Week 5: Threat Modeling & Vulnerability Classification

This report models threats for five Alexa skills captured via the Alexa mobile app using mitmproxy/mitmweb. We applied STRIDE for security, LINDDUN for privacy, and consolidated findings into a vulnerability taxonomy with concrete mitigations.

Scope & Skills Assessed

1) Sleep Sounds by Sleep Jar (media streaming)

2) Question of the Day (Matchbox)

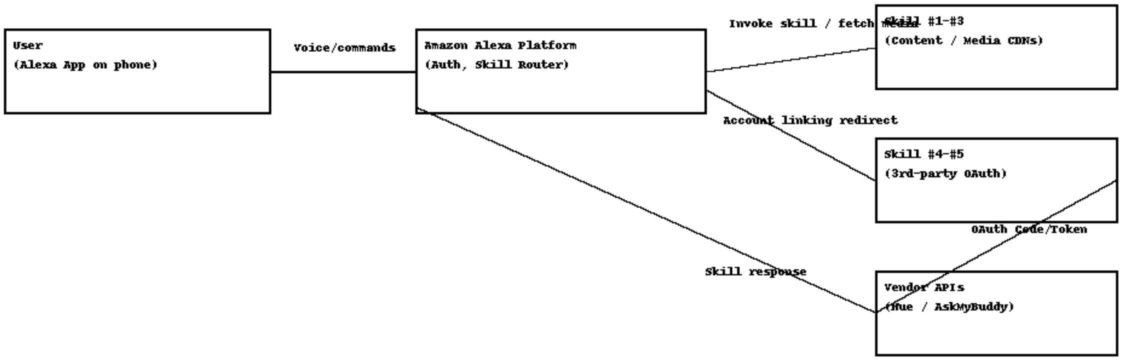
3) Cat Facts (content)

4) Ask My Buddy (account linking)

5) Philips Hue (account linking + device cloud)

High-Level Data Flow

The diagram below summarizes the primary interactions observed during skill use and account linking:



STRIDE Threat Modeling

Threat	Where / Asset	Example in Flow	Likely Impact	Mitigations
Spoofing	Account Linking / OAuth Client	Phishing-like pages or tampered redirect URIs	Account takeover / token theft	PKCE + state, exact redirect URIs, HTTPS-only, CSP
Tampering	Media playlists / responses	Unsigned m3u8/ts segments on CDNs	Content injection / malvertising	Signed URLs, TLS pinning (where possible), integrity checks
Repudiation	User consent logs	Ambiguous permission prompts	Disputes over consent/data use	Fine-grained consent records, immutable logs
Information Disclosure	Excess scopes / profile data	Requesting profile+email+location when not needed	Privacy loss; broad data exposure	Least privilege scopes; periodic scope reviews
Denial of Service	Skill backends / media CDNs	Burst requests; missing rate limits	Service disruption; throttling	Rate limiting; caching; retries with backoff
Elevation of Privilege	Weak access separation	Single token grants multiple device actions	Unauthorized control/data access	Role-based scopes; token binding; short TTLs; rotation

LINDDUN Privacy Analysis

Category	Data / Subject	Example	Risk	Mitigation
Linkability	User sessions across skills	Shared identifiers across vendors/CDNs	Cross-service tracking	Rotate pseudonyms; minimize shared IDs
Identifiability	PII (email/name)	Over-privileged OAuth scopes	User deanonymization	Collect only required claims; DPIA
Non-repudiation	Consent evidence	Implicit opt-ins via app UI	Weak accountability	Explicit prompts; user-accessible logs
Detectability	Traffic patterns	Predictable media fetch bursts	Skill usage inference	Padding, caching, aggregation
Disclosure of info	Media URLs/tokens	Unsigned playlists; broad cache	Leak of content or tokens	Signed URLs; short TTLs
Unawareness	Purpose/transparency	Opaque linking pages	User misunderstanding	Clear scopes/purposes; granular revoke
Non-compliance	Consent, retention	No retention limits	Policy/regulatory risk	Documented retention; user deletion

