**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ**

**TRUYỀN THÔNG VIỆT – HÀN**

**KHOA KỸ THUẬT MÁY TÍNH & ĐIỆN TỬ**

**A logo with a black background

Description automatically generated**

**BÁO CÁO MÔN HỌC**

**BẢO MẬT VÀ AN TOÀN THÔNG TIN**

**Đề tài: Tìm hiểu và triển khai công cụ Burp Suite**

Sinh viên thực hiện : **HUỲNH VĨNH VINH MSV: 21IT392**

: **NGUYỄN HOÀNG VIỆT MSV: 21IT252**

: **CAO BÁ VƯƠNG MSV: 20IT248**

Lớp : **21NS**

Giảng viên hướng dẫn : **TS. HOÀNG HỮU ĐỨC**

**Đà nẵng, tháng 5 năm 2024**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ**

**TRUYỀN THÔNG VIỆT – HÀN**

**KHOA KỸ THUẬT MÁY TÍNH & ĐIỆN TỬ**

**A logo with a black background

Description automatically generated**

**BÁO CÁO MÔN HỌC**

**BẢO MẬT VÀ AN TOÀN THÔNG TIN**

**Đề tài: Tìm hiểu và triển khai công cụ Burp Suite**

Sinh viên thực hiện : **HUỲNH VĨNH VINH MSV: 21IT392**

: **NGUYỄN HOÀNG VIỆT MSV: 21IT252**

: **CAO BÁ VƯƠNG MSV: 20IT248**

Lớp : **21NS**

Giảng viên hướng dẫn : **TS. HOÀNG HỮU ĐỨC**

**Đà nẵng, tháng 5 năm 2024**

# **LỜI MỞ ĐẦU**

Trong thế giới ngày nay, việc bảo vệ thông tin và dữ liệu trực tuyến trở nên ngày càng quan trọng hơn bao giờ hết. Với sự gia tăng của các cuộc tấn công mạng và lỗ hổng bảo mật, việc triển khai các công cụ hiệu quả để đánh giá và bảo vệ hệ thống trở thành một ưu tiên hàng đầu đối với các tổ chức và cá nhân làm việc trong lĩnh vực công nghệ thông tin.

Trong khuôn khổ của báo cáo này, chúng tôi sẽ tập trung vào đánh giá và triển khai công cụ Burp Suite, một trong những công cụ quan trọng nhất được sử dụng trong kiểm thử bảo mật ứng dụng web. Burp Suite là một bộ công cụ toàn diện, cung cấp nhiều tính năng mạnh mẽ để phát hiện, khai thác và kiểm soát các lỗ hổng bảo mật trong ứng dụng web.

Trong phần tiếp theo của báo cáo, chúng tôi sẽ trình bày một cái nhìn tổng quan về công cụ Burp Suite, bao gồm các tính năng chính và cách sử dụng chúng để phát hiện và khai thác lỗ hổng bảo mật. Sau đó, chúng tôi sẽ tập trung vào quá trình triển khai của Burp Suite trong môi trường thực tế, bao gồm cách cấu hình và tinh chỉnh công cụ để đảm bảo hiệu suất và độ chính xác tối ưu.

Hi vọng rằng thông qua báo cáo này, độc giả sẽ có cái nhìn sâu sắc hơn về vai trò và ứng dụng của công cụ Burp Suite trong việc bảo vệ ứng dụng web. Chúng tôi hy vọng rằng kiến thức và thông tin được trình bày sẽ cung cấp cho độc giả những cơ sở vững chắc để áp dụng Burp Suite một cách hiệu quả trong công việc hàng ngày của họ

# **LỜI CẢM ƠN**

Để đồ án này đạt kết quả tốt đẹp, chúng em đã nhận được sự hỗ trợ, giúp đỡ của thầy cô. Với tình cảm sâu sắc, chân thành, cho phép chúng em được bày tỏ lòng biết ơn sâu sắc đến tất cả quý thầy cô đã tạo điều kiện giúp đỡ trong quá trình học tập, nghiên cứu và phát triển đề tài.

Trước hết chúng em xin gửi tới quý thầy cô Khoa Khoa học máy tính- Đại học CNTT & TT Việt - Hàn - Đại Học Đà Nẵng lời chào trân trọng, lời chúc sức khỏe và lời cảm ơn sâu sắc nhất. Với sự quan tâm, chỉ bảo tận tình và truyền đạt những kiến thức bổ ích cho chúng em suốt thời gian học kỳ vừa rồi, giúp em có thêm nhiều kiến thức và hiểu rõ hơn các vấn đề mình nghiên cứu, đến nay chúng em đã có thể hoàn thành đề tài môn học.

