng đậm thì tương ứng với độ nguy hiểm càng cao.



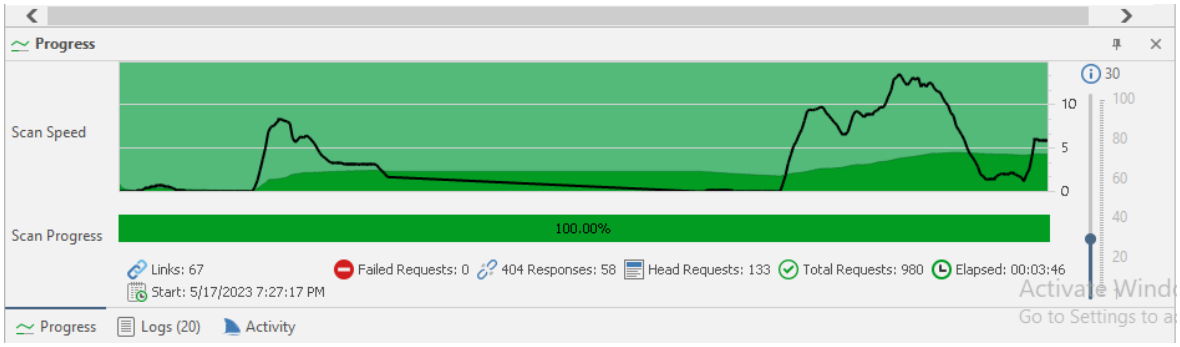
Hình 2.8: Issues

Khi nhấp vào ngẫu nhiên một vấn đề trên Issues thì màn hình hiển thị Vulnerability mô tả vấn đề, sự ảnh hưởng, giải pháp, tài liệu tham khảo về vấn đề tương ứng.



