BASTION

SECURITY GROUP

# JWT WTF?

## A Look Into Common JWT Vulnerabilities

05/09/2025

# Thank You to Our Sponsors and Hosts!

OWASP
NEW
ZEALAND
owasp.org.nz

Waipapa
Taumata Rau
University
of Auckland

AppSec
NZ
appsec.org.nz

BASTION
SECURITY GROUP

SECURE
CODE
WARRIOR

exabeam™

safe advisory.

CyberCX

plexure

SECDIM

Without them, this conference couldn’t happen.

# whoami

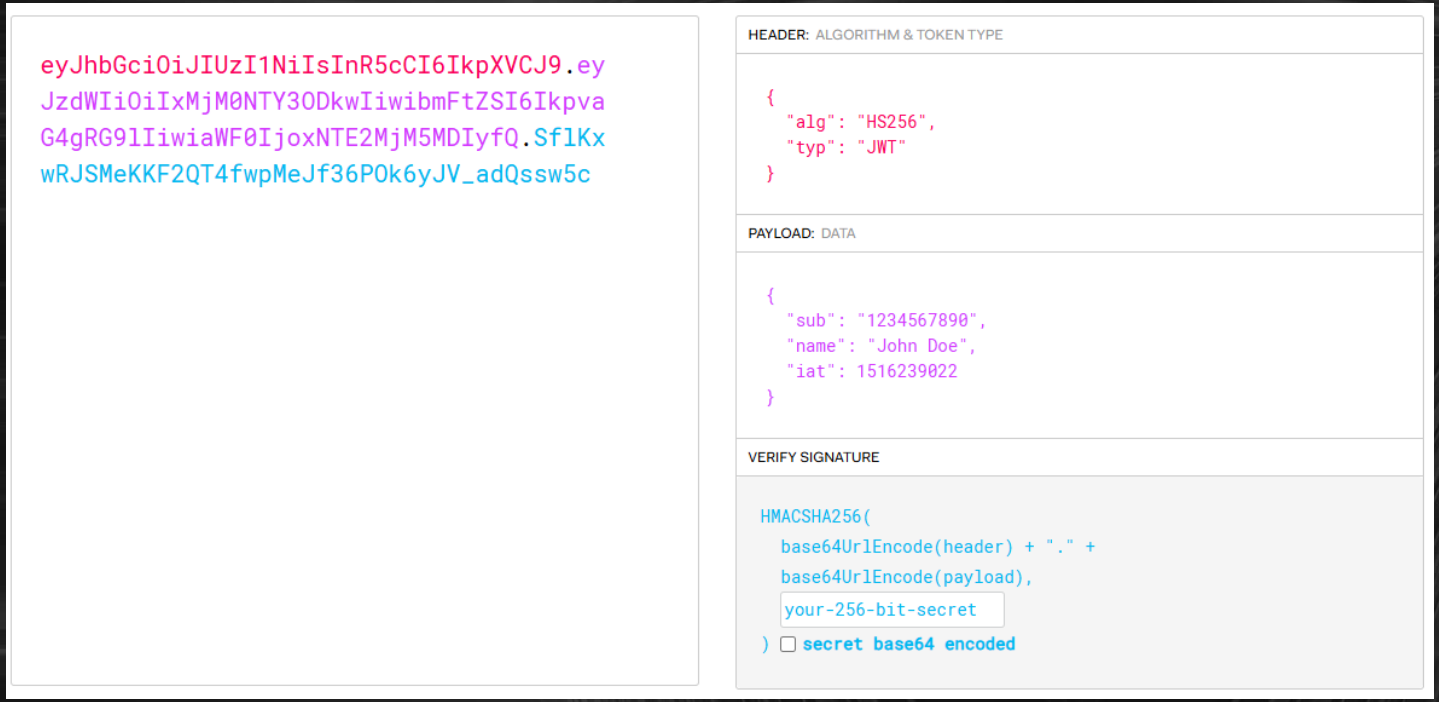
- Lead Security Consultant at Bastion Security
- Pentester for over 6 years
- Previously done internal security consultancy for a bank.

