JSON Web Token Security Cheat Sheet

PentesterLab

Header	.	Payload	.	Signature
eyJ0eXAiOiJK V1QiLCJh bGci OiJIUzI1NiJ9 `urlsafe_base64*({"..."})`	.	**eyJ**sb2dpbi I6ImFkb WluIn0 `urlsafe_base64*({"..."})`	.	FSfvCBAwypJ4abF6jFLmR7 JgZhkW674 Z8dIdAIRyt1 ... `urlsafe_base64*(...)`

* urlsafe_base64 with no padding: https://tools.ietf.org/html/rfc7515#appendix-C

Header review:

- ☑ Support for "None" algorithm disabled
- ☑ No Injection in the "kid" element
- ☑ Embedded "jwk" elements are not trusted
- ☑ Whitelist of algorithms enforced
- ☑ Replay protection via "jti" element

Payload review:

- ☑ Check for sensitive information stored in the payload
- ☑ Check for token's expiry enforced via "exp" or "iat" elements

Signature review:

- ☑ Check if the signature is enforced
- ☑ Try to brute force the secret key
- ☑ Check for time constant verification for HMAC
- ☑ Ensure that keys and secrets are stored outside of source
- ☑ Check that keys and secrets are different between environments