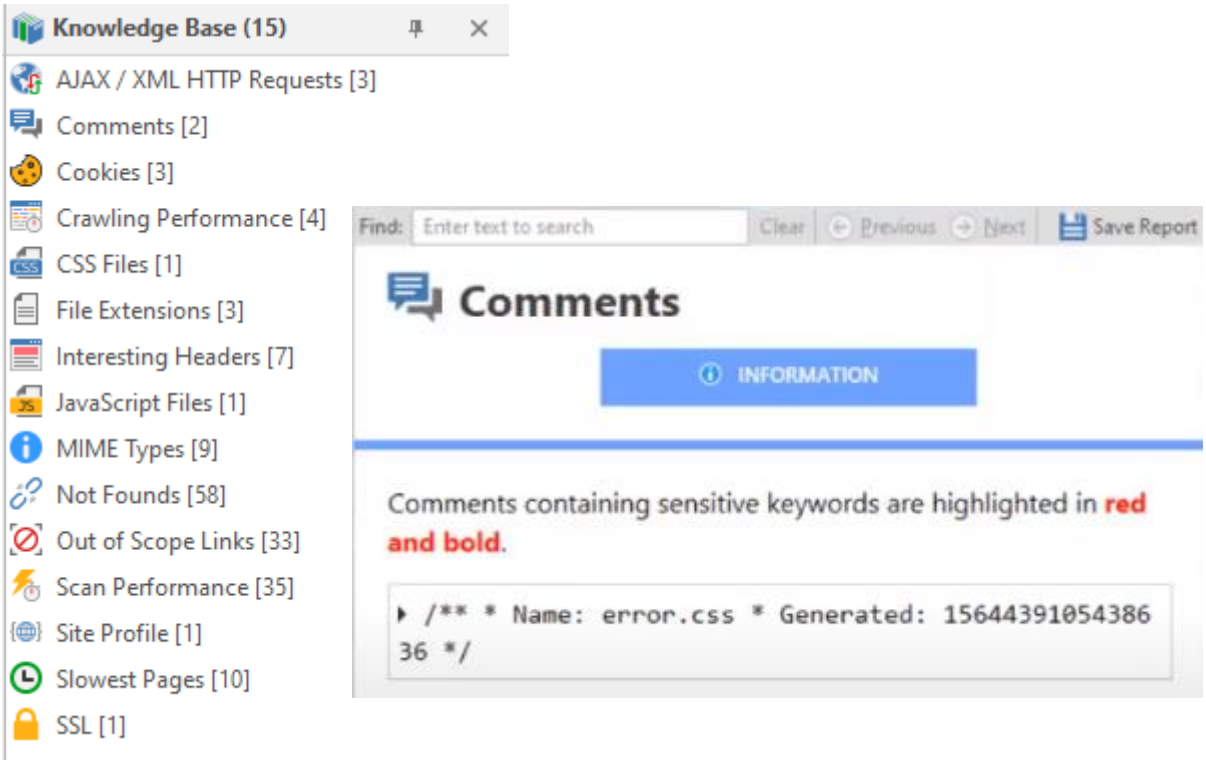
Hình 2.9: Vulnerability

- Progress: hiển thị thông tin về tốc độ và tiến trình quét, bao gồm cả tiến trình quét đến đâu. Và các thông tin khác như: Start, Faled Requests, 404 Responses, Head Requests, Total Requests, Elapsed. Cột bên phải cho biết bao nhiêu requests/s.



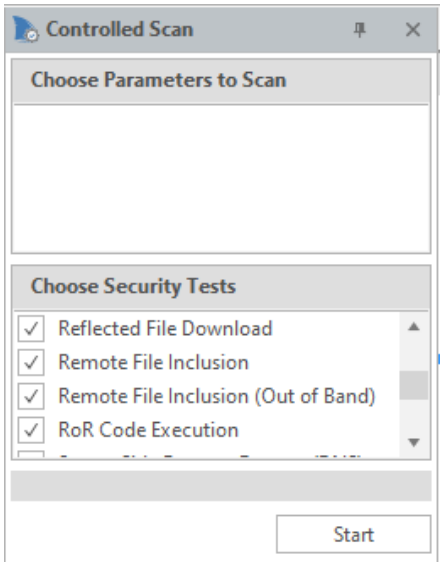
Hình 2.10: Progress

- Knowledge Base: hiển thị danh sách các thông tin bổ sung trong quá trình quét, được sắp xếp vào các nhóm khác nhau. Nếu click vào bất kì sẽ hiện ra mô tả tương ứng.



