Cyber Offense and Defense

UNIVERSITÀ DELLA CALABRIA

il Campus per eccellenza

JWT attacks

Mario Alviano

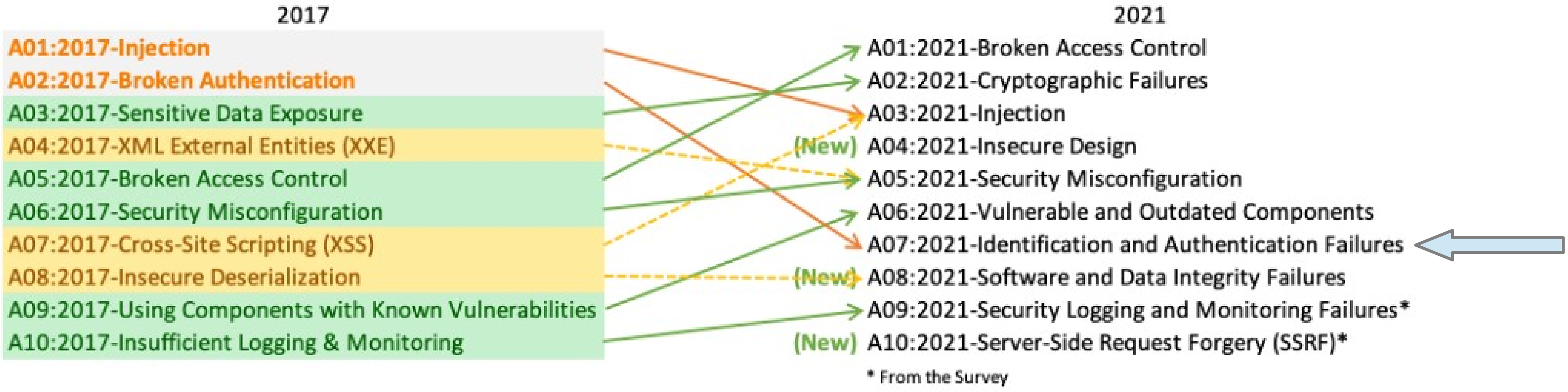
Main References

Bug Bounty Bootcamp – Chapter 3 (something)

https://portswigger.net/web-security/jwt

OWASP Top Ten

A broad consensus about the most critical security risks to web applications



2017

A01:2017-Injection

A02:2017-Broken Authentication

A03:2017-Sensitive Data Exposure

A04:2017-XML External Entities (XXE)

A05:2017-Broken Access Control

A06:2017-Security Misconfiguration

A07:2017-Cross-Site Scripting (XSS)

