# 웹과 네트워크 패킷

202112021 박채우

# 목차

1. 웹의 이해
2. 웹의 프로토콜
3. 실습
4. 패킷 보안 기술

# 웹의 이해

- World Wide Web, WWW가 정식명칭으로 사용된다.
- 세계적 규모로 이루어진 거미집 모양의 망이라는 뜻으로 사용되며 1989년 팀 버너스 리의 연구프로젝트로 시작했다.
- 전 세계의 연구자들과 연구자료 등을 공유하는 방법을 위한 프로그램으로 고안되었다.

- 초기의 웹은 전자메일 등과 같은 인터넷 상에서 동작하는 하나의 서비스였으나 현재에는 인터넷의 절대적인 위치를 차지하고 있다.

# 웹의 이해

- 초기 웹 기획단계에서 웹은 하이퍼텍스트 프로젝트로 불렸다.

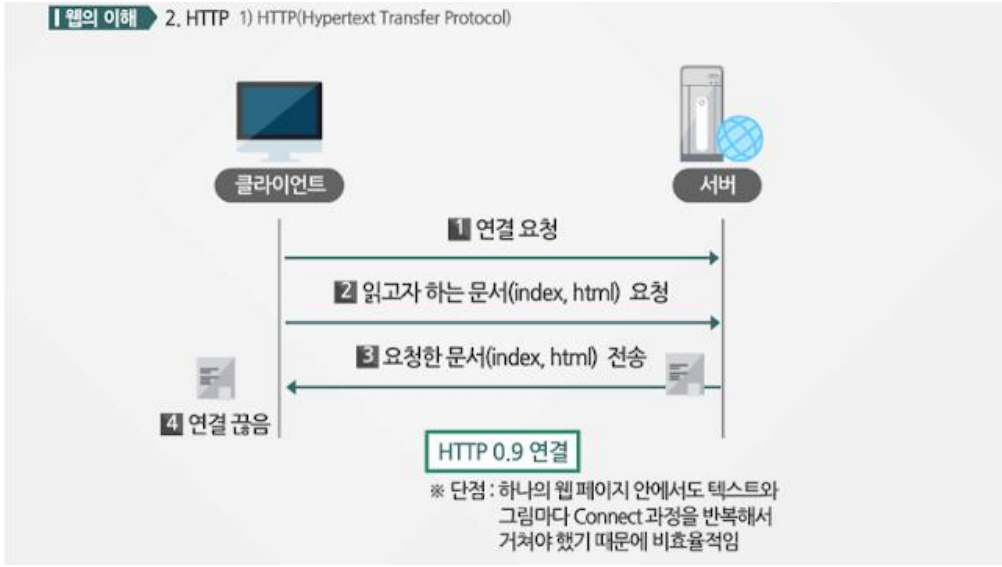
- 현재 웹 문서에서 쓰이고 있는 HTML은 하이퍼텍스트와 관련이 있다.
- 또한 HTTP 역시 하이퍼텍스트와 관련이 있다.

- HTTP와 같이 SMTP, POP, FTP, Telnet 등 다양한 프로토콜이 사용된다.

# 웹의 프로토콜

## 1. HTTP 프로토콜

- 초기 HTTP는 버전도 없었고 후에 나오는 버전과 구분하기 위해 0.9버전이라는 이름이 붙었다.
- HTTP/0.9는 단순 읽기기능만 존재하였다.

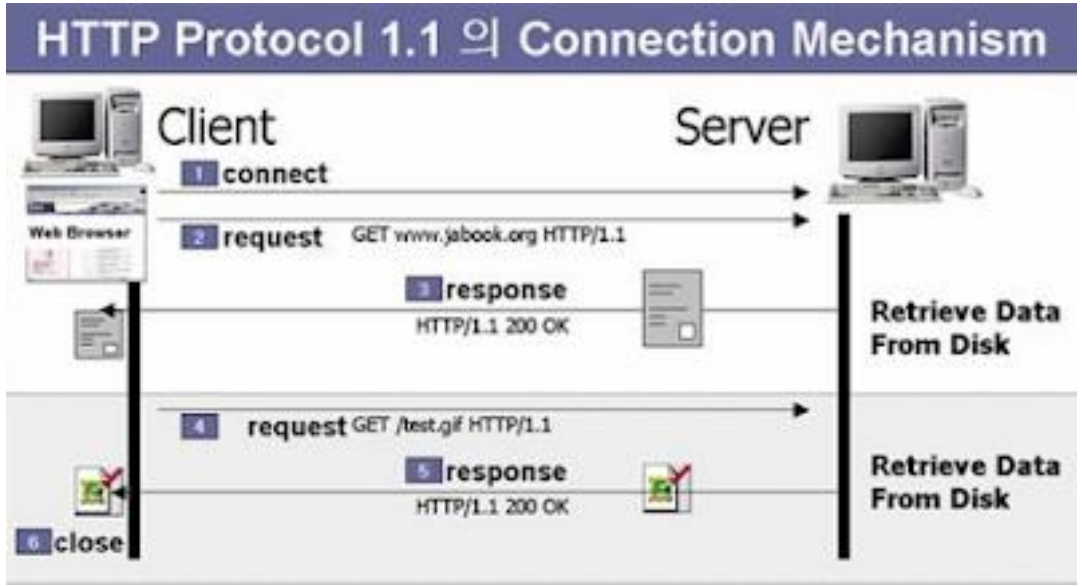


# 웹의 프로토콜

## 1. HTTP 프로토콜

- 초기 HTTP의 문제를 개량한 HTTP/1.0과 HTTP/1.1 버전이 1996년, 1999년에 발표되었다.

- 0.9버전과는 다르게 한번의 connect 과정 이후 계속 서버와 클라이언트 사이에서 문서나 그림 등을 교환할 수 있다.



# 웹의 프로토콜

## HTTP의 메소드

GET : 가장 일반적인 HTTP 요청 형태이다. 클라이언트가 서버에게 요청하는 데이터의 인수를 URL의 형태로 전송하여 자료를

```
GET /restapi/v1.0 HTTP/1.1
Accept: application/json
Authorization: Bearer UExBMDFUMDRQV1MwMnzpdvtYYNWMSJ7CL8h0zM6q6a9ntw
```

POST : GET과는 다르게 URL의 형태로 서버에게 요청하지 않는다. POST 메소드는 헤더에 데이터를 작성 후 전송하기 때문에 데이터가 URL에 드러나지 않는다.

이외에 헤더 부분에 해당하는 데이터만 요청하는 HEAD, 특정 서버의 프록시에 클라이언트가 서버에게 연결을 요청하는 CONNECT 등 다양한 메소드가 있다.

# GET과 POST

| | **get** | **post** |
|---|---|---|
| History | 인자들이 URL의 일부분이기 때문에 히스토리에 남는다. | 히스토리에 저장되지 않는다. |
| Bookmark | URL로 응답되기 때문에 북마크 저장이 가능하다. | 북마크 저장이 불가능하다. |
| Restrictions on from data type | 아스키코드만 전달이 가능하다. | 제한이 없으며 바이너리 데이터도 가능하다. |
| Security | 인자가 URL에 기록되고 브라우저 히스토리에도 기록이 남기 때문에 보안에 약하다. | 인자들이 히스토리와 서버로그에도 저장되지 않기 때문에 상대적으로 안전하다. |
| Usability | 보안에 약하기 때문에 민감한 개인정보등을 전송하는데 사용해선 안된다. | 상대적으로 안전하기 때문에 게시판 등에 글을 작성하는 등 요청에 사용된다. |

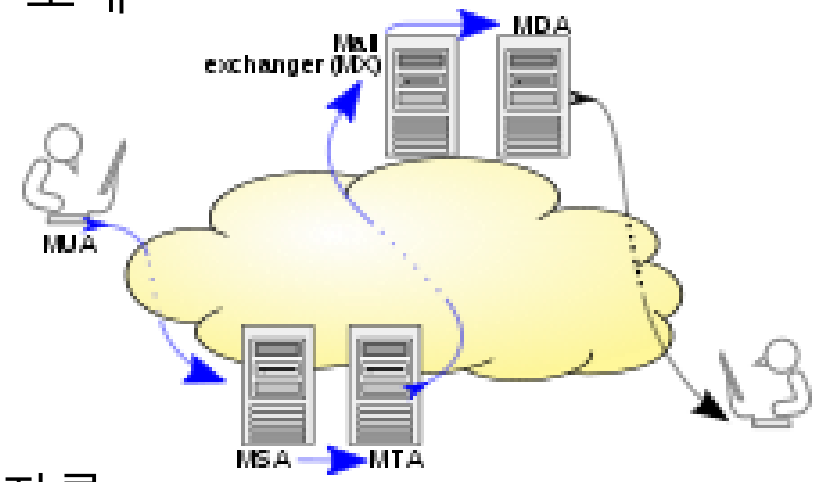
# 웹의 프로토콜

## 2. SMTP 프로토콜

- 간이 전자 우편 통신 프로토콜은 인터넷에서 이메일을 보내기 위해 사용하는 프로토콜이다.

- 연결지향적이고 텍스트 기반으로 작동하는 프로토콜 즉 클라이언트와 서버 사이에 세션이 생성되며 명령을 통해 메일을 송수신한다.

- 세 가지 명령이 있으며 수신자를 지정하는 MAIL, 송신자를 지정하는 RCPT, 메시지 내용을 결정하는 DATA가 있다.



S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM: < bob@example.org >
S: 250 Ok
C: RCPT TO: < alice@example.com >
S: 250 Ok
C: RCPT TO: < theboss@example.com >
S: 250 Ok
C: DATA
S: 354 End data with  < CR >  < LF > . < CR >  < LF >
C: From: "Bob Example"  < bob@example.org >
C: To: "Alice Example"  < alice@example.com >
C: Cc: theboss@example.cm
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}

# 웹의 프로토콜

## 3. POP 프로토콜

- 포스트 오피스 프로토콜은 원격 서버로부터 이메일을 불러오는데 사용하며 POP3를 마지막 표준 프로토콜으로 사용한다.