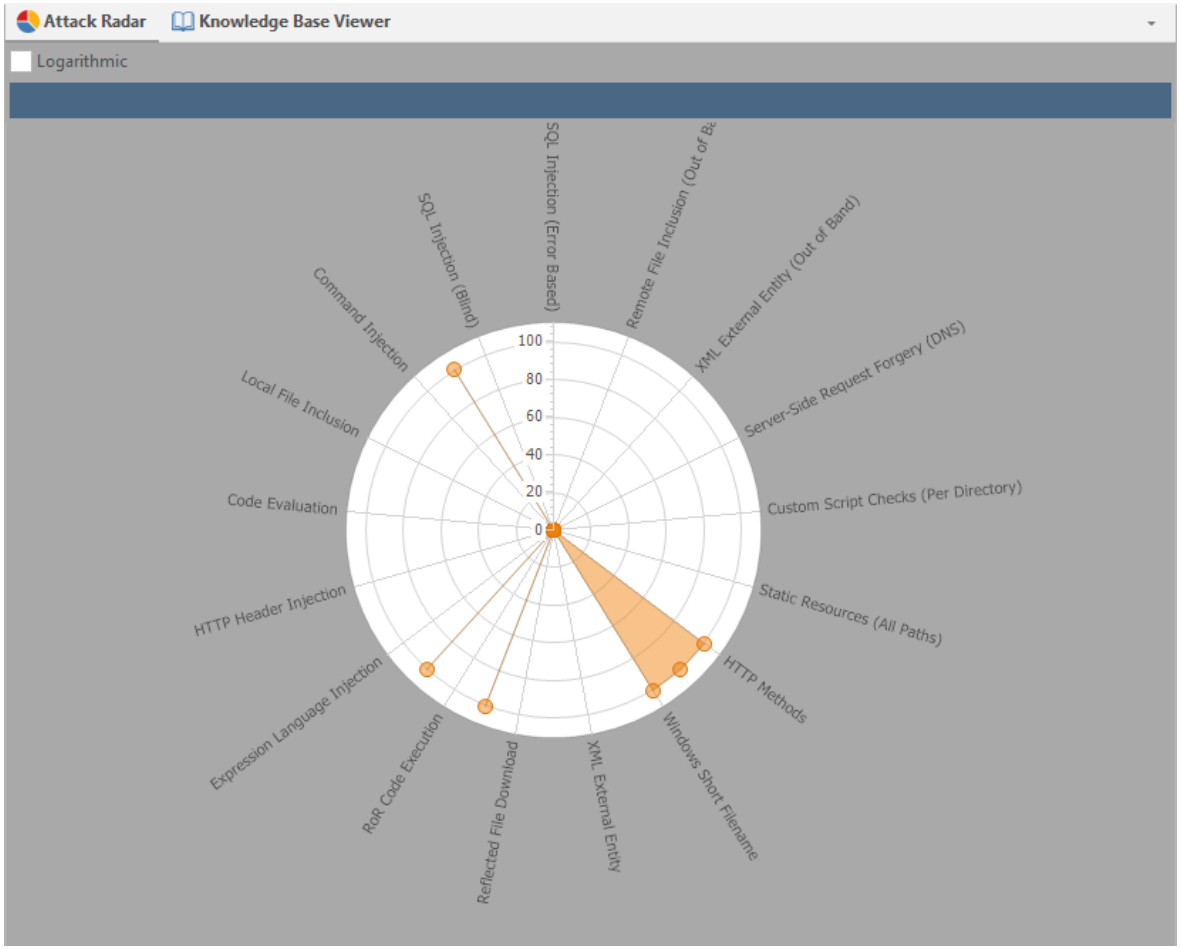
Hình 2.11: Knowledge Base

- Controlled Scan: tại đây có thể chọn kiểm tra bảo mật đặc biết muốn thực hiện trên Website.



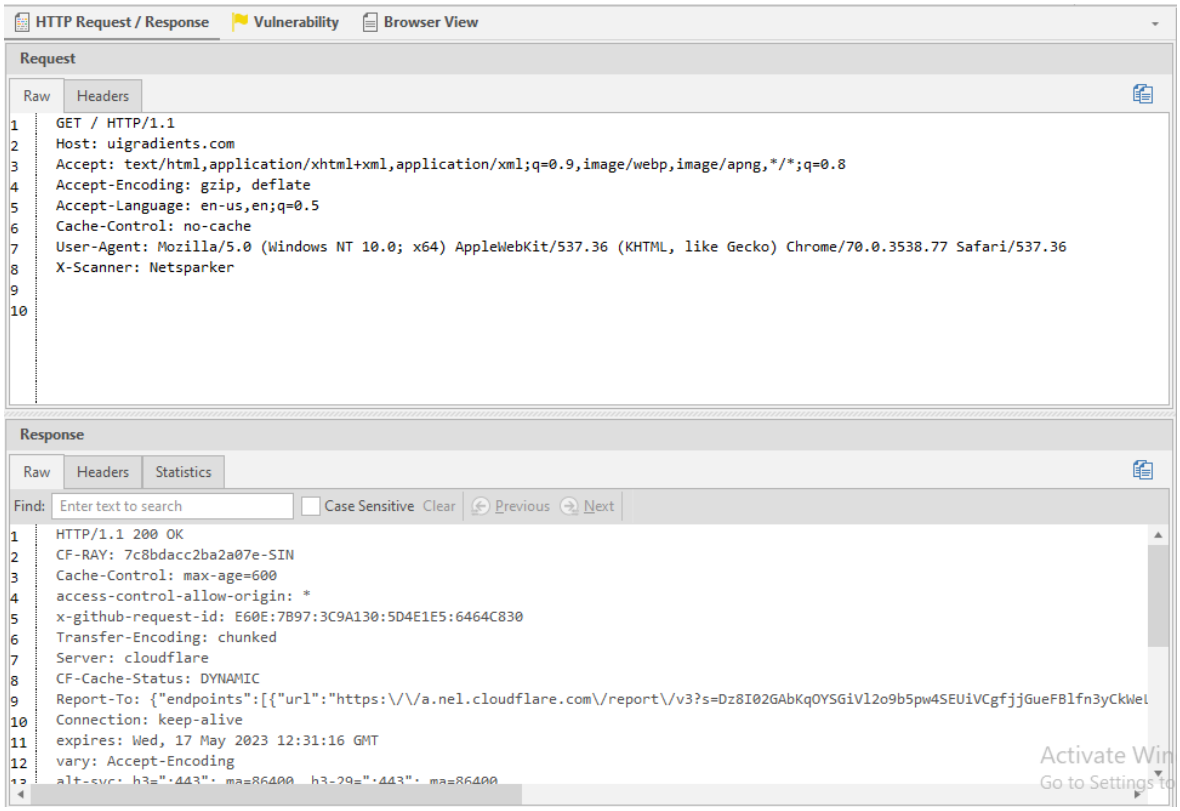
Hình 2.12: Controlled Scan

- Attack Radar: hiển thị một biểu đồ tròn cho thấy tiến trình đang diễn ra của một lần kiểm tra bảo mật. Trong quá trình và sau khi kết thúc quá trình quét, biểu đồ cho thấy tất cả các kiểm tra bảo mật đã được thực hiện và bao nhiêu lỗ hổng được tìm thấy tương ứng ở mỗi loại.



