

THE CALL IS COMING FROM INSIDE THE HOUSE

API ABUSE BY AUTHENTICATED USERS

AMIR SHARIF
SECURE SOFTWARE BY DESIGN
AUGUST 7 2024

DISCUSSION OUTLINE

1. Definitions
2. Concrete examples
3. Spectrum of severity
4. Hacker how-to
5. New challenges
6. Mitigations

1 DEFINITIONS

Sometimes an authenticated user can be malicious

Broken Object Level Authorization

(BOLA, OWASP API1:20 23)

“APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface of Object Level Access Control issues. Object level authorization checks should be considered in every function that accesses a data source using an ID from the user.”

Broken Function Level Authorization

(BFLA, OWASP API5:20 23)

“Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers can gain access to other users’ resources and/or administrative functions.”

And several associated vulnerabilities

API3:2023 Broken Object Property Level Authorization

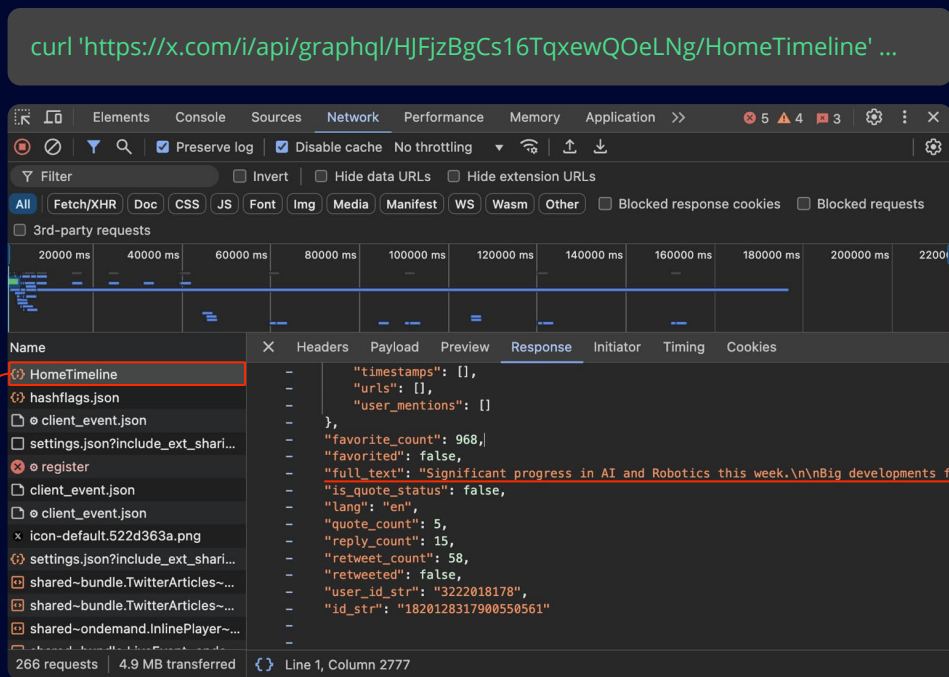
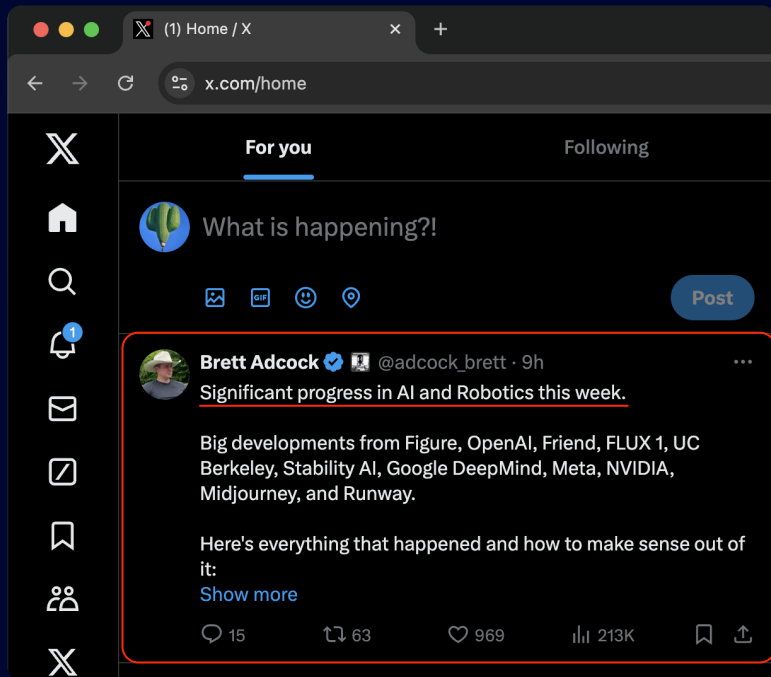
API4:2023 Unrestricted Resource Consumption