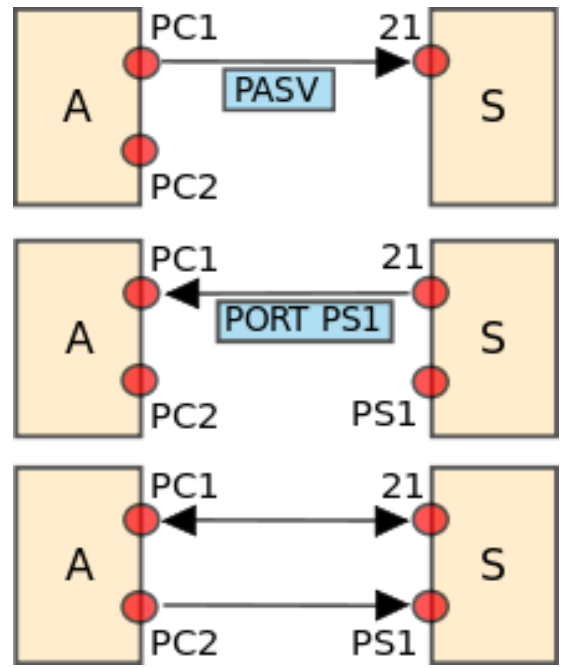
- 유사한 프로토콜로 IMAP 프로토콜이 있다. IMAP와 차이점은 서버에서 이메일을 불러온 이후 POP 프로토콜은 서버에서 이메일 삭제하는 반면 IMAP 프로토콜은 그대로 남겨두고 다양한 동작을 수행할 수 있다.

# 웹의 프로토콜

## 4. FTP 프로토콜

- 파일 전송 프로토콜은 서버와 클라이언트 사이에서 파일을 전송하기 위해 만들어진 프로토콜이다. 현재까지도 계속 사용하고 있는 프로토콜이다.

- FTP에서는 명령 연결과 데이터 전송용 연결, 2가지 연결로 이루어져 있다.
- 명령 연결에서는 클라이언트에서 지시하는 명령을 서버로 전달하는 역할을 한다.
- 데이터 전송용 연결에서는 각 파일의 전송이 필요할 때마다 새로운 연결이 생성되는 방식이다.


PC1
21
A
PASV
S
PC2
PC1
21
A
PORT PS1
S
PC2
PS1
PC1
21
A
S
PC2
PS1

# 웹의 프로토콜

5. Telnet 프로토콜

- 텔넷 프로토콜은 원격에서 호스트의 컴퓨터에 접속하기 위해 사용하는 인터넷 프로토콜이다. 네트워크 상의 컴퓨터에 로그인하여 원격으로 컴퓨터의 기능을 사용할 수 있게 해주는 프로토콜이다.

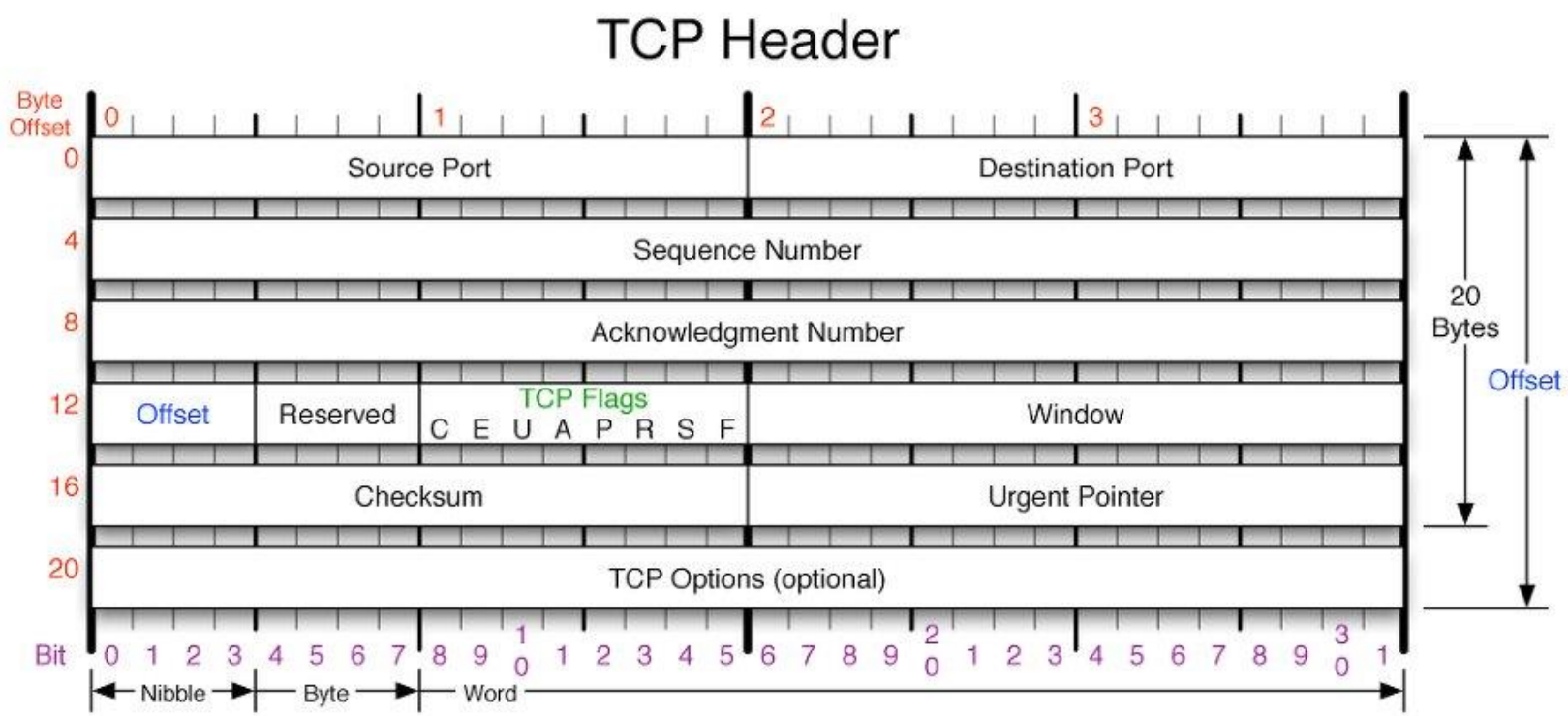
- 텔넷은 보안에 취약(암호화가 이루어지지 않는 프로토콜)하기 때문에 요즘은 SSH(Secure Shell)을 사용하는 추세이다.

# 패킷

- packet은 네트워크 전송의 용량 단위이다. 전송 될 때 교환되는 내용물로 조각조각 분할된 파일데이터에 주소와 에러 데이터 등이 기록된다.

- 실제의 데이터를 패킷단위로 분할하기 때문에 Time-slice 방식으로 처리가 가능하다.

- 네트워크 패킷은 사용자의 데이터와 제어정보로 이루어져 있으며 사용자의 데이터는 페이로드라고 부르기도 한다.


TCP Header
Byte Offset
0
4
8
12
16
20
0
1
2
3
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Offset
Reserved
TCP Flags
C E U A P R S F
Window
Checksum
Urgent Pointer
TCP Options (optional)
20 Bytes
Offset
Bit
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
Nibble
Byte
Word

# 실습

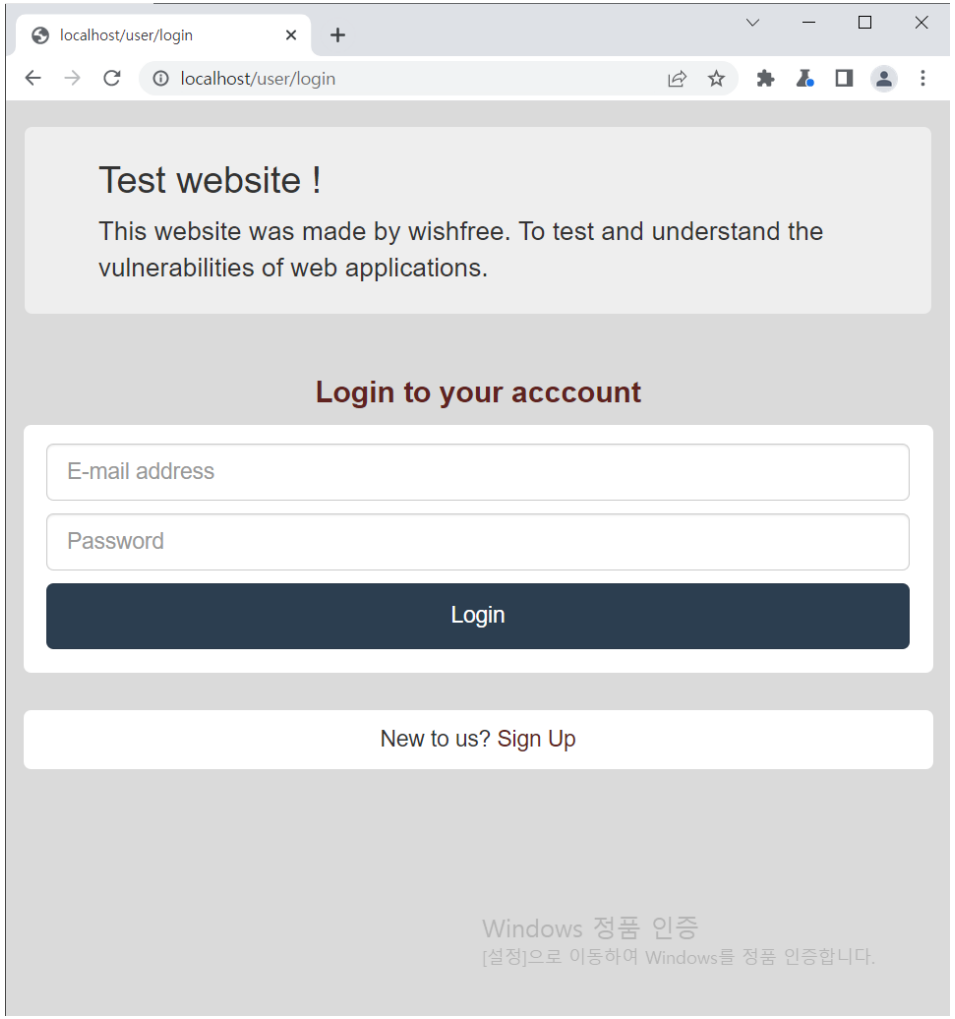
# Burp suite


- 웹 애플리케이션에서 취약점을 진단하는데 유용한 도구이다.
- 웹프록시를 사용해서 프록시 분석을 할 때 네트워크 패킷을 프로그램으로 받을 수 있게 한다.
- 클라이언트 요청정보 및 서버의 응답정보를 받을 수 있고 서버로 전송되는 정보를 변경하는 방법을 통해서 취약점을 분석할 수 있다.

