Franz Payer

Tactical Network Solutions

http://cyberexplo.it

EXPLOITING MUSIC STREAMING WITH JAVASCRIPT

Acknowledgements

- Zachary Cutlip
- Craig Heffner
- Tactical Network Solutions

What I’m going to talk about

- Music streaming basics
- Security investigation process
- Music player mimicking
- Exploit demo
- Man-in-the-middle interception
- Questions

What is streaming?

- A way to constantly receive and present data while it is being delivered by a provider – Wikipedia
- 2 methods
  - Custom protocol
  - HTTP

Where's the vulnerability?

- Music files can be retrieved by mimicking the client player
- Web traffic is easily intercepted
- Can be done entirely from the browser

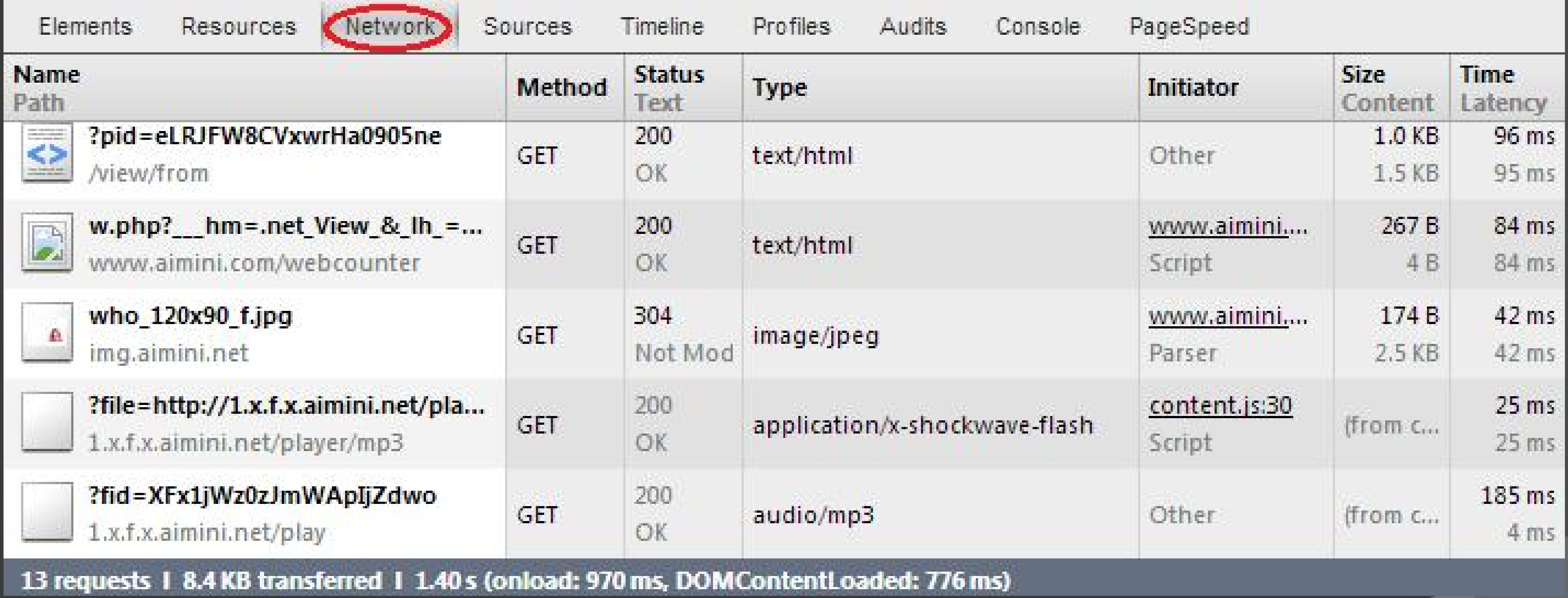
Process

- Locate music file in network traffic
- Inspect any parameters in the request
- Locate origin of those parameters
  - Page URL
  - Page source
  - JavaScript
- Attempt to replicate the request

Target: Aimini

- Flash
- Almost nonexistent security
- Good first target
  - Don’t even need to look at the code

