TRƯỜNG ĐẠI HỌC KHOA HỌC

**KHOA CÔNG NGHỆ THÔNG TIN**

A blue and white sign with a white letter and a red circle

Description automatically generated  
  
  
TIỂU LUẬN MÔN HỌC

**AN NINH MẠNG**

**Tìm hiểu các kỹ thuật tấn công Clickjacking trên dịch vụ Web và thử nghiệm các cách thức phòng chống.**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn:**  Võ Việt Dũng | **Nhóm sinh viên thực hiện:**  1.Võ Văn Cường - 22T1020047  2. Nguyễn Trần Văn Phước Đức - 22T1020075  3. Mai Hồng Phúc - 22T1020324  4. Dương Phước Anh Quân - 22T1020345  5. Phan Thanh Vũ - 22T1020803  **Nhóm:** 3  **Lớp:** Công Nghệ Thông Tin K46  **Năm học:** 2024/2025 |

***Huế 1/2025***

# ***Lời nói đầu***

Trong thời đại công nghệ số phát triển mạnh mẽ và vượt bật như hiện nay, công nghệ thông tin đã trở thành một phần không thể thiếu trong cuộc sống hiện đại, đóng vai trò quan trọng trong việc kết nối con người, xử lý thông tin và thúc đẩy sự phát triển của xã hội. Nhờ vào công nghệ thông tin, các hoạt động như giao tiếp, giáo dục, y tế và kinh doanh được thực hiện nhanh chóng và hiệu quả hơn, mang đến nhiều lợi ích vượt trội như tiết kiệm thời gian, chi phí và nâng cao chất lượng cuộc sống.

Tuy nhiên, cùng với sự phát triển mạnh mẽ đó, mối nguy cơ về mất an toàn an ninh mạng ngày càng gia tăng. Các cuộc tấn công mạng, đánh cắp thông tin cá nhân, và lừa đảo trực tuyến đang đặt ra nhiều thách thức lớn cho các cá nhân và tổ chức trên toàn thế giới trong đó có Việt Nam. Do đó, việc nâng cao nhận thức về an ninh mạng và chủ động áp dụng các biện pháp phòng ngừa là yếu tố then chốt để đảm bảo an toàn trong môi trường mạng.

Nhận thức được tầm quan trọng của các giải pháp an ninh mạng, nên nhóm chúng em đã chọn đề tài “Tìm hiểu các kỹ thuật tấn công Clickjacking trên dịch vụ Web và thử nghiệm các cách thức phòng chống” để nghiên cứu, với mục đích là để tìm tòi học hỏi và nâng cao kiến thức của bản thân về thế giới Internet hiện nay.

**Mục Lục**

[*Lời nói đầu* 2](#_Toc187329002)

[Chương I. Tìm hiểu về Clickjacking. 4](#_Toc187329003)

[1.Khái niệm clickjacking 4](#_Toc187329004)

[1.1.Clickjacking là gì? 4](#_Toc187329005)

[1.2.Clickjacking xảy ra khi nào? 4](#_Toc187329006)

[2.Mục đích của những kẻ tấn công sử dụng Clickjacking 4](#_Toc187329007)

[2.1.Mục đích của những kẻ tấn công 4](#_Toc187329008)

[2.2.Cách người dùng phòng chống các cuộc tấn công clickjacking. 5](#_Toc187329009)

[Chương II. Kỹ thuật tấn công và phòng thủ Clickjacking 6](#_Toc187329010)

[1. Các kỹ thuật tấn công Clickjacking 6](#_Toc187329011)

[1.1.Một số kỹ thuật tấn công Clickjacking 6](#_Toc187329012)

[1.2.Ưu và nhược điểm của các cuộc tấn công Clickjacking 7](#_Toc187329013)

[2. Phòng thủ Clickjacking. 8](#_Toc187329014)

[2.1.Các biện pháp phòng thủ. 8](#_Toc187329015)

[2.2.Cách kiểm tra. 9](#_Toc187329016)

[Chương III. Demo tấn công và phòng thủ Clickjacking 10](#_Toc187329017)

[1. Demo tấn công bằng Clickjacking 10](#_Toc187329018)

[2. Demo phòng thủ Clickjacking 12](#_Toc187329019)

[Chương IV: Kết Luận 14](#_Toc187329020)

[**1. Kết quả đạt được** 14](#_Toc187329021)

[**2. Ưu và nhược điểm** 14](#_Toc187329022)

[**3.Hướng phát triển** 15](#_Toc187329023)

[Nguồn tài liệu tham khảo 16](#_Toc187329024)