Đặc biệt chúng em xin gửi lời cảm ơn chân thành nhất đến giảng viên TS. Hoàng Hữu Đức đã quan tâm giúp đỡ tận tình chúng em hoàn thành tốt đồ án này trong thời gian qua.

Với điều kiện thời gian cũng như kinh nghiệm còn hạn chế, đồ án này sẽ không thể tránh được những thiếu sót. Chúng em rất mong nhận được sự chỉ bảo, đóng góp ý kiến của các thầy cô, để chúng em có thể bổ sung, nâng cao kinh nghiệm và kỹ năng của bản thân để phục vụ cho công việc thực tế sau này.

Chúng em xin chân thành cảm ơn!

# **NHẬN XÉT**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

Đà Nẵng, ngày… tháng…năm 2024

Giảng viên hướng dẫn

TS. Hoàng Hữu Đức

# **MỤC LỤC**

[**LỜI MỞ ĐẦU** I](#_Toc166275330)

[**LỜI CẢM ƠN** II](#_Toc166275331)

[**NHẬN XÉT** III](#_Toc166275332)

[**MỤC LỤC** IV](#_Toc166275333)

[**CHƯƠNG 1: TỔNG QUAN VỀ AN NINH MẠNG** 1](#_Toc166275334)

[**1.1 Sự Cần Thiết của An Ninh Mạng** 1](#_Toc166275335)

[**1.2 Các Mối Đe Dọa Chính** 1](#_Toc166275336)

[**1.3 Các Biện Pháp Bảo Mật** 1](#_Toc166275337)

[**1.4 Tích Hợp An Ninh Mạng vào Quản Lý Toàn Diện** 2](#_Toc166275338)

[**1.5 Sự Cần Thiết của Các Công Cụ Đánh Giá Bảo Mật Website** 2](#_Toc166275339)

[**1.5. Công Cụ Burp Suite** 2](#_Toc166275340)

[**CHƯƠNG 2: CƠ SỞ LÝ THUYẾT VỀ BURP SUITE** 4](#_Toc166275341)

[**2.1 Tổng quan về Burp Suite** 4](#_Toc166275342)

[**2.1.1 Khái niệm** 4](#_Toc166275343)

[**2.1.2 Các chức năng chính của phần mềm Burp Suite** 5](#_Toc166275344)

[**2.1.3 Lợi ích của phần mềm Burp Suite** 9](#_Toc166275345)

[**2.1.4 Phiên bản của phần mềm Burp Suite** 9](#_Toc166275346)

[**2.1.5. Cài đặt Burp suite** 10](#_Toc166275347)

[**2.2 Mô hình hoạt động của Burp suite** 12](#_Toc166275348)

[**2.3 Cách sử dụng phần mềm Burp suite** 13](#_Toc166275349)

[**2.3.1. Cài đặt Burp Suite** 13](#_Toc166275350)

[**2.3.2. Cấu hình Burp Suite** 14](#_Toc166275351)

[**2.3.3. Bắt đầu kiểm tra** 14](#_Toc166275352)

[**CHƯƠNG 3: CÀI ĐẶT VÀ TRIỂN KHAI CÁC CHỨC NĂNG PROXY, INTRUDER VÀ REPEATER CỦA BURP SUITE** 16](#_Toc166275353)

[**3.1 Cài đặt Burp suite** 16](#_Toc166275354)

[**3.2 Proxy** 16](#_Toc166275355)

[**3.3 Intruder** 19](#_Toc166275356)

[**3.4 Repeater** 21](#_Toc166275357)

[**KẾT LUẬN** 22](#_Toc166275358)

[**1. Kết quả thu được** 22](#_Toc166275359)

[**2. Về hạn chế** 22](#_Toc166275360)

[**DANH MỤC TÀI LIỆU THAM KHẢO** 23](#_Toc166275361)

# **CHƯƠNG 1: TỔNG QUAN VỀ AN NINH MẠNG**

An ninh mạng đang trở thành một trong những vấn đề nổi bật nhất của thế giới kỹ thuật số, đặc biệt là trong lĩnh vực web. Với sự phát triển nhanh chóng của Internet và sự bùng nổ của ứng dụng web, mối đe dọa liên quan đến an ninh mạng đang trở nên phức tạp và đa dạng hơn bao giờ hết. Chương này sẽ cung cấp một cái nhìn tổng quan về an ninh mạng, tập trung vào các vấn đề đặc biệt liên quan đến web.