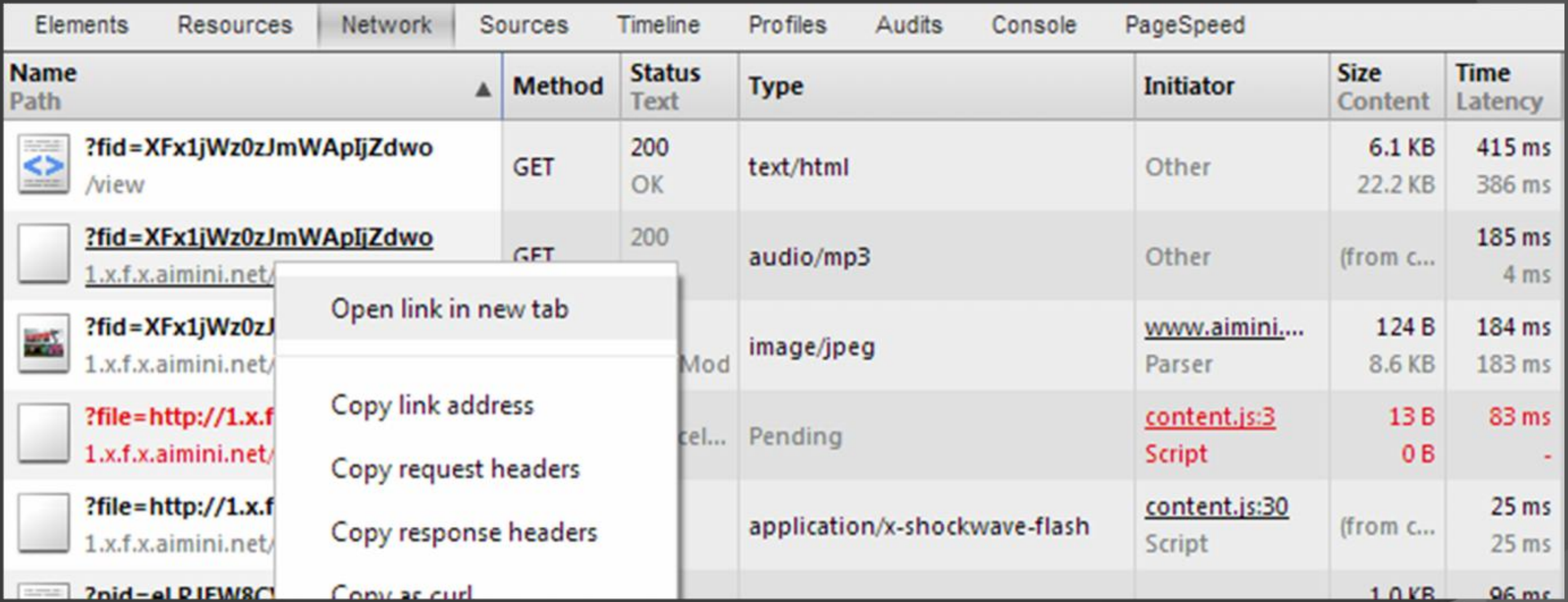
Analyzing the target



Name Path	Method	Status Text	Type	Initiator	Size Content	Time Latency
?pid=eLRJFW8CVxwrHa0905ne /view/from	GET	200 OK	text/html	Other	1.0 KB 1.5 KB	96 ms 95 ms
w.php?__hm=.net_View_&_lh_=... www.aimini.com/webcounter	GET	200 OK	text/html	www.aimini.... Script	267 B 4 B	84 ms 84 ms
who_120x90_f.jpg img.aimini.net	GET	304 Not Mod	image/jpeg	www.aimini.... Parser	174 B 2.5 KB	42 ms 42 ms
?file=http://1.x.f.x.aimini.net/pla... 1.x.f.x.aimini.net/player/mp3	GET	200 OK	application/x-shockwave-flash	content.js:30 Script	(from c...	25 ms 25 ms
?fid=XFx1jWz0zJmWApIjZdwo 1.x.f.x.aimini.net/play	GET	200 OK	audio/mp3	Other	(from c...	185 ms 4 ms

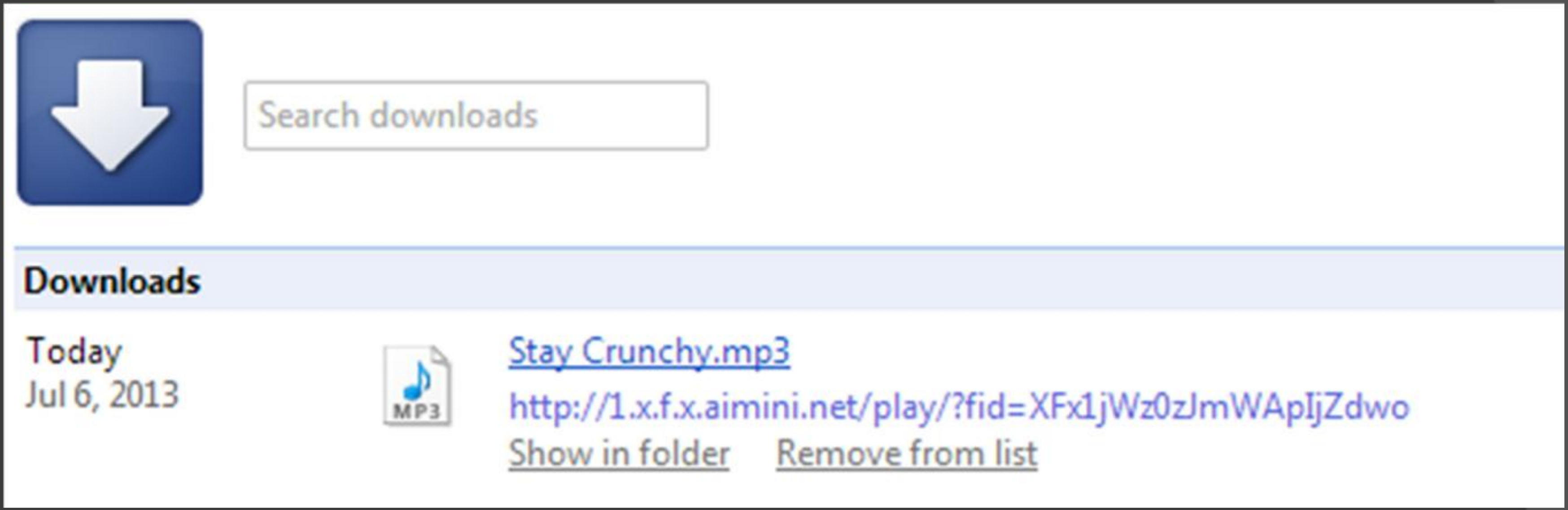
13 requests I 8.4 KB transferred I 1.40 s (onload: 970 ms, DOMContentLoaded: 776 ms)

The cheap way out



Name Path	Method	Status Text	Type	Initiator	Size Content	Time Latency
?fid=XFx1jWz0zJmWApIjZdwo /view	GET	200 OK	text/html	Other	6.1 KB 22.2 KB	415 ms 386 ms
?fid=XFx1jWz0zJmWApIjZdwo 1.x.f.x.aimini.net/	GET	200	audio/mp3	Other	(from c...	185 ms 4 ms
?fid=XFx1jWz0zJ 1.x.f.x.aimini.net/		Mod	image/jpeg	www.aimini.... Parser	124 B 8.6 KB	184 ms 183 ms
?file=http://1.x.f 1.x.f.x.aimini.net/		cel...	Pending	content.js:3 Script	13 B 0 B	83 ms -
?file=http://1.x.f 1.x.f.x.aimini.net/			application/x-shockwave-flash	content.js:30 Script	(from c...	25 ms 25 ms
?pid=eLRJEW8C					1.0 KB	96 ms