API6:2023 Unrestricted Access to Sensitive Business Flows

API10:2023 Unsafe Consumption of APIs

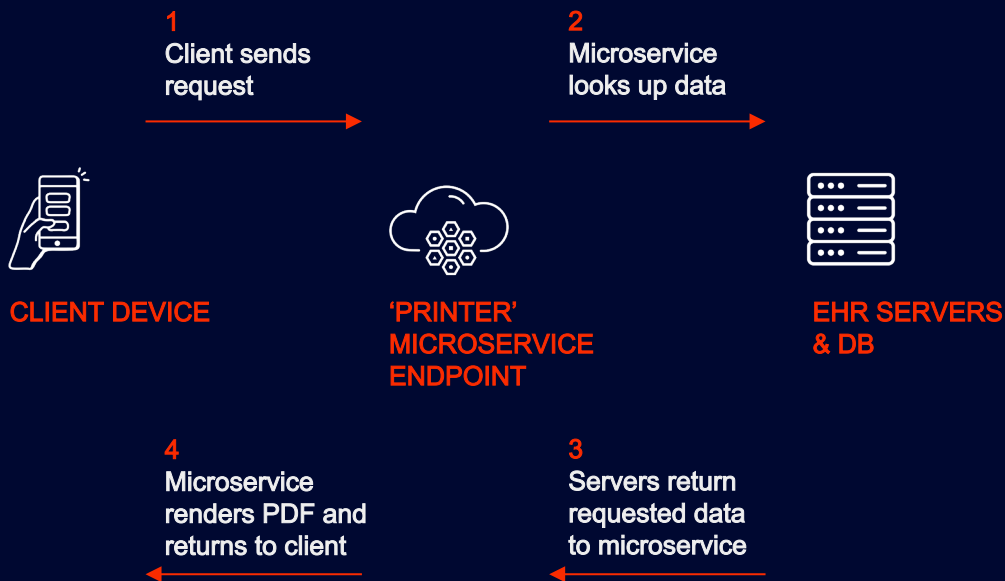
1 DEFINITIONS

Modern web apps are reliant on frontend APIs that developers often assume are only called via valid client interactions



2 CONCRETE EXAMPLES

BOLA: An EHR that allows practice managers to generate printable claims can be manipulated to leak data about unaffiliated patients



```
curl -G 'https://print.ehr.com/claim.do' \
-d 'claim_action=LOGIN' \
-d 'auth=YL1kwdUY1WWZqWXJ' \
-d 'claimId=101' \
-d 'PAGE_NAME=PDF' \
-H 'cookie: SESSIONID=10BFCCBF3ED;'
```

2 CONCRETE EXAMPLES


BFLA: An EHR that allows physicians to mutate or delete patient encounter data...

Status

Checked Out

Jane Blackberry

#999



Appointment Summary

Rendering provider

Appleseed, John MD

...

Diagnoses

Z76.89


Persons encountering health services...

Services

Procedure

Code	Description	Diagnoses
99203	OFFICE OR OTHER OUTPATIENT VISIT FOR THE EVALUATION AND MANAGEMENT OF A NEW PATIENT	Z7689

EDIT




2 CONCRETE EXAMPLES

BFLA: ... that unintentionally also gives those privileges to patients

Status
Checked Out

Jane Blackberry
#999



Appointment Summary
Rendering provider
Appleseed, John MD
...

Diagnoses
Z76.89
Persons encountering health services...

Services

Procedure Code	Description	Diagnoses
99203	OFFICE OR OTHER OUTPATIENT VISIT FOR THE EVALUATION AND MANAGEMENT OF A NEW PATIENT	Z7689