## **1.1 Sự Cần Thiết của An Ninh Mạng**

An ninh mạng không chỉ là một vấn đề kỹ thuật mà còn là một vấn đề an ninh quốc gia và toàn cầu. Các cuộc tấn công mạng có thể gây ra tổn thất về thông tin, tài chính, và thậm chí là về tính mạng của con người.

Sự phát triển của Internet và sự lan rộng của các thiết bị kết nối mạng đã tạo ra nhiều cơ hội mới cho các kẻ tấn công, từ cá nhân đến tổ chức tội phạm và cả các quốc gia.

## **1.2 Các Mối Đe Dọa Chính**

* Tấn Công Ddos (Distributed Denial of Service): Các cuộc tấn công này nhằm vào việc làm cho dịch vụ trực tuyến không thể sử dụng bằng cách làm quá tải hệ thống bằng cách gửi lưu lượng truy cập giả mạo từ nhiều nguồn khác nhau.
* Tấn Công XSS (Cross-Site Scripting): Tấn công này nhằm vào việc chèn mã độc hại vào các trang web và ứng dụng web để lừa đảo người dùng hoặc lấy cắp thông tin.
* Tấn Công SQL Injection: Tấn công này sử dụng các lỗ hổng trong cơ sở dữ liệu để thực hiện các lệnh SQL độc hại, có thể dẫn đến việc lấy cắp hoặc thay đổi dữ liệu trong cơ sở dữ liệu.
* Tấn Công Phishing: Tấn công này thường sử dụng các email giả mạo hoặc trang web giả mạo để lừa đảo người dùng để tiết lộ thông tin cá nhân, như tên người dùng, mật khẩu hoặc thông tin tài khoản ngân hàng.

## **1.3 Các Biện Pháp Bảo Mật**

* Bảo vệ Mạng Lưới: Triển khai các giải pháp bảo vệ mạng lưới như tường lửa, hệ thống phát hiện xâm nhập (IDS), hệ thống ngăn chặn xâm nhập (IPS), và giải pháp VPN (Virtual Private Network) để bảo vệ dữ liệu khi truyền qua Internet.
* Bảo Mật Ứng Dụng: Thực hiện kiểm tra mã độc, mã hóa dữ liệu, và bảo vệ chống lại các tấn công XSS, SQL Injection bằng cách sử dụng các framework và thư viện bảo mật phù hợp.
* Giáo Dục và Huấn Luyện: Tăng cường giáo dục và huấn luyện cho người sử dụng cuối và nhân viên về các mối đe dọa mạng và các biện pháp phòng ngừa.

## **1.4 Tích Hợp An Ninh Mạng vào Quản Lý Toàn Diện**

An ninh mạng không chỉ là vấn đề của các chuyên gia an ninh mạng mà còn là trách nhiệm của tất cả các phòng ban trong một tổ chức. Nó phải được tích hợp vào mọi khía cạnh của quản lý tổ chức.

Một chiến lược an ninh mạng hiệu quả không chỉ bao gồm các công nghệ bảo mật mạng mà còn bao gồm chính sách, quy trình và văn hóa tổ chức.

## **1.5 Sự Cần Thiết của Các Công Cụ Đánh Giá Bảo Mật Website**

* Phát hiện Lỗ Hổng Bảo Mật: Các công cụ đánh giá bảo mật website như Burp Suite, OWASP ZAP, và Acunetix cung cấp các tính năng và công cụ để phát hiện các lỗ hổng bảo mật như XSS, SQL Injection, và CSRF. Việc phát hiện lỗ hổng này sớm có thể giúp tổ chức thực hiện biện pháp phòng ngừa kịp thời trước khi xảy ra các cuộc tấn công.
* Đánh Giá Mức Độ Rủi Ro: Bằng cách sử dụng các công cụ đánh giá bảo mật, các chuyên gia có thể đánh giá mức độ rủi ro của website dựa trên các lỗ hổng bảo mật đã phát hiện. Điều này giúp tổ chức ưu tiên các lỗ hổng cần được khắc phục đầu tiên để tăng cường an ninh mạng.
* Tuân Thủ và Đánh Giá Conformity: Các công cụ đánh giá bảo mật cũng có thể được sử dụng để kiểm tra tuân thủ và đánh giá conformity với các tiêu chuẩn an ninh mạng và quy định pháp luật như GDPR, PCI DSS, và ISO 27001. Việc này giúp tổ chức đảm bảo rằng họ tuân thủ các yêu cầu bảo mật và tránh được các phạt và hậu quả pháp lý.
* Giảm Thiểu Rủi Ro Liên Quan Đến Dữ Liệu: Các công cụ đánh giá bảo mật giúp tổ chức giảm thiểu rủi ro liên quan đến dữ liệu bằng cách xác định và khắc phục các lỗ hổng bảo mật có thể dẫn đến sự mất mát hoặc lộ thông tin quan trọng.
* Cải Thiện Hệ Thống Bảo Mật Tổng Thể: Bằng cách sử dụng các công cụ đánh giá bảo mật, tổ chức có thể cải thiện hệ thống bảo mật tổng thể của họ bằng cách tăng cường phát hiện và giảm thiểu các lỗ hổng bảo mật trong quá trình phát triển và vận hành của ứng dụng web.

