Vulnerability: Broken Access Control

Severity: Critical

OWASP TOP 10: A 01:2021 – Broken Access Control

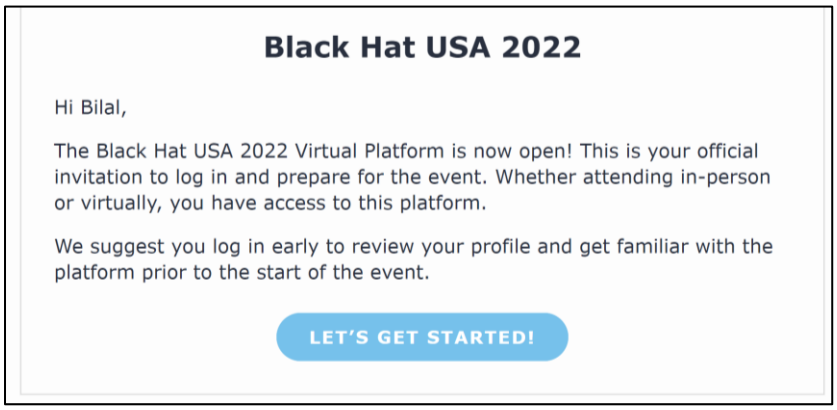
Observation

It has been identified that there is a Broken Access Control between Informa Tech's virtual event platform and Akamai's Content Delivery Network (CDN). This can allow an unauthenticated and unauthorized user(s) to view, download, and illegally distribute Black Hat briefings videos that are only shared with users who actually paid to attend the Black Hat conference in-person or virtually. This issue can cause a significant revenue loss to Black Hat event organizers since unauthorized users will be able to view and download highly sought-after premium videos for free.

Technical Details:

Black Hat Event Virtual Platform

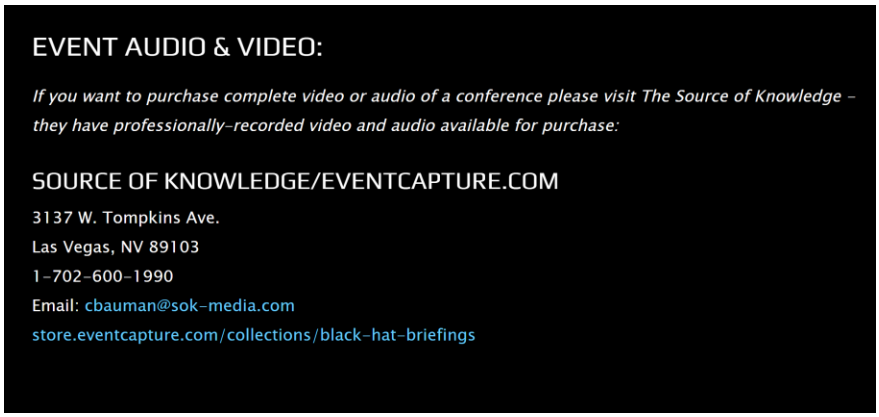
Users who purchase Black Hat conference tickets are given the option to sign up on an event's virtual platform. Invitation to join and access the virtual platform is sent to users via email (please refer screenshot 1 below). Once the user creates their account on the virtual platform, it provides them with the option to view the Black Hat event schedule, connect with other attendees, speakers, sponsors and most importantly, it gives them the access to view Black Hat Briefings live and its recordings.



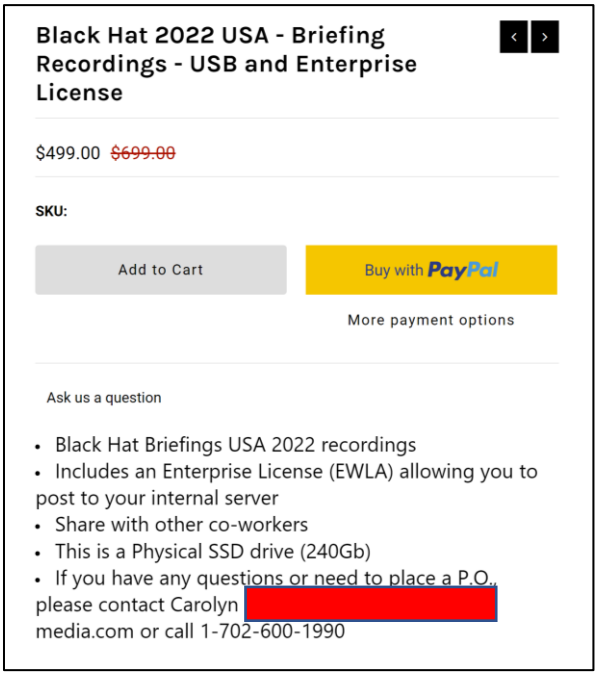
Screenshot 1: Invitation email received by the attendee after purchasing Black Hat conference ticket.