Hình 2.13: Attack Radar

- HTTP Requests/Response: hiển thị Requests và Responsse mà máy quét nhập được từ máy chủ. Để xem được HTTP Requests/Response nhấp và Issus-> HTTP Requests/Response hiện trên tab View.



Hình 2.14: HTTP Requests/ Response

- Requests Builder: cho phép bạn làm việc với các yêu cầu HTTP requests bao gồm:

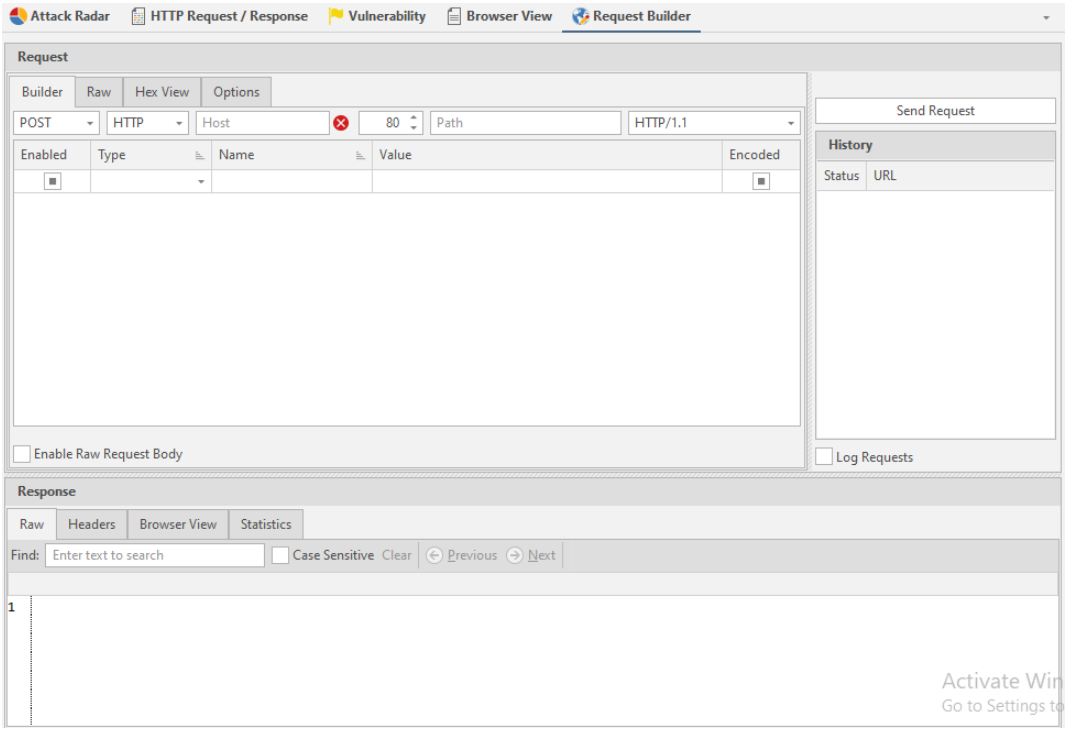
  + Gửi yêu cầu đến mục tiêu.

  + Sửa đổi các yêu cầu HTTP đã nhập.

  + Tạo các yêu cầu HTTP riêng, khi thực hiện đã giá thủ công, khác phục sự cố cụ thể hoặc cố găng xác định lổ hổng web hợp lí.