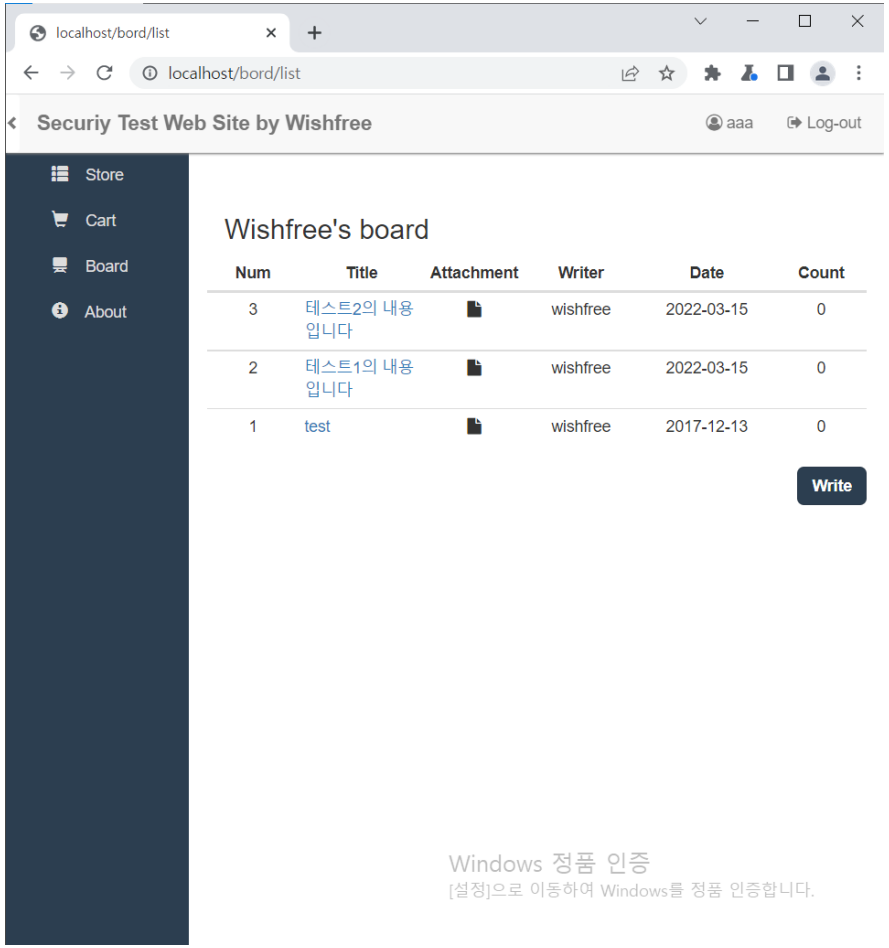
# 실습

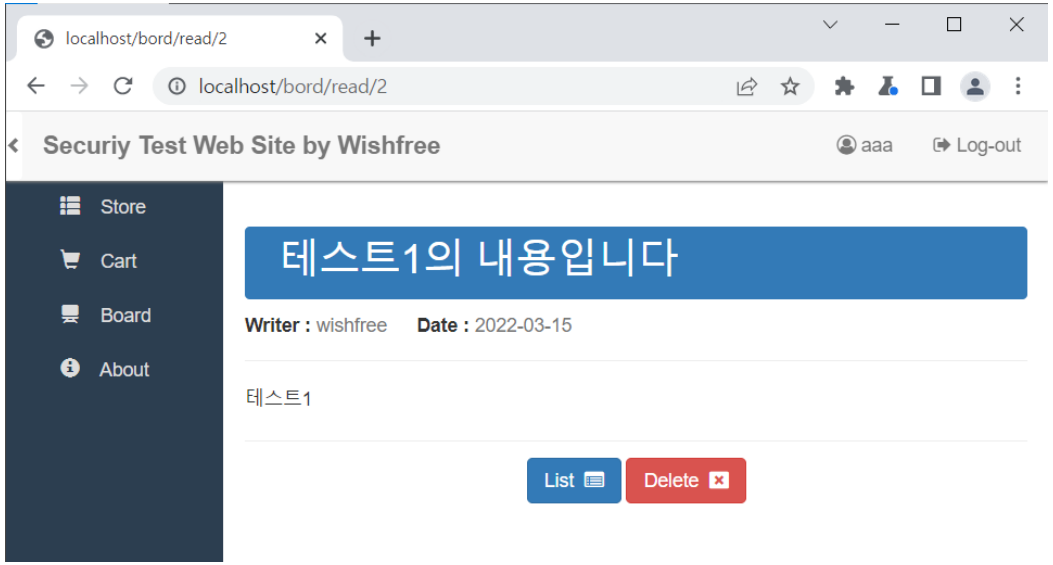
- 실습환경 : 윈도우
- 툴 : 버프 스위트

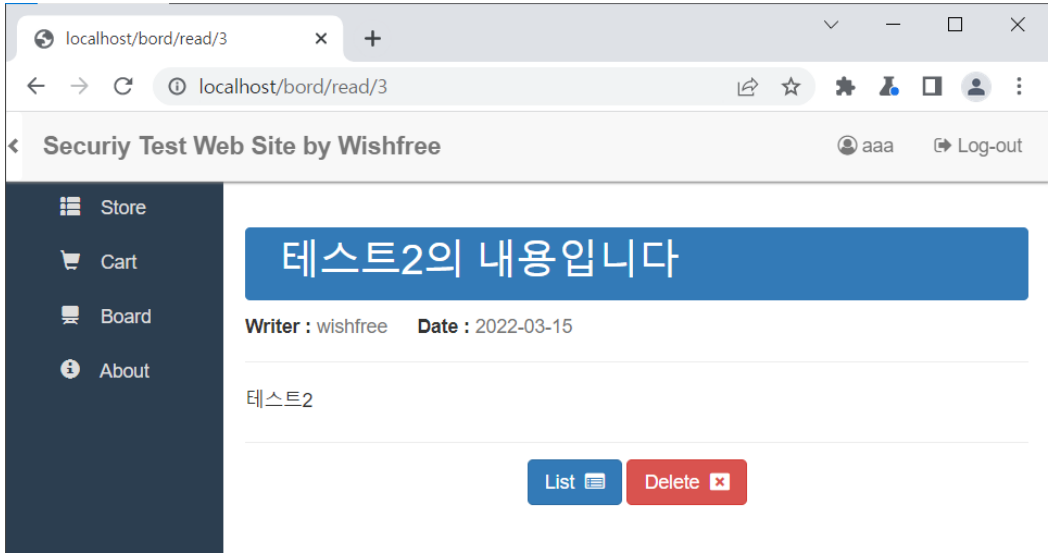
```
C:₩Users>cd..

C:₩>cd test

C:₩Test>cd test

C:₩Test₩Test>nodemon index.js
[nodemon] 2.0.15
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): *.*
[nodemon] watching extensions: js,mjs,json
[nodemon] starting `node index.js`
Web server is running on port 80!
```



# 실습

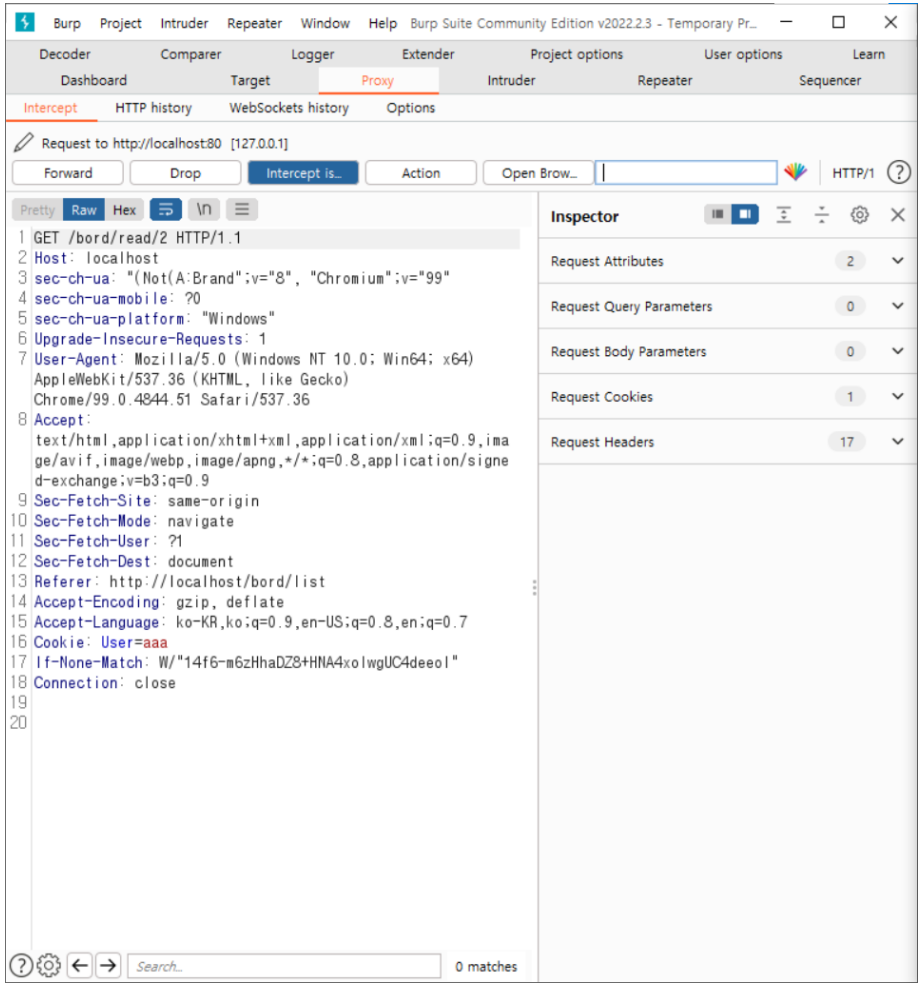

localhost/bord/list
localhost/bord/list
Securiy Test Web Site by Wishfree
aaa
Log-out
Store
Cart
Board
About
Wishfree's board
Num
Title
Attachment
Writer
Date
Count
3
테스트2의 내용입니다
wishfree
2022-03-15
0
2
테스트1의 내용입니다
wishfree
2022-03-15
0
1
test
wishfree
2017-12-13
0
Write
Windows 정품 인증
[설정]으로 이동하여 Windows를 정품 인증합니다.