Tìm hiểu các kỹ thuật tấn công Clickjacking trên dịch vụ Web và thử nghiệm các cách thức phòng chống**.**

# **Chương I. Tìm hiểu về Clickjacking.**

## 1.Khái niệm clickjacking

### 1.1.Clickjacking là gì?

Clickjacking, hay còn được gọi là **tấn công giao diện người dùng giả mạo (UI redress attack)**, là một kỹ thuật mà kẻ tấn công lừa người dùng nhấp vào một thứ khác với những gì người dùng nghĩ. Thủ thuật này thường được thực hiện bằng cách chồng các thành phần trong suốt hoặc mờ đục lên một trang web hợp pháp, vì vậy khi người dùng nhấp vào cái mà họ nghĩ là một nút hoặc liên kết vô hại, họ thực sự đang tương tác với một phần tử ẩn do kẻ tấn công kiểm soát.

### 1.2.Clickjacking xảy ra khi nào?

Clickjacking xảy ra khi kẻ tấn công lừa một người dùng không nghi ngờ nhấp vào một phần tử vô hình. Yếu tố đó được ẩn trong giao diện người dùng và khó phát hiện ra.

## 2.Mục đích của những kẻ tấn công sử dụng Clickjacking

### 2.1.Mục đích của những kẻ tấn công

Mục đích của cuộc tấn công clickjacking là để lôi kéo người dùng truy cập trang web nhấp vào [trang web bị tấn công](https://vi.itpedia.nl/2022/03/27/gehackt-door-geinfecteerde-website-te-bezoeken/) khi nhấp chuột, kích hoạt một hành động trên một trang web có khung nội tuyến giả mạo khác. Các nhấp chuột này có thể dẫn đến việc xóa người dùng, cập nhật quyền hoặc các hành động khác. Chúng là các nhấp chuột và hành động thường đã được thực hiện trên trang web, nhưng bây giờ có một lớp ẩn giữa chúng thực hiện các hành động của họ.

* **Mục đích cụ thể của những kẻ tấn công bao gồm:**

**+ Đánh cắp thông tin cá nhân:** Bằng cách nhấp vào các nút ngụy trang , người dùng có thể vô tình gửi thông tin cá nhân như tên, số điện thoại, email, địa chỉ, hoặc cá thông tin quan trong liên quan đến tài sản cá nhân cho kẻ tấn công

**+ Chiếm quyền điều khiển tài khoản:** Kẻ tấn công có thể chiếm quyền điều khiển tài khoản của người dùng bằng cách lừa họ nhấp vào các liên kết hay nút đăng nhập hoặc thay đổi mật khẩu bằng các giao diện giống với các giao diện web uy tín khác.

**+ Thực hiện các giao dịch trái phép:** Kẻ tấn công có thể lừa người dùng nhấp vào các liên kết chuyển tiền hoặc thanh toán, khiến họ thực hiện các giao dịch tài chính không mong muốn.

**+ Phát tác các phần mềm độc hại:** Người dùng có thể bị lừa nhấn vào các liên kết tải xuống phần mềm hoặc tệp tin, từ đó phát tán các phần mềm độc hại hoặc virus lên máy tính của họ nhằm chiếm quyền kiểm soát hoặc đánh cắp thông tin cá nhân.

**+ Tăng lượt xem hoặc lượt click:** Kẻ tấn công sử dụng clickjacking dưới dạng nút ẩn trên các trang web để tăng lượt xem hoặc lượt click giả mạo cho trang web, quảng cáo, hoặc nội nào đó nhằm mục đích kinh doanh hoặc tăng doanh thu quảng cáo.

### 2.2.Cách người dùng phòng chống các cuộc tấn công clickjacking.

* **Cập nhật phần mềm thường xuyên**: Đảm bảo trình duyệt và phần mềm bảo mật luôn được cập nhật để bảo vệ khỏi các cuộc tấn công.
* **Kích hoạt cài đặt bảo mật trên trình duyệt**: Sử dụng các cài đặt bảo mật tích hợp sẵn và các phần mở rộng giúp chặn nội dung độc hại.
* **Tránh các liên kết đáng ngờ**: Hạn chế nhấp vào các liên kết từ nguồn không rõ ràng hoặc email lạ.
* **Cập nhật kiến thức**: Thường xuyên đọc các mẹo và tin tức về an ninh mạng để cập nhật các mối đe dọa và biện pháp phòng chống mới nhất.