DELETE

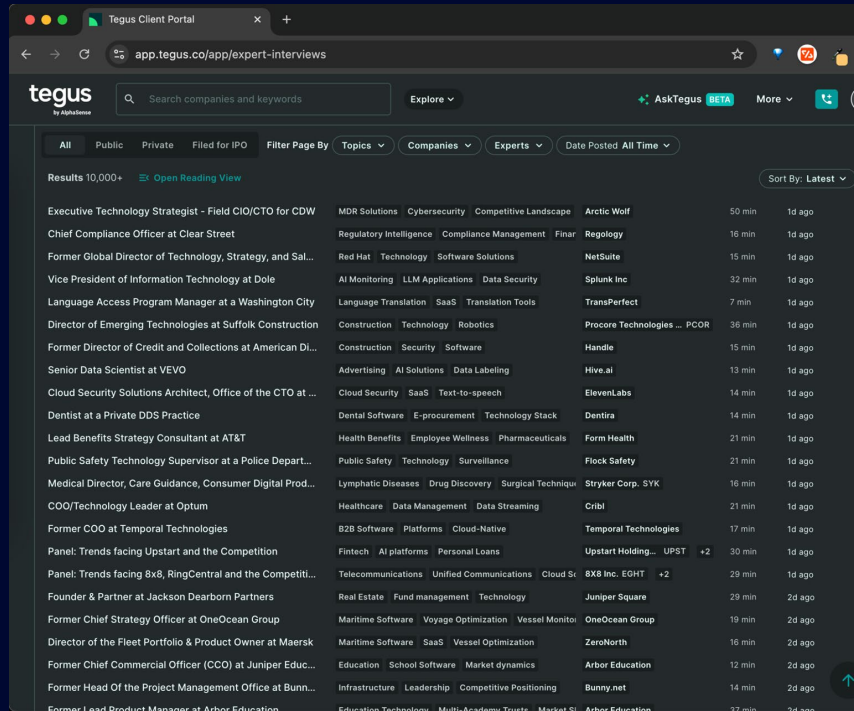
```
curl -X POST 'https://ehr.com/encountersAdmin \  
' -H 'Content-Type: application/x-www-form-urlencoded' \  
' -H 'Cookie: SESSIONID=91cb4a2b' \  
' -H 'X-CSRF-Token: abab1212' \  
' --data-raw 'adminAction=delEncounter&idEncounter=789789&idPatient=999'
```

EDIT

```
curl -X POST 'https://ehr.com/encountersAdmin \  
' -H 'Content-Type: application/x-www-form-urlencoded' \  
' -H 'Cookie: SESSIONID=91cb4a2b' \  
' -H 'X-CSRF-Token: abab1212' \  
' --data-raw 'adminAction=updateEncounter&idPractice=123&idEncounter=789789&addCode=99203%2C90792&callingPage=encountersAdmin&targetPage=encountersAdmin&browserId=123456'
```

2 CONCRETE EXAMPLES

Unrestricted Resource Consumption is significantly more common across frontend APIs



```
curl 'https://app.tegus.co/graphql/client' \  
-H 'accept: application/json, text/plain, */*' \  
-H 'cookie: ...' \  
-H 'x-client-version: f8e336bae' \  
-H 'x-csrf-token: KRIGCURMZVxXOGN' \  
-H 'x-datadog-origin: rum' \  
-H 'x-datadog-sampling-priority: 1' \  
-H 'x-requested-with: XMLHttpRequest' \  
--data-raw '${... "first":20,"after":"MTE5"}'
```


3 SPECTRUM OF SEVERITY

Many companies are aware of these vulnerabilities but ~~do not~~ prioritize refactoring because the impact is not always substantial

PERCEIVED
BUSINESS
IMPACT
SEVERITY

Net Benefit

Low Severity

High

Urgent

'Shadow API'

Nuisance

Privacy violation

Product failure

Considered undocumented, unofficial integration APIs

Can lead to resource exhaustion and loss of API product revenue

Leakages of user data that, if made public, will be considered urgent

Service interruptions that can lead to severe product malfunctions

(esp. data mutations/deletions)

3 SPECTRUM OF SEVERITY

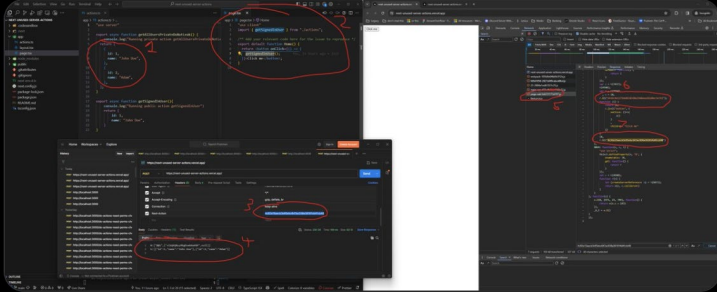
Modern web frameworks automatically default to generating flexible API endpoints that expose assets – and users are increasingly savvy