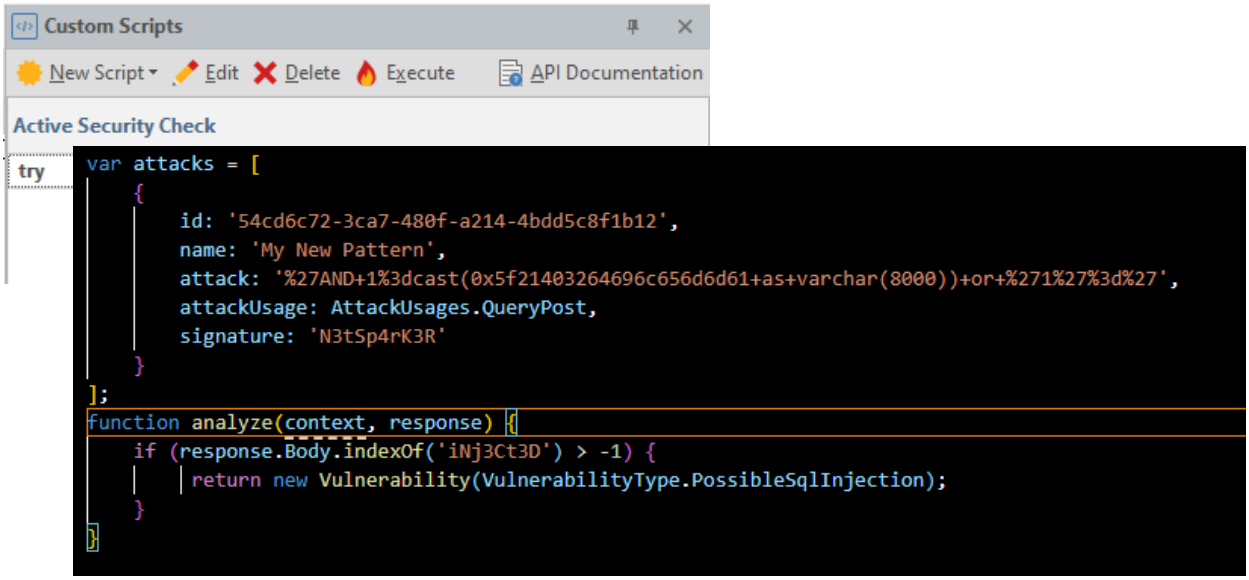
  + Phân tích sâu hơn và khai thác mà quá trình quét lổ hổng Web đã xác định trong quá trình quét.

  + phân tích phản hồi HTTP mà ứng dụng Web gửi lại.



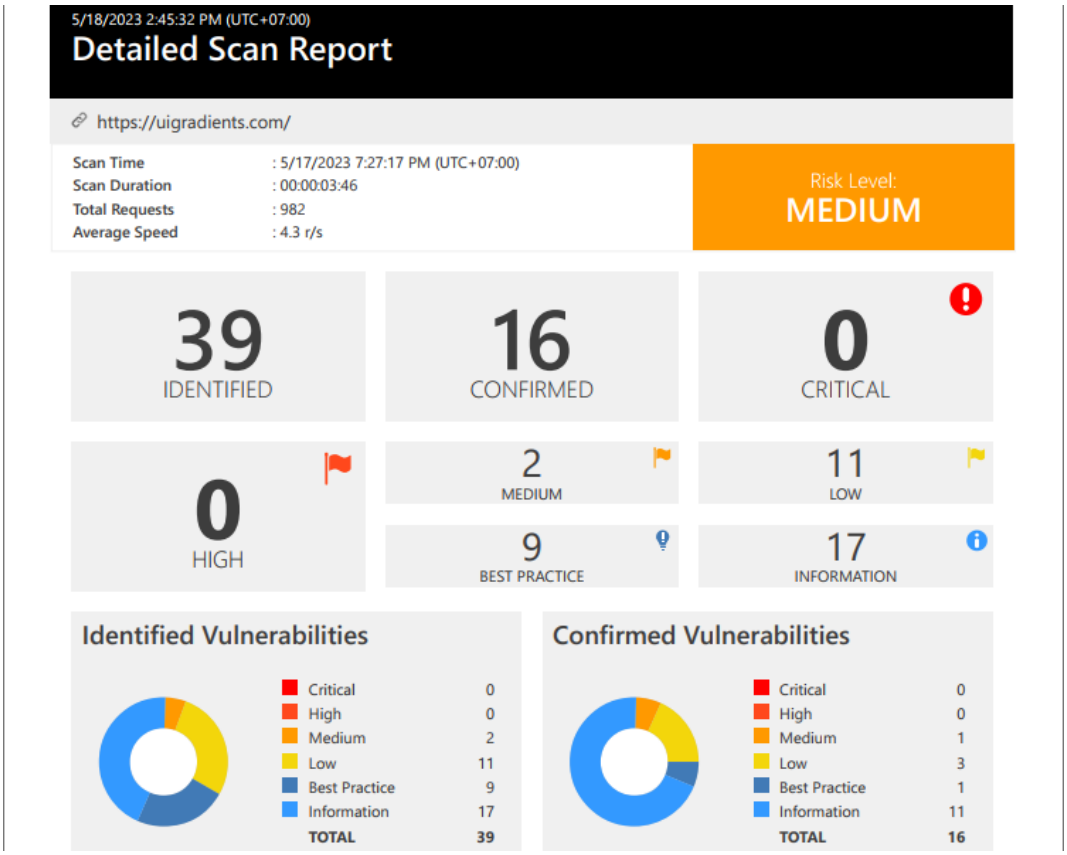
Hình 2.15: Request Builder

- Custom Scripts: cho phép mở rộng khả năng phát hiện lỗ hổng bằng cách viết các tập lệnh cung cấp các kiểu tấn công phân tích các phản hồi HTTP và phát hiện lỗ hổng tiềm ẩn.