Sử dụng các công cụ đánh giá bảo mật website không chỉ là một phần quan trọng của quy trình kiểm thử an ninh mạng mà còn là một yếu tố cần thiết để đảm bảo an toàn và bảo mật của dữ liệu và thông tin trên internet.

## **1.5. Công Cụ Burp Suite**

Burp Suite là một bộ công cụ mạnh mẽ được phát triển bởi PortSwigger để hỗ trợ các chuyên gia kiểm thử an ninh mạng trong việc phát hiện và khai thác các lỗ hổng bảo mật trên ứng dụng web.

Bao gồm các thành phần chính như Burp Proxy, Burp Scanner, Burp Spider, Burp Repeater, và Burp Intruder, Burp Suite cung cấp một loạt các tính năng và công cụ cho việc kiểm thử an ninh mạng, từ phát hiện lỗ hổng cho đến thử nghiệm và khai thác chúng.

* Burp Proxy cho phép người dùng theo dõi và chỉnh sửa các yêu cầu và phản hồi HTTP/S giữa trình duyệt và máy chủ web, giúp phát hiện các lỗ hổng như XSS và SQL Injection.
* Burp Scanner tự động phát hiện các lỗ hổng bảo mật trong ứng dụng web, giúp giảm thiểu thời gian kiểm thử bằng cách tự động hóa quy trình này.
* Burp Spider tự động khám phá và lập bản đồ các ứng dụng web, giúp người dùng xác định các điểm đầu vào và điểm đích tiềm năng cho các cuộc tấn công.
* Burp Repeater cho phép người dùng tái sử dụng các yêu cầu HTTP/S và thay đổi các thông số để kiểm tra các lỗ hổng và kiểm tra lại các kết quả.
* Burp Intruder là một công cụ mạnh mẽ cho phép tùy chỉnh và tự động hóa các cuộc tấn công đối với các tham số của yêu cầu web, giúp xác định các lỗ hổng như Brute Force và parameter tampering.

Burp Suite là một công cụ quan trọng trong hộp công cụ của các chuyên gia kiểm thử an ninh mạng và là một phần không thể thiếu trong quá trình kiểm thử an ninh ứng dụng web.

# **CHƯƠNG 2: CƠ SỞ LÝ THUYẾT VỀ BURP SUITE**

## **2.1 Tổng quan về Burp Suite**

### **2.1.1 Khái niệm**

**A logo for a company

Description automatically generated**

Hình 1: Burp Suite

Burp Suite là trình quét bảo mật phổ biến được sử dụng rộng rãi nhất hiện nay được tích hợp với nhiều tính năng mạnh mẽ cùng các phần mềm mở rộng tùy chọn có khả năng kiểm tra được tính bảo mật của ứng dụng web và cả các thành phần khác nhau có trong web nữa.

Burp Suite sẽ giúp người dùng đánh giá một số các tiêu chí bảo mật như kiểm tra các vấn đề về phiên bản người dùng, tiến hành kiểm tra cơ chế xác thực, liệt kê và đánh giá các tham số đầu vào của ứng dụng, ...

Burp Suite được hiểu là một ứng dụng được tích hợp nhiều tính năng phục vụ kiểm tra tính bảo mật của ứng dụng web. Các tính năng này sẽ phục vụ kiểm tra bảo mật những thành phần khác nhau trong ứng dụng web hiện đại ngày nay.

Burp Suite giúp người dùng đánh giá các tiêu chí bảo mật web như: Tiến hành kiểm tra cơ chế xác thực, kiểm tra các vấn đề về phiên bản người dùng hay liệt kê cũng như đánh giá các tham số đầu vào của ứng dụng trang web.