Rhys Sullivan @RhysSullivan

If you care about security for your NextJS app, **stop using top level "use server"** – it's way too easy to leak data

Top level "use server" creates endpoints for all exported functions, even if they are never used on the client

One accidental export can cause a ton of damage



12:27 AM · Jul 2, 2024 · 249.2K Views

59 168 1.1K 871

Theo - t3.gg @t3dotgg

I was trying to book a doctor's appointment earlier and the form was broken, so I spoofed it via CURL and was able to book 🤖

```
curl 'https://app.circlemedical.com/v1/patients' \
-H 'accept: application/json, text/plain, */*' \
-H 'accept-language: en-US,en;q=0.9' \
-H 'content-type: application/json' \
-H 'dnt: 1' \
-H 'origin: https://booking-v2.circlemedical.com' \
-H 'priority: u=1, i' \
-H 'referer: https://booking-v2.circlemedical.com/' \
-H 'sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"' \
-H 'sec-ch-ua-mobile: ?0' \
-H 'sec-ch-ua-platform: "macOS"' \
-H 'sec-fetch-dest: empty' \
-H 'sec-fetch-mode: cors' \
-H 'sec-fetch-site: same-site' \
-H 'user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36' \
-H 'x-user-email: [REDACTED]' \
-H 'x-user-token: [REDACTED]'
```

