



확실히 오래 성하는 지킴이들  
融保工

## 버프 스위트 소개 & 설치

-기획부-



# 목차

---

- 활동 일정

## 1. Burp suite란 무엇인가?

- 프록시 서버
- 버프스위트

## 2. Burp suite 설치 방법





# 버프스위트 개념

- 웹 브라우저

□ 웹 브라우저 - 인터넷망에서 정보를 검색하는 데 사용하는 응용 프로그램 (ex - 인터넷 익스플로러, 크롬, 파이어폭스 ..)

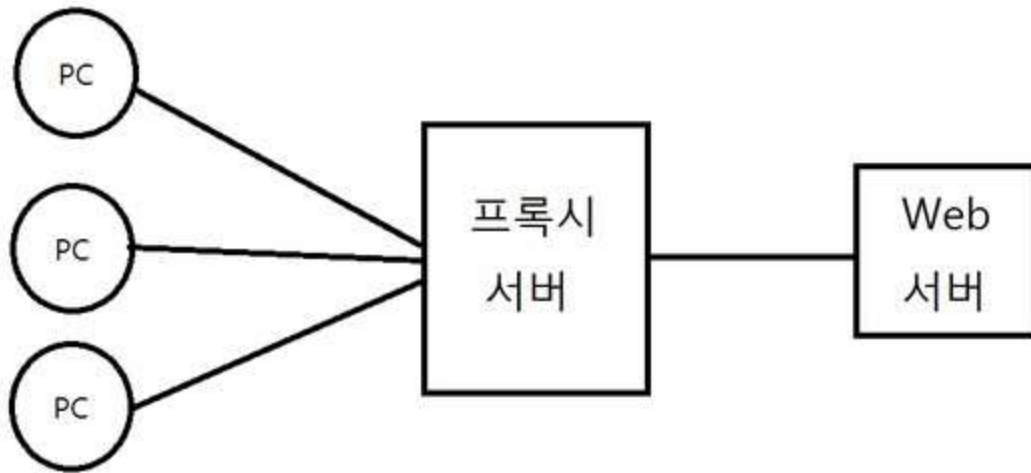




# 버프스위트 개념

## ■ proxy

□ 프록시 서버 (proxy server) – 클라이언트가 자신을 통해서 다른 네트워크 서비스에 간접적으로 접속할 수 있게 해 주는 컴퓨터 시스템이나 응용 프로그램



- 서버와 클라이언트의 중간다리 역할을 수행한다.
- 데이터를 전송할 때, **pc**에서 서버로 직접 전송하는 것이 아니라 프록시를 통해 전송하는 것임.





# 버프스위트 개념

## ■ Burp suite

### □ Burp suite

- 버프 스위트는 프록시 도구 중 하나이며, 버프 스위트를 이용하면 서버와 클라이언트가 교환하는 패킷을 중간에서 살펴볼 수 있다.
- **HTTP/S** 트래픽을 가로채고 수정하기 위한 웹 프록시 기능을 포함한다.