# **Chương II. Kỹ thuật tấn công và phòng thủ** Clickjacking

## 1. Các kỹ thuật tấn công Clickjacking

### 1.1.Một số kỹ thuật tấn công Clickjacking

Một trong những hình thức clickjacking phổ biến nhất là chồng chéo nội dung độc hại lên đầu trang hiện có (lớp phủ nội dung). Kẻ tấn công có thể đạt được clickjacking bằng một số cách:

* **Iframe ẩn**: Kẻ tấn công tải iframe 1 × 1 vô hình ngăn người dùng nhìn thấy nội dung. Phần tử mục tiêu của iframe vô hình, chẳng hạn như một nút trên trang web, được đặt chính giữa dưới con trỏ của nạn nhân, giúp dễ dàng đánh lừa người dùng nhấp vào nội dung độc hại.
* **Sự kiện con trỏ**: Kẻ tấn công tạo một thẻ div nổi bao phủ hoàn toàn phần tử giao diện người dùng mục tiêu. Kẻ tấn công đặt thuộc tính sự kiện con trỏ CSS thành 'không có', khiến các nhấp chuột đi qua chúng, đăng ký chúng trên iframe đằng sau nó.
* **Lớp phủ trong suốt:** kẻ tấn công đặt một cửa sổ trong suốt lên trên phần tử mà người dùng sẽ nhấp vào. Nạn nhân không nhìn thấy cửa sổ trong suốt và nghĩ rằng họ đang nhấp vào nút hoặc phần tử liên kết hợp pháp. Nhưng vì cửa sổ trong suốt của kẻ tấn công là nội dung trên cùng của trang, nên kẻ tấn công chiếm quyền điều khiển lần nhấp.
* **Thay thế nội dung nhanh chóng**: Trong cuộc tấn công này, tin tặc tạo ra các lớp phủ mờ để che các phần tử mục tiêu trên trang web. Hành động được thực hiện gần như ngay lập tức (mili giây), ngay trước khi nạn nhân truy cập trang web. Kỹ thuật này đòi hỏi kẻ tấn công phải có khả năng dự đoán thời điểm nhấp chuột với độ chính xác nhất định. Lớp phủ có thể nhìn thấy chỉ đủ lâu để chặn nhấp chuột trước khi ẩn nó.
* **Con trỏ chuột ma**: Sử dụng thẻ div nổi, hacker có thể tạo thêm một con trỏ chuột và đặt nó ở một khoảng cách cố định so với con trỏ chuột thật của nạn nhân. Sau đó, tin tặc sẽ sửa đổi trang để con trỏ lừa đảo nổi bật hơn.Kẻ tấn công cũng đặt một phần tử mà nạn nhân phải nhấp vào trang. Nạn nhân nhìn thấy một con trỏ giả bắt chước chuyển động chuột của chính anh ta và điều đó đánh lừa anh ta nhấp vào phần tử độc hại trước khi nhận ra điều gì đã xảy ra.

### 1.2.Ưu và nhược điểm của các cuộc tấn công Clickjacking

**Ưu điểm:**

**-** Khó phát hiện: Clickjacking thường diễn ra một cách khuất phục, khiến nạn nhân không nhận thức được mình đang bị lừa.

**-**Tinh vi và linh hoạt: Kẻ tấn công có thể sử dụng nhiều phương pháp khác nhau để che giấu các đường link độc hại, làm cho tấn công trở nên khó phòng ngừa.

**-** Tính chất đa nhiệm: Clickjacking có thể được kết hợp với các loại tấn công khác như CSRF (Cross-Site Request Forgery) để tăng tính hiệu quả của tấn công.

**Nhược điểm:**

- Gây thiệt hại lớn: Clickjacking có thể dẫn đến việc lừa đảo thông tin cá nhân, chuyển tiền không mong muốn, hoặc thực hiện các hành động không mong muốn.

-Mất niềm tin: Người dùng có thể mất niềm tin vào các trang web và dịch vụ mạng, ảnh hưởng đến danh tiếng và uy tín của doanh nghiệp.

-Khó phục hồi: Việc phát hiện và khắc phục các hậu quả của clickjacking có thể là một quá trình phức tạp và mất nhiều thời gian.

## 2. Phòng thủ Clickjacking.

### 2.1.Các biện pháp phòng thủ.

Để phòng ngừa các cuộc tấn công Clickjacking, ta có thể thực hiện các biện pháp bảo mật sau:

* Sử dụng tiêu đề X-Frame-Options

Tiêu đề HTTP của [**X-Frame**](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)**-Options**ngăn chặn việc sử dụng trang web cho các iframe vô hình.

