SoundCloud Security Audit

Konstantino Sparakis
Jack Reidy

Abstract

In this paper, the overall security of the website SoundCloud is discussed. SoundCloud is an online social media music and audio distribution service, based in Berlin, Germany. that enables users to share, upload, stream music and promote their originally created music. They provide strong security against most known attacks, however, there are still exploits that can affect users.

Introduction

SoundCloud outlines its terms of use on its website including its policy on cookies and copyright infringement. SoundCloud claims to operate on two principles of security. First - "You should know exactly what [SoundCloud] does with your information" [6.] and second - "You should have full control over your information" [6.]

The policy for cookies is stated as followed - "If you choose to use the Platform without blocking or disabling cookies or opting out of other technologies, you will indicate your consent to our use of these cookies and other technologies and to our use (in accordance with this policy and the rest of our Privacy Policy) of any personal information that we collect using these technologies" [7.] The most important part of it is that users agree to policy unless they themselves opt out and remove the cookies. This is an arduous process for the average user to undergo and as such it is likely that SoundCloud will implement its technology on the vast majority of users. SoundCloud also permits third party sites to implement their cookies on users.

General Security

SoundCloud almost exclusively operates using HTTPS, all except for one webpage: http://soundcloud.com/settings/connections, which is open to man in the middle attacks as we discuss below. This page is old and after contacting SoundCloud about it, they confirmed they are aware of this and working to change it. Overall though, They provide secure connections for their users throughout the platform. For login, SoundCloud uses OAuth through Google or Facebook logins. There is no 2-factor authentication with this method. Their certificate operates with a two certificate hierarchy. The first is issued by GlobalSign Domain Validation CA SHA-256 which is then certified via the root trusted GlobalSign Root CA.

The ISA Attack

Following the storyline, ISA has access to one big vulnerability. The SoundCloud connections page is served in HTTP. This page is responsible for allowing customers to link their soundcloud with other services such as Facebook, Google, Tumblr, and Twitter. To test this out we sniffed the traffic with Wireshark through a VM. We then connected to Tumblr to find that all the tokens being passed around are accessible:

Since the ISA has man in the middle privileges once they get access to these tokens they can impersonate SoundCloud, sending posts and interacting with these services. Also the cookies are included in these HTTP posts meaning ISA can also do a Cookie Session Hijacking allow them to use SoundCloud as the user.

```
[truncated]Cookie: sc_anonymous_id=401470-964305-542
 Cookie pair: sc_anonymous_id=401470-964305-542525-8
 Cookie pair: __utma=179375142.387457318.1493753446.
```

With such access if they got access to a popular artist account and sent phishing messages to their fans, they could convince them to download and install malware this could be very dangerous. They could also, do phishing through bots as discussed below but this is more high profile.

Advertisements

Advertisements come in audio and image form. At the end of finishing listening to a song an advertisement may pop up, you see an image followed by an audio stream of the ad. You are usually allowed to skip the advertisement after 15 seconds. However, they don't seem to confirm that their users completely finish watching the advertisement. By refreshing the page you can skip the ad. This leads us to believe with some javascript tinkering there should be a method to completely avoid ads.

Potential XSS Attacks

We found out that song titles, and song comments were actually susceptible to stored XSS attacks and this was only discovered and reported two years ago as seen in this youtube video [3.]. This raises the question what other shared user inputs could still be vulnerable or has Soundcloud gone ahead and tested and attempted to fix all? Other then this the only URL we were concerned against was https://soundcloud.com/pro?ref=t061 as it is a newer page and might not have been screened for XSS.

Potential CSRF Attacks

Soundcloud uses CSRF tokens in all its forms to prevent CSRF attacks. But recently in March of 2017 [5.], a white hat hacker was able to find a case where the CSRF token was not working properly and execute a CSRF attack. This raises questions about all other tokens as well. Is the site truly secure against CSRF?