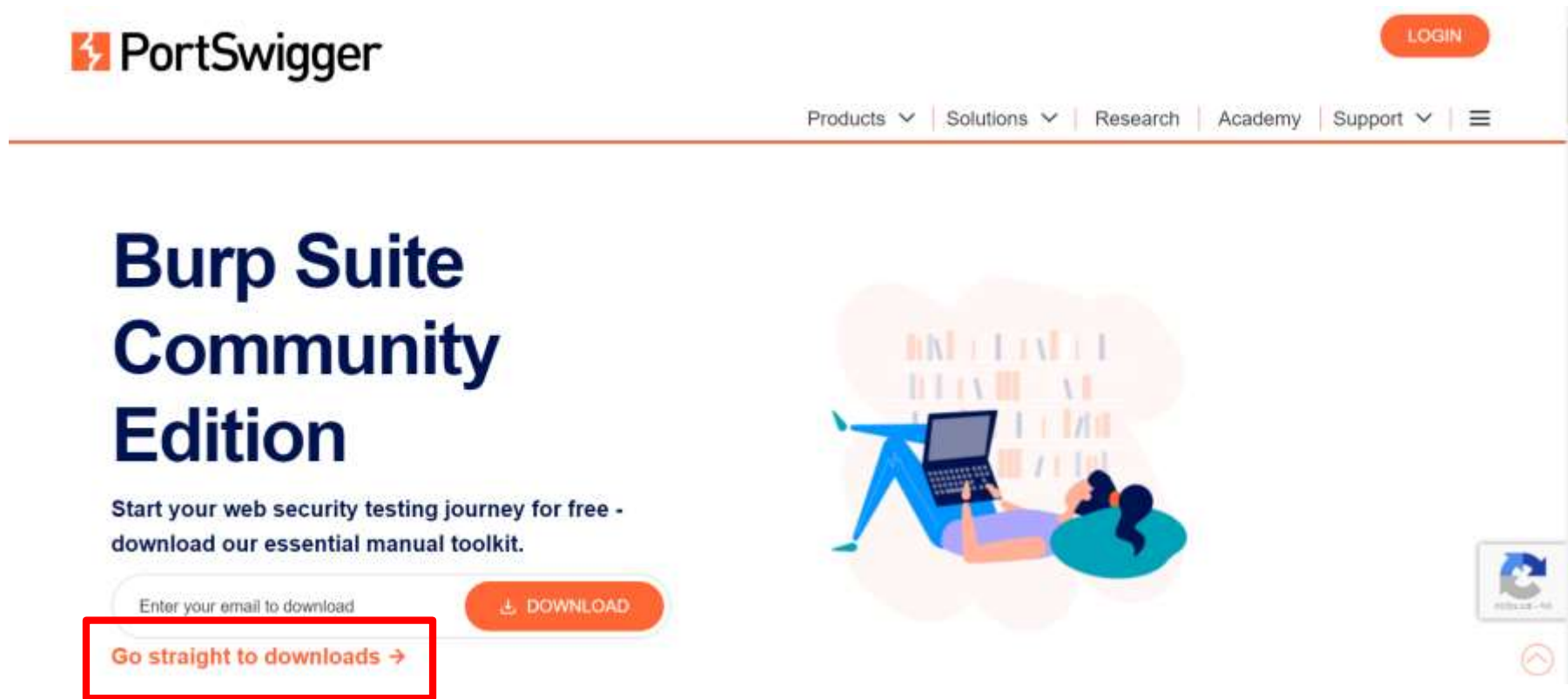
다운로드 ) <https://portswigger.net/burp/communitydownload>





# 버프스위트 설치

- Burp suite



링크를 통해 사이트 접속 후 Go straight to downloads 클릭





# 버프스위트 설치

- Burp suite

[LOGIN](#)[Products](#) ▾ | [Solutions](#) ▾ | [Research](#) | [Academy](#) | [Support](#) ▾ | [Menu](#)

## Professional / Community 2024.7.5

Stable

30 August 2024 at 12:12 UTC

Burp Suite Community Edition ▾

Windows (x64) ▾

⬇️ DOWNLOAD

[show checksums](#)