All Black Hat attendees are given access to view Black Hat Briefings recordings on this virtual event platform for 30 days after the event. It is also important to note that the virtual platform does not gives its users the option to download any of the Briefings videos accessible to them via virtual event platform.

Users can also purchase Black Hat Briefing recordings and Enterprise License from "SOURCE OF KNOWLEDGE/EVENTCAPTURE.COM" (please refer screenshot 2 and 3 below).



Screenshot 2: section taken from https://www.blackhat.com/html/contact.html



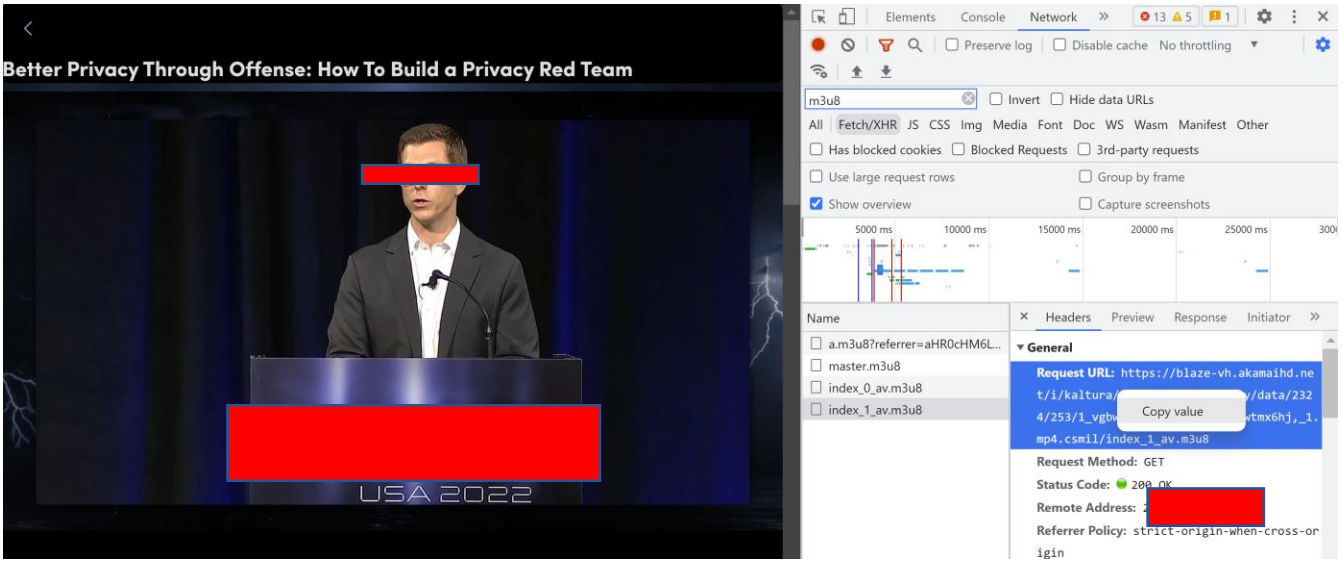
Screenshot 3: Black Hat Briefing Recordings - Audio and Video can be purchased from the following URL https://store.eventcapture.com/collections/black-hat-briefings

Vulnerability:

It is observed that the Black Hat event's virtual platform does not have sufficient access controls in place to prevent unauthenticated and unauthorized user(s) to view and download Black Hat videos that are only shared with users who actually paid to attend the Black Hat conference in-person or virtually. This issue can cause a significant revenue loss to Black Hat and Informa Tech since unauthorized users will be able to view and download videos for free.