**DENY**: Không cho phép trang web nào nhúng vào trang web của bạn

**SAMEORIGIN**: Chỉ cho phép các trang cùng nguồn (cùng domain) nhúng trang của bạn.

**ALLOW-FROM uri**: Cho phép một URI cụ thể nhúng trang của bạn.

Ví dụ: Bạn muốn ngăn chặn bất kỳ trang nào nhúng vào trang của bạn, có thể sử dụng:

X-Frame-Options: DENY

* **Content Security Policy (CSP)**:

CSP là một lớp bảo mật bổ sung giúp ngăn chặn các cuộc tấn công như XSS và clickjacking.

Sử dụng chỉ thị **frame-ancestors** để kiểm soát các nguồn được phép nhúng vào trang của bạn.

Ví dụ: Để chỉ cho phép các trang từ cùng nguồn nhúng trang của bạn, bạn có thể sử dụng:

Content-Security-Policy: frame-ancestors 'self'

* **Kiểm tra độ tin cậy của trang web:**

Hãy xác định rõ ràng các trang web mà bạn tin cậy để nhúng nội dung của bạn. Không cho phép nhúng từ các trang có nguồn gốc không rõ ràng hoặc không tin cậy.

* **Sử dụng JavaScript để kiểm tra xem trang của bạn có bị nhúng không.**

Bạn có thể thêm một đoạn mã JavaScript để kiểm tra xem trang của bạn có đang được nhúng trong iframe hay không. Nếu có, bạn có thể chuyển hướng người dùng đến trang ban đầu để tránh clickjacking.

Ví dụ:

if (top !== self) {

top.location = self.location.href;

}

* **Thiết lập cookie xác thực SameSite=Strict**

Clickjacking của cookie phiên cũng có thể được ngăn chặn. Chúng ta có thể thiết lập cookie xác thực trên cùng một trang web trong tiêu đề phản hồi HTTP của mình. Tuy nhiên, điều này không ngăn chặn hành vi iframe độc hại, nhưng ngăn người dùng đăng nhập vào trang web khi nó đang ở trong một iframe.

**Set**-Cookie: **authorization**=secret; same site

### 2.2.Cách kiểm tra.

Một cách dễ dàng để kiểm tra xem trang web có dễ bị Clickjacking hay không là sử dựng HTML.

1.Tạo trang HTML với iframe.

2.Đặt trang web cần kiểm tra vào trong iframe đó

3.Chúng ta cần đặt trang HTML này trên một máy chủ web khác để thử nghiệm cách thức một cuộc tấn công Clickjacking.

**Kết luận phòng thủ Clickjacking:**

Những kẻ tấn công có thể dễ dàng thực hiện việc tấn công bằng Clickjacking. Bất kỳ hành động nào trên trang web mà người dùng có thể thực hiện bằng cú click chuột điều có thể bị tấn công từ clickjacking

Để giảm thiểu rủi ro trong các cuộc tấn công, chúng ta nên sử dụng các biện pháp phòng thủ Clickjacking cho trang web của mình như sử dụng  X-Frame-Options. Cũng như sử dụng các chính sách bảo mật nội dung để giảm thiểu rủi ro và bảo vệ và chống lại các cuộc tấn công bằng clickjacking. Điều duy nhất người dùng có thể làm là cảnh giác.

# **Chương III. Demo tấn công và phòng thủ Clickjacking**

## 1. Demo tấn công bằng Clickjacking

Trang bị tấn công: index.html

A screenshot of a computer

Description automatically generated

Trang tấn công: attack.html

Sử dụng thẻ iframe để nhúng và hiển thị nội dung của trang index.html lên trang attack.html

    <iframe src="index.html" width="1500" height="600" frameborder="0"></iframe>

A screen shot of a computer code

Description automatically generated

Sử dụng thuộc tính css cho form đăng nhập attack.html:

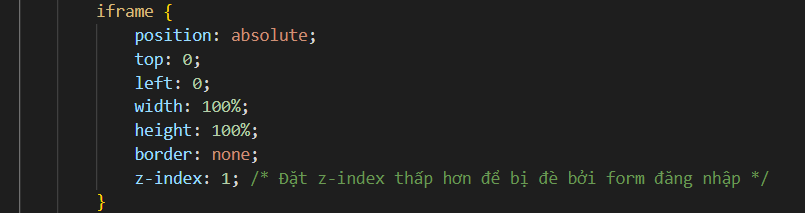
z – index: 2; // đặt z-index cao hơn để hiển thị trên iframe

opacity: 0; // Làm cho form đăng nhập trong suốt để người dùng không nhìn thấy

A computer screen shot of a black screen

Description automatically generated

z – index: 1; //để iframe bị đè bởi form đăng nhập



Sau khi sử dụng thẻ iframe thì giao diện trang index.html đã hiển thị trên attack.html

