

Add Security to API Endpoints with JWT



Deeksha Sharma

CO-FOUNDER AND ENGINEER

@deekshasharma25 www.bonsailabs.com

Agenda

- How to generate JWT
- JWT in Cookie vs Auth Header
- Code refactor front end - with cookies
- Test with POSTMAN

Generating JSON Web Token

Stateless vs Stateful JWT



Stateful JWT

Transporting JWT

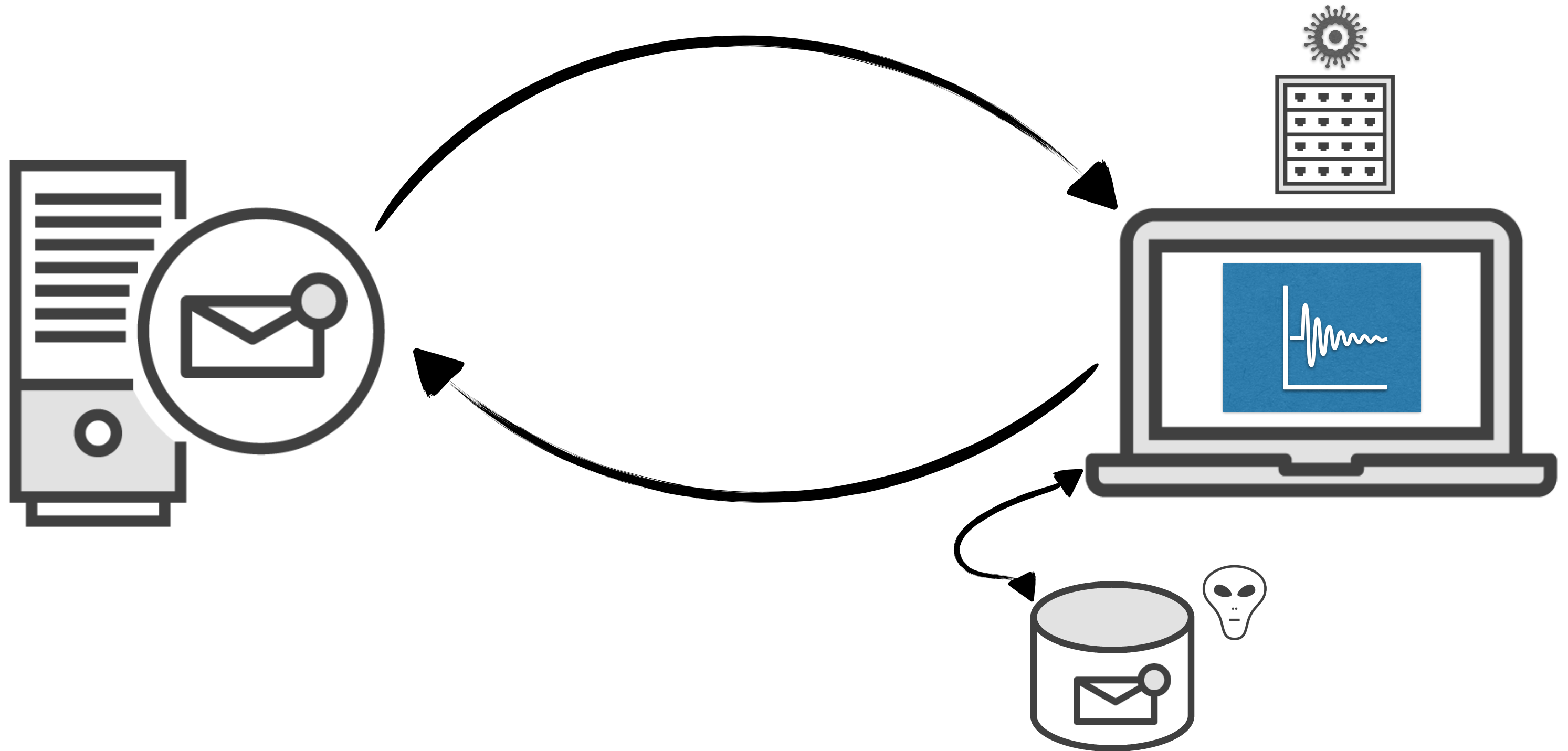


The diagram consists of two blue circles with black outlines, positioned side-by-side. The left circle contains the text 'JWT in Auth Header' and the right circle contains the text 'JWT in Cookie'. Both circles are centered vertically and horizontally relative to the title above them.