Vulnerability Taxonomy & Evidence

Category	Observation / Evidence	Risk	Recommendation
Data Over-collection	OAuth scopes include profile/email where not necessary	Medium	Limit to least-privilege; justify each scope
Weak OAuth (PKCE/state)	Multiple redirects; possible missing state validation on vendors	High	Enforce PKCE+state; exact redirect matching
Token Hygiene	Long-lived tokens; unclear rotation	High	Short TTL; refresh rotation; revoke on logout
Transport/Content Security	Unsigned m3u8/ts assets from CDN	Medium	Signed URLs; integrity checks
Injection/Tampering	Media path manipulation feasible if unprotected	Medium	Input validation; integrity; secure storage
DoS/Abuse	Observable burst traffic; no clear rate limit headers	Medium	Rate limits; caching; backoff
User-Confusion Consent	Generic prompts; unclear data use	Medium	Granular, purpose-based prompts; user dashboard

Alexa Platform Constraints vs Real- World Risks

Platform Constraints (What Amazon Controls)	Real-World Risks (Vendor / Skill Owner)
Skill certification focuses on functionality + content policy	Certification does not fully audit third-party OAuth servers
Traffic is TLS-terminated by platform	Downstream media/OAuth endpoints may have weaker controls
Standardized permission categories	Vendors may request broader scopes than required
Account linking UX limited in-app	Phishing-like off-domain login pages can confuse users

Key Recommendations

- Enforce PKCE + state on all account linking; exact redirect URIs.

- Use least-privilege OAuth scopes; document purpose for each claim.

- Short token TTLs, automatic rotation, revoke on unlink.

- Signed media URLs, integrity checks for playlists/segments.

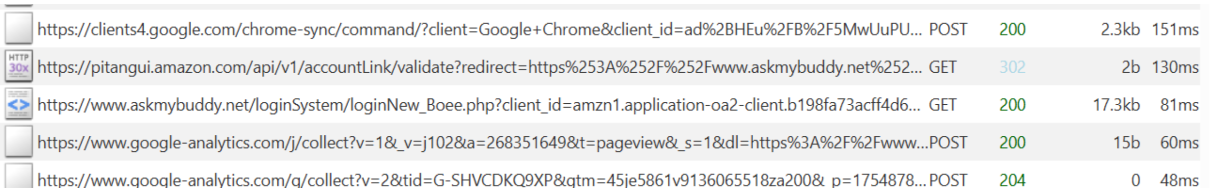
- Rate limiting + caching; client retry with exponential backoff.

- Clear, granular, purpose-based consent prompts and a user permission dashboard.

- Add static/dynamic tests in certification for scopes, PKCE/state, and signed content.