Hình 2.16: Custom Scripts (Active security Check)

- Detailed Scan Report: cung cấp bản tóm tắt và cái nhìn chuyên sâu về trạng thái bảo mật của trang Web được quét.



Hình 2.17: Detailed Scan Report

- Detailed Scan report gồm 5 phần: Scan Metadata, Vulnerabilities, Vulnerability Summary, Vulnerability Names and Details, Show Scan Details.

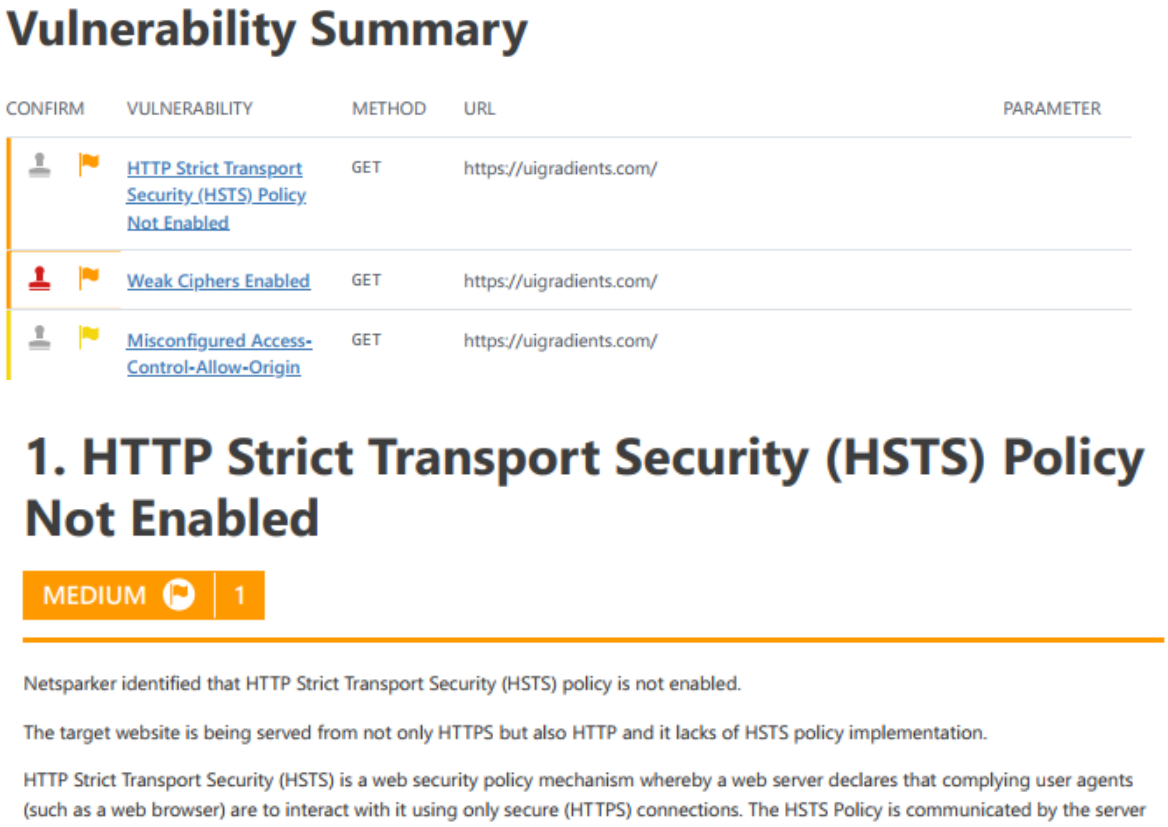
  + Scan Metadata: cung cấp thông tin về mục tiêu quét, thời gian quét, tổng số request, tốc độ trung bình, mức độ rủi ro.

  + Vulnerabilities: cung cấp cái nhìn tổng qua về số và đồ họa.