Burp Suite là một trong những công cụ kiểm tra thâm nhập và tìm lỗ hổng phổ biến nhất và thường được sử dụng để kiểm tra bảo mật ứng dụng web. Burp Suite là một công cụ dựa trên proxy được sử dụng để đánh giá tính bảo mật của các ứng dụng dựa trên web và thực hiện kiểm tra thực hành. Với hơn 40.000 người dùng, Burp Suite là trình quét lỗ hổng bảo mật trên web được sử dụng rộng rãi nhất trên thế giới. Nó có các mô đun mạnh mẽ và được đóng gói với các phần mở rộng tùy chọn có thể tăng hiệu quả kiểm tra ứng dụng web. Burp Suite là một công cụ pentest ứng dụng web. Đây không phải là một công cụ “ăn sẵn” như Acunetix, mà nó chỉ hỗ trợ một số việc cho tester trong quá trình pentest. Với một chút cố gắng, bất kỳ ai cũng có thể sử dụng Burp Suite để kiểm thử các ứng dụng web. Các tính năng nâng cao của Burp sẽ giúp tester nâng cao kỹ năng và trình độ của mình hơn nữa. Ngoài ra, giao diện của Burp cũng rất trực quan và thân thiện. Chúng ta có thể nhìn rõ request được gửi (Request) cũng như phản hồi từ phía server (Response)

### **2.1.2 Các chức năng chính của phần mềm Burp Suite**

Khi tiến hành tìm hiểu Burp Suite là gì thì chắc chắn bạn không thể bỏ qua các chức năng chính của phần mềm Burp Suite dưới đây:

Decoder là chức năng giúp giải mã (decode) và mã hóa (encode) các chuỗi theo nhiều dạng format khác nhau. Để sử dụng Decoder, bạn vào tab decoder và nhập các dữ liệu cần giải mã hoặc mã hoá.

A screenshot of a computer

Description automatically generated

Hình 2: Decoder

Proxy Server được thiết kế để bắt các yêu cầu và tuỳ ý sửa đổi chúng trước khi gửi lên máy chủ. Người dùng cần bật Burp Suite và vào tab proxy, sau đó option đánh dấu vào ô Running để sử dụng chức năng này.

A screenshot of a computer

Description automatically generated

Hình 3:Proxy Server

Chức năng Repeater cho phép người dùng sử dụng request được gửi đến máy chủ và có thể nhanh chóng sửa đổi nội dung yêu cầu một cách tuỳ ý trong nhiều lần khác nhau. Để có thể sử dụng Repeater, trước tiên bạn phải vào tab repeater có trong Burp Suite, sau đó lựa chọn mục tiêu ở góc trên bên phải và điền địa chỉ IP hoặc tên miền của mục tiêu vào cổng port tương ứng.

A screenshot of a computer

Description automatically generated

Hình 4:Repeater

Comparer là tính năng được sử dụng để phân biệt được sự khác nhau giữa các yêu cầu (requests) và phản hồi (reponses), so sánh một cách dễ dàng các tệp tin và các dữ liệu có dung lượng lớn.

A screenshot of a computer

Description automatically generated

Hình 5:Comparer

Web spider là tính năng duyệt web tự động được dùng với mục đích xác định cấu trúc của một trang web. Để có thể sử dụng tính năng này, bạn cần vào tab Sitemap và Target, sau đó thực hiện thao tác click chuột phải vào mục tiêu và lựa chọn spider cho máy chủ.

### **2.1.3 Lợi ích của phần mềm Burp Suite**

Burp Suite được nhiều doanh nghiệp áp dụng rất nhiều trong việc đánh giá web bởi họ hiểu được Burp Suite là gì cũng như những lợi ích mà phần mềm này có thể mang lại:

* Miễn phí: Burp Suite có hai phiên bản mà bạn có thể lựa chọn bao gồm phiên bản miễn phí (free) và phiên bản trả phí (pro). Bạn có thể lựa chọn phiên bản miễn phí để sử dụng được hết các tính năng chung của Burp Suite như Web spider, Comparer, Proxy Server, Repeater, Decoder,... hoặc lựa chọn phiên bản trả phí để sử dụng thêm chức năng scan web.
* Tiện lợi: Burp Suite được tích hợp rất nhiều các công cụ, tính năng khác nhau giúp tạo nên sự tiện lợi khi sử dụng hơn cho người dùng bởi Burp Suite đã giúp bạn mở được nhiều công cụ một lúc và bạn sẽ không cần phải tự mình làm điều đó.
* Dễ dàng sử dụng: Người dùng có thể sử dụng và chạy được nhiều ứng dụng Burp Suite một cách dễ dàng chỉ với một môi trường java và click đúp chuột vào các file chạy. Bên cạnh đó, giao diện Burp Suite cũng vô cùng thân thiện với những người dùng nhờ khả năng phát triển ngôn ngữ java.