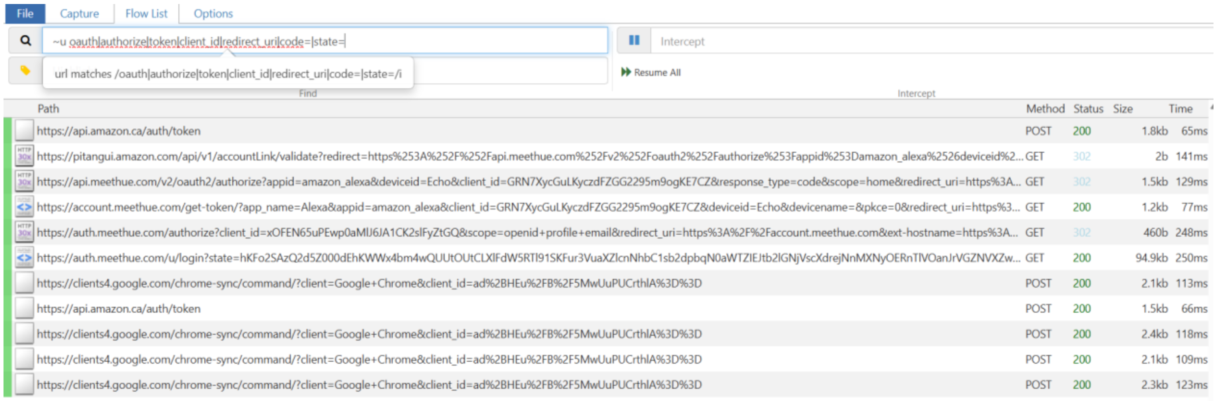
Evidence Screenshots

askbuddy skill.png



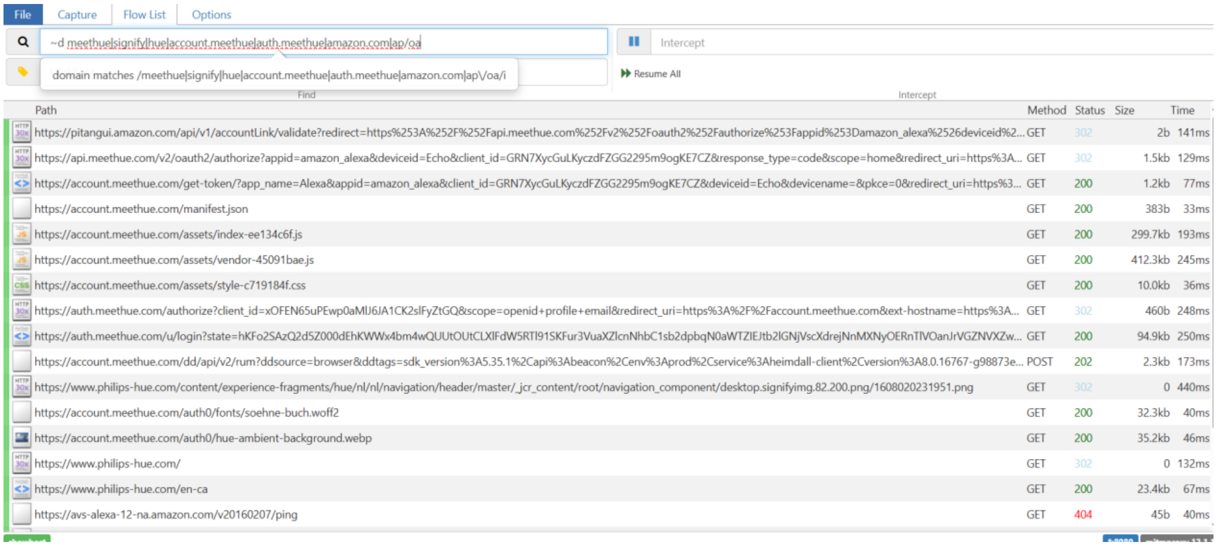
```
https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPU... POST  200   2.3kb  151ms
https://pitangui.amazon.com/api/v1/accountLink/validate?redirect=https%253A%252F%252Fwww.askmybuddy.net%252... GET  302   2b  130ms
https://www.askmybuddy.net/loginSystem/loginNew_Boee.php?client_id=amzn1.application-oa2-client.b198fa73acff4d6... GET  200  17.3kb  81ms
https://www.google-analytics.com/j/collect?v=1&_v=j102&a=268351649&t=pageview&_s=1&dl=https%3A%2F%2Fwww...POST  200  15b  60ms
https://www.google-analytics.com/g/collect?v=2&tid=G-SHVCDKQ9XP&gtm=45je5861v9136065518za200&_p=1754878...POST  204  0  48ms
```

