

Forum:[Hack Forums](#)

Thread: [Decrypting an MP3 file served from a web app](#)

Anomynous - September 12, 2020, 1:03 pm

Trying to do a site rip on a popular meditation app Insight Timer. I was able to easily do this with some of their competitors, but this specific service encrypts the mp3's that are served from their web app. Their premium subscription enables offline downloading, and has a 30 day trial, so I might sign up for it and see if that makes it easier, but I thought this would be a fun challenge for hackforums.

I can share fiddler traffic dumps if enough people are interested in taking a crack at it. Otherwise you can just go to insighttimer.com and play any of the tracks, you'll see the encrypted mp3's i'm talking about. Chrome Dev Tools -> Network tab after hitting play.

BalloonsAreFun - September 12, 2020, 3:04 pm

Here you go:

Code `https://libraryaudio.insighttimer.com/{fileID}%2Faudio%2Fstandard_quality.mp3?alt=media`
Example file:

https://libraryaudio.insighttimer.com/y1h4b8n8h3s8d5m9r7k0r2c6y3b0r4v1u3g2s4l0%2Faudio%2Fstandard_quality.mp3?alt=media

Anomynous - September 12, 2020, 3:09 pm

Awesome, gonna run HTTrack on insighttimer.com and GREP out all the fileID's.

If you have a moment, can you tell me how you managed to find the standard_quality suffix? In Dev Tools/fiddler the mp3 that was being served had audio_encrypted instead.

BalloonsAreFun - September 12, 2020, 4:37 pm

(Sep 12, 2020 03:09 PM)Anomynous Wrote: [\[CITE\]](#) Awesome, gonna run HTTrack on insighttimer.com and GREP out all the fileID's.

If you have a moment, can you tell me how you managed to find the standard_quality suffix? In Dev Tools/fiddler the mp3 that was being served had audio_encrypted instead.
Just used some Google Dorks instead of trying scan anything on the domain.

This might be of use to you as well for scraping (where the suffix was pulled from):
<https://libraryitems.insighttimer.com/>

Anomynous - September 12, 2020, 4:49 pm

(Sep 12, 2020 04:37 PM)BalloonsAreFun Wrote: [\[CITE\]](#) Just used some Google Dorks instead of trying scan anything on the domain.

This might be of use to you as well for scraping (where the suffix was pulled from):
(link)

Brilliant, thanks buddy. If I run into a similar situation in the future on another site, I'll try these strategies.

Cheers.