The cheap way out

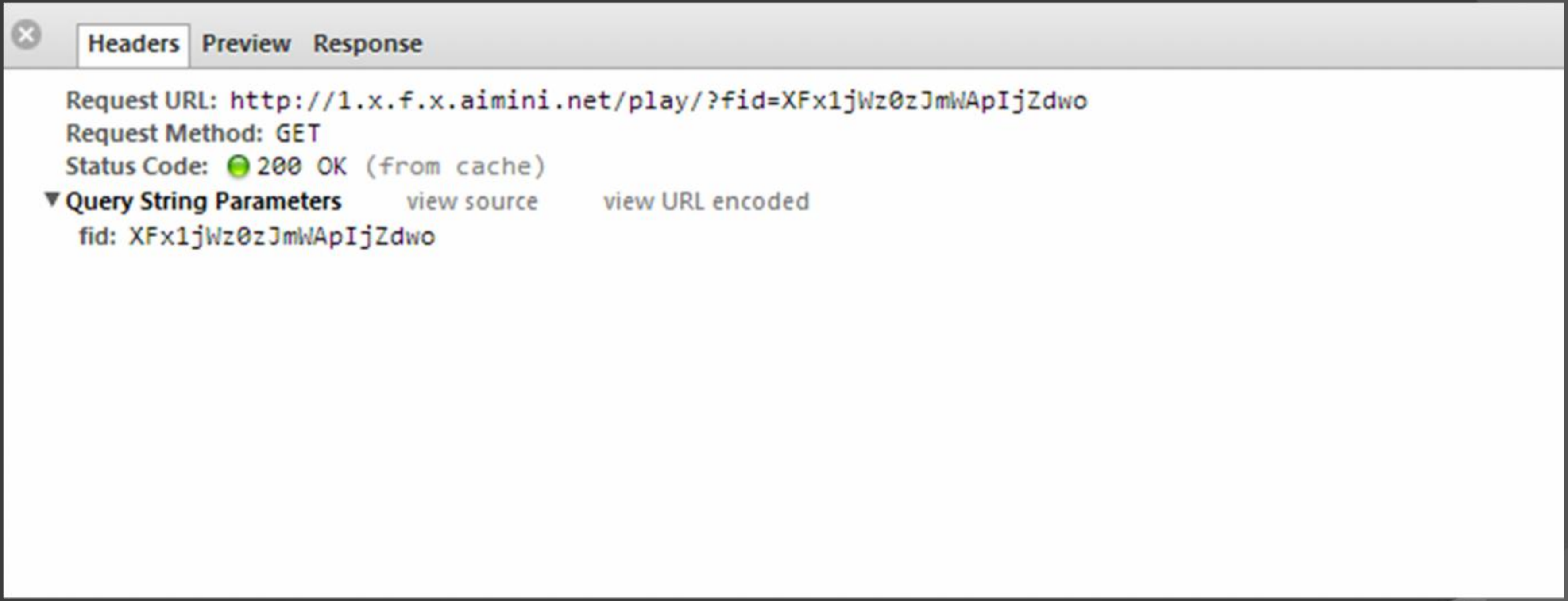


Downloads

Today
Jul 6, 2013

Stay Crunchy.mp3
http://1.x.f.x.aimini.net/play/?fid=XFx1jWz0zJmWApIjZdwo

Analyzing the target: song file

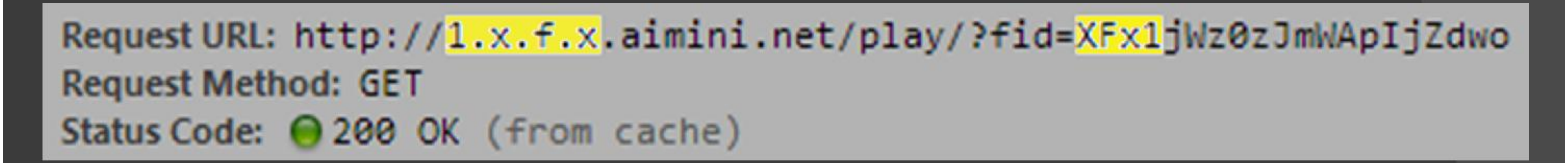


Request URL: http://1.x.f.x.aimini.net/play/?fid=XFx1jWz0zJmWApIjZdwo
Request Method: GET
Status Code: ● 200 OK (from cache)

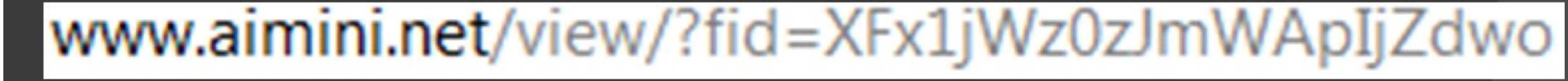
▼ Query String Parameters

fid: XFx1jWz0zJmWApIjZdwo

Analyzing the target: song file



```
Request URL: http://1.x.f.x.aimini.net/play/?fid=XFx1jWz0zJmWApIjZdwo
Request Method: GET
Status Code: ● 200 OK (from cache)
```



www.aimini.net/view/?fid=XFx1jWz0zJmWApIjZdwo

Demo Time

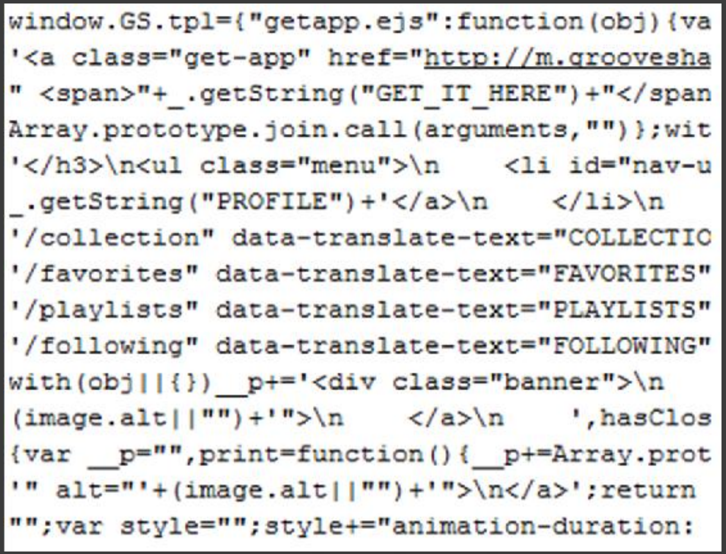
aimini

Target: Grooveshark

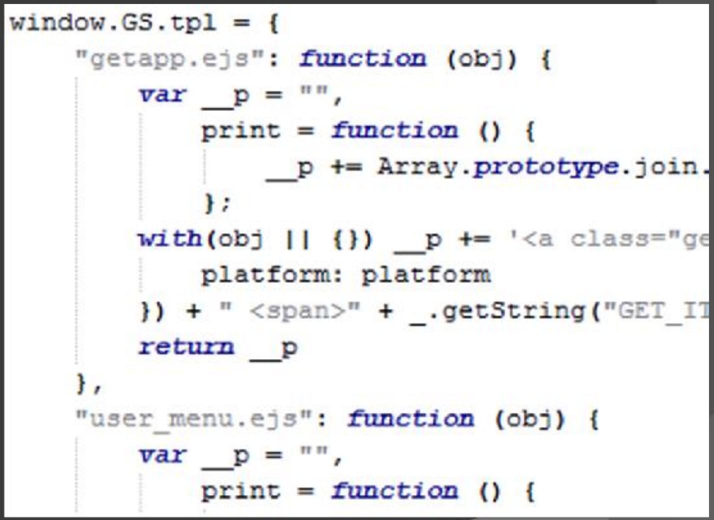
- HTML5
- Several factors of authentication
- Minified JavaScript
- Not for the faint of heart