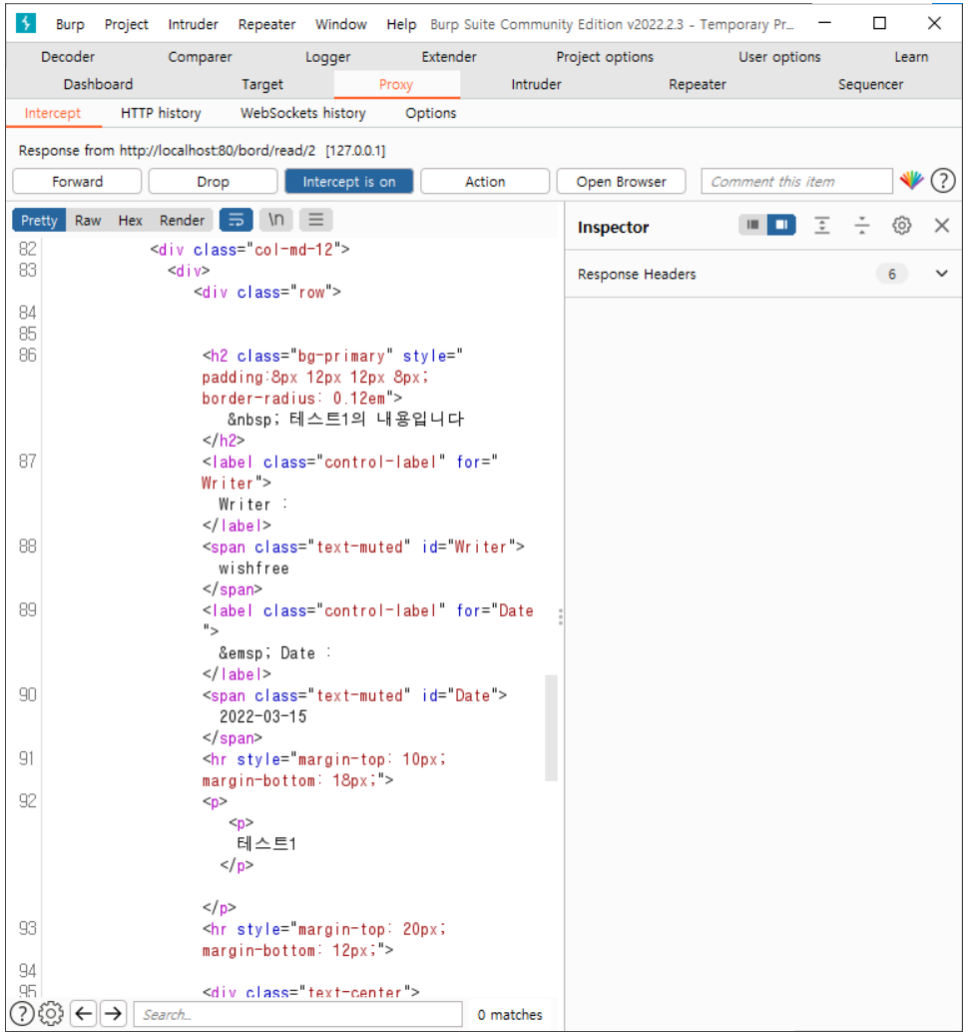

localhost/bord/read/2
localhost/bord/read/2
Securiy Test Web Site by Wishfree
aaa
Log-out
Store
Cart
Board
About
테스트1의 내용입니다
Writer : wishfree
Date : 2022-03-15
테스트1
List
Delete


localhost/bord/read/3
localhost/bord/read/3
Securiy Test Web Site by Wishfree
aaa
Log-out
Store
Cart
Board
About
테스트2의 내용입니다
Writer : wishfree
Date : 2022-03-15
테스트2
List
Delete

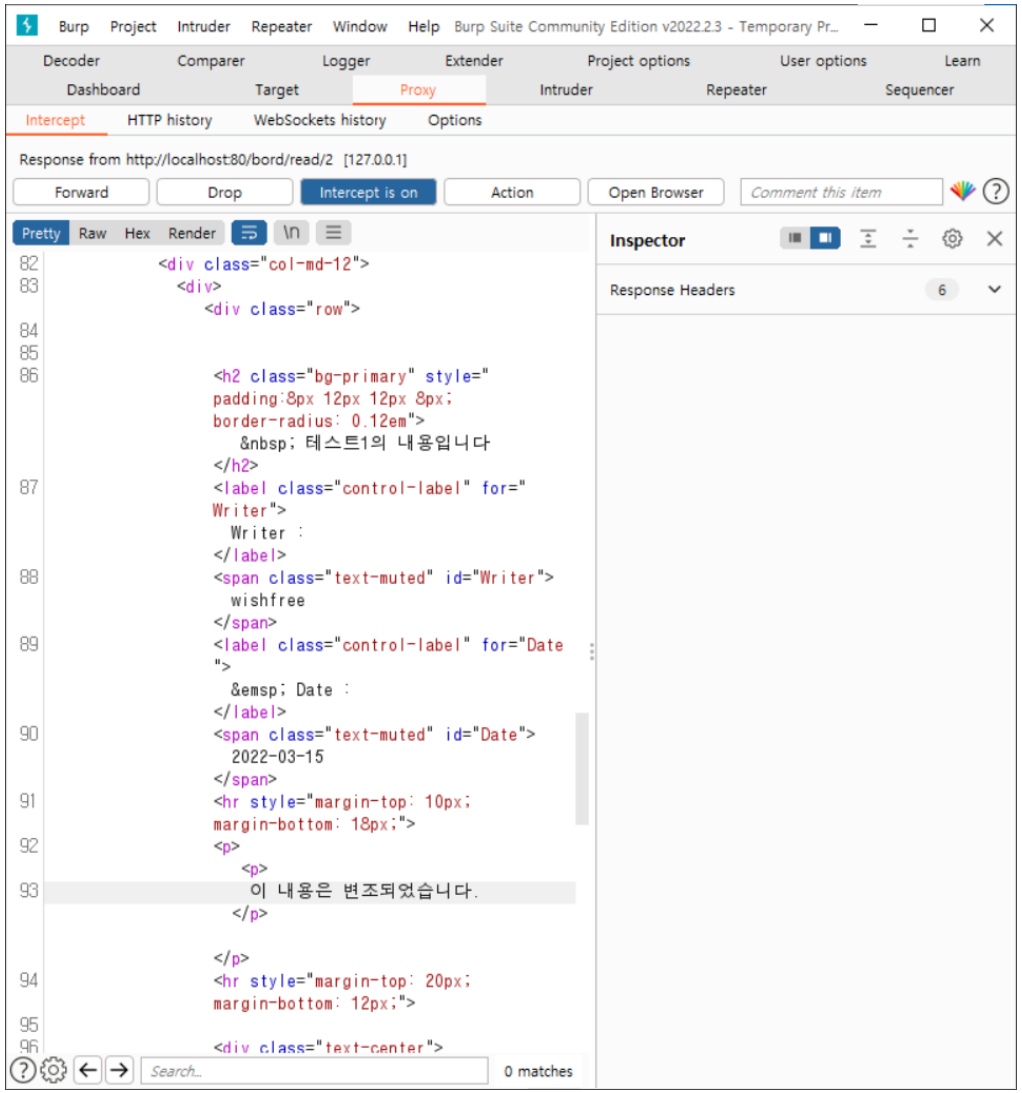
# 실습

서버에서 클라이언트로 보내는 패킷을 변조하기



# 실습


Burp Project Intruder Repeater Window Help Burp Suite Community Edition v2022.2.3 - Temporary Pr...
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
Intercept HTTP history WebSockets history Options
Response from http://localhost:80/bord/read/2 [127.0.0.1]
Forward Drop Intercept is on Action Open Browser Comment this item
Pretty Raw Hex Render
Inspector
Response Headers 6
82 
83 

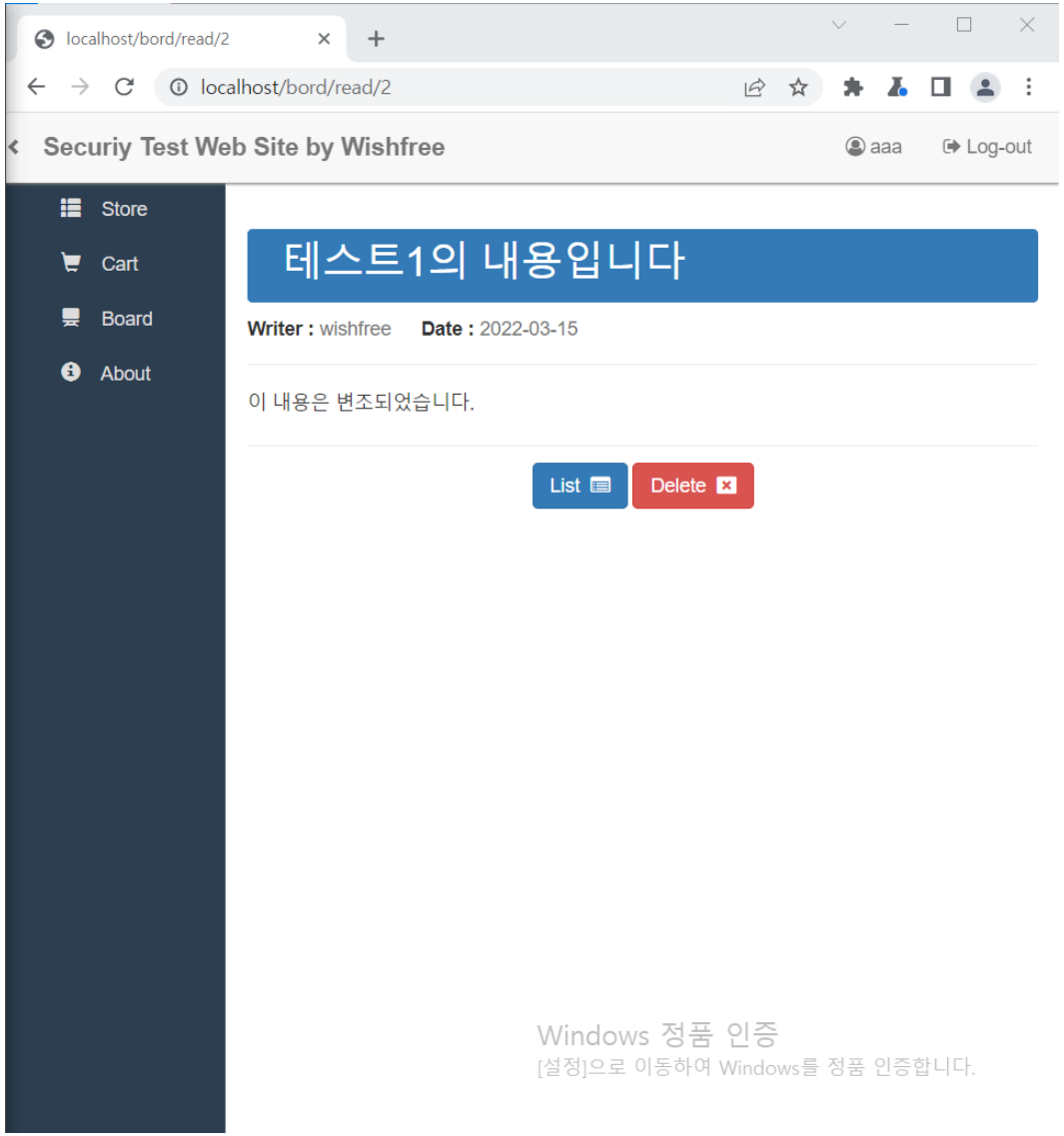
84
85
86 <h2 class="bg-primary" style="
padding:8px 12px 12px 8px;
border-radius: 0.12em">
  테스트1의 내용입니다
</h2>
87 <label class="control-label" for="
Writer">
Writer :
</label>
88 
wishfree