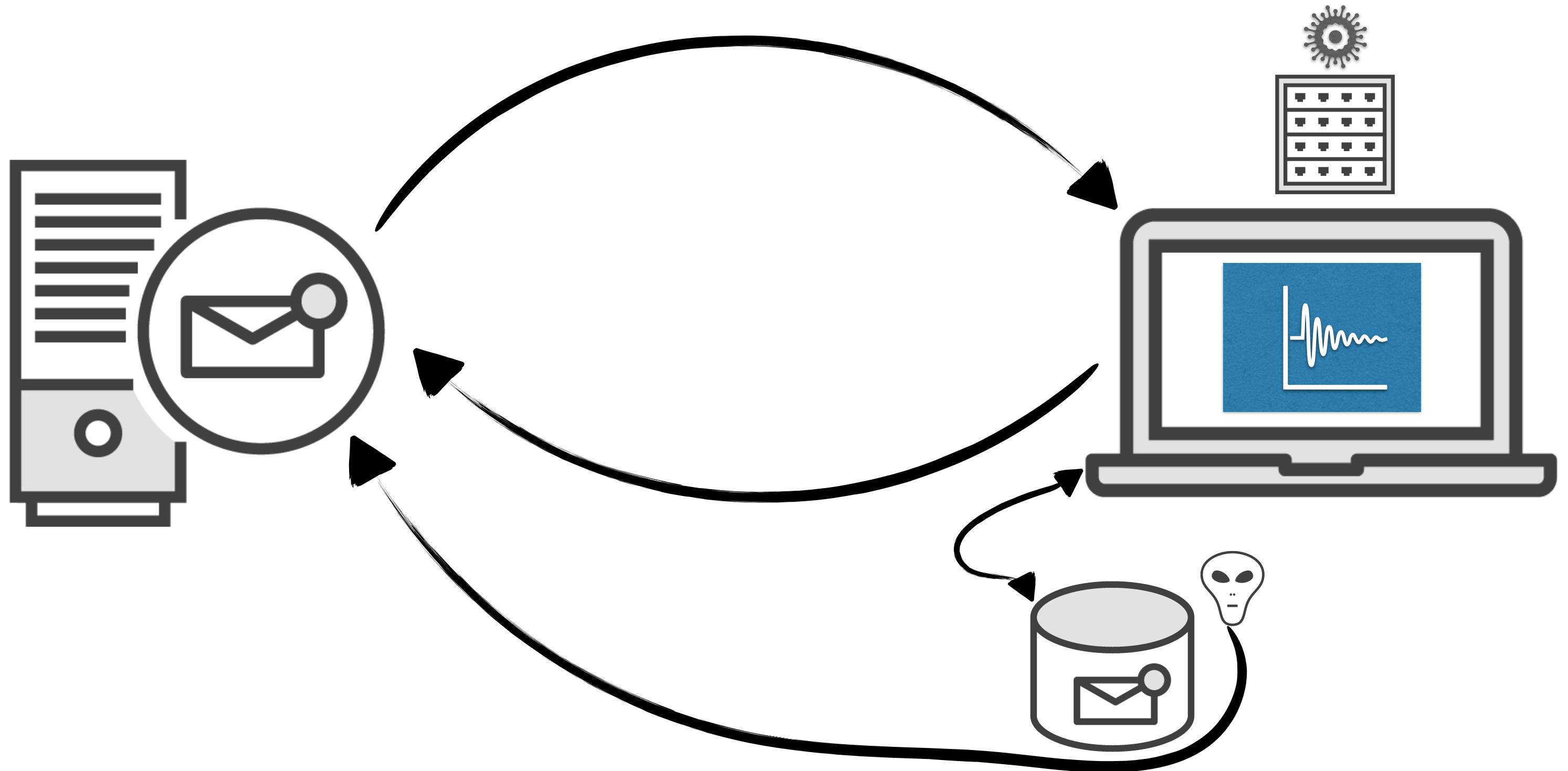
**JWT in
Auth Header**

**JWT in
Cookie**

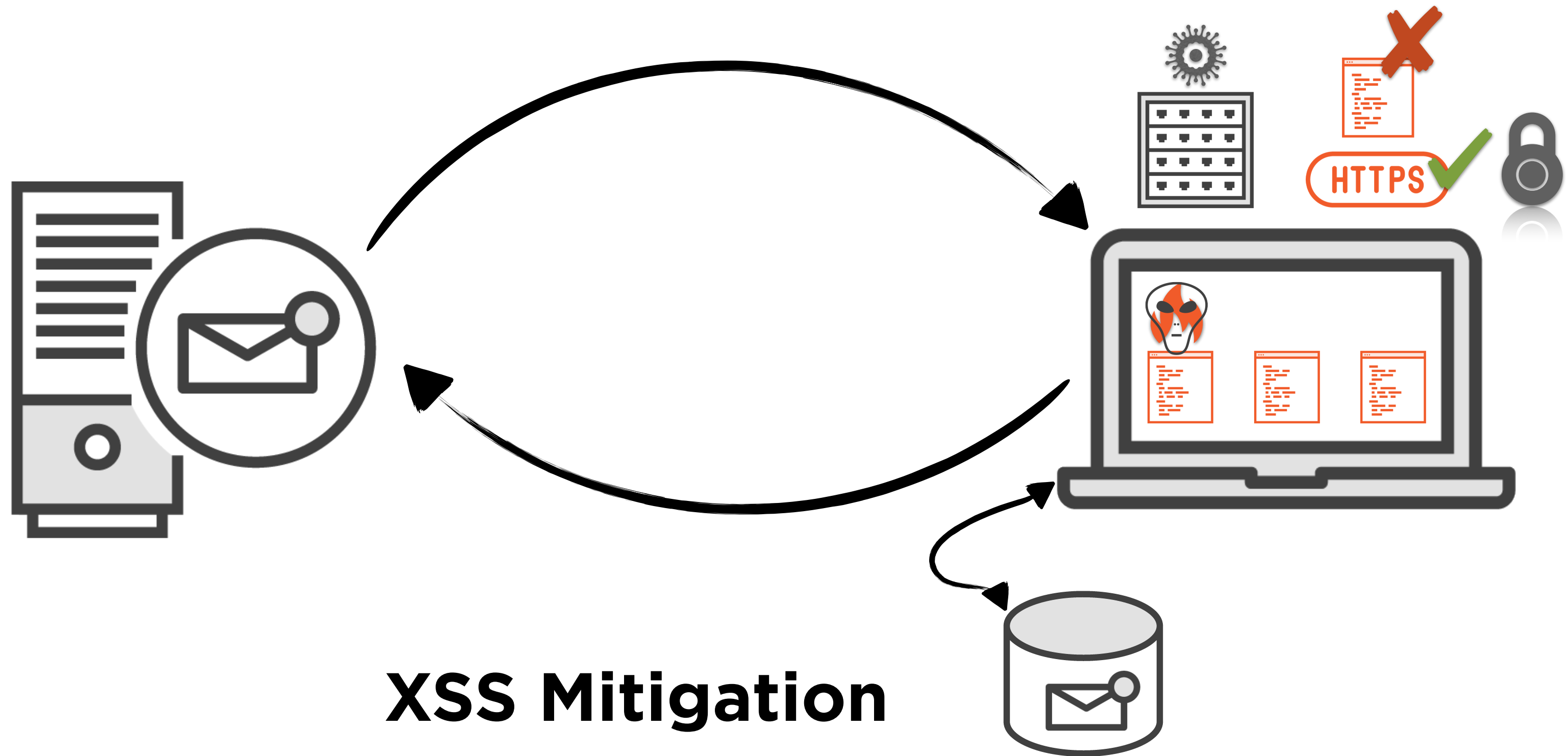
JWT in Auth Header



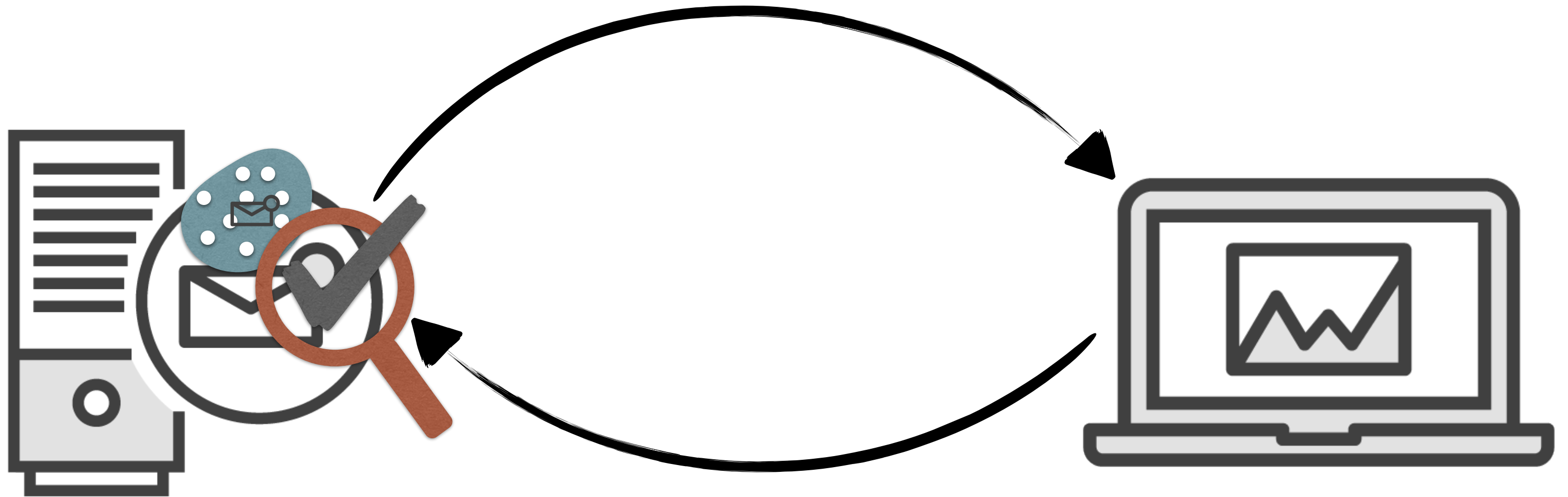
JWT in Auth Header