JavaScript beautifier

- You're going to need it
- http://jsbeautifier.org/

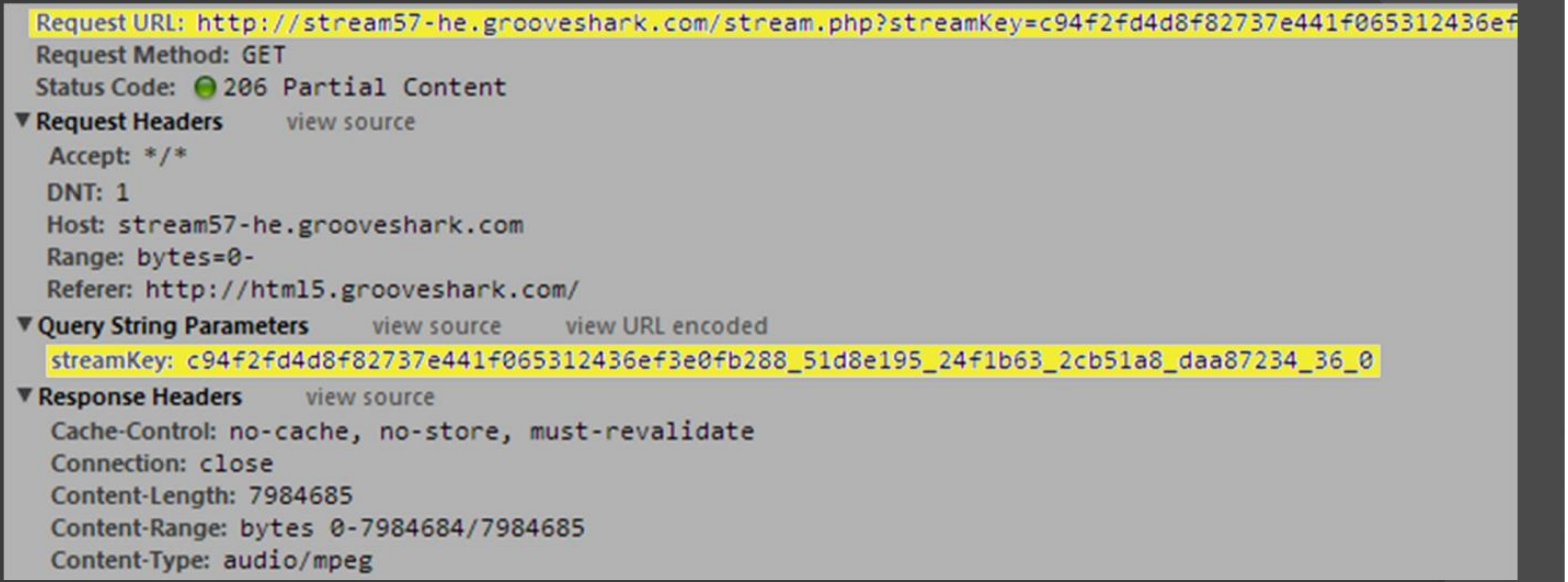


```
window.GS.tpl={"getapp.ejs":function(obj){va
'<a class="get-app" href="http://m.groovesha
" <span>"+_.getString("GET_IT_HERE")+"</span
Array.prototype.join.call(arguments,"")};wit
'</h3>\n<ul class="menu">\n    <li id="nav-u
_.getString("PROFILE")+'</a>\n    </li>\n
'/collection" data-translate-text="COLLECTIO
'/favorites" data-translate-text="FAVORITES"
'/playlists" data-translate-text="PLAYLISTS"
'/following" data-translate-text="FOLLOWING"
with(obj||{})__p+='<div class="banner">\n
(image.alt||"")+'">\n    </a>\n    ',hasClos
{var __p="",print=function(){__p+=Array.prot
'" alt="'+(image.alt||"")+'">\n</a>';return
"";var style="";style+="animation-duration:
```



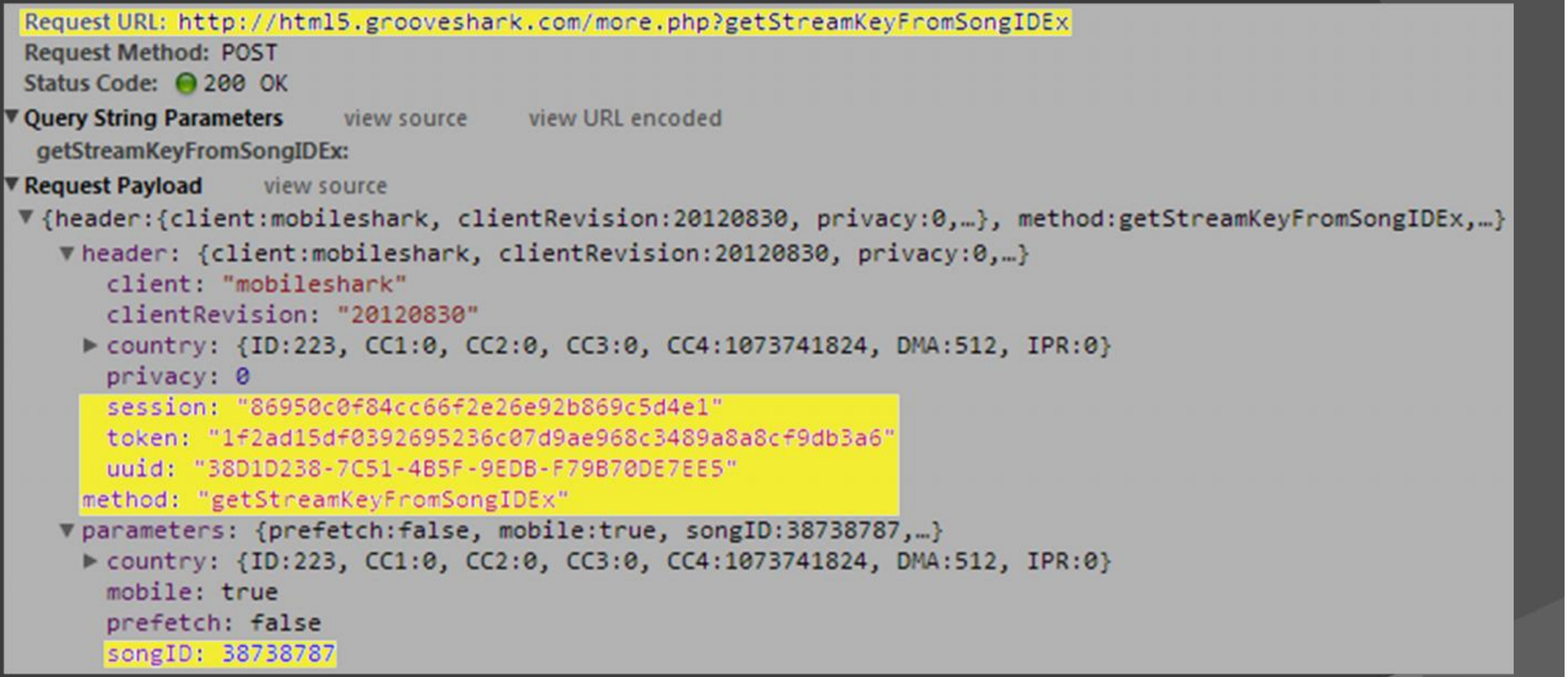
```
window.GS.tpl = {
    "getapp.ejs": function (obj) {
        var __p = "",
            print = function () {
                __p += Array.prototype.join.
            };
        with(obj || {}) __p += '<a class="ge
            platform: platform
        }) + " <span>" + _.getString("GET_IT
        return __p
    },
    "user_menu.ejs": function (obj) {
        var __p = "",
            print = function () {
```