philips_hue1.png



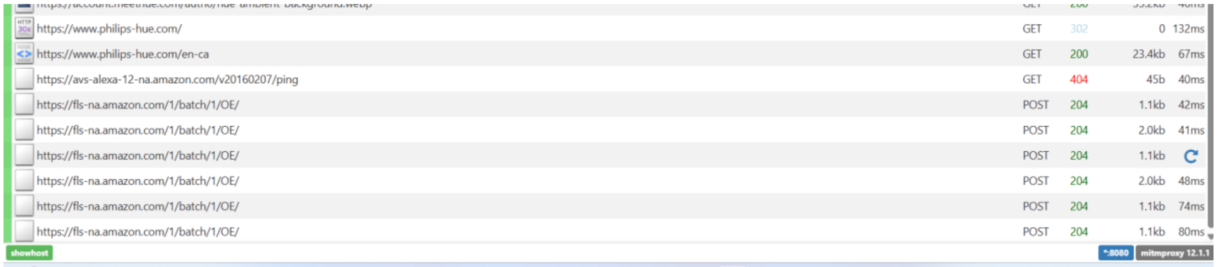
```
~u oauth|authorize|token|client_id|redirect_uri|code=|state=
url matches /oauth|authorize|token|client_id|redirect_uri|code=|state=/i

Path                                                                                                                                                                Method Status Size   Time
https://api.amazon.ca/auth/token                                                                                                                                    POST   200    1.8kb  65ms
https://pitangui.amazon.com/api/v1/accountLink/validate?redirect=https%253A%252F%252Fapi.meethue.com%252Fv2%252Foauth2%252Fauthorize%253Fappid%253Damazon_alexa%2526deviceid%2... GET 302 2b 141ms
https://api.meethue.com/v2/oauth2/authorize?appid=amazon_alexa&deviceid=Echo&client_id=GRN7XycGuLKyczdFZGG2295m9ogKE7CZ&response_type=code&scope=home&redirect_uri=https%3A... GET 302 1.5kb 129ms
https://account.meethue.com/get-token/?app_name=Alexa&appid=amazon_alexa&client_id=GRN7XycGuLKyczdFZGG2295m9ogKE7CZ&deviceid=Echo&devicename=&pkce=0&redirect_uri=https%3... GET 200 1.2kb 77ms
https://auth.meethue.com/authorize?client_id=xOFEN65uPEwp0aMlJ6JA1CK2slFyZtGQ&scope=openid+profile+email&redirect_uri=https%3A%2F%2Faccount.meethue.com&ext-hostname=https%3A... GET 302 460b 248ms
https://auth.meethue.com/u/login?state=hKFo2SAzQ2d5Z000dEhKWWx4bm4wQUUtOUtCLXlFdW5RTl91SKFur3VuaXZlcnNhbC1sb2dpbqN0aWTZIEJtb2lGNjVscXdrejNnMXNyOERnTlVOanJrVGZNVXZw... GET 200 94.9kb 250ms
https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPUCrthlA%3D%3D                                                  POST   200    2.1kb  113ms
https://api.amazon.ca/auth/token                                                                                                                                    POST   200    1.5kb  66ms
https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPUCrthlA%3D%3D                                                  POST   200    2.4kb  118ms
https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPUCrthlA%3D%3D                                                  POST   200    2.1kb  109ms
https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPUCrthlA%3D%3D                                                  POST   200    2.3kb  123ms
```