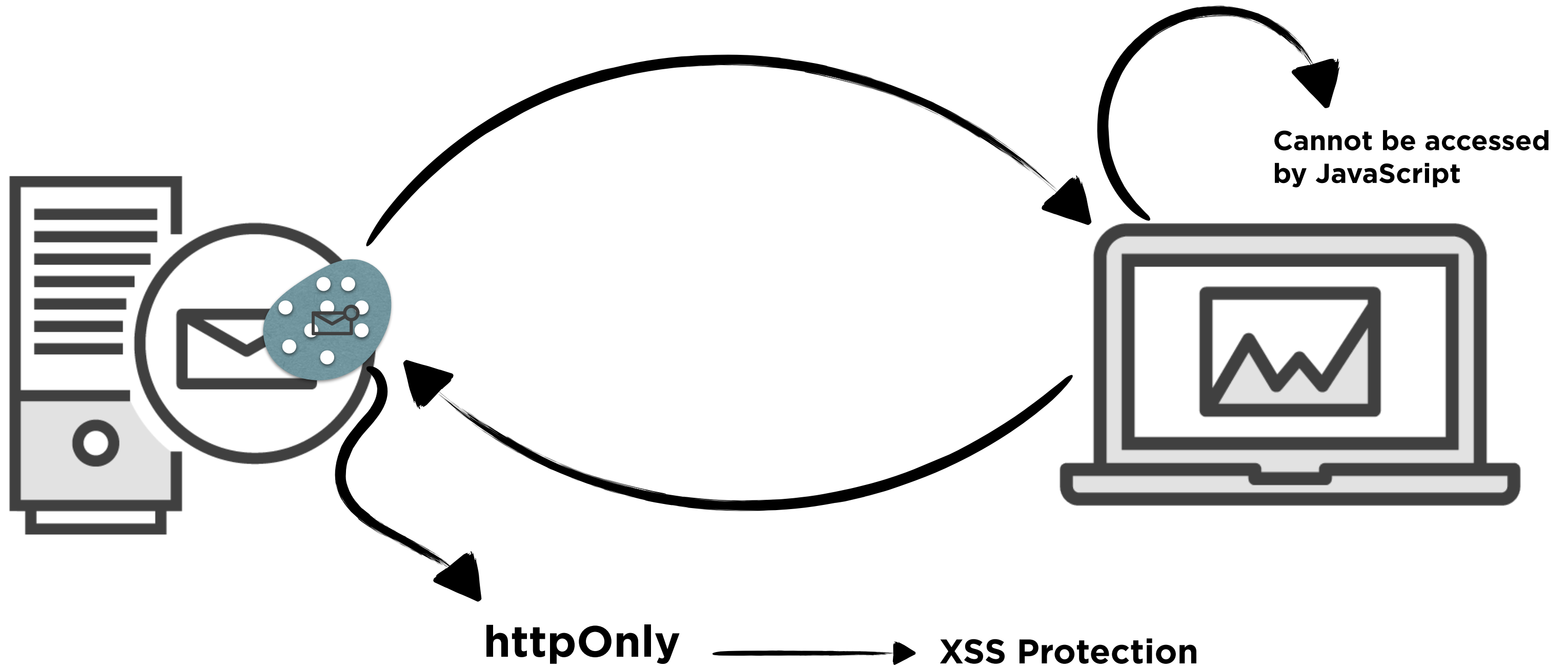
JWT in Auth Header



JWT in Cookie

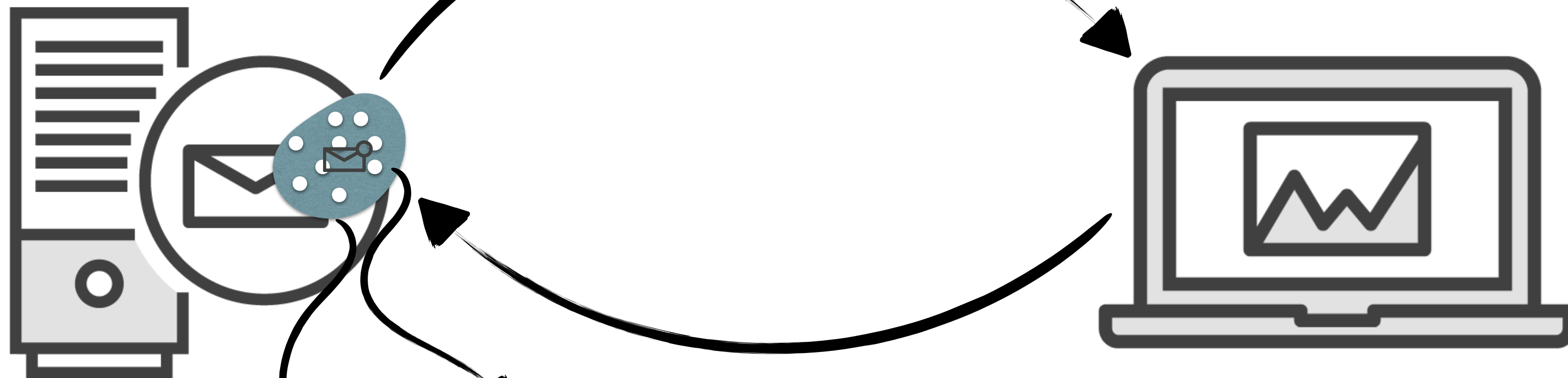


JWT in Cookie



JWT in Cookie

Cross Site Request Forgery
(CSRF)



httpOnly

XSS Protection

SameSite=Strict

CSRF Protection

JWT - Bookie App

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

Header

JWT - Bookie App

```
{  
  "iss": "BOOKIE_ORG",  
  "sub": "deeksha30",  
  "aud": ["SHOW_FAVORITE", "LOGIN", "SHOW_BOOKS"],  
  "exp": "1h"  
}
```

Payload

JWT - Bookie App

```
{  
  "nbf": 1479203274,  
  "iat": 1479205078,  
  "jti": "yu5CSpyHI",  
}
```