Analyzing the target: song file



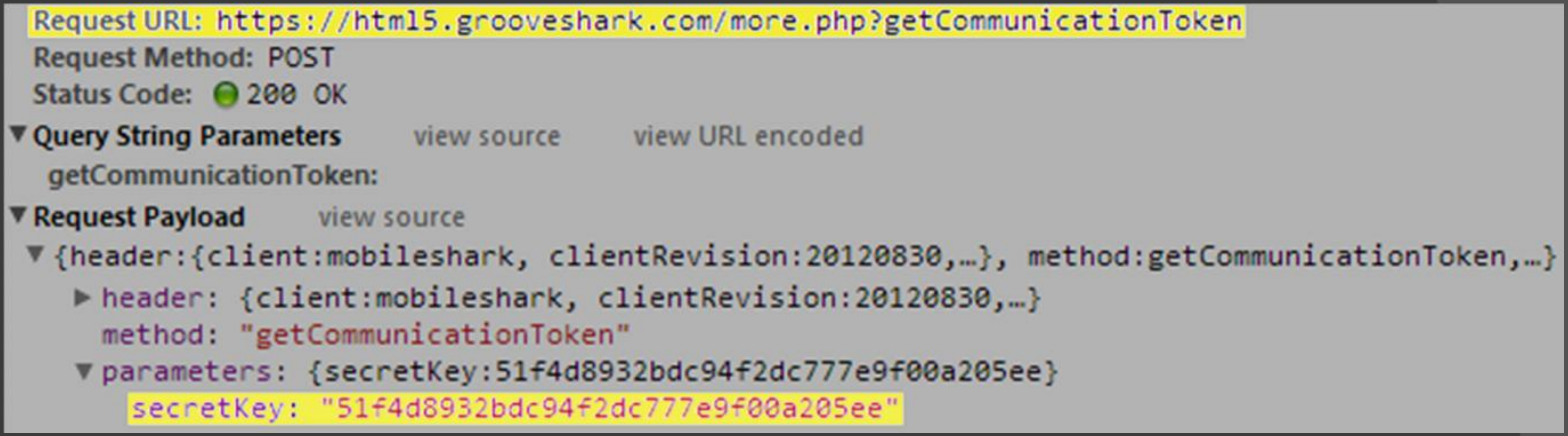
```
Request URL: http://stream57-he.grooveshark.com/stream.php?streamKey=c94f2fd4d8f82737e441f065312436ef
Request Method: GET
Status Code: 206 Partial Content
▼ Request Headers      view source
   Accept: */*
   DNT: 1
   Host: stream57-he.grooveshark.com
   Range: bytes=0-
   Referer: http://html5.grooveshark.com/
▼ Query String Parameters      view source      view URL encoded
   streamKey: c94f2fd4d8f82737e441f065312436ef3e0fb288_51d8e195_24f1b63_2cb51a8_daa87234_36_0
▼ Response Headers      view source
   Cache-Control: no-cache, no-store, must-revalidate
   Connection: close
   Content-Length: 7984685
   Content-Range: bytes 0-7984684/7984685
   Content-Type: audio/mpeg
```

Analyzing the target: more.php



```
Request URL: http://html5.grooveshark.com/more.php?getStreamKeyFromSongIDEx
Request Method: POST
Status Code: ● 200 OK
▼ Query String Parameters      view source      view URL encoded
  getStreamKeyFromSongIDEx:
▼ Request Payload      view source
 ▼ {header:{client:mobileshark, clientRevision:20120830, privacy:0,…}, method:getStreamKeyFromSongIDEx,…}
   ▼ header: {client:mobileshark, clientRevision:20120830, privacy:0,…}
      client: "mobileshark"
      clientRevision: "20120830"
    ▶ country: {ID:223, CC1:0, CC2:0, CC3:0, CC4:1073741824, DMA:512, IPR:0}
      privacy: 0
      session: "86950c0f84cc66f2e26e92b869c5d4e1"
      token: "1f2ad15df0392695236c07d9ae968c3489a8a8cf9db3a6"
      uuid: "38D1D238-7C51-4B5F-9EDB-F79B70DE7EE5"
    method: "getStreamKeyFromSongIDEx"
   ▼ parameters: {prefetch:false, mobile:true, songID:38738787,…}
    ▶ country: {ID:223, CC1:0, CC2:0, CC3:0, CC4:1073741824, DMA:512, IPR:0}
      mobile: true
      prefetch: false
      songID: 38738787
```

Analyzing the target: more.php

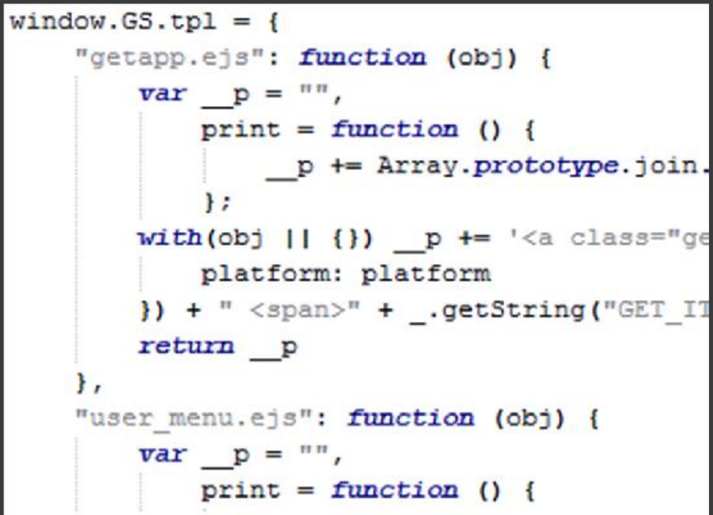


```
Request URL: https://html5.grooveshark.com/more.php?getCommunicationToken
Request Method: POST
Status Code: ● 200 OK
▼ Query String Parameters      view source      view URL encoded
   getCommunicationToken:
▼ Request Payload      view source
  ▼ {header:{client:mobileshark, clientRevision:20120830,…}, method:getCommunicationToken,…}
     ▶ header: {client:mobileshark, clientRevision:20120830,…}
       method: "getCommunicationToken"
     ▼ parameters: {secretKey:51f4d8932bdc94f2dc777e9f00a205ee}
         secretKey: "51f4d8932bdc94f2dc777e9f00a205ee"
```