  + Vulnerability Summary: cung cấp bản tóm tắt thông tin vè từng URL dễ bị tấn công được phát hiện và phân loại dựa trên mức độ nghiêm trọng.

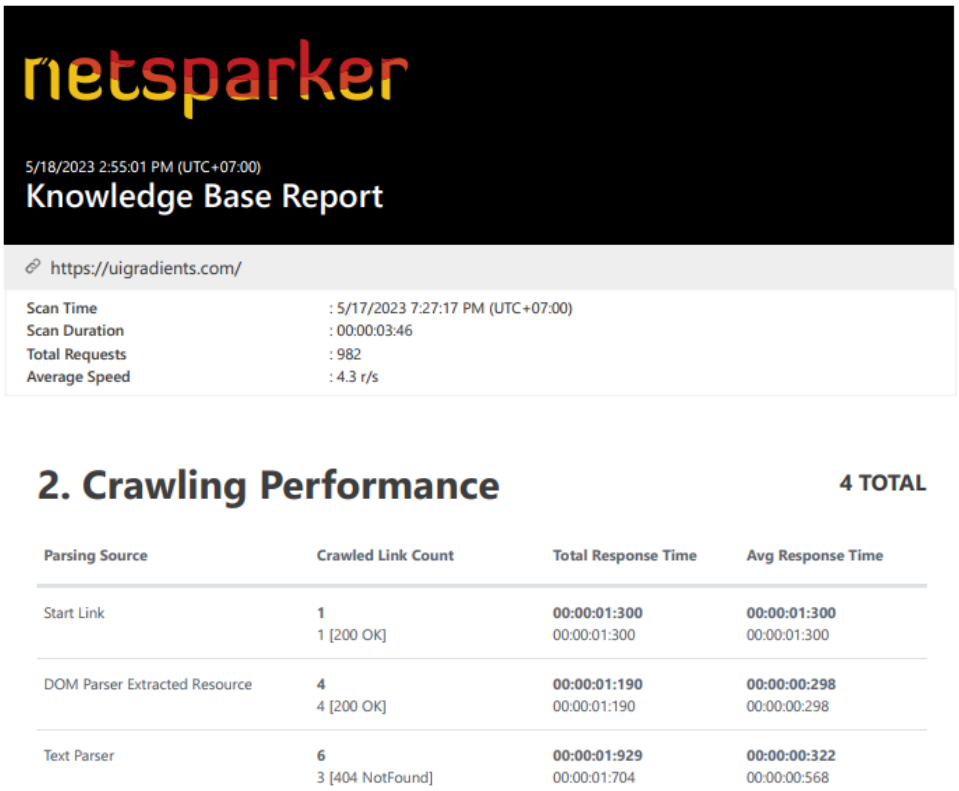
  + Vulnerability Names and Details: mô tả các sự cố và lổ hổng đã được xác định (tác động, sự ảnh hưởng, việc cần thực hiện, biện pháp khắc phục và tài liệu tham khảo).

+ Show Scan Details: cung cấp một số cài đặt cấu hình mà chính sách mà Netsparker sử dụng để diều chỉnh trong quá trình quét nhằm đạt được phạm vi tốt hơn.



Hình 2.18: các thành phần mô tả rủi ro trong Detaied Scan Report

- Knowledge Base Report: cung cấp thông tin chi tiết về quá trình quét. Liệt kê lổ hôngr và sự cố, được nhóm theo mức độ nghiêm trọng, nó cũng liệt kê một số thông tin hữu ích về quá trình quét để làm nổi bật các vấn đề bảo mật tiềm ẩn khác.


netsparker

5/18/2023 2:55:01 PM (UTC+07:00)

Knowledge Base Report

https://uigradients.com/

Scan Time	: 5/17/2023 7:27:17 PM (UTC+07:00)
Scan Duration	: 00:00:03:46
Total Requests	: 982
Average Speed	: 4.3 r/s