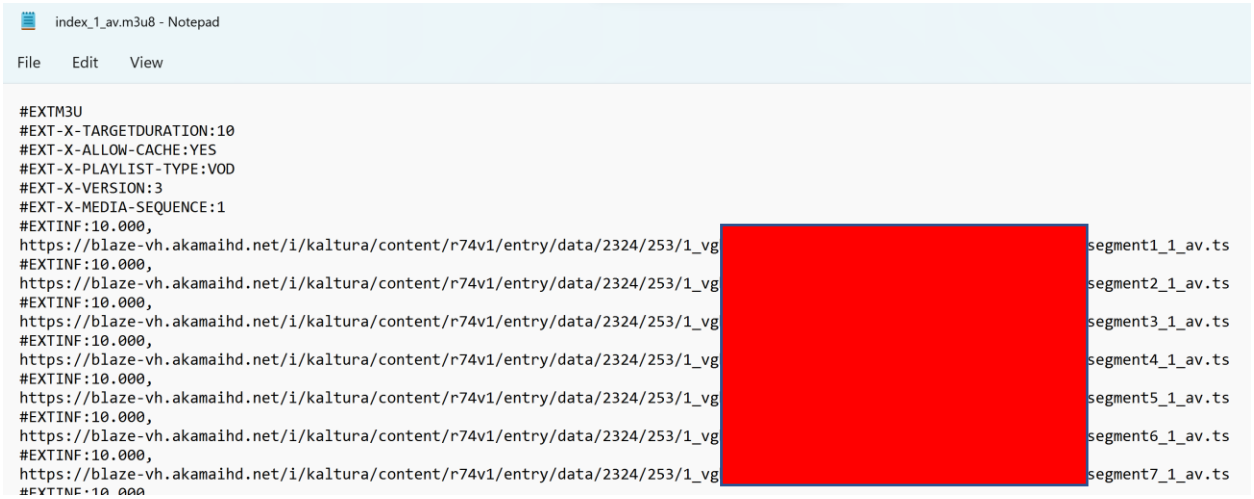
Users with malicious intent who have authenticated access to the event's virtual event can simply copy the link of the Recorded Briefing's .m3u8 playlist file from the web page's source code and share it with

anyone. Please refer screenshot 4. According to lifwire.com[1], a file with the M3U8 file extension is a UTF-8 Encoded audio and video Playlist file. They are plain text files that can be used by both audio and video players to describe where media files are located.



Screenshot 4: Once Briefings video is loaded in the User's web browser, an authenticated User can simply copy the link to the .m3u8 playlist file.

If we download and inspect the contents of the Briefing's .m3u8 playlist file, it is noted that it consists of hundreds of URLs of 10 second video stream segments hosted on akamaihd.net which is a Content Delivery Network (CDN). Please refer to the screenshot 5 below.