3:52 PM · Jul 11, 2024 · 377.6K Views

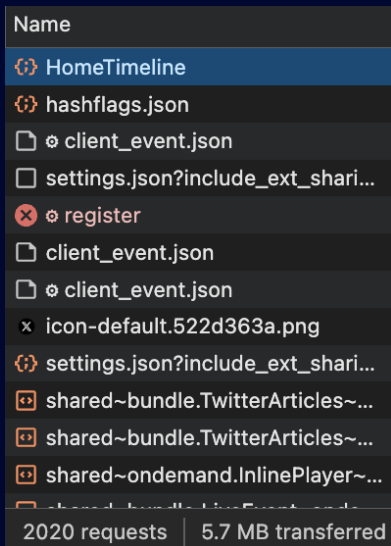
171 234 6.6K 667

4 HACKER HOWTO

Hunting for and exploiting these vulnerabilities is as easy as 1, 2, 3

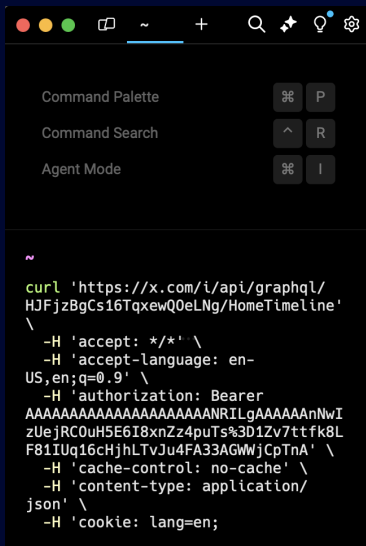
1 Catalog endpoints

Manual review of product network requests



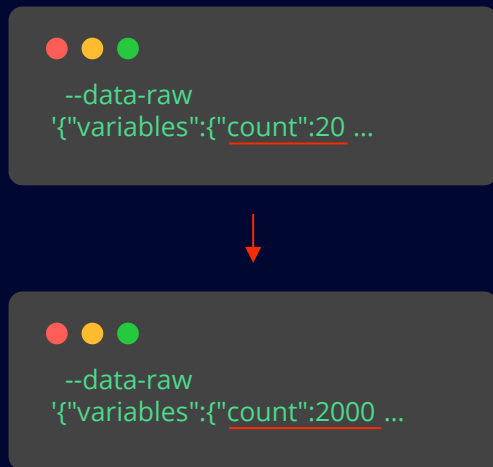
2 Try to replay requests

Replay requests to determine auth validation



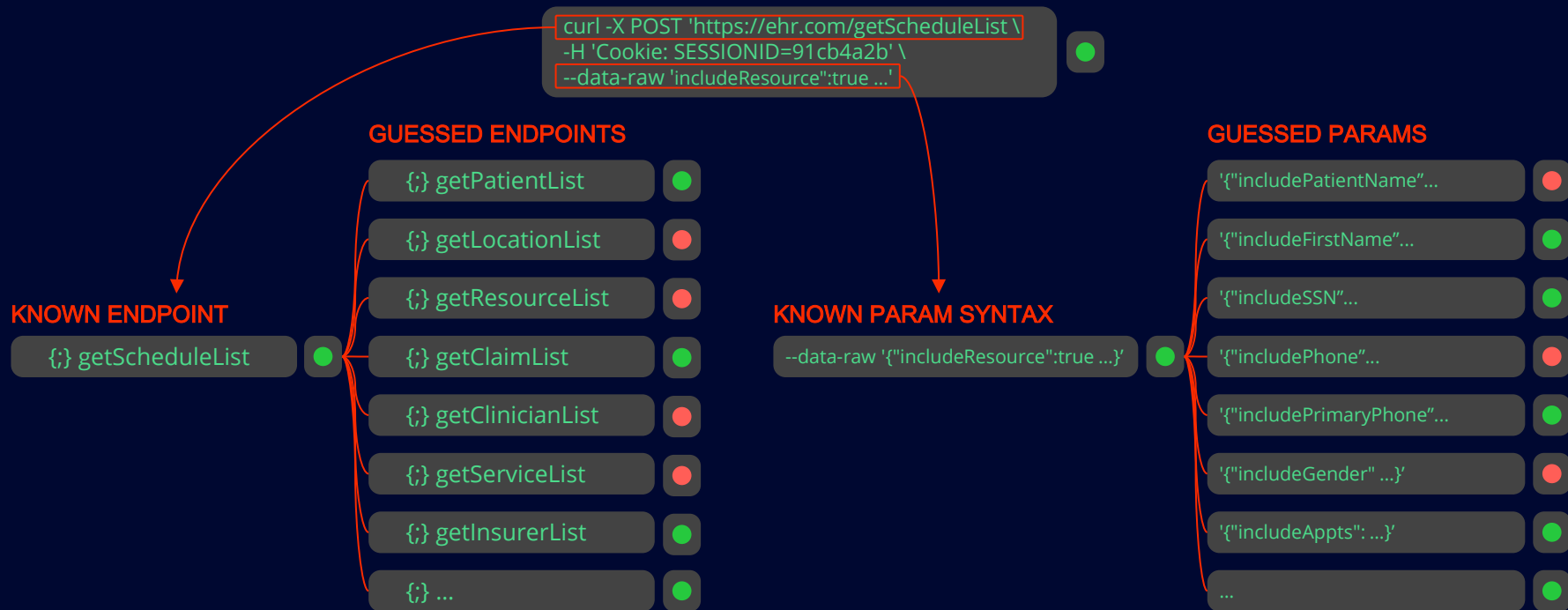
3 Make educated guesses

Adjust payloads based on semantic meaning and see!



5 NEW CHALLENGES

More sophisticated entities will automate this process, using LLMs to programmatically drive previously manual semantic analysis



5 NEW CHALLENGES

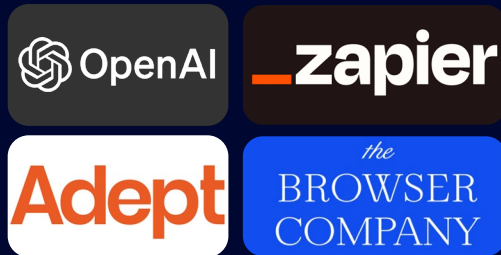
Some teams are rumored to be attempting to productionize these ‘scanners’ as general, cross-product API integration ‘SDKs’

LEGACY ANALOG



Manually built screen-scraping integrations into financial institutions’ online portals. At maturity negotiated dedicated integrations.

MODERN GENERALISTS



Experimenting with agents that approximate cross-product backend integrations.

6 MITIGATIONS

If you're looking for a quick solution, turn off your servers. Alternatively try one of these approaches...

MONITOR

WHAT

All network traffic, using cookies and session IDs to map requests back to specific users. Look for volumes of requests, resource demands, failed requests, and 'unnatural' patterns.

WHY

Determine the scope and scale of potential threats for your product.

TEST

WHAT

All API endpoints used by your frontend client and any endpoints that are actively called in network logs. Use various authenticated user accounts to deterministically attempt to leak or mutate unauthorized content.

WHY

The best way to find out about a potential vulnerability is with a test, before merging to prod.

REFACTOR

WHAT

Obfuscate all keys and IDs using hashes instead of guessable incrementing integers. Minimize and 'encrypt' frontend API calls to make them less legible. Use an intermediary microservice to route and filter requests, acting as a turbocharged cookie authenticator.

WHY

Establishes an effective firewall against unauthorized and invalid API calls.

AMIR SHARIF

amir@bondstreetresearch.com

SECURE SOFTWARE BY DESIGN

AUGUST 7 2024



thank you