A08:2017-Insecure Deserialization

A09:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

(New) A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

(New) A08:2021-Software and Data Integrity Failures

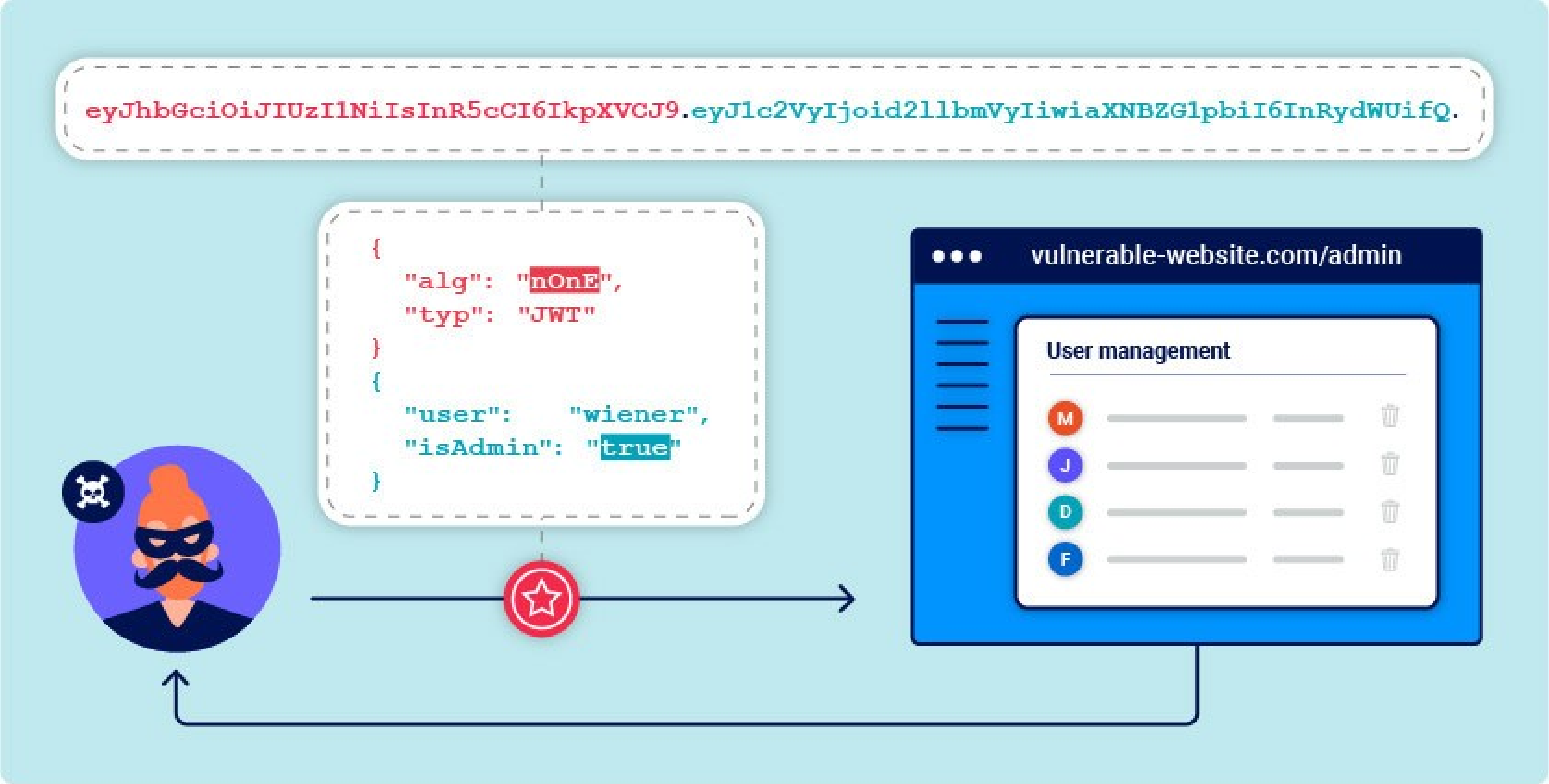
A09:2021-Security Logging and Monitoring Failures*

(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

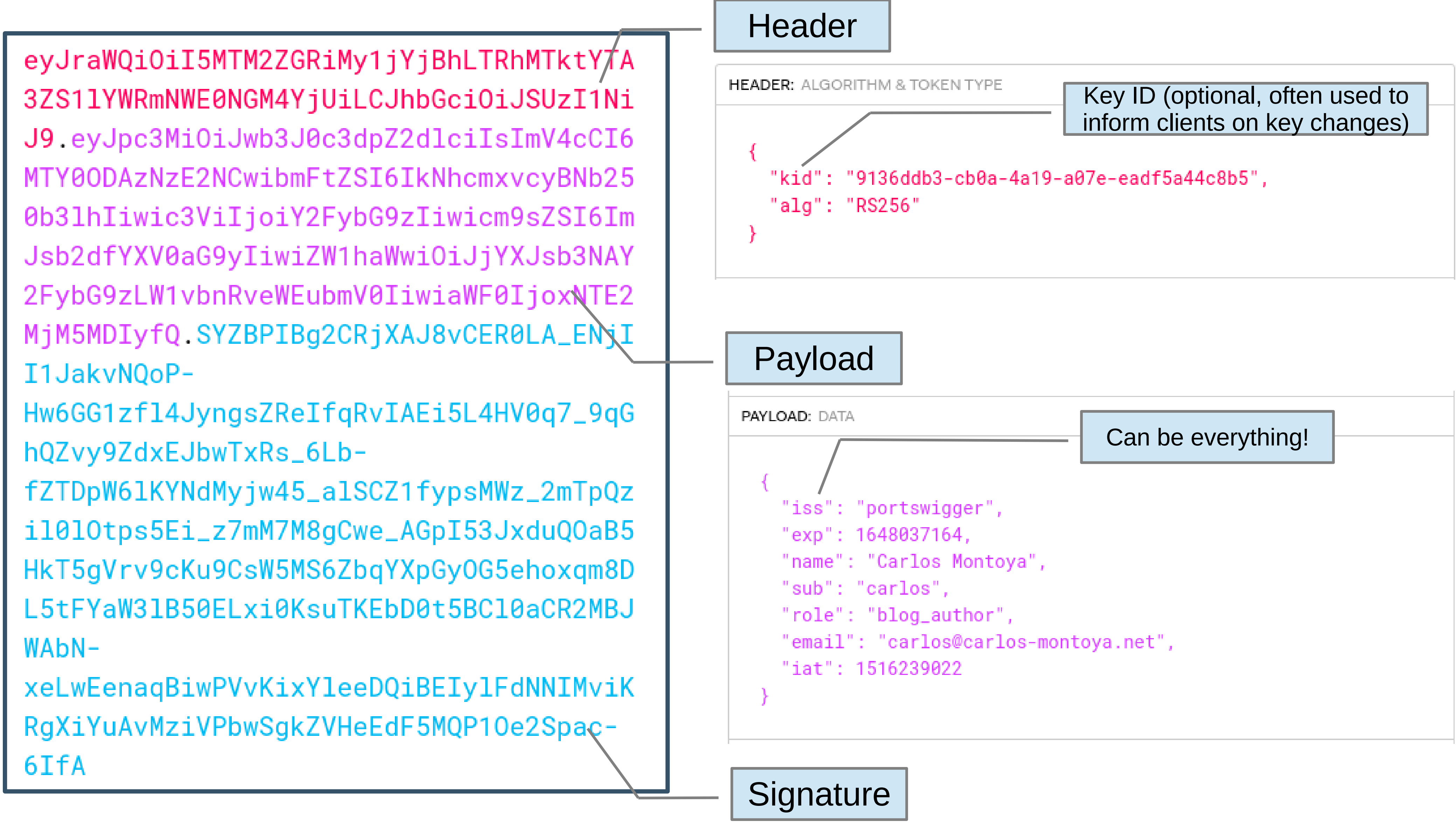
JSON Web Tokens (JWTs)