philips_hue_oauth2.png



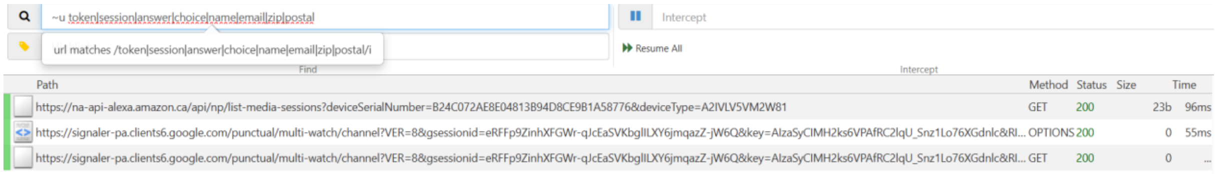
```
~d meethue|signify|hue|account.meethue|auth.meethue|amazon.com|ap/oa
domain matches /meethue|signify|hue|account.meethue|auth.meethue|amazon.com|ap\/oa/i

Path                                                                                                                                                                Method Status Size     Time
https://pitangui.amazon.com/api/v1/accountLink/validate?redirect=https%253A%252F%252Fapi.meethue.com%252Fv2%252Foauth2%252Fauthorize%253Fappid%253Damazon_alexa%2526deviceid%2... GET 302 2b 141ms
https://api.meethue.com/v2/oauth2/authorize?appid=amazon_alexa&deviceid=Echo&client_id=GRN7XycGuLKyczdFZGG2295m9ogKE7CZ&response_type=code&scope=home&redirect_uri=https%3A... GET 302 1.5kb 129ms
https://account.meethue.com/get-token/?app_name=Alexa&appid=amazon_alexa&client_id=GRN7XycGuLKyczdFZGG2295m9ogKE7CZ&deviceid=Echo&devicename=&pkce=0&redirect_uri=https%3... GET 200 1.2kb 77ms
https://account.meethue.com/manifest.json                                                                                                                           GET    200    383b     33ms
https://account.meethue.com/assets/index-ee134c6f.js                                                                                                                GET    200    299.7kb  193ms
https://account.meethue.com/assets/vendor-45091bae.js                                                                                                               GET    200    412.3kb  245ms
https://account.meethue.com/assets/style-c719184f.css                                                                                                               GET    200    10.0kb   36ms
https://auth.meethue.com/authorize?client_id=xOFEN65uPEwp0aMlJ6JA1CK2slFyZtGQ&scope=openid+profile+email&redirect_uri=https%3A%2F%2Faccount.meethue.com&ext-hostname=https%3A... GET 302 460b 248ms
https://auth.meethue.com/u/login?state=hKFo2SAzQ2d5Z000dEhKWWx4bm4wQUUtOUtCLXlFdW5RTl91SKFur3VuaXZlcnNhbC1sb2dpbqN0aWTZIEJtb2lGNjVscXdrejNnMXNyOERnTlVOanJrVGZNVXZw... GET 200 94.9kb 250ms
https://account.meethue.com/dd/api/v2/rum?ddsource=browser&ddtags=sdk_version%3A5.35.1%2Capi%3Abeacon%2Cenv%3Aprod%2Cservice%3Aheimdall-client%2Cversion%3A8.0.16767-g98873e... POST 202 2.3kb 173ms
https://www.philips-hue.com/content/experience-fragments/hue/nl/nl/navigation/header/master/_jcr_content/root/navigation_component/desktop.signifyimg.82.200.png/1608020231951.png GET 302 0 440ms
https://account.meethue.com/auth0/fonts/soehne-buch.woff2                                                                                                           GET    200    32.3kb   40ms
https://account.meethue.com/auth0/hue-ambient-background.webp                                                                                                       GET    200    35.2kb   46ms
https://www.philips-hue.com/                                                                                                                                        GET    302    0        132ms
https://www.philips-hue.com/en-ca                                                                                                                                   GET    200    23.4kb   67ms
https://avs-alexa-12-na.amazon.com/v20160207/ping                                                                                                                   GET    404    45b      40ms
```

philips_hue_oauth3.png



Path	Method	Status	Size	Time
https://account.meethue.com/auth/hue-ambient-background.webp	GET	200	[illegible]	[illegible]
https://www.philips-hue.com/	GET	302	0	132ms
https://www.philips-hue.com/en-ca	GET	200	23.4kb	67ms
https://avs-alexa-12-na.amazon.com/v20160207/ping	GET	404	45b	40ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	1.1kb	42ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	2.0kb	41ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	1.1kb	↻
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	2.0kb	48ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	1.1kb	74ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	1.1kb	80ms