89 <label class="control-label" for="Date
">
  Date :
</label>
90 
2022-03-15

91 <hr style="margin-top: 10px;
margin-bottom: 18px;">
92 

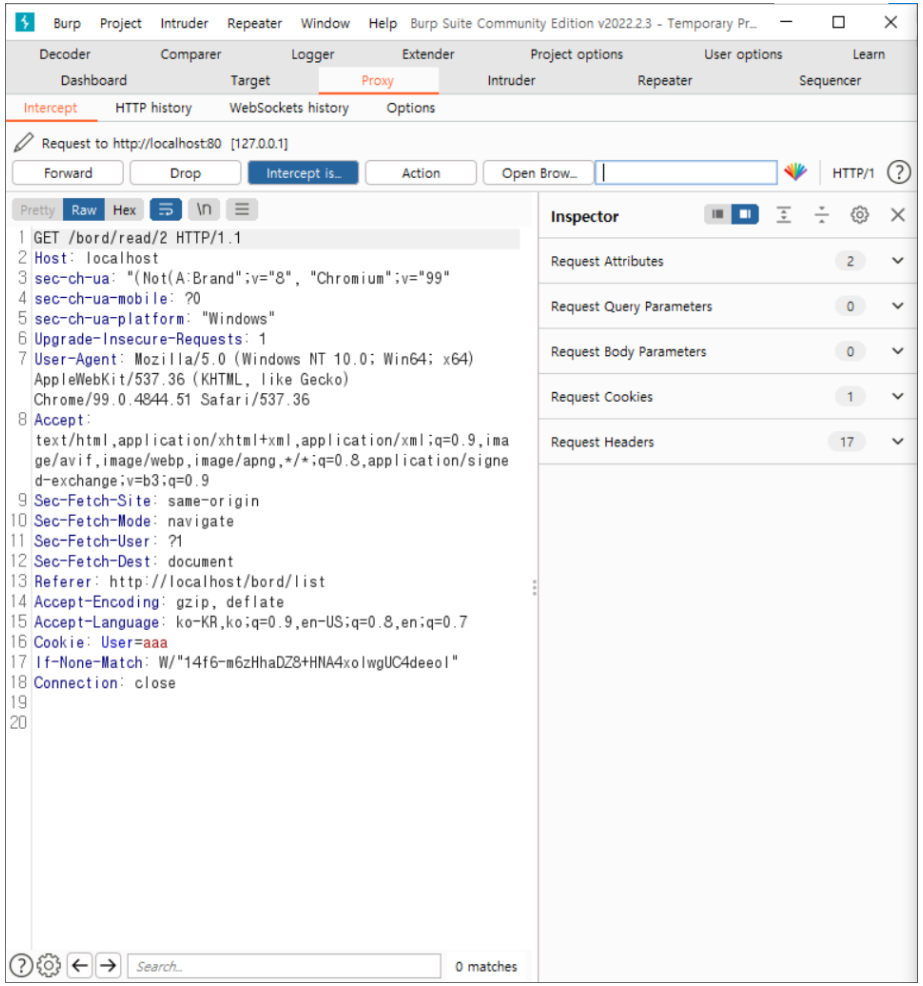
93 이 내용은 변조되었습니다.

94 <hr style="margin-top: 20px;
margin-bottom: 12px;">
95
96 
Search...
0 matches

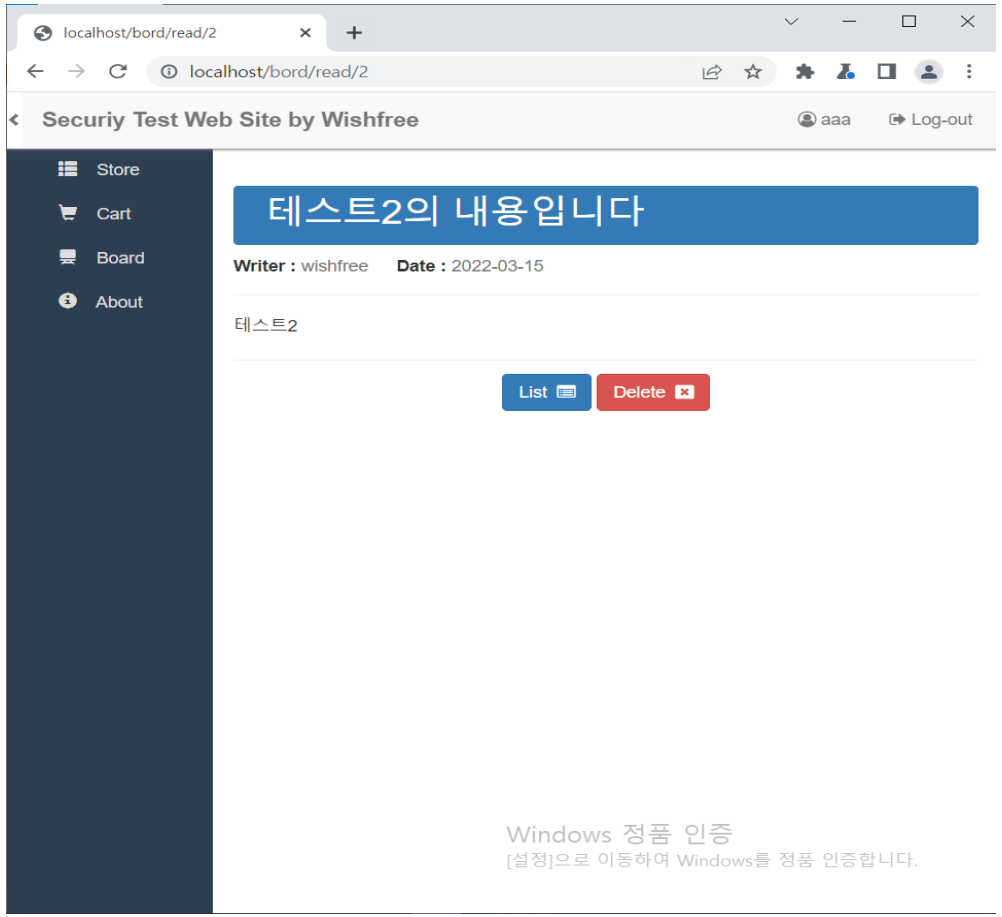

localhost/bord/read/2
localhost/bord/read/2
Securiy Test Web Site by Wishfree
aaa
Log-out
Store
Cart
Board
About
테스트1의 내용입니다
Writer : wishfree
Date : 2022-03-15
이 내용은 변조되었습니다.
List
Delete
Windows 정품 인증
[설정]으로 이동하여 Windows를 정품 인증합니다.