Standardized format for sending cryptographically **signed** JSON data. Often used for AuthN and AuthZ.



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoid2llbmVyIiwiaXNBZG1pbiI6InRydWUifQ.
```

```
{
   "alg":  "nOnE",
   "typ":  "JWT"
}
{
   "user":    "wiener",
   "isAdmin":  "true"
}
```



```
eyJraWQiOiI5MTM2ZGRiMy1jYjBhLTRhMTktYTA
3ZS1lYWRmNWE0NGM4YjUiLCJhbGciOiJSUzI1Ni
J9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6
MTY0ODAzNzE2NCwibmFtZSI6IkNhcmxvcyBNb25
0b3lhIiwic3ViIjoiY2FybG9zIiwicm9sZSI6Im
Jsb2dfYXV0aG9yIiwiZW1haWwiOiJjYXJsb3NAY
2FybG9zLW1vbnRveWEubmV0IiwiaWF0IjoxNTE2
MjM5MDIyfQ.SYZBPIBg2CRjXAJ8vCER0LA_ENjI
I1JakvNQoP-
Hw6GG1zfl4JyngsZReIfqRvIAEi5L4HV0q7_9qG
hQZvy9ZdxEJbwTxRs_6Lb-
fZTDpW6lKYNdMyjw45_alSCZ1fypsMWz_2mTpQz
il0lOtps5Ei_z7mM7M8gCwe_AGpI53JxduQOaB5
HkT5gVrv9cKu9CsW5MS6ZbqYXpGyOG5ehoxqm8D
L5tFYaW3lB50ELxi0KsuTKEbD0t5BCl0aCR2MBJ
WAbN-
xeLwEenaqBiwPVvKixYleeDQiBEIylFdNNIMviK
RgXiYuAvMziVPbwSgkZVHeEdF5MQP1Oe2Spac-
6IfA
```

Header

HEADER: ALGORITHM & TOKEN TYPE

Key ID (optional, often used to inform clients on key changes)

```
{
  "kid": "9136ddb3-cb0a-4a19-a07e-eadf5a44c8b5",
  "alg": "RS256"
}
```

Payload

PAYLOAD: DATA

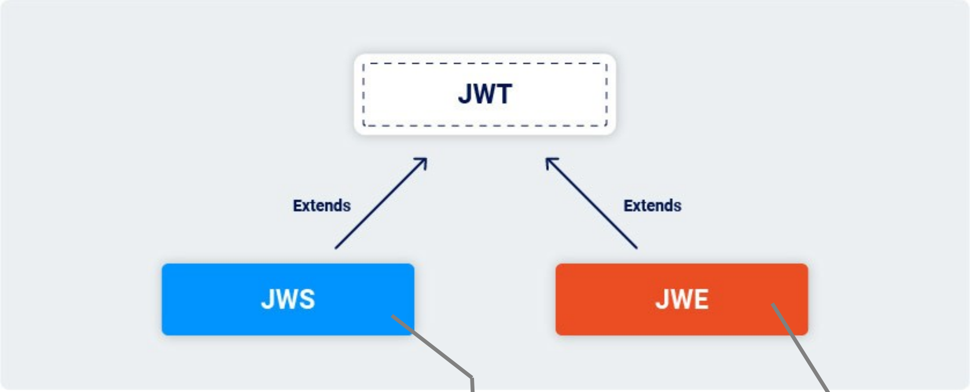
Can be everything!