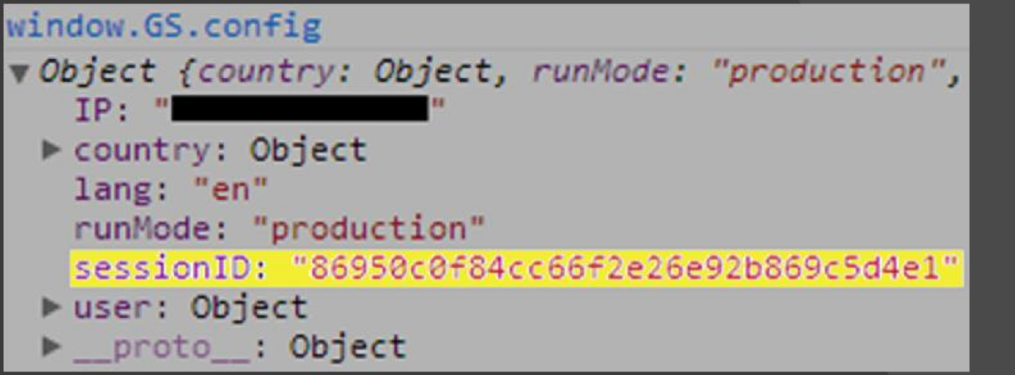
So now what?

- We need:
  - streamKey
- How do we get it?
  - more.php - getStreamKeyFromSongIDEx
  - Session - ?
  - Token - ?
  - UUID - ?
  - songID - ?
- more.php - getCommunicationToken

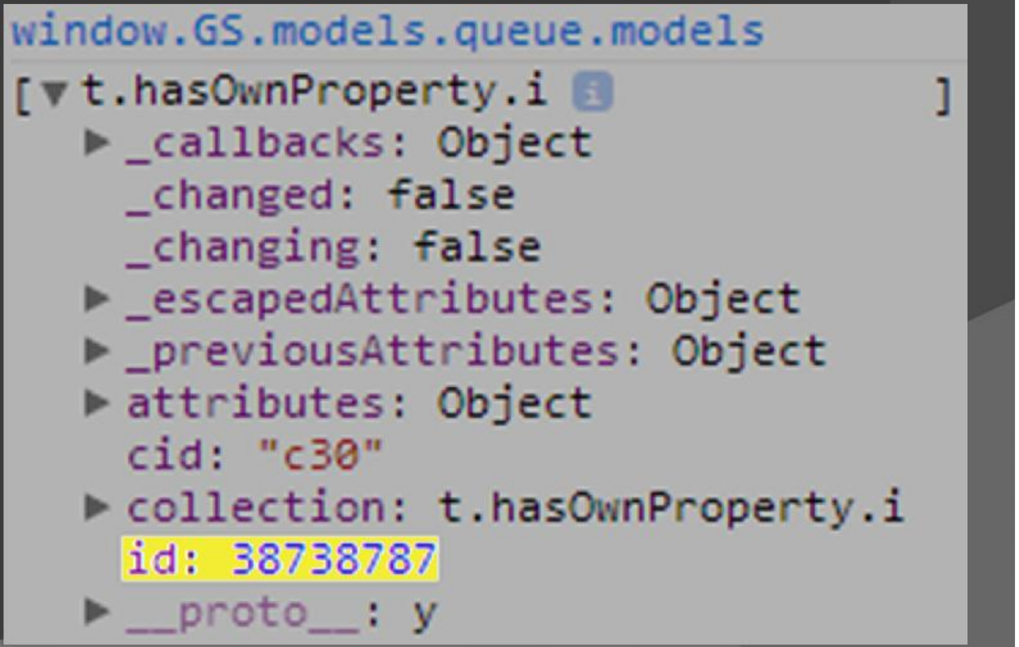
Looking for variables – app.min.js



```
window.GS.tpl = {
    "getapp.ejs": function (obj) {
        var __p = "",
            print = function () {
                __p += Array.prototype.join.
            };
        with(obj || {}) __p += '<a class="ge
            platform: platform
        }) + " <span>" + _.getString("GET_IT
        return __p
    },
    "user_menu.ejs": function (obj) {
        var __p = "",
            print = function () {
```



```
window.GS.config
▼Object {country: Object, runMode: "production",
   IP: "[redacted]"
 ▶ country: Object
   lang: "en"
   runMode: "production"
   sessionID: "86950c0f84cc66f2e26e92b869c5d4e1"
 ▶ user: Object
 ▶ __proto__: Object
```

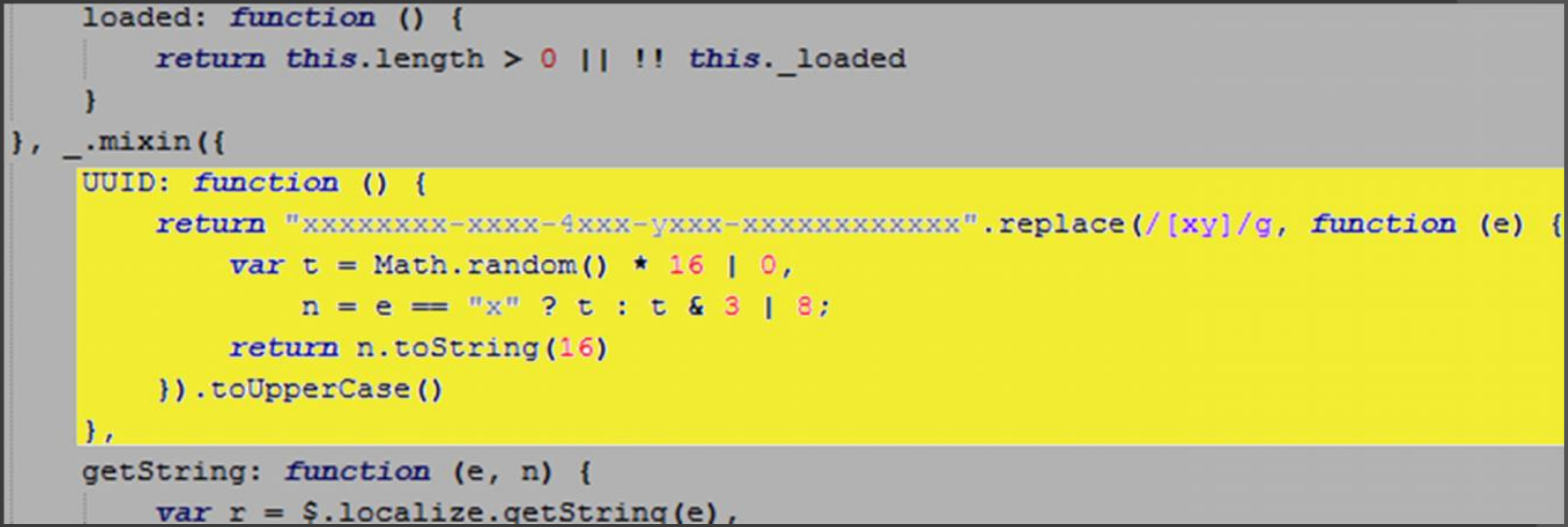


```
window.GS.models.queue.models
[▼t.hasOwnProperty.i ℹ                      ]
   ▶ _callbacks: Object
     _changed: false
     _changing: false
   ▶ _escapedAttributes: Object
   ▶ _previousAttributes: Object
   ▶ attributes: Object
     cid: "c30"
   ▶ collection: t.hasOwnProperty.i
     id: 38738787
   ▶ __proto__: y
```