# Agenda

- What is a JWT?
- Common attacks against JWTs
- ~~Live Demo~~ Pre-Recorded Demo
- Security best practices
- Q&A

# What is a JWT?

- A way of representing information between parties
  - Commonly used for Authentication and Authorisation
- Digitally signed - trusted and verifiable
- Consists of a header, payload and signature



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKx
wRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```

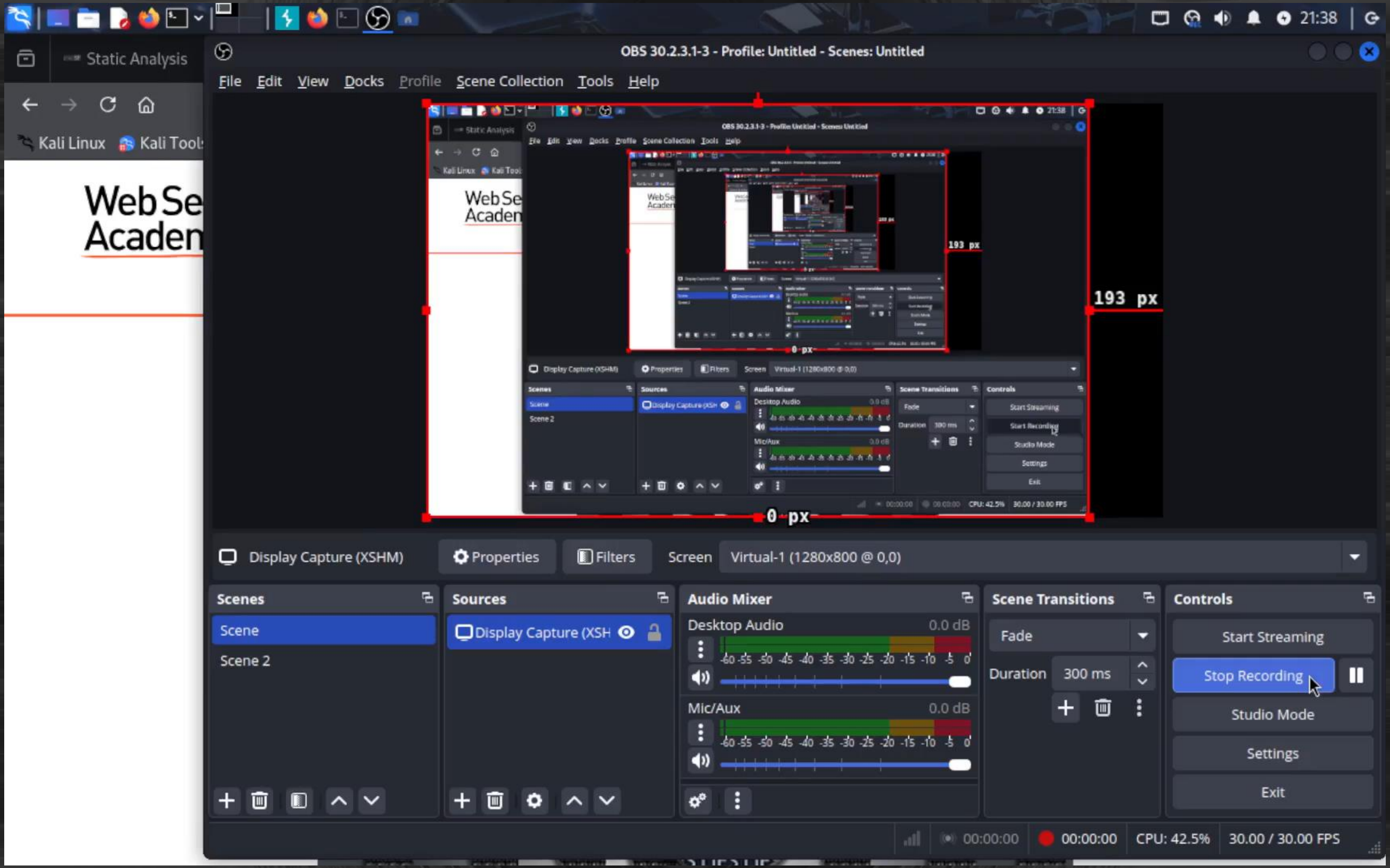
# What Can We Attack?