Cipher Suites

Using a popular tool Qualys SSL Lab [1.], we were able to find that Soundcloud's SSL setup is graded A. This means that overall they do have a good security setup for their Https/SSL connections. Their preferred cipher suite is TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f), which uses the P256 Elliptic curve, this would seem secure but this is no longer clear, as the NSA has moved away and deprecated using it [2.]. But we found when looking into the cipher suites was that they still support TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa). This is considered a weak cipher suite, but to their credit, it is at the end of the list and most likely only there for computers that only have support for 3DES and not AES. Also another note, in their preferred suites, they have all 128-bit Encryptions listed above their 256 bit counter parts. This must be due to quicker speed. But we still believe having 256-bit use of block ciphers are still preferable and they are compromising their user's security in exchange for performance.

Illegal Song Downloading

Because the service streams the song content to you, you are able to compile the stream to get the entire file. There are quite a few tools that help you do this such as chrome extension “Soundcloud Downloader.” The reason this is an issue is because this is a blatant violation to a lot of artist copyrights over the music they sell to make a living.

Spotify has addressed this problem by encrypting its stream with a key, but in order to decrypt the stream that means you must have a local copy of the key, meaning with some reverse engineering it is easy to break this. This technology usually falls under the Digital Rights Management (DRM) types of technology. But this technology is clearly insufficient to fully protect the artist and It seems SoundCloud is not interested in engaging in an ongoing battle with people downloading their music and has turned a blind eye to this issue.

Like, Follow and Spam Bots

“We have a pretty good method of detecting the batches once their accounts get activated but we haven't managed to block their access from signing up without blocking legitimate accounts.”

- Soundcloud Support Team [4.]

One issue that plagues the security of SoundCloud is the presence of bots and fake accounts. These accounts will spam users with phishing attempts, spam and so on. Some users even pay services to supply them with fake likes, reposts and follows on their accounts. This is an issue for most social media platforms as it can be very lucrative to have views on their pages. Especially considering up and coming artists attempting to get more publicity.

Cookies & User Tracking

Because of the use of third party cookies users can typically have upwards of one hundred cookies monitoring their use during a single session. These cookies come from Google, Facebook, Twitter, Rubicon, DoubleClick and many others. They store a lot of information using these cookies including: search items, preferences, and last 250 tracks streamed. Third party cookies store more information that is designed to improve advertisements for the users. The data stored by some of these third party cookies may be purchased for use by advertisers or whomever. SoundCloud implements many of its cookies with the secure flag implying they will only be transmitted via HTTPS. This prevents many attacks involving stealing cookies from users. But through the one HTTP page discovered above an attacker could still have access to the cookies for a man in the middle attack.

Conclusion

What we once assumed was a rather secure website, after a close security audit it is no longer clear if the same could be said. What SoundCloud does right is supporting white hat developers and they fix issues rather quickly once brought to their attention. That one HTTP page is the only page that gave us serious concerns because of the data it handles, but SoundCloud has reassured us it will be fixed soon.

At the end of the day, there isn’t any critical information to protect on soundcloud other than OAuth tokens to other service. But making sure their users are not falling prey to phishing is a legitimate concern. Overall We have found that SoundCloud provides a reasonable amount of security for its average users to be secure from the most common threats on the internet they are also rather honest and fair about their user tracking and cookie usage.

Sources

1. https://www.ssllabs.com/ssltest/analyze.html?d=www.soundcloud.com&s=52.84.12.186
2. https://threatpost.com/nsas-divorce-from-ecc-causing-crypto-hand-wringing/115150/
3. https://www.youtube.com/watch?v=FSBS60mRDn0
4. https://soundcloudcommunity.com/soundcloud-on-your-computer-230066/ive-been-getting-these-annoying-spam-bots-my-likes-and-followers-they-come-hoards-5-20-6814229
5. https://www.youtube.com/watch?v=u2OUBWheA2k
6. https://soundcloud.com/pages/privacy
7. https://soundcloud.com/pages/cookies

Thank you Note:

Thank you guys for all your Hard Work grading and reading through everything. Have a great summer!