

Burpsuite 插件之 JSON-Web-Tokens

By:裁决

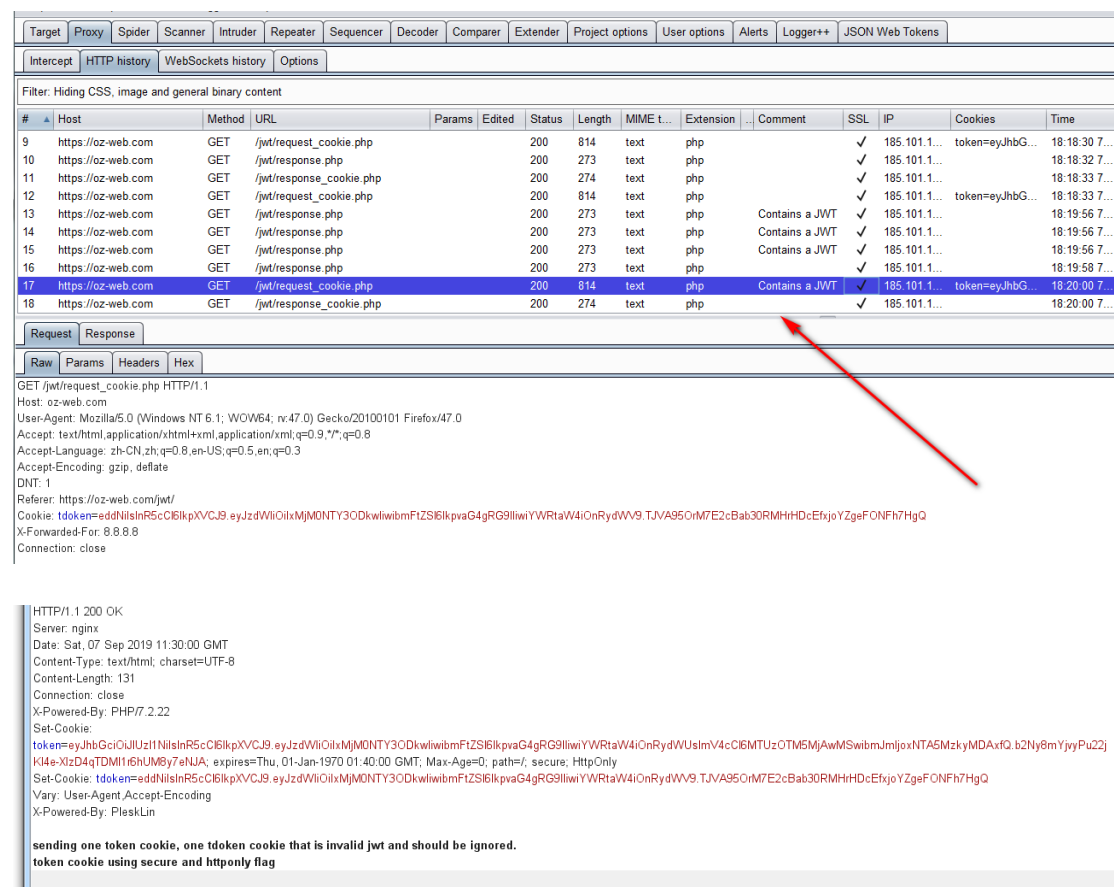
项目主页: <https://github.com/PortSwigger/json-web-tokens>

关于 JWT 不懂得可以去这里:

http://www.ruanyifeng.com/blog/2018/07/json_web_token-tutorial.html

使用演示:

访问项目主页的演示环境 <https://oz-web.com/jwt/>, 之后访问页面, burp 抓包



The screenshot shows the Burp Suite interface with the HTTP history tab selected. The table below lists the intercepted requests. Row 17 is highlighted, showing a GET request to /jwt/request_cookie.php with a status of 200. The comment for this request is 'Contains a JWT'. A red arrow points to this row.