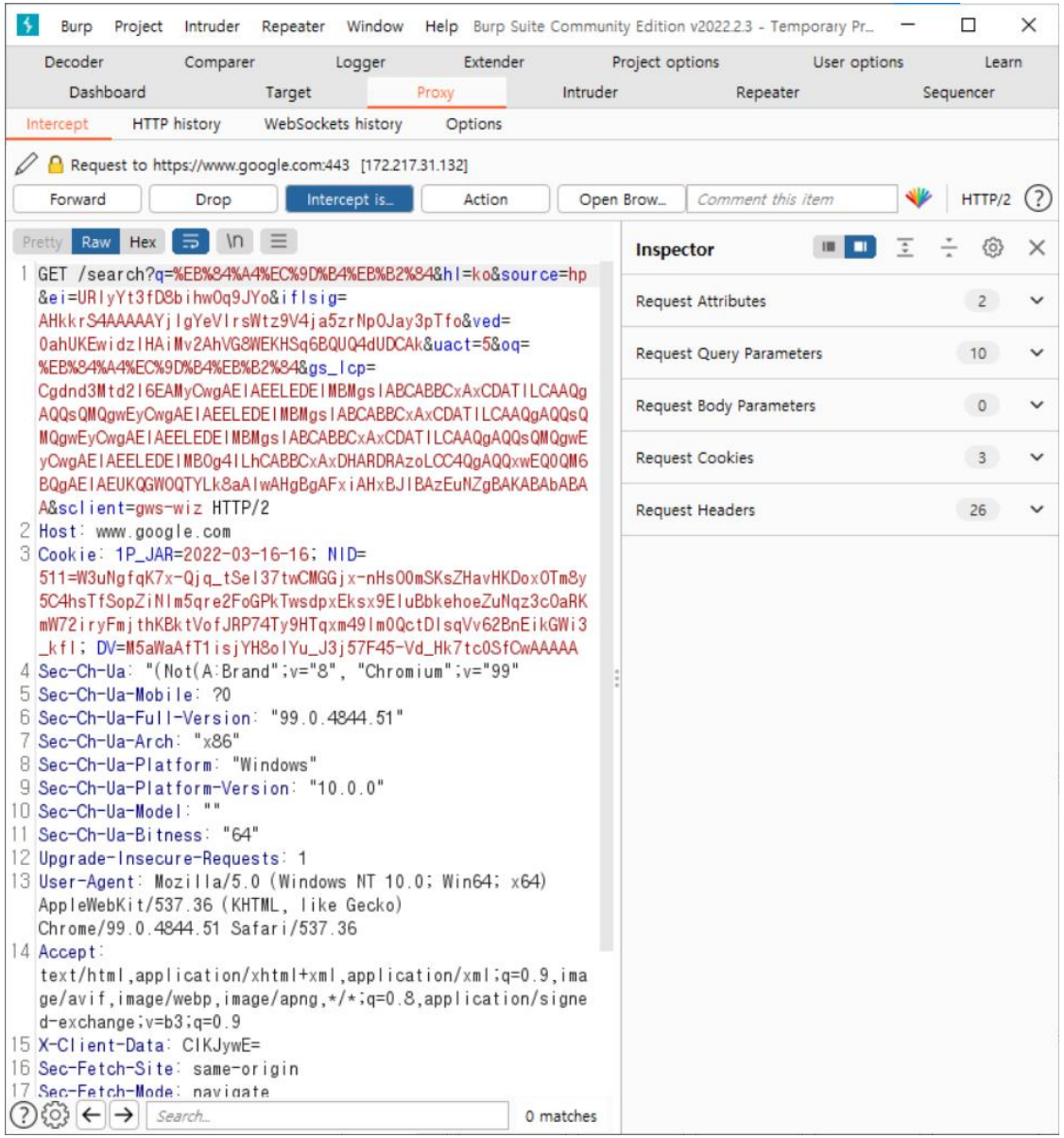
# 실습

클라이언트에서 서버로 보내는 패킷을 변조하기

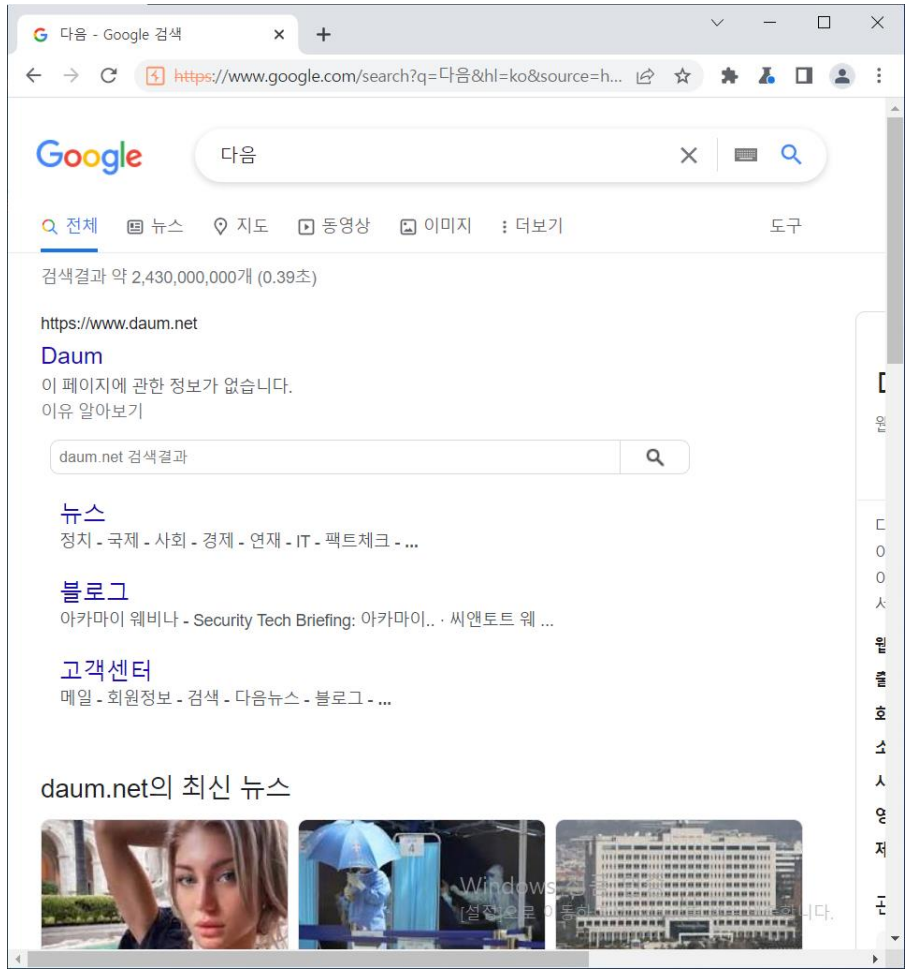


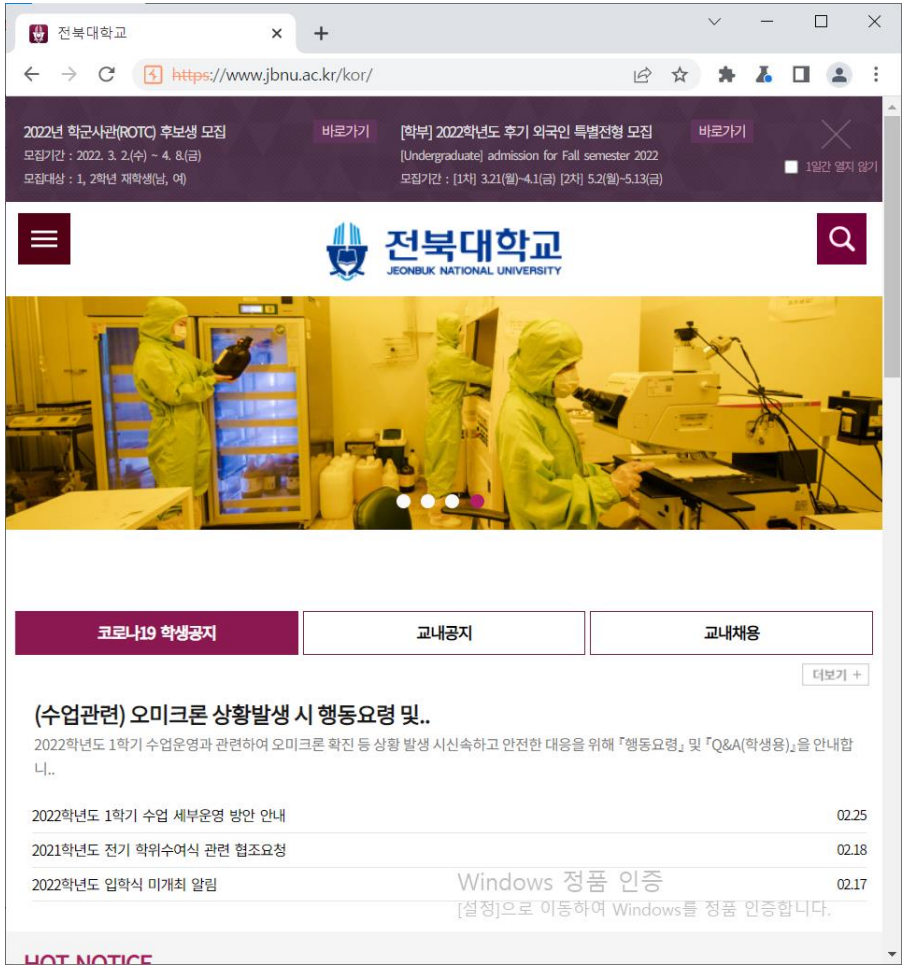

```
1 GET /bord/read/3 HTTP/1.1
```

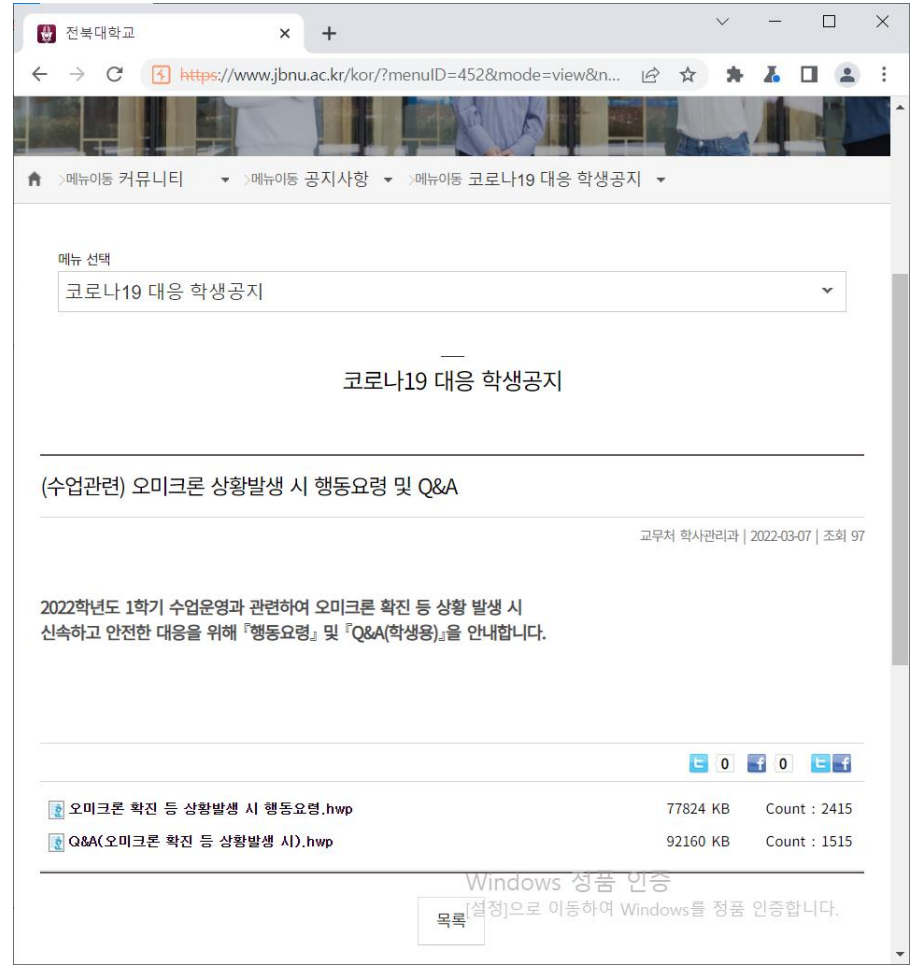


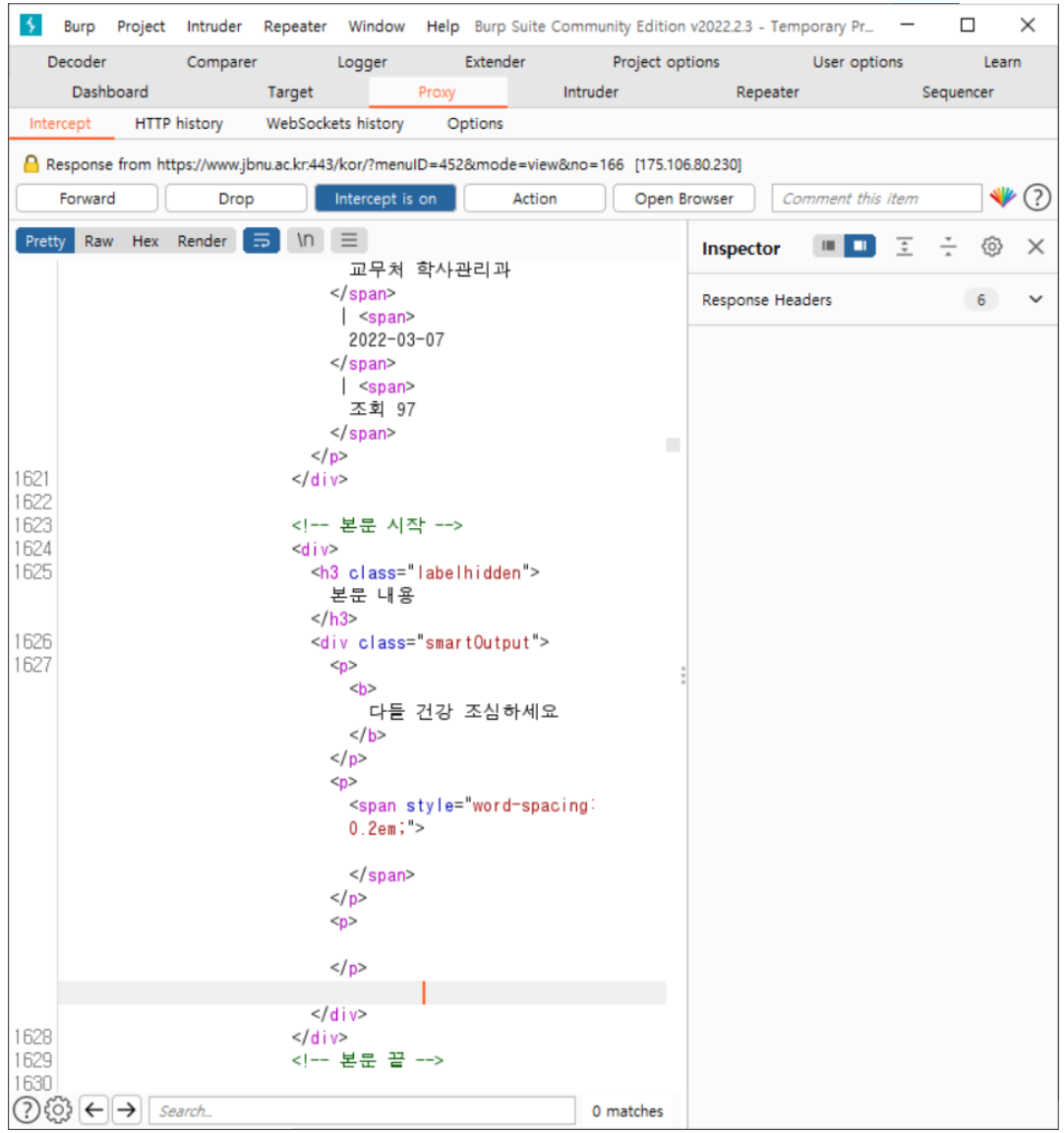

Burp Project Intruder Repeater Window Help Burp Suite Community Edition v2022.2.3 - Temporary Pr...
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
Intercept HTTP history WebSockets history Options
Request to https://www.google.com:443 [172.217.31.132]
Forward Drop Intercept is... Action Open Brow... Comment this item HTTP/2
Pretty Raw Hex \n
1 GET /search?q=%EB%8B%A4%EC%9D%8C&hl=ko&source=hp&ei=URlyYt3fD8bihwOq9JYo&iflsig=AHkkrS4AAAAAYjlgYeVlrsWtz9V4ja5zrNpOJay3pTfo&ved=0ahUKEwidzlHAiMv2AhVG8WEKHSq6BQUQ4dUDCAk&uact=5&oq=%EB%8B%A4%EC%9D%8C&gs_lcp=Cgdnd3Mtd2l6EAMyCwgAEIAEELEDEIMBMgsIABCABBCxAxCDATILCAAQgAQQsQMQgwEyCwgAEIAEELEDEIMBMgsIABCABBCxAxCDATILCAAQgAQQsQMQgwEyCwgAEIAEELEDEIMBMgsIABCABBCxAxCDATILCAAQgAQQsQMQgwEyCwgAEIAEELEDEIMBOg4ILhCABBCxAxDHARDRAzoLCC4QgAQQxwEQ0QM6BQgAEIAEUKQGWOQTYLk8aAlwAHgBgAFxiAHxBJIBAzEuNZgBAKABAbABAA&sclient=gws-wiz HTTP/2
2 Host: www.google.com
