# JSON Web Tokens (JWT)

# Sessions

- login(request, user)
- CsrfViewMiddleware
- SessionMiddleware
- Everything works
- The web framework for perfectionists with **deadlines**

```
<img src=
"http://localhost:8080/gui/
?action=setsetting&
s=webui.password&
v=eviladmin">
```

# JWT (JSON web tokens)

**Refresh token - Valid if it exists in database**

Example:ee452d11-c10f-47ce-bbec-56cc20223b04

**Access token - Expires every X minutes**

Example:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ

## Encoded PASTE A TOKEN HERE


```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzd
WIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9
lIiwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RM
HrHDcEfxjoYZgeFONFh7HgQ
```


## Decoded EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
) secret base64 encoded
```

Signature Verified

BLOG

# Critical vulnerabilities in JSON Web Token libraries

Which libraries are vulnerable to attacks and how to prevent them.

Tim McLean

March 31, 2015

# JWT Advantages

- Access token not saved in a database
- CSRF

# JWT Disadvantages

- Security **(?)**
- Relatively new **(?)**
- Sessions are build-in django established, secure and well documented
- Potentially big tokens**(?)**