- Header - Algorithm
- Payload - User Claims
- Signature
- The entire token - Replay attacks

# No Verification

- Vulnerability: Server does not validate the signature at all.
- Attack: Change the JWT claim as you see fit!

# Demo



OBS 30.2.3.1-3 - Profile: Untitled - Scenes: Untitled

Display Capture (XSHM)

Screen: Virtual-1 (1280x800 @ 0,0)

Scenes: Scene, Scene 2

Sources: Display Capture (XSH

Desktop Audio 0.0 dB

Mic/Aux 0.0 dB

Scene Transitions: Fade

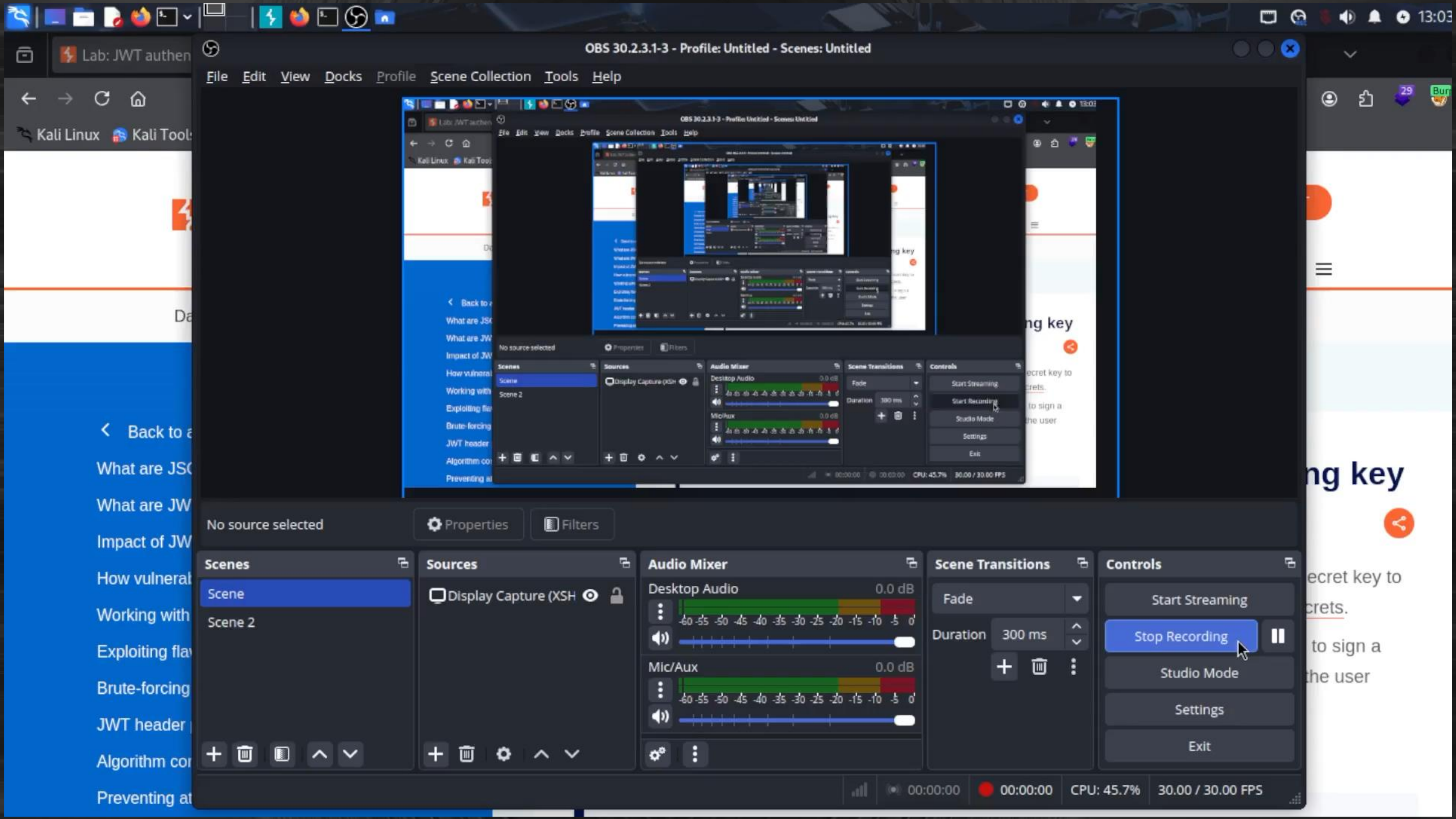
Duration: 300 ms

00:00:00 00:00:00 CPU: 42.5% 30.00 / 30.00 FPS

# Weak Secret Key

- Vulnerability: When the HMAC algorithm is used with a weak secret key.
- Attack: Using a valid JWT, we can bruteforce it to get the secret.
- Using this secret, we can sign our own valid tokens.