cat_facts.png

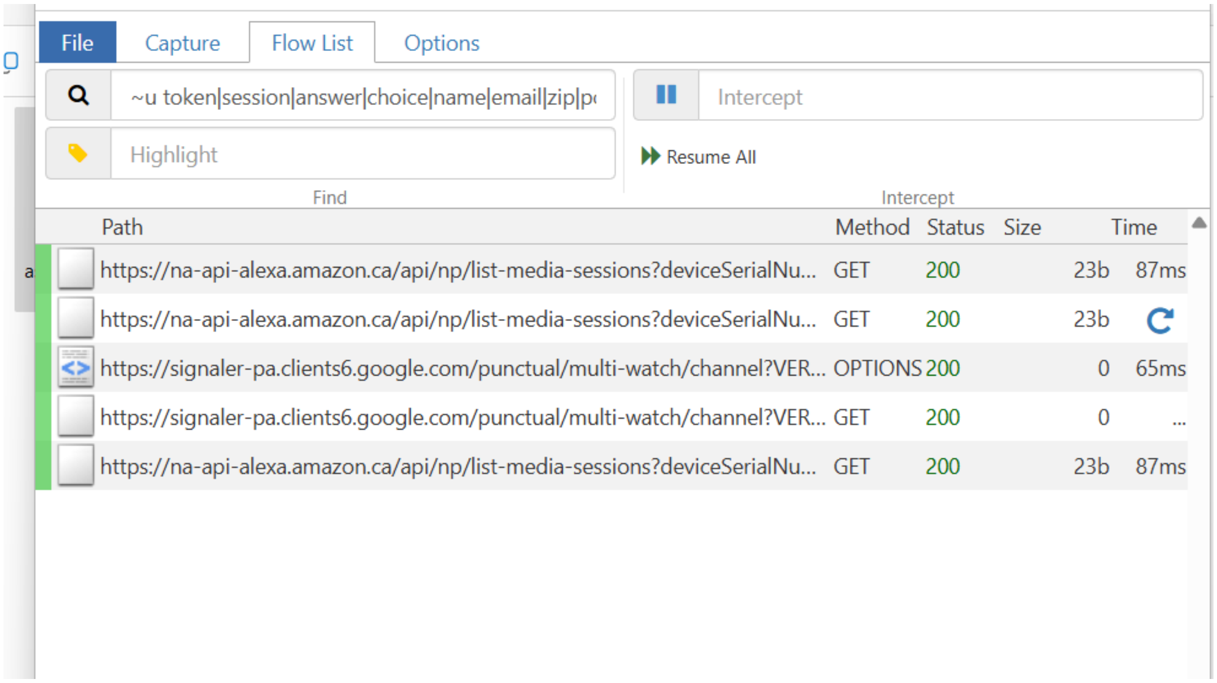


~u token|session|answer|choice|name|email|zip|postal

url matches /token|session|answer|choice|name|email|zip|postal/i

Path	Method	Status	Size	Time
https://na-api-alexa.amazon.ca/api/np/list-media-sessions?deviceSerialNumber=B24C072AE8E04813B94D8CE9B1A58776&deviceType=A2IVLV5VM2W81	GET	200	23b	96ms
https://signaler-pa.clients6.google.com/punctual/multi-watch/channel?VER=8&gsessionid=eRFFp9ZinhXFGWr-qJcEaSVKbglILXY6jmqazZ-jW6Q&key=AIzaSyCIMH2ks6VPAfRC2lqU_Snz1Lo76XGdnlc&RI...	OPTIONS	200	0	55ms
https://signaler-pa.clients6.google.com/punctual/multi-watch/channel?VER=8&gsessionid=eRFFp9ZinhXFGWr-qJcEaSVKbglILXY6jmqazZ-jW6Q&key=AIzaSyCIMH2ks6VPAfRC2lqU_Snz1Lo76XGdnlc&RI...	GET	200	0	...