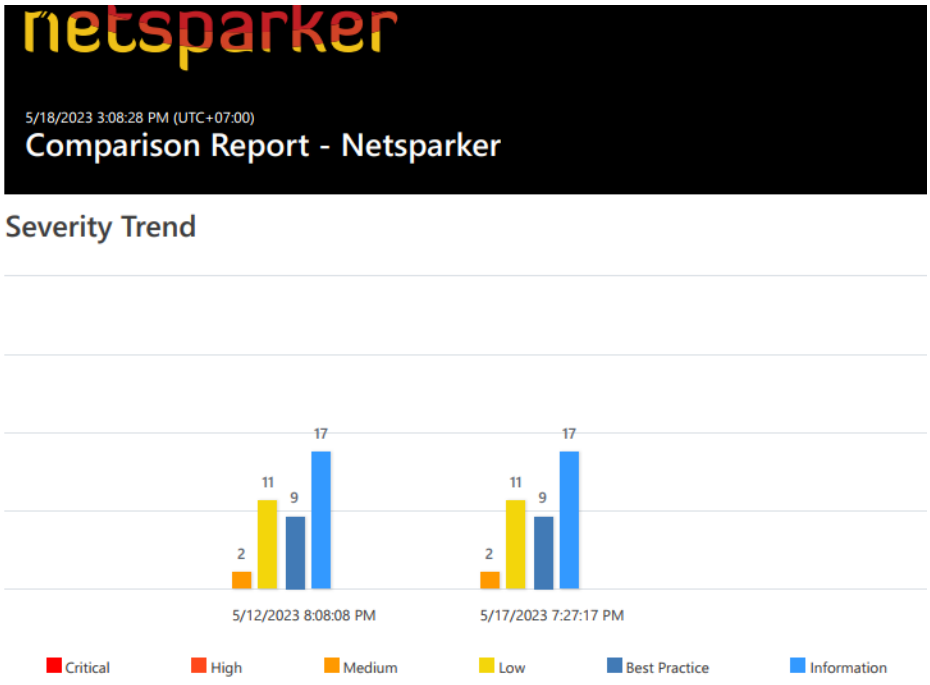
2. Crawling Performance

4 TOTAL

Parsing Source	Crawled Link Count	Total Response Time	Avg Response Time
Start Link	1 1 [200 OK]	00:00:01:300 00:00:01:300	00:00:01:300 00:00:01:300
DOM Parser Extracted Resource	4 4 [200 OK]	00:00:01:190 00:00:01:190	00:00:00:298 00:00:00:298
Text Parser	6 3 [404 NotFound]	00:00:01:929 00:00:01:704	00:00:00:322 00:00:00:568

Hình 2.19: Knowledge Base Report

- Comparision Report: cho phép so sánh hai hay nhiều báo cáo quét. điều này giúp theo dõi được thay đổi của ứng dụng Web đã quét.



Hình 2.20: Comparision Report

CHƯƠNG IV: KẾT LUẬN

Trong đồ án này nhóm đã nghiên cứu về công cụ hỗ trợ bảo mật Netspaker, sử dụng công cụ để tìm các lỗ hỏng bảo mật trê website.

Netsparker là một công cụ kiểm thử bảo mật toàn diện, đa nền tảng, có khả năng phát hiện được nhiều lỗ hổng bảo mật khác nhau trên các ứng dụng web và máy chủ web. Công cụ này có khả năng tự động phát hiện lỗ hổng bảo mật và cung cấp báo cáo chi tiết về các lỗ hổng này, giúp các nhà phát triển và quản trị viên hệ thống có thể nhanh chóng và hiệu quả khắc phục các lỗ hổng bảo mật trên hệ thống của mình.

Tuy nhiên, cũng có một số nhược điểm của Netsparker, bao gồm giá cả đắt đỏ và không thể phát hiện tất cả các loại lỗ hổng bảo mật. Ngoài ra, Netsparker cũng có những điểm mạnh và yếu so với các công cụ khác trong cùng lĩnh vực. Ví dụ như với các công cụ như OWASP ZAP hay Burp Suite, chúng ta có thể tùy chỉnh và điều chỉnh các yêu cầu và phản hồi trong quá trình kiểm thử bảo mật, trong khi Netsparker không cho phép điều này.

Nhưng, với khả năng tự động phát hiện lỗ hổng bảo mật và các tính năng nâng cao khác, Netsparker vẫn là một công cụ quan trọng và hữu ích cho việc kiểm thử bảo mật trên các ứng dụng web và máy chủ web.

Nhóm đã nghiên cứu sử dụng tài liệu kết hợp với các kiến thức đã học. tuy nhiên do thời gian và khả năng của nhóm còn hạn chế nên vẫn chưa tìm hiểu được hết những tính năng khác của công cụ. trong tương lai nhóm sẽ nghiên cứu sâu và hoàn thiện hơn về công cụ.

TÀI LIỆU THAM KHẢO

[1] https://www.invicti.com/statics/help/netsparker-help.pdf

[2] https://www.invicti.com/support/

[3] https://www.youtube.com/watch?v=C4OoGSRgQxw&t=314s