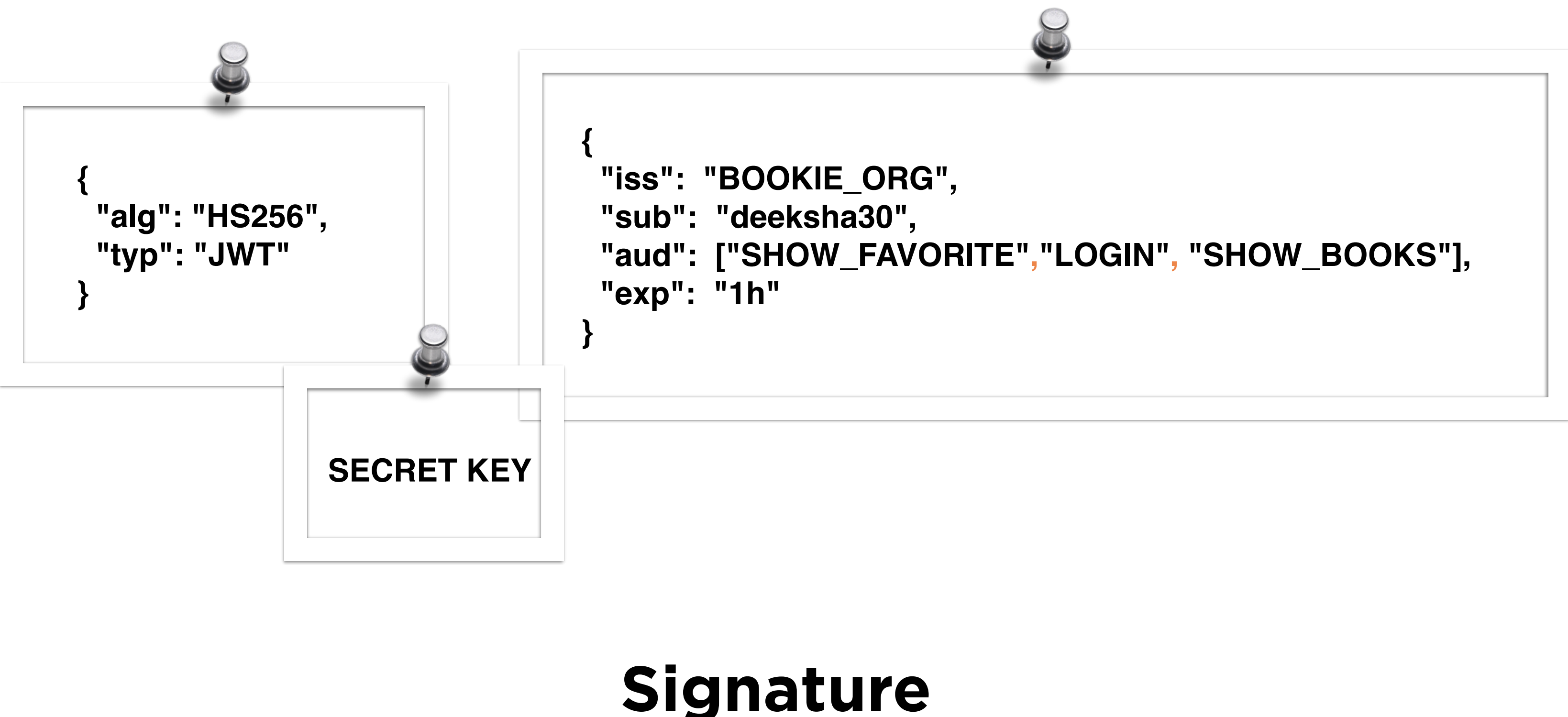
Other Registered Claims

JWT - Bookie App

```
{  
  "iss": "BOOKIE_ORG",  
  "sub": "deeksha30",  
  "aud": ["SHOW_FAVORITE", "LOGIN", "SHOW_BOOKS"],  
  "exp": "1h",  
  "scope": "member",  
}
```

Private Claims

JWT - Bookie App



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

```
{  
  "iss": "BOOKIE_ORG",  
  "sub": "deeksha30",  
  "aud": ["SHOW_FAVORITE", "LOGIN", "SHOW_BOOKS"],  
  "exp": "1h"  
}
```

SECRET KEY

Signature

Git Branches

JWT Cookie

module04_jwt_security_cookies

JWT Auth Header

module04_jwt_security_bearer_token

Summary

- How JWT is generated
- JWT in Cookie vs Auth Header
- Front end - with cookies
- Tested backend API with POSTMAN