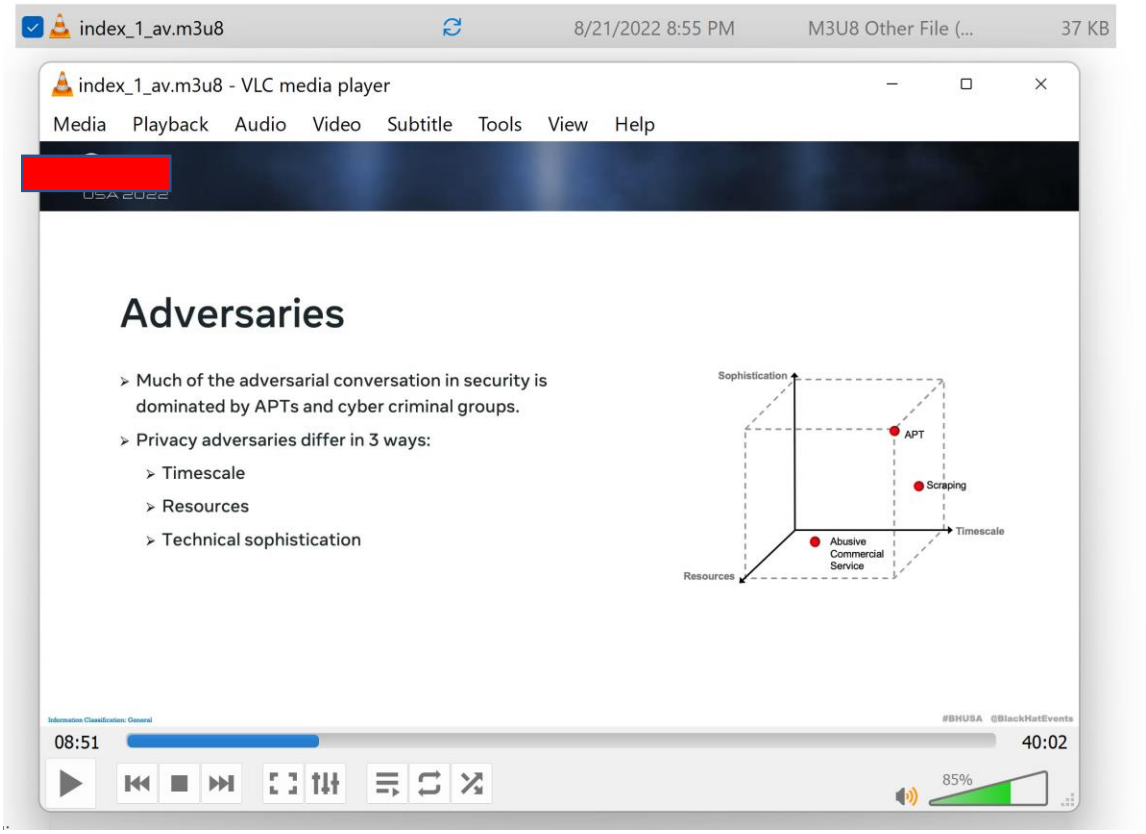


Screenshot 5: .m3u8 playlist file can consists of hundreds of URLs pointing to 10 second video stream segments hosted on the CDN provider.

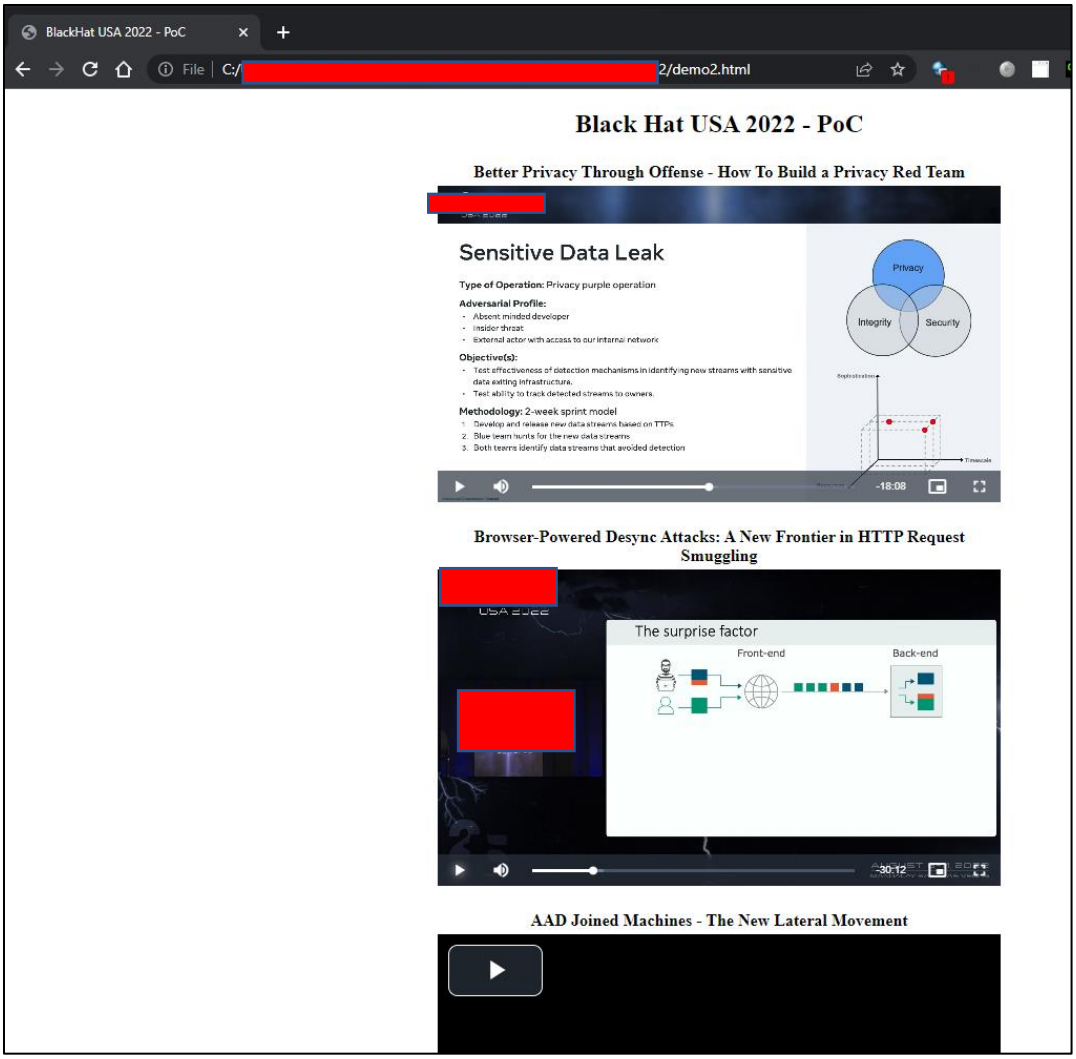
[1] https://www.lifewire.com/m3u8-file-2621956