# Demo

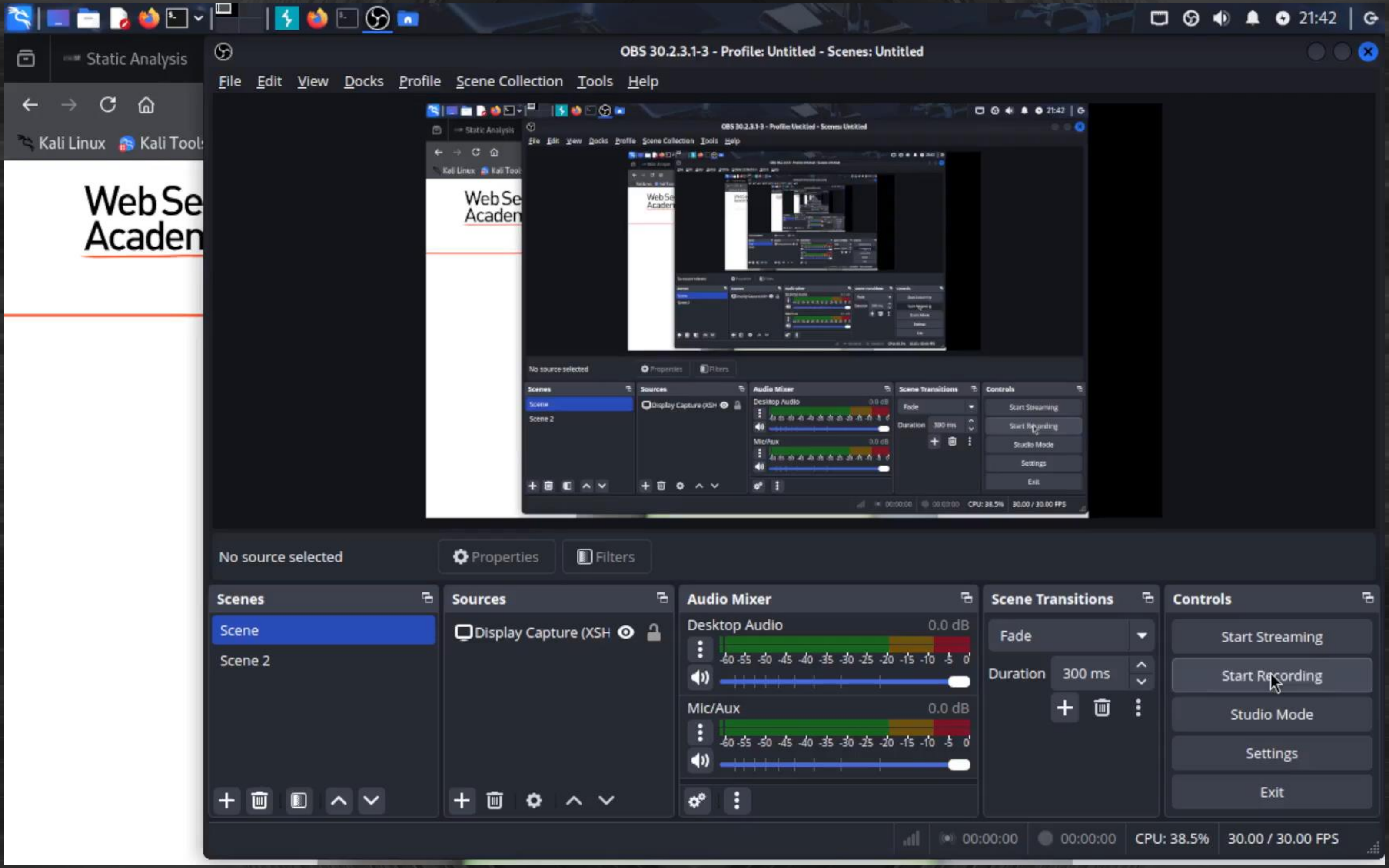


OBS 30.2.3.1-3 - Profile: Untitled - Scenes: Untitled
File
Edit
View
Docks
Profile
Scene Collection
Tools
Help
Lab: JWT authen
Kali Linux
Kali Tools
Back to a
What are JSO
What are JW
Impact of JW
How vulnerab
Working with
Exploiting flav
Brute-forcing
JWT header
Algorithm cor
Preventing at
ng key
ecret key to
crets.
to sign a
the user
No source selected
Properties
Filters
Scenes
Scene
Scene 2
Sources
Display Capture (XSH
Audio Mixer
Desktop Audio
0.0 dB
Mic/Aux
0.0 dB
Scene Transitions
Fade
Duration
300 ms
Controls
Start Streaming
Stop Recording
Studio Mode
Settings
Exit
00:00:00
00:00:00
CPU: 45.7%
30.00 / 30.00 FPS
13:03

# alg: none

- Vulnerability: Server accepts unsigned tokens
- Attack: Change header to { "alg": "none" } and remove the signature
- Profit?

# Demo



21:42
Static Analysis
Kali Linux
Kali Tools
Web Se
Acaden
OBS 30.2.3.1-3 - Profile: Untitled - Scenes: Untitled
File
Edit
View
Docks
Profile
Scene Collection
Tools
Help
No source selected
Properties
Filters
Scenes
Scene
Scene 2
Sources
Display Capture (XSH
Audio Mixer
Desktop Audio
0.0 dB
Mic/Aux
0.0 dB
-60 -55 -50 -45 -40 -35 -30 -25 -20 -15 -10 -5 0
Scene Transitions
Fade
Duration
300 ms
Controls
Start Streaming
Start Recording
Studio Mode
Settings
Exit
00:00:00
00:00:00
CPU: 38.5%
30.00 / 30.00 FPS