A screenshot of a computer

Description automatically generated

Khi người dùng bị lừa truy cập vào trang attack.html mà không hề nhận thức được hay chú ý đến liên kết của trang web, họ có thể bị lừa nhập tài khoản và mật khẩu vào trang tấn công clickjacking. Toàn bộ thông tin tài khoản và mật khẩu sau đó sẽ được gửi trực tiếp đến kẻ tấn công, để từ đó họ có thể truy cập vào các tài khoản này một cách bất hợp pháp.

## 2. Demo phòng thủ Clickjacking

- Sử dụng tiêu đề HTTP X-Frame-Options:

    <meta http-equiv="X-Frame-Options" content="DENY" />

A screen shot of a computer code

Description automatically generated

- Sử dụng **JavaScript Frame Busting** để phát hiện nếu trang web đang bị nhúng trong một iframe và điều hướng người dùng ra khỏi iframe.

A screen shot of a computer code

Description automatically generated

# **Chương IV: Kết Luận**

## **1. Kết quả đạt được**

Trong quá trình thực hiện đề tài, nhóm em đã được học thêm nhiều kiến thức bổ ích về an ninh mạng, nhóm em đã nghiên cứu được các kiến thức cơ bản về an ninh mạng, các kiểu tấn công cũng như các giải pháp an ninh mạng hiện nay. Ngoài ra, nhóm chúng em cũng đã tìm hiểu được những kiến thức cơ bản về clickjacking, bao gồm những cách tấn công mà kẻ tấn công có thể sử dụng và những giải pháp phòng thủ cho vấn đề tấn công clickjacking. Mặc dù chỉ là những kiến thức cơ bản nhưng đó là một phần nổ lực cố gắng nghiên cứu về đề tài của chúng em.

## **2. Ưu và nhược điểm**

Về các thành viên trong nhóm:

* Ưu điểm:
* Có khả năng tìm tòi học hỏi kiến thức và làm việc nhóm.
* Triển khai được các biện pháp.
* Việc thực hiện các demo và mô phỏng các cuộc tấn công và phòng thủ giúp nhóm có cơ hội thực hành và kiểm chứng kiến thức đã học.
* Nhược điểm:
* Kiến thức chuyên sâu còn hạn chế.
* Phụ thuộc quá nhiều vào nguồn tài liệu.
* Còn gặp nhiều khó khăn trong việc thực nghiệm.

Về phòng thủ clickjacking

* Ưu điểm:
* Dễ triển khai, hiệu quả cao
* Bảo vệ toàn diện
* Ngăn chặn tấn công từ phía máy chủ
* Nhược điểm:
* Không bảo vệ tuyệt đối
* Cấu hình phức tạp: Đối với các trang web lớn và phức tạp, việc cấu hình CSP và kiểm tra nguồn gốc của các yêu cầu có thể đòi hỏi nhiều công sức và dễ dẫn đến lỗi nếu không được cấu hình đúng cách.
* Hạn chế khả năng nhúng: Các biện pháp như X-Frame-Options: DENY hoặc CSP có thể ngăn chặn trang web được nhúng trên các trang web khác một cách hợp pháp, ảnh hưởng đến các ứng dụng hợp tác hoặc tích hợp dịch vụ.

## **3.Hướng phát triển**

Vì thời gian tìm hiểu còn hạn hẹp nên thực nghiệm trên chưa được hoàn thiện tốt nhất. Trong tương lai, nhóm chúng em sẽ không ngừng nỗ lực học hỏi và khám phá thêm nhiều kiến thức mới. Mục tiêu là tìm hiểu đầy đủ và tối ưu hóa các giải pháp, đáp ứng hiệu quả các yêu cầu về an ninh mạng.

# **Nguồn tài liệu tham khảo**

1.Clickjacking là gì và làm cách nào để ngăn chặn nó?

<https://vi.itpedia.nl/2022/10/02/wat-is-clickjacking-en-hoe-voorkomen-we-het/>

2.Clickjacking attack là gì? Cách phát hiện và phòng tránh hiệu quả.

<https://bizflycloud.vn/>

3. Kiểm tra lỗ hổng bảo mật Clickjacking

<https://websitehcm.com/kiem-tra-lo-hong-bao-mat-clickjacking/?form=MG0AV3>