Since there are no access controls in place between Informa Tech virtual event platform and the akamaihd.net CDN to prevent unauthorized access, a malicious user can do the following:

- Download and distribute .m3u8 playlist file for each Black Hat Briefing which can be easily viewed in a VLC video player (please refer screenshot 6).
- Using the downloaded .m3u8 playlist file, a malicious user can download the entire video recording of the briefing. A proof-of-concept BASH script is provided in Appendix A.
- A malicious User can simply embed the link to the .m3u8 playlist file on attacker-controlled website. This is referred to as Hot Linking. Please refer screenshot 7.



Screenshot 6: Downloaded .m3u8 playlist file for the Black Hat Briefing can be easily viewed using a VLC video player.



Screenshot 7: A malicious user can simply embed the link to the hosted .m3u8 playlist file on their website(s). This can be achieved simply using a HTML file as seen above.

The above-mentioned issues completely remove the requirement of users logging on to Informa Tech's Black Hat event virtual platform to view highly sought-after premium content. The above also eliminates the requirement of purchasing the audio and video recordings which can significantly impact Black Hat event organizer's revenue.

Solution:

Akamai's Media Security Policy - User Guide provides[2] complete technical guidance on how to host media securely on Akamai's CDN.

There are multiple security best practices provided in Akamai's Media Security Policy document including the use of Token-based authentication mechanisms which are commonly used across the Internet as security to validate user rights.

According to Akamai, Token Authentication security prevents a Media Services stream from link sharing and/or player hijacking attacks by ensuring that the stream is only delivered to the authenticated user. This feature is based on hybrid tokens that are generated using a "trusted shared secret" between the content owner and our network—a primary token is short-lived and is used to secure a playlist; while an available secondary cookie token is long-lived and valid for the play time of the media content to protect subsequent segments that are delivered after the manifest file**.**

[2] https://techdocs.akamai.com/msl/pdfs/media-security-policy-user-guide.pdf

Appendix A - Proof of Concept BASH Script

The following BASH script can be used to download the Black Hat Briefing Recording.

Please note:

- ffmpeg is required to run this script successfully

- This script has been tried and tested on Kali Linux

```
wget <URL to the .m3u8 playlist file>
cat *.m3u8 | grep  https > urls.txt
for i in $(cat urls.txt); do wget $i -q; done
for i in `\ls *.ts | sort -V`; do echo "file '$i'"; done >> mylist.txt
./ffmpeg/ffmpeg -f concat -i mylist.txt -c copy -bsf:a aac_adtstoasc video.mp4
rm *.ts
rm *.m3u8
rm *.txt
```