Recap

- We need:
  - streamKey
- How do we get it?
  - more.php - getStreamKeyFromSongIDEx
  - Session – window.GS.config
  - Token - ?
  - UUID - ?
  - songID - window.GS.models.queue.models
- more.php - getCommunicationToken

Looking for variables – app.min.js

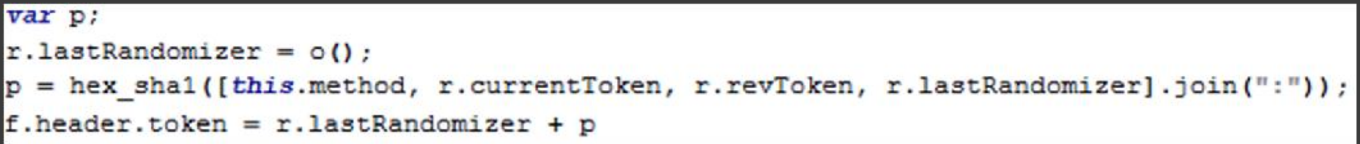


```
    loaded: function () {
        return this.length > 0 || !! this._loaded
    }
}, _.mixin({
    UUID: function () {
        return "xxxxxxxx-xxxx-4xxx-yxxx-xxxxxxxxxxxx".replace(/[xy]/g, function (e) {
            var t = Math.random() * 16 | 0,
                n = e == "x" ? t : t & 3 | 8;
            return n.toString(16)
        }).toUpperCase()
    },
    getString: function (e, n) {
        var r = $.localize.getString(e),
```

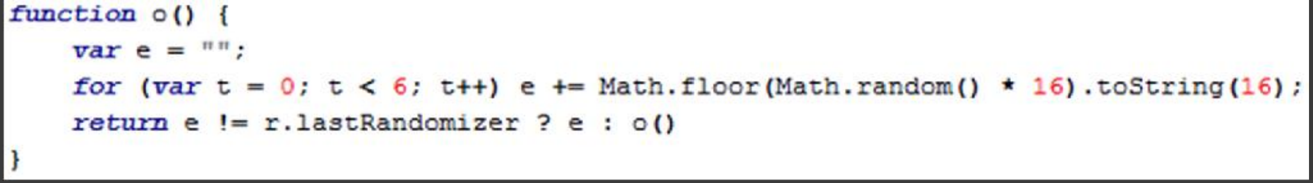
Recap

- We need:
  - streamKey
- How do we get it?
  - more.php - getStreamKeyFromSongIDEx
  - Session – window.GS.config
  - Token - ?
  - UUID – copied function from app.min.js
  - songID - window.GS.models.queue.models
- more.php - getCommunicationToken

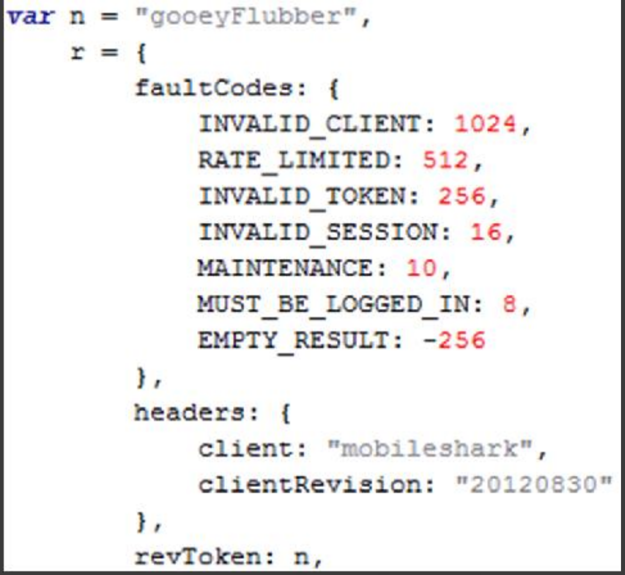
Looking for variables – app.min.js



```
var p;
r.lastRandomizer = o();
p = hex_sha1([this.method, r.currentToken, r.revToken, r.lastRandomizer].join(":"));
f.header.token = r.lastRandomizer + p
```

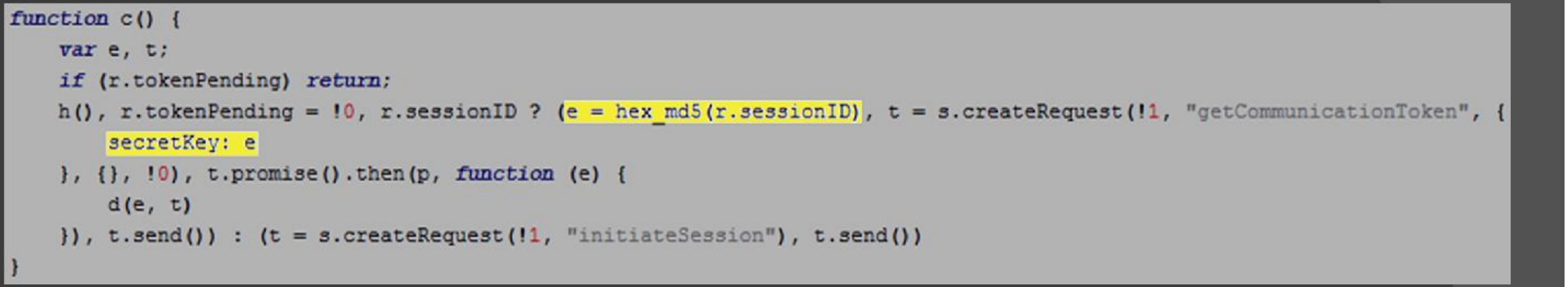


```
function o() {
    var e = "";
    for (var t = 0; t < 6; t++) e += Math.floor(Math.random() * 16).toString(16);
    return e != r.lastRandomizer ? e : o()
}
```



```
var n = "gooeyFlubber",
    r = {
        faultCodes: {
            INVALID_CLIENT: 1024,
            RATE_LIMITED: 512,
            INVALID_TOKEN: 256,
            INVALID_SESSION: 16,
            MAINTENANCE: 10,
            MUST_BE_LOGGED_IN: 8,
            EMPTY_RESULT: -256
        },
        headers: {
            client: "mobileshark",
            clientRevision: "20120830"
        },
        revToken: n,
```

