BU Department of Computer Science

bu.edu/cs

SOUNDCLOUD
Security Audit

What Is SoundCloud?

Soundcloud is a social media, online music sharing and streaming platform. Users can follow friends and their favorite artists and can also post their own music for the world to listen to. The streaming service comes into play where you can like songs, repost them on your profile and make playlist allowing you to listen on the go or at home.

Soundcloud is a company founded and based in Berlin

Privacy Policy

Operates under two Principles

- You should know exactly what [SoundCloud] does with your information
- You should have full control over your information

Cookie Usage

- Users can have nearly 100 at a given moment
- Allows third party cookies from sites like Google, Facebook, Twitter, Rubicon, DoubleClick and several others
- Some of these sites allow for the purchasing of data obtained through cookies

User Tracking

- IP address of your device
- Search terms entered
- Preferences set
- Third party cookies allow users to be tracked across the web

Advertisements

- Ads come in the form of streaming audio and jpg.
- Ads can be avoided in theory by tinkering with the javascript since SoundCloud doesn't check if you actually listened.
- Refreshing page or restarting mobile app allows you to avoid ads when they begin playing.

General Security

Authentication

- OAuth 2.0 via Google or FB login, or just a SoundCloud login.
- No 2 Factor Authentication
- They scan to see if your password might have been compromised through another service you use and ask you to reset.

- **Streaming is done via HTML5 no Flash components being used. This was switched over in 2015.**

- **Uses HTTPS exclusive except for One Http page.**

Certificates

Two certificate hierarchy, given to soundcloud by GlobalSign Domain Validation CA - SHA256 - G2. Which gets its certificate from GlobalSign which is trusted at the root level.

CipherSuites

- Default : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- Weakest: TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - Elliptic curve P256 Is used in default, NSA no longer uses Elliptic curves is this secure?
  - CipherSuite favors 128-bit over 256-bit schemes, which is clearly a performance vs security tradeoff.
  - Supports TLS 1.0, 1.1 & 1.2 making it open to downgrade attacks.

Illegal Song Downloading

- No real preventative measure being taken to stop people from ripping & downloading MP3's Illegally.
- Websites and apps such as "SoundCloud Downloader" exist for Mac and even as Chrome Extensions.
- Allows people to copyright infringe on Artist
- Could implement DRM solutions to make it more difficult but there is no real solution to defend against this.

Like, Follow, & Spam Bots

- Users can purchase fake likes and follows on unofficial 3rd party sites.
- Spam bots post phishing links in comments and through out website.
- Soundcloud claims it is extremely hard to prevent these bots from registering without blocking out legitimate users, but it is easy to detect them because of their activity

Potential XSS?

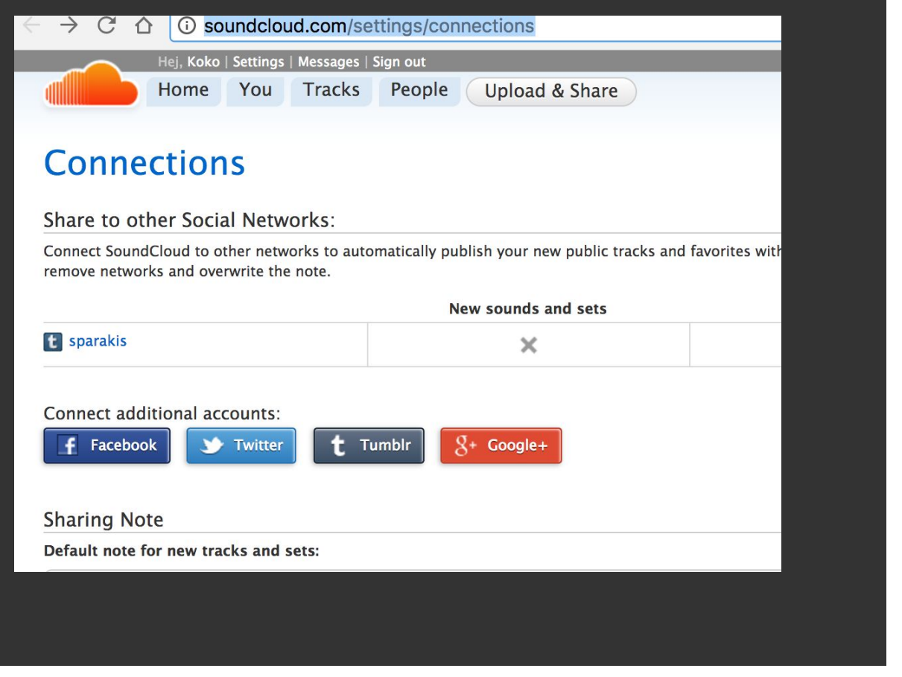
- Stored XSS vulnerabilities found back in May 2015, could there still be new ones?
  - The attack focused on adding javascript to song comments and titles.
- Potential avenues of attack Search Query and Join Pro Membership page?
- Overall most URL requests are very clean and simple not allowing XSS.

Potential CSRF?

- SoundCloud uses CSRF Tokens to avoid these attacks.
- March 2017 a CSRF token was found to not work properly allowing for one to execute a CSRF attack on the soundcloud communities page.
- Could there be more broken tokens?

One HTTP Page?

- We have found the connections Page seems not to be up to date And uses http.
- This leaves a vulnerability allowing a man in the middle to get OAuth Tokens for Fb, Twitter and other services or Soundcloud.


soundcloud.com/settings/connections
Hej, Koko | Settings | Messages | Sign out
Home
You
Tracks
People
Upload & Share
Facebook
Twitter
Tumblr
Google+

Connections

Share to other Social Networks:

Connect SoundCloud to other networks to automatically publish your new public tracks and favorites with remove networks and overwrite the note.

New sounds and sets

sparakis ×

Connect additional accounts:

Sharing Note

Default note for new tracks and sets:

CS558 Network Security | Spring 2017 | Konstantino Sparakis | John Reidy

@BUCompSci