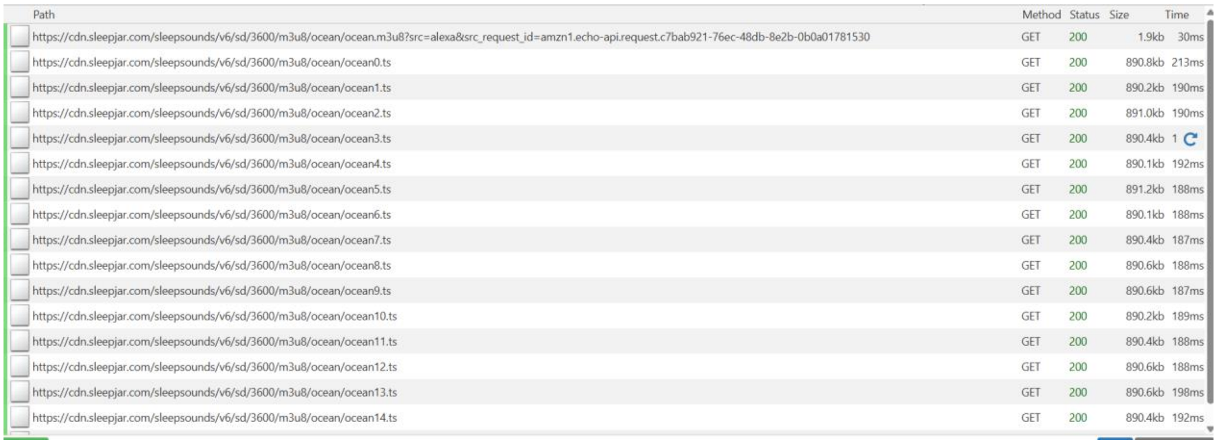
qotd.png



~u token|session|answer|choice|name|email|zip|p

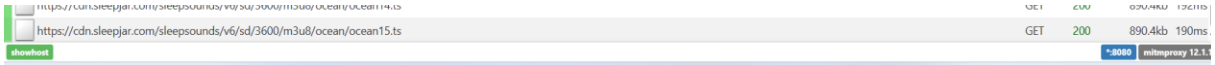
Path	Method	Status	Size	Time
https://na-api-alexa.amazon.ca/api/np/list-media-sessions?deviceSerialNu...	GET	200	23b	87ms
https://na-api-alexa.amazon.ca/api/np/list-media-sessions?deviceSerialNu...	GET	200	23b	↻
https://signaler-pa.clients6.google.com/punctual/multi-watch/channel?VER...	OPTIONS	200	0	65ms
https://signaler-pa.clients6.google.com/punctual/multi-watch/channel?VER...	GET	200	0	...
https://na-api-alexa.amazon.ca/api/np/list-media-sessions?deviceSerialNu...	GET	200	23b	87ms

sleep_soundspic.png



Path	Method	Status	Size	Time
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean.m3u8?src=alexa&src_request_id=amzn1.echo-api.request.c7bab921-76ec-48db-8e2b-0b0a01781530	GET	200	1.9kb	30ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean0.ts	GET	200	890.8kb	213ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean1.ts	GET	200	890.2kb	190ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean2.ts	GET	200	891.0kb	190ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean3.ts	GET	200	890.4kb	1 ↻
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean4.ts	GET	200	890.1kb	192ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean5.ts	GET	200	891.2kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean6.ts	GET	200	890.1kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean7.ts	GET	200	890.4kb	187ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean8.ts	GET	200	890.6kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean9.ts	GET	200	890.6kb	187ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean10.ts	GET	200	890.2kb	189ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean11.ts	GET	200	890.4kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean12.ts	GET	200	890.6kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean13.ts	GET	200	890.6kb	198ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean14.ts	GET	200	890.4kb	192ms

sleep_soundspic2.png



https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean14.ts	GET	200	890.4kb	192ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean15.ts	GET	200	890.4kb	190ms