```
{
  "iss": "portswigger",
  "exp": 1648037164,
  "name": "Carlos Montoya",
  "sub": "carlos",
  "role": "blog_author",
  "email": "carlos@carlos-montoya.net",
  "iat": 1516239022
}
```

Signature

JWT signature

```
eyJraWQiOiI5MTM2ZGRiMy1jYjBhLTRhMTktYTA
3ZS1lYWRmNWE0NGM4YjUiLCJhbGciOiJSUzI1Ni
J9.eyJpc3MiOiJwb3J0c3dpZ2dlciIsImV4cCI6
MTY0ODAzNzE2NCwibmFtZSI6IkNhcmxvcyBNb25
0b3lhIiwic3ViIjoiY2FybG9zIiwicm9sZSI6Im
Jsb2dfYXV0aG9yIiwiZW1haWwiOiJjYXJsb3NAY
2FybG9zLW1vbnRveWEubmV0IiwiaWF0IjoxNTE2
MjM5MDIyfQ.SYZBPIBg2CRjXAJ8vCER0LA_ENjI
I1JakvNQoP-
Hw6GG1zfl4JyngsZReIfqRvIAEi5L4HV0q7_9qG
hQZvy9ZdxEJbwTxRs_6Lb-
fZTDpW6lKYNdMyjw45_alSCZ1fypsMWz_2mTpQz
il0lOtps5Ei_z7mM7M8gCwe_AGpI53JxduQOaB5
HkT5gVrv9cKu9CsW5MS6ZbqYXpGyOG5ehoxqm8D
L5tFYaW3lB50ELxi0KsuTKEbD0t5BCl0aCR2MBJ
WAbN-
xeLwEenaqBiwPVvKixYleeDQiBEIylFdNNIMviK
RgXiYuAvMziVPbwSgkZVHeEdF5MQP1Oe2Spac-
6IfA
```



JSON Web Signature

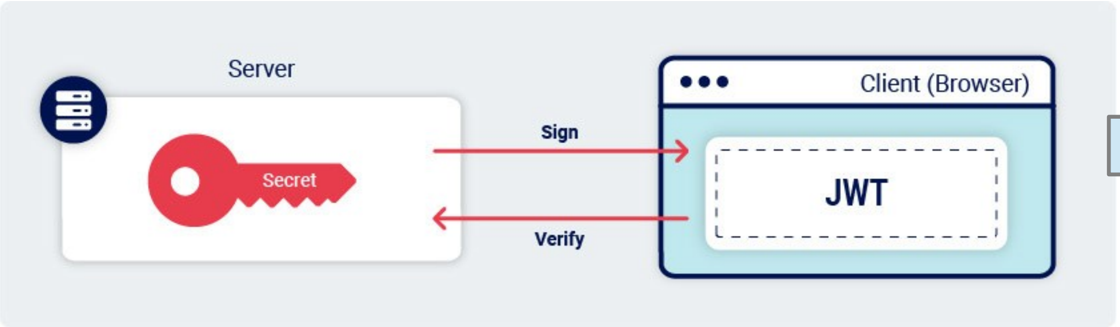
JSON Web Encryption

Most of the time,
JWT actually refers to JWS.

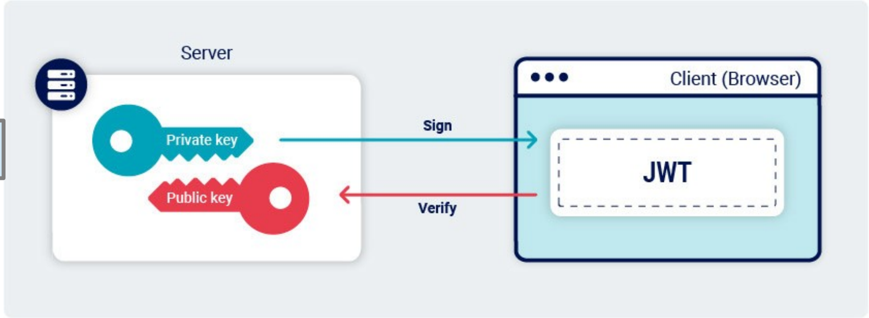
In JWS the header and payload are signed by HMAC (hash-based message authentication code).

Vulnerabilities

- Accepting tokens with no signature
- Accepting tokens with tampered algorithm
- Weak encryption keys
- Misunderstand symmetric and asymmetric encryption
- Using JWS and thinking data is not readable



VS



Questions