Looking for variables – app.min.js



```
function c() {
    var e, t;
    if (r.tokenPending) return;
    h(), r.tokenPending = !0, r.sessionID ? (e = hex_md5(r.sessionID), t = s.createRequest(!1, "getCommunicationToken", {
        secretKey: e
    }, {}, !0), t.promise().then(p, function (e) {
        d(e, t)
    }), t.send()) : (t = s.createRequest(!1, "initiateSession"), t.send())
}
```

Demo Time

Things I learned

- Downloading music is a waste of time
- Impossible to completely protect streaming
- Hacking easier than coding?

Things you should know

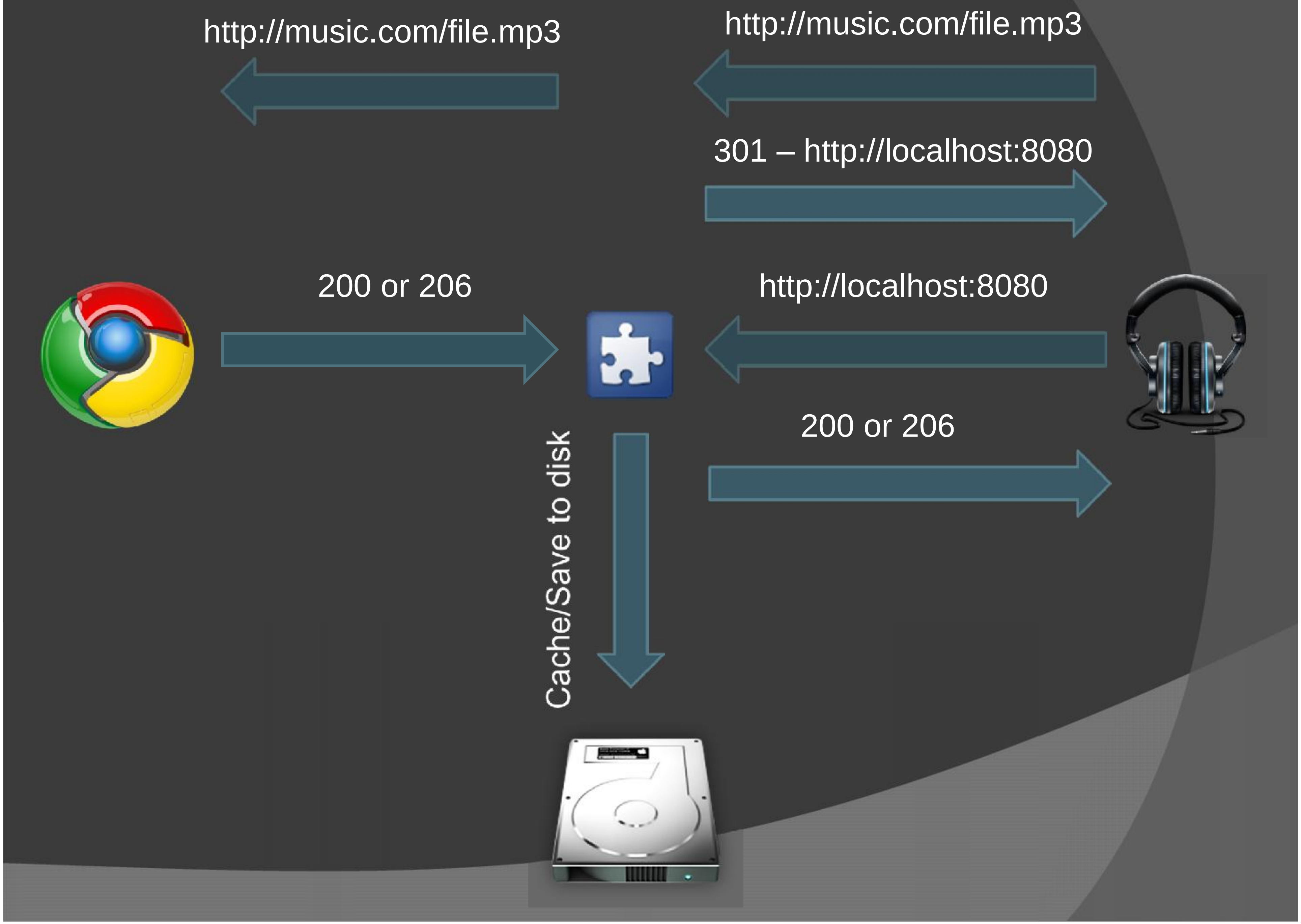
- People have bad security (shocker)
- Several services will patch their stuff now
- Several services won’t patch their stuff
- The same web-traffic logging will work with some video streaming websites too.

Mitigations

- Current technology
  - One-time use tokens
  - Encrypted streams (rtmpe)
  - Returning songs in pieces
  - Code obfuscation
- Future proofing:
  - HTML5 audio tag with DRM support
- “HTTP Live Streaming as a Secure Streaming Method” – Bobby Kania, Luke Gusukuma

But Wait, There's More

- Man-in-the-middle
- Multiple steps to install
  - Requires an additional Google-App
  - Enable dev mode
  - Enable Experimental Extension APIs chrome://flags


http://music.com/file.mp3
http://music.com/file.mp3
301 – http://localhost:8080
200 or 206
http://localhost:8080
200 or 206
Cache/Save to disk

Why no demo?

- Unstable
  - Cannot access socket after 1 or 2 requests
  - Requires browser-restart to fix
- Unrealistic
  - Who would actually install this?
- Try again in a few months
  - Node.js community support
  - Chromify
  - Browserify

References

- One Click Music
  - http://cyberexplo.it/static/OneClickMusic.crx
- HTTP Live Streaming as a Secure Streaming Method
  - http://vtechworks.lib.vt.edu/bitstream/handle/10919/18662/Instructions%20for%20HTTP%20Live%20Streaming%20Final.pdf
- JS Beautifier
  - http://jsbeautifier.org/
- Chromify
  - https://code.google.com/p/chromify/
- Browserify
  - https://github.com/substack/node-browserify

Questions?