3 Cookie: 1P_JAR=2022-03-16-16; NID=511=W3uNgfqK7x-Qjq_tSel37twCMGGjx-nHs00mSKsZHavHKDox0Tm8y5C4hsTfSopZiNlm5qre2FoGPkTwsdpxEksx9EluBbkehoeZuNqz3c0aRKmW72iryFmjthKBktVofJRP74Ty9HTqxm49lm0QctDlsqVv62BnEikGWi3_kfl; DV=M5aWaAfT1isjYH8olYu_J3j57F45-Vd_Hk7tc0SfCwAAAAA
4 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Full-Version: "99.0.4844.51"
7 Sec-Ch-Ua-Arch: "x86"
8 Sec-Ch-Ua-Platform: "Windows"
9 Sec-Ch-Ua-Platform-Version: "10.0.0"
10 Sec-Ch-Ua-Model: ""
11 Sec-Ch-Ua-Bitness: "64"
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
15 X-Client-Data: CIKJywE=
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
Search... 0 matches
Inspector
Request Attributes 2
Request Query Parameters 10
Request Body Parameters 0
Request Cookies 3
Request Headers 26


1 GET /search?q=%EB%8B%A4%EC%9D%8C&hl=ko&sc

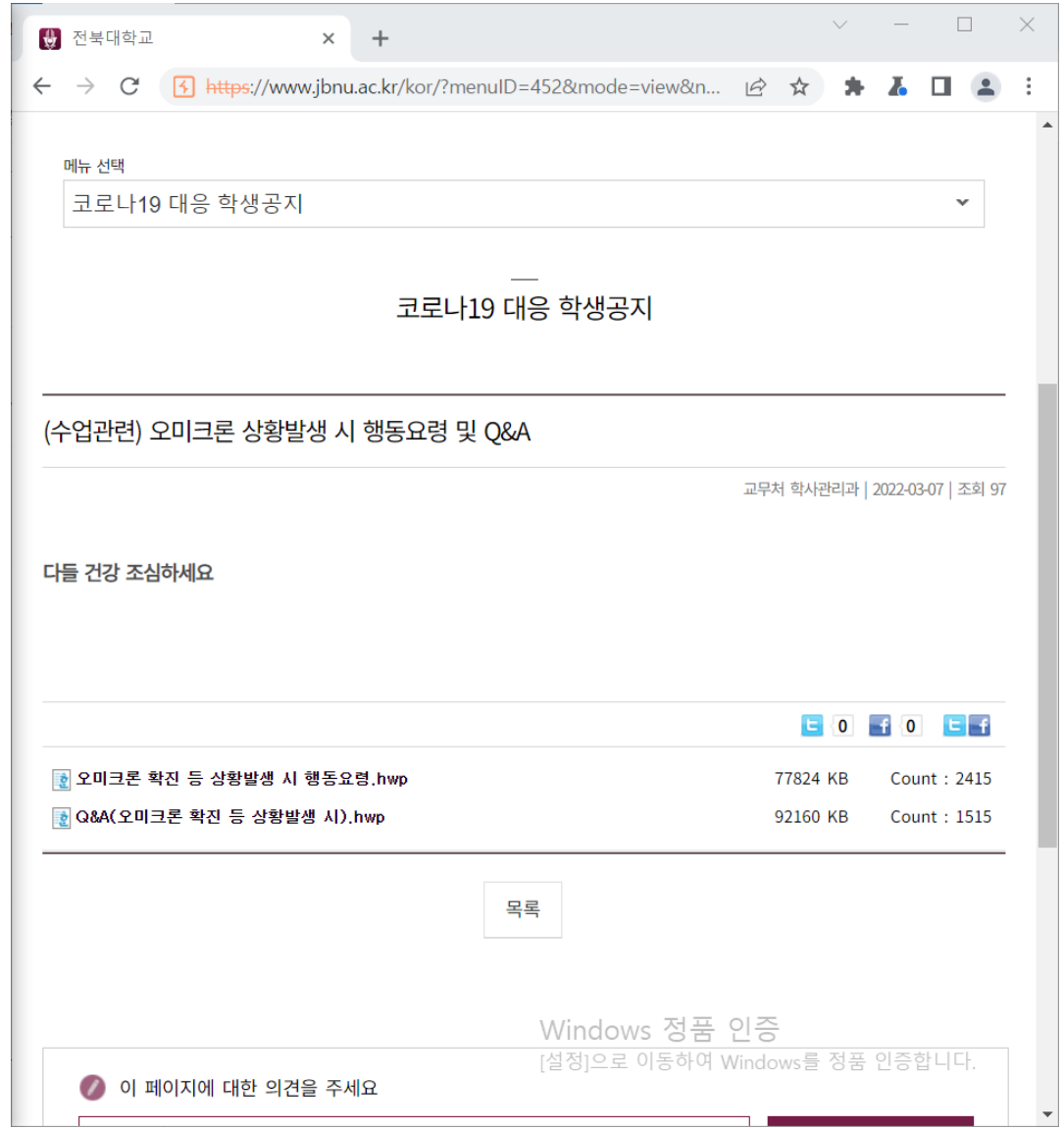

다음 - Google 검색
https://www.google.com/search?q=다음&hl=ko&source=h...
Google
다음
전체 뉴스 지도 동영상 이미지 더보기 도구
검색결과 약 2,430,000,000개 (0.39초)
https://www.daum.net
Daum
이 페이지에 관한 정보가 없습니다.
이유 알아보기
daum.net 검색결과
뉴스
정치 - 국제 - 사회 - 경제 - 연재 - IT - 팩트체크 - ...
블로그
아카마이 웨비나 - Security Tech Briefing: 아카마이.. · 씨앤토트 웨 ...
고객센터
메일 - 회원정보 - 검색 - 다음뉴스 - 블로그 - ...
daum.net의 최신 뉴스