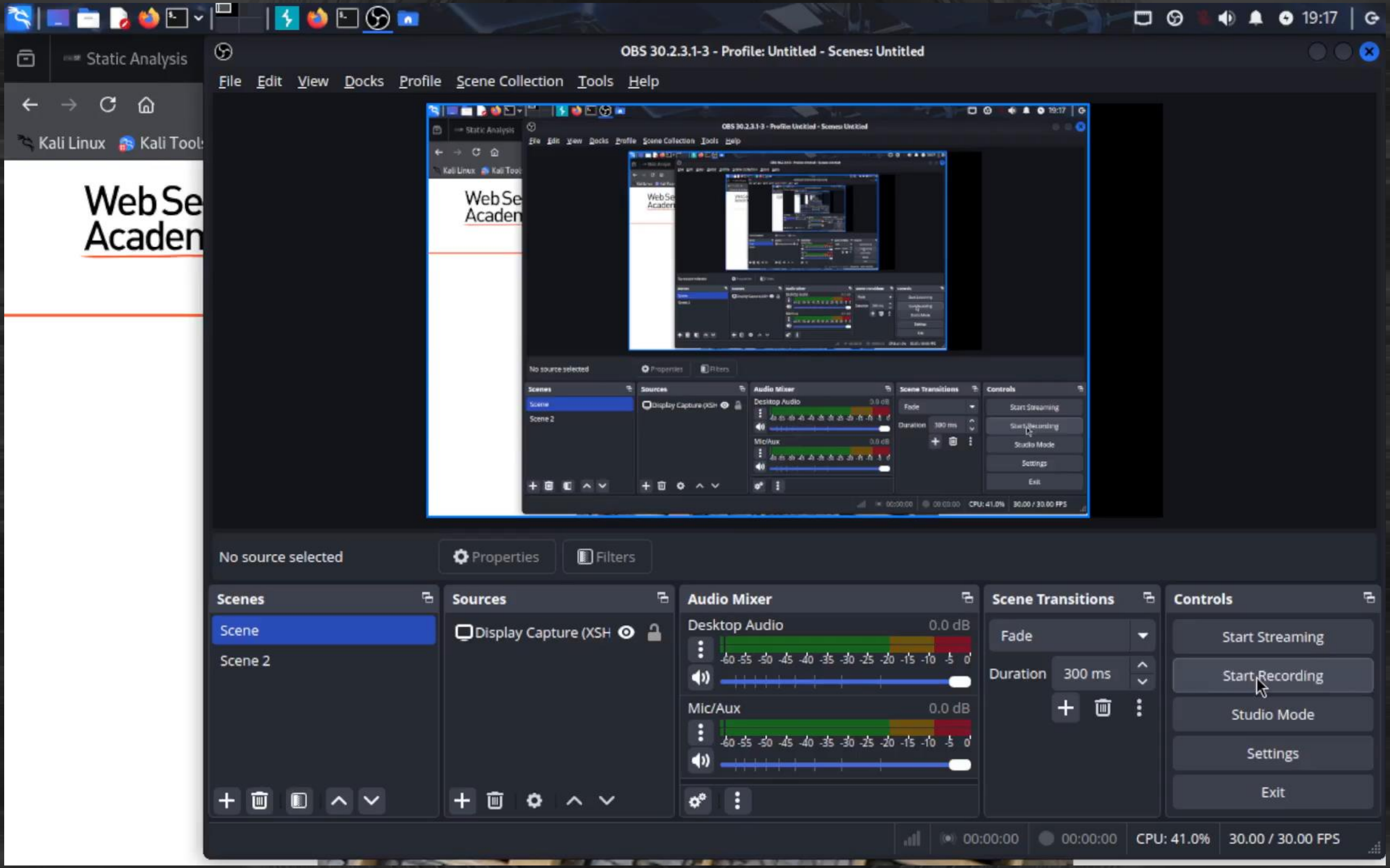
# sPoNgEbOb yOuR wAy tO vIcToRy

- Avoid denylisting - Fix the root cause.
- Auth0 - JWT Validation Bypass in Authentication API

# Key Confusion

- Arises when JWT libraries use a single method for verifying signatures.
- We can force the server to use the HMAC symmetric algorithm instead of RSA
- In a flawed implementation, we can use the server’s public key to sign JWTs.
- Since the server uses the same public key to verify the JWT, we can create valid JWTs.

# Demo


OBS 30.2.3.1-3 - Profile: Untitled - Scenes: Untitled
File
Edit
View
Docks
Profile
Scene Collection
Tools
Help
Static Analysis
Kali Linux
Kali Tools
Web Se
Acaden
19:17
No source selected
Properties
Filters
Scenes
Scene
Scene 2
Sources
Display Capture (XSH
Audio Mixer
Desktop Audio
0.0 dB
Mic/Aux
0.0 dB
Scene Transitions
Fade
Duration
300 ms
Controls
Start Streaming
Start Recording
Studio Mode
Settings
Exit
00:00:00
00:00:00
CPU: 41.0%
30.00 / 30.00 FPS

# So How To Secure?

- Use proven libraries and keep them updated
  - Stick with battle-tested libraries
- Use strong, modern algorithms such as RS256
  - Explicitly reject alg: none and all its variants - don’t rely on library defaults
- Always treat user input as untrusted
  - Validate all claims on the server-side
- Do security reviews.
  - Peer Reviews, Penetration Testing, SCA/SAST Tooling.

# Questions?

BASTION

SECURITY GROUP