### **2.1.4 Phiên bản của phần mềm Burp Suite**

A screenshot of a computer

Description automatically generated

Hình 6: Burp Suite Professinal

A blue screen with white text

Description automatically generated

Hình 7: Burp Siute Community Education

### **2.1.5. Cài đặt Burp suite**

$ sudo apt install burpsuite

A screenshot of a computer screen

Description automatically generated

$ burpsuite

A screenshot of a computer program

Description automatically generated

Giao diện burp suite:

A screenshot of a computer

Description automatically generated

Hình 8: Giao diện burp suite

Trình duyệt Chromium:

A screenshot of a computer

Description automatically generated

Hình 9: Trình duyệt Chromium

## **2.2 Mô hình hoạt động của Burp suite**

Burp Suite hoạt động như một proxy HTTP giữa trình duyệt web và máy chủ web. Khi bạn truy cập một trang web, Burp Suite sẽ chặn lưu lượng truy cập HTTP và cho phép bạn xem và sửa đổi nó trước khi được gửi đến máy chủ web.

Dưới đây là mô hình hoạt động của Burp Suite:

A diagram of a block diagram

Description automatically generated

Hình 10: Mô hình hoạt động của Burp Suite

Burp Suite bao gồm nhiều công cụ khác nhau có thể được sử dụng để kiểm tra thâm nhập các ứng dụng web. Các công cụ này có thể được sử dụng để:

* Giám sát lưu lượng truy cập HTTP: Proxy HTTP cho phép bạn giám sát tất cả lưu lượng truy cập HTTP giữa trình duyệt web và máy chủ web.
* Tự động quét các lỗ hổng bảo mật: Scanner có thể tự động quét các lỗ hổng bảo mật phổ biến.
* Thực hiện các cuộc tấn công brute force: Intruder có thể được sử dụng để thực hiện các cuộc tấn công brute force và fuzzing.
* Ghi lại và phát lại các yêu cầu HTTP: Repeater cho phép bạn ghi lại và phát lại các yêu cầu HTTP.
* Kiểm tra các lỗ hổng bảo mật liên quan đến trình tự: Sequencer cho phép bạn kiểm tra các lỗ hổng bảo mật liên quan đến trình tự.
* Giải mã và mã hóa dữ liệu: Decoder cho phép bạn giải mã và mã hóa dữ liệu.
* So sánh hai tập tin: Comparer cho phép bạn so sánh hai tập tin.
* Thêm các chức năng mới vào Burp Suite: Extender cho phép bạn thêm các chức năng mới vào Burp Suite.

Burp Suite là một công cụ mạnh mẽ và linh hoạt có thể được sử dụng để kiểm tra thâm nhập các ứng dụng web. Nó là một công cụ hữu ích cho các nhà kiểm tra bảo mật ở mọi cấp độ kinh nghiệm.

## **2.3 Cách sử dụng phần mềm Burp suite**

Dưới đây là các bước cơ bản để sử dụng Burp Suite:

### **2.3.1. Cài đặt Burp Suite**

Truy cập https://portswigger.net/burp/download.html và tải xuống phiên bản phù hợp với hệ điều hành của bạn.

### **2.3.2. Cấu hình Burp Suite**

Chọn proxy HTTP trong trình duyệt web của bạn:

* + Firefox:
    - Mở menu Firefox.
    - Chọn "Tùy chọn".
    - Nhấp vào tab "Mạng".
    - Chọn "Cài đặt proxy".
    - Chọn "Cấu hình thủ công".
    - Nhập địa chỉ proxy là "127.0.0.1" và cổng proxy là "8080".
    - Nhấp vào "OK".
  + Chrome:
    - Mở menu Chrome.
    - Chọn "Cài đặt".
    - Nhấp vào tab "Nâng cao".
    - Chọn "Mở cài đặt proxy".
    - Nhấp vào tab "Kết nối".
    - Chọn "Cài đặt proxy cho mạng của bạn".
    - Nhập địa chỉ proxy là "127.0.0.1" và cổng proxy là "8080".
    - Nhấp vào "Lưu".
  + Cấu hình Burp Suite để sử dụng proxy HTTP:
    - Mở Burp Suite.
    - Chọn tab "Proxy".
    - Nhấp vào tab "Options".
    - Chọn "Use Burp as a proxy".
    - Nhấp vào "OK".