전북대학교
https://www.jbnu.ac.kr/kor/
2022년 학군사관(ROTC) 후보생 모집
모집기간 : 2022. 3. 2.(수) ~ 4. 8.(금)
모집대상 : 1, 2학년 재학생(남, 여)
바로가기
[학부] 2022학년도 후기 외국인 특별전형 모집
[Undergraduate] admission for Fall semester 2022
모집기간 : [1차] 3.21(월)~4.1(금) [2차] 5.2(월)~5.13(금)
바로가기
1일간 열지 않기
전북대학교
JEONBUK NATIONAL UNIVERSITY
코로나19 학생공지
교내공지
교내채용
더보기 +
(수업관련) 오미크론 상황발생 시 행동요령 및..
2022학년도 1학기 수업운영과 관련하여 오미크론 확진 등 상황 발생 시신속하고 안전한 대응을 위해 『행동요령』 및 『Q&A(학생용)』을 안내합니..
2022학년도 1학기 수업 세부운영 방안 안내 02.25
2021학년도 전기 학위수여식 관련 협조요청 02.18
2022학년도 입학식 미개최 알림 02.17
Windows 정품 인증
[설정]으로 이동하여 Windows를 정품 인증합니다.
HOT NOTICE


전북대학교
https://www.jbnu.ac.kr/kor/?menuID=452&mode=view&n...
메뉴이동 커뮤니티
메뉴이동 공지사항
메뉴이동 코로나19 대응 학생공지
메뉴 선택
코로나19 대응 학생공지
코로나19 대응 학생공지
(수업관련) 오미크론 상황발생 시 행동요령 및 Q&A
교무처 학사관리과 | 2022-03-07 | 조회 97
2022학년도 1학기 수업운영과 관련하여 오미크론 확진 등 상황 발생 시
신속하고 안전한 대응을 위해 『행동요령』 및 『Q&A(학생용)』을 안내합니다.
0
0
오미크론 확진 등 상황발생 시 행동요령.hwp 77824 KB Count : 2415
Q&A(오미크론 확진 등 상황발생 시).hwp 92160 KB Count : 1515
목록
Windows 정품 인증
[설정]으로 이동하여 Windows를 정품 인증합니다.


Burp Project Intruder Repeater Window Help Burp Suite Community Edition v2022.2.3 - Temporary Pr...
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
Intercept HTTP history WebSockets history Options
Response from https://www.jbnu.ac.kr:443/kor/?menuID=452&mode=view&no=166 [175.106.80.230]
Forward Drop Intercept is on Action Open Browser Comment this item
Pretty Raw Hex Render \n
Inspector
Response Headers 6
교무처 학사관리과
2022-03-07
조회 97
<!-- 본문 시작 -->
<h3 class="labelhidden">
본문 내용
</h3>

다들 건강 조심하세요
<!-- 본문 끝 -->
Search...
0 matches


전북대학교
https://www.jbnu.ac.kr/kor/?menuID=452&mode=view&n...
메뉴 선택
코로나19 대응 학생공지
코로나19 대응 학생공지
(수업관련) 오미크론 상황발생 시 행동요령 및 Q&A
교무처 학사관리과 | 2022-03-07 | 조회 97
다들 건강 조심하세요
오미크론 확진 등 상황발생 시 행동요령.hwp 77824 KB Count : 2415
Q&A(오미크론 확진 등 상황발생 시).hwp 92160 KB Count : 1515
목록
Windows 정품 인증
[설정]으로 이동하여 Windows를 정품 인증합니다.
이 페이지에 대한 의견을 주세요

# 패킷 보안 기술

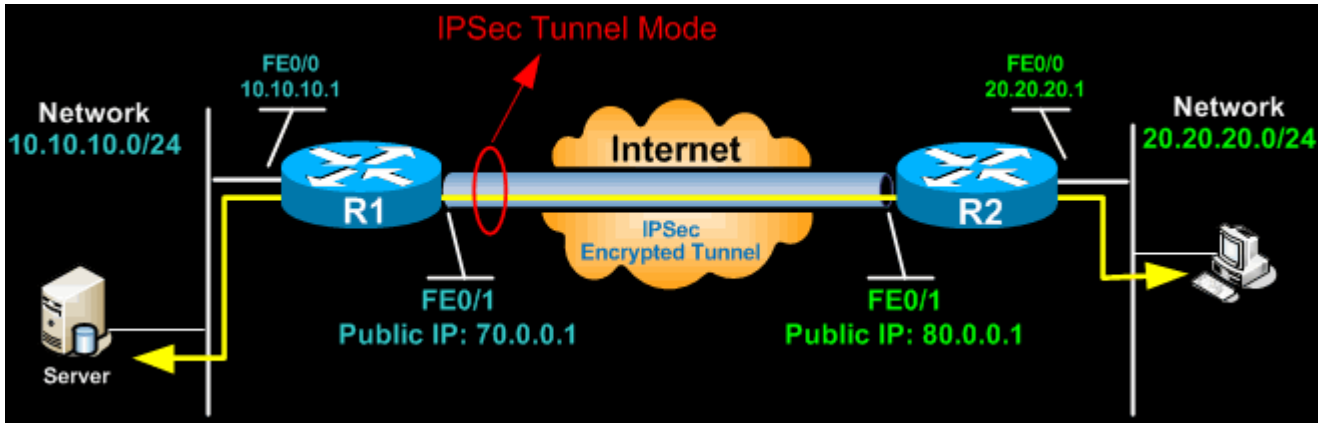
- 서버에서 클라이언트로 보낸 값을 다시 참조하지 않는게 중요하다.

- IPsec, SSL, S-HTTP 프로토콜을 사용한다.

# 패킷 보안 기술

## 1. IPsec 프로토콜

- Ipsec 프로토콜은 각 통신 세션의 IP 패킷을 암호화하고 인증 과정을 통해 통신하는 인터넷 프로토콜이다.
- 즉 네트워트 계층에서 IP 패킷 단위의 데이터 변조 방지 및 은닉기능을 제공하는 프로토콜



# 패킷 보안 기술

## 2. SSL 프로토콜

- 과거에 전송 계층 보안(TLS)로 명칭되었으며 현재는 보안 소켓 레이어로 사용되는 암호 규약이다.

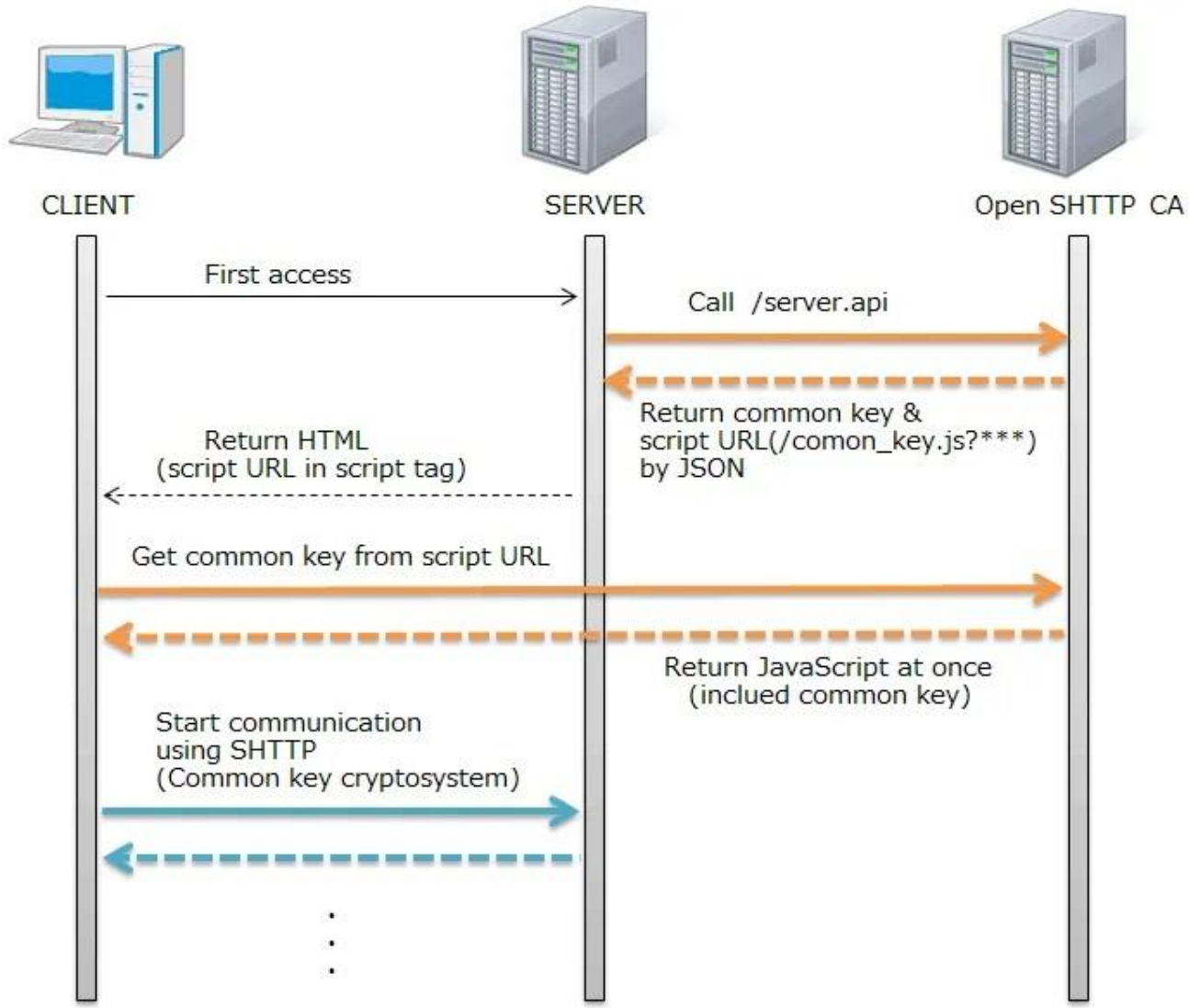
- 인터넷 계층과 응용 계층 사이에서 작동하는 프로토콜이며 웹 브라우징, 메일, 메신저 등 다양한 곳에서 사용되고 있다.

# 패킷 보안 기술

3. S-HTTP 프로토콜

- 과거에 전송 계층 보안(TLS)로 명칭되었으며 현재는 보안 소켓 레이어로 사용되는 암호 규약이다.

- 인터넷 계층과 응용 계층 사이에서 작동하는 프로토콜이며 웹 브라우징, 메일, 메신저 등 다양한 곳에서 사용되고 있다.


CLIENT
SERVER
Open SHTTP CA
First access
Call /server.api
Return common key &
script URL(/comon_key.js?***)
by JSON
Return HTML
(script URL in script tag)
Get common key from script URL
Return JavaScript at once
(inclued common key)
Start communication
using SHTTP
(Common key cryptosystem)

# 하이퍼텍스트

- 독자가 한 문서에서 다른 문서로 쉽게 이동할 수 있도록 만들어진 텍스트 등을 뜻한다.

- > 다른문서와 연관관계를 가진 텍스트들을 총칭하는 의미이다.