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Comment	SSL	IP	Cookies	Time
9	https://oz-web.com	GET	/jwt/request_cookie.php			200	814	text	php		✓	185.101.1...	token=eyJhbG...	18:18:30 7...
10	https://oz-web.com	GET	/jwt/response.php			200	273	text	php		✓	185.101.1...		18:18:32 7...
11	https://oz-web.com	GET	/jwt/response_cookie.php			200	274	text	php		✓	185.101.1...		18:18:33 7...
12	https://oz-web.com	GET	/jwt/request_cookie.php			200	814	text	php		✓	185.101.1...	token=eyJhbG...	18:18:33 7...
13	https://oz-web.com	GET	/jwt/response.php			200	273	text	php	Contains a JWT	✓	185.101.1...		18:19:56 7...
14	https://oz-web.com	GET	/jwt/response.php			200	273	text	php	Contains a JWT	✓	185.101.1...		18:19:56 7...
15	https://oz-web.com	GET	/jwt/response.php			200	273	text	php	Contains a JWT	✓	185.101.1...		18:19:56 7...
16	https://oz-web.com	GET	/jwt/response.php			200	273	text	php		✓	185.101.1...		18:19:58 7...
17	https://oz-web.com	GET	/jwt/request_cookie.php			200	814	text	php	Contains a JWT	✓	185.101.1...	token=eyJhbG...	18:20:00 7...
18	https://oz-web.com	GET	/jwt/response_cookie.php			200	274	text	php		✓	185.101.1...		18:20:00 7...

Request: GET /jwt/request_cookie.php HTTP/1.1
Host: oz-web.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: https://oz-web.com/jwt/
Cookie: ttoken=eddNlslR5cC6lkpXVCJ9.eyJzdWl0aXNjMjMONTY3ODkwlwibmFtZSI6IkpvaG4gRG9lIiwiaWVhYWRtaW4iOiNRYdWV9.TjVA95OrM7E2cBab30RMHhDcEfHjYzgeFONFh7HgQ
X-Forwarded-For: 8.8.8.8
Connection: close

Response: HTTP/1.1 200 OK
Server: nginx
Date: Sat, 07 Sep 2019 11:30:00 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 131
Connection: close
X-Powered-By: PHP/7.2.22
Set-Cookie: token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWl0aXNjMjMONTY3ODkwlwibmFtZSI6IkpvaG4gRG9lIiwiaWVhYWRtaW4iOiNRYdWV9.TjVA95OrM7E2cBab30RMHhDcEfHjYzgeFONFh7HgQ; expires=Thu, 01-Jan-1970 01:40:00 GMT; Max-Age=0; path=/; secure; HttpOnly
Set-Cookie: ttoken=eddNlslR5cC6lkpXVCJ9.eyJzdWl0aXNjMjMONTY3ODkwlwibmFtZSI6IkpvaG4gRG9lIiwiaWVhYWRtaW4iOiNRYdWV9.TjVA95OrM7E2cBab30RMHhDcEfHjYzgeFONFh7HgQ
Vary: User-Agent, Accept-Encoding
X-Powered-By: PleskLin

sending one token cookie, one ttoken cookie that is invalid jwt and should be ignored.
token cookie using secure and httponly flag

RequestResponse

RawHeadersHexJSON Web Tokens

Secret

JWT

Headers = {
 "alg": "HS256",
 "typ": "JWT"
}

Payload = {
 "sub": "1234567890",
 "name": "John Doe",
 "admin": true,
 "exp": 1539392001,
 "nbf": 1509392001
}

Signature = "b2Ny8mYjvyPu22jKI4e-X1zD4qTDMI1r6hUM8y7eNJA"

解出来了
你也可以复制 JWT 到里面工具窗口下解密

Enter JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJkbWJ0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0Ij06MTUzOTM5MjAwMSwibmJmljoxtA5MzkyMDAxfQ.b2Ny8mYjvyPu22jKI4e-X1zD4qTDMI1r6hUM8y7eNJA

Enter Secret / Key

Invalid key
Empty key

Decoded JWT

Headers = {
 "alg": "HS256",
 "typ": "JWT"
}

Payload = {
 "sub": "1234567890",
 "name": "John Doe",
 "admin": true,
 "exp": 1539392001,
 "nbf": 1509392001
}

Signature = "b2Ny8mYjvyPu22jKI4e-X1zD4qTDMI1r6hUM8y7eNJA"

图片又不是真的
你激动啥和小孩似的