### **2.3.3. Bắt đầu kiểm tra**

* Sử dụng Spider để quét trang web:
  + Chọn tab "Spider".
  + Nhập URL của trang web bạn muốn quét.
  + Nhấp vào "Start".
* Sử dụng Scanner để quét các lỗ hổng bảo mật:
  + Chọn tab "Scanner".
  + Nhấp vào "Start scan".
* Sử dụng Intruder để thực hiện các cuộc tấn công brute force và fuzzing:
  + Chọn tab "Intruder".
  + Chọn "Attack type".
  + Nhập dữ liệu tấn công.
  + Nhấp vào "Start attack".
* Sử dụng Repeater để ghi lại và phát lại các yêu cầu HTTP:
* Chọn tab "Repeater".
* Nhập URL của yêu cầu HTTP bạn muốn ghi lại.
* Nhấp vào "Send".
* Sửa đổi yêu cầu HTTP.
* Nhấp vào "Send".
* Sử dụng Sequencer để kiểm tra các lỗ hổng bảo mật liên quan đến trình tự:
  + Chọn tab "Sequencer".
  + Nhập URL của yêu cầu HTTP bạn muốn kiểm tra.
  + Nhấp vào "Start".
* Sử dụng Decoder để giải mã và mã hóa dữ liệu:
  + Chọn tab "Decoder".
  + Chọn loại dữ liệu bạn muốn giải mã hoặc mã hóa.
  + Nhập dữ liệu.
  + Nhấp vào "Decode" hoặc "Encode".
* Sử dụng Compare để so sánh hai tập tin:
  + Chọn tab "Comparer".
  + Chọn hai tập tin bạn muốn so sánh.
  + Nhấp vào "Compare".
* Sử dụng Extender để thêm các chức năng mới vào Burp Suite:
  + Chọn tab "Extender".
  + Chọn "Extension Manager".
  + Tìm kiếm extender bạn muốn cài đặt.
  + Nhấp vào "Install".

# **CHƯƠNG 3: CÀI ĐẶT VÀ TRIỂN KHAI CÁC CHỨC NĂNG PROXY, INTRUDER VÀ REPEATER CỦA BURP SUITE**

## **3.1 Cài đặt Burp suite**

- Sử dụng Burp Suite phiên bản: Burp Suite community Edition

A screenshot of a computer

Description automatically generated

* Link Download: https://portswigger.net/burp/communitydownload

A person lying on the floor with a computer

Description automatically generated

## **3.2 Proxy**

Proxy hiển thị chi tiết các request đi qua Burp Proxy. Tại đây, bạn có các tùy chọn Forward, Drop, Chỉnh sửa hay chuyển sang các action khác (repeater, intruder, etc...)

A screenshot of a computer

Description automatically generated

Open browser và sử dụng trang web đào tạo trường Công nghệ thông tin và truyền thông Việt - Hàn

Link: <https://daotao.vku.udn.vn/>

A screenshot of a computer

Description automatically generated

Trong phần chức năng Proxy của Burp suite:

* Phần đầu tiên hiển thị các yêu cầu và phản hồi HTTP giữa máy khách và máy chủ

A screenshot of a computer

Description automatically generated

* Trong ô bên trái Request hiển thị chi tiết của một yêu cầu gồm các thông tin như: phương thức GET/POST, Host, Cookie, User-Agent,...

A screenshot of a computer program

Description automatically generated

* Response: cho phép chúng ta đọc tất cả các dòng code của trang web

A screenshot of a computer program

Description automatically generated

* Inspector: phần tổng hợp các yêu cầu: Request attributes, Request cookies, Request headers, Response headers.

A screenshot of a computer

Description automatically generated

* Giám sát và phân tích giao tiếp HTTP: Proxy ghi lại các yêu cầu và phản hồi HTTP giữa máy khách và máy chủ. Điều này giúp nhà phát triển và nhà kiểm thử bảo mật hiểu được cách ứng dụng hoạt động và xác định các lỗ hổng bảo mật.
* Kiểm tra và chỉnh sửa yêu cầu và phản hồi: Người dùng có thể xem và chỉnh sửa yêu cầu và phản hồi HTTP trước khi chúng được gửi đi hoặc nhận về từ máy chủ. Điều này giúp trong việc kiểm tra các vấn đề về an ninh và hiệu suất.
* Thực hiện các cuộc tấn công phân tích và bảo mật: Proxy cho phép người dùng thực hiện các cuộc tấn công phân tích như kiểm tra kiểu tấn công giả mạo (spoofing), sử dụng công cụ kiểm tra như SQL injection, XSS, và nhiều hơn nữa để phát hiện và khai thác các lỗ hổng bảo mật trong ứng dụng web.
* Ghi lại hoạt động để làm chứng: Lịch sử HTTP được ghi lại bởi proxy có thể được sử dụng làm chứng cứ trong quá trình kiểm thử bảo mật hoặc trong các cuộc điều tra sau khi xảy ra sự cố.
* Tạo ra báo cáo và tài liệu: Dữ liệu từ HTTP history có thể được sử dụng để tạo ra báo cáo về các phát hiện, lỗ hổng bảo mật, và các vấn đề khác liên quan đến ứng dụng web.

## **3.3 Intruder**

Intruder cho phép test ứng dụng web bằng cách gửi các payloads đã được định nghĩa trước lên server, sau đó xem xét kết quả trả về.

Trong demo này đăng nhập vào 1 trang web bằng tài khoản và mật khẩu đơn giản: <http://testphp.vulnweb.com/login.php>

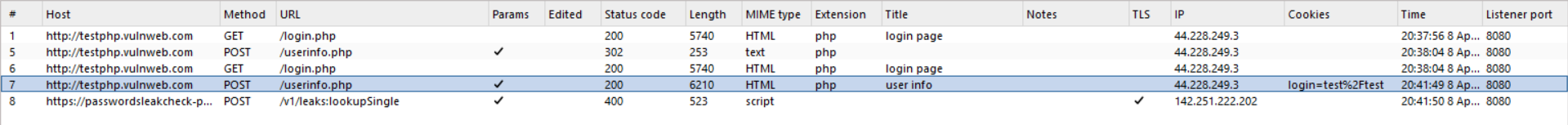
A screenshot of a computer

Description automatically generated

Và Mặc định tài khoản và mật khẩu là “test”.  
A screenshot of a computer

Description automatically generated

Và bắt gói tin loginbên tab Proxy



Chuyển qua Intruder

A screenshot of a computer

Description automatically generated

Và burp suite có thể quét được username và pass của web chúng ta vừa login.

## **3.4 Repeater**

Repeater có thể tùy ý thay đổi và gửi lại những request khác nhau tới server. Đồng thời sẽ nhận về response từ server để có thể phân tích được gói tin.

A screenshot of a computer

Description automatically generated

# **KẾT LUẬN**

## **1. Kết quả thu được**

Bản thân tích lũy được kinh nghiệm trong việc tìm hiểu về công cụ Burp Suite cũng như bảo mật web. Đã tìm hiểu và trải nghiệm được khi kiểm tra bảo mật của một trang web là như thế nào.

## **2. Về hạn chế**

- Do thời gian khá hạn chế nên xây dựng mô phỏng nhỏ.

- Chưa hiểu biết sâu rộng về thế giới bảo mật web.

- Các công cụ kiểm tra lỗ hổng là một phần quan trong trong quá trình kiểm thử cũng như Burp Suite rất tốt và rộng, khi làm việc với Burp Suite thì có nhiều thứ chưa hiểu rõ, và chúng em cần thêm thời gian trải nghiệm thực tế.

# **DANH MỤC TÀI LIỆU THAM KHẢO**

**Các trang web tham khảo:**

[1] Công cụ Burp Suite: [Download Burp Suite Community Edition - PortSwigger](https://portswigger.net/burp/communitydownload)

[2] Tổng quan về Burp Suite: https://bizfly.vn/techblog/burp-suite-la-gi.html

[3] [Burp Suite Cơ Bản - Dò Lỗ Hổng Bảo Mật Trên Ứng Dụng Web](https://viblo.asia/p/burp-suite-co-ban-do-lo-hong-bao-mat-tren-ung-dung-web-L4x5xreqZBM)

[4] [Lợi ích khi sử dụng phần mềm Burp Suite trong đánh giá bảo mật](https://smartnet.net.vn/loi-ich-khi-su-dung-phan-mem-burp-suite-trong-danh-gia-bao-mat/)

[5] [Web Pentest - Bài 1: Burp Academy và Giới thiệu về Burp Suite | WhiteHat.vn](https://whitehat.vn/threads/web-pentest-bai-1-burp-academy-va-gioi-thieu-ve-burp-suite.14724/)