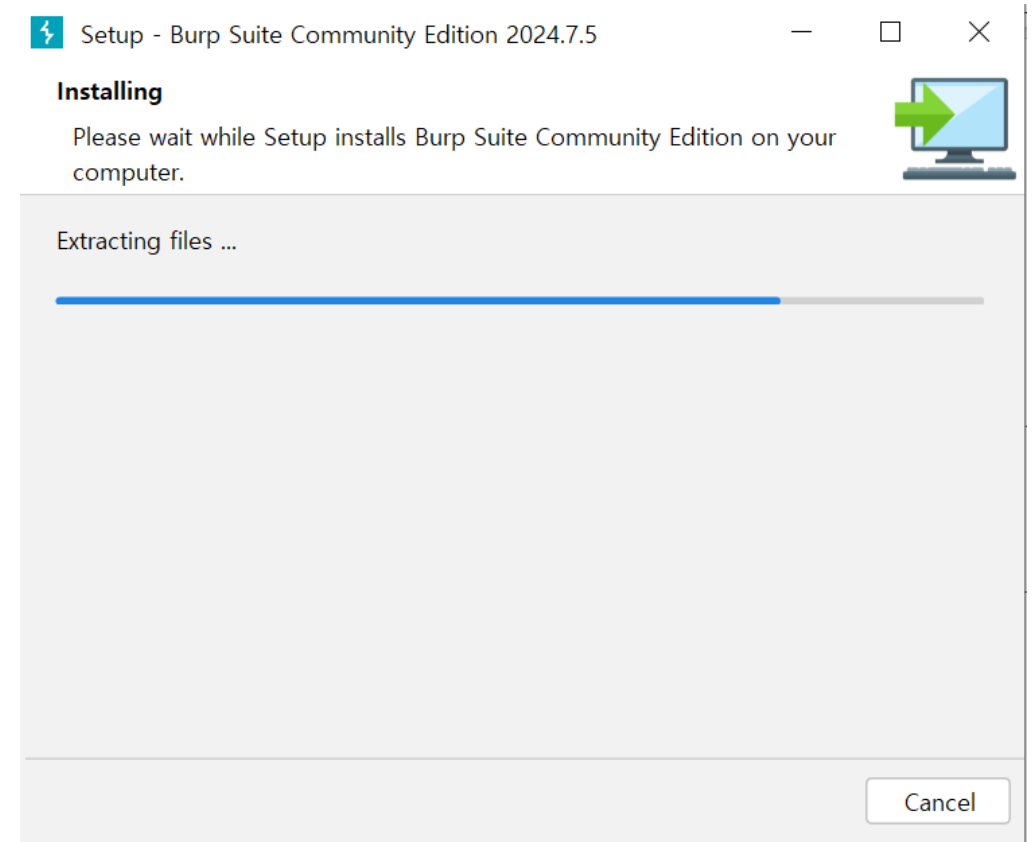
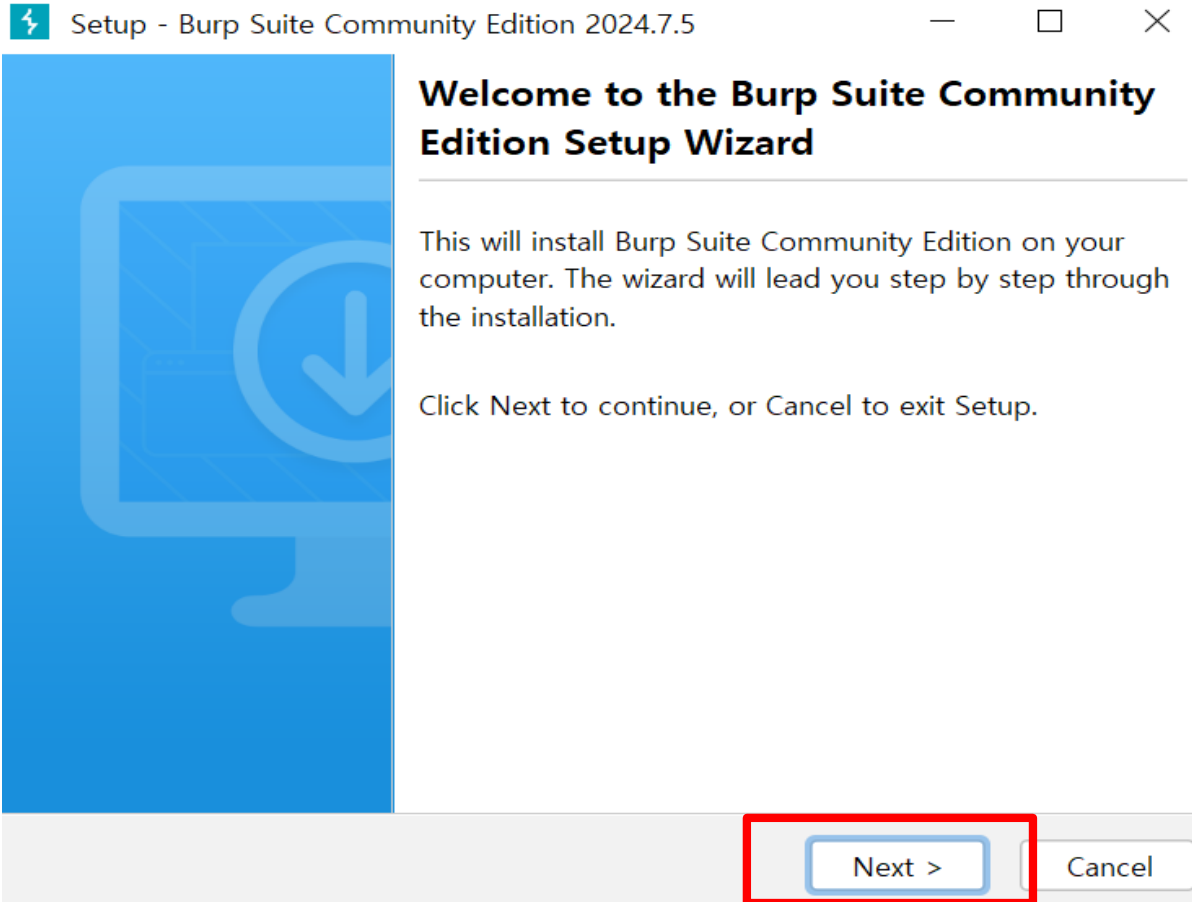
This release introduces major performance upgrades, significant enhancements to our Intercept feature, and a new **Scanned insertion points** column to the **Audit items** table. We've expanded our OpenAPI scanning to include endpoints that require HTTP headers, and added a toggle for **Site map** views. We've also made some quality of life improvements, fixed some bugs, and updated the Montoya API.





# 버프스위트 설치

## ■ Burp suite



오른쪽 사진과 같은 다운로드 창이 뜰 때까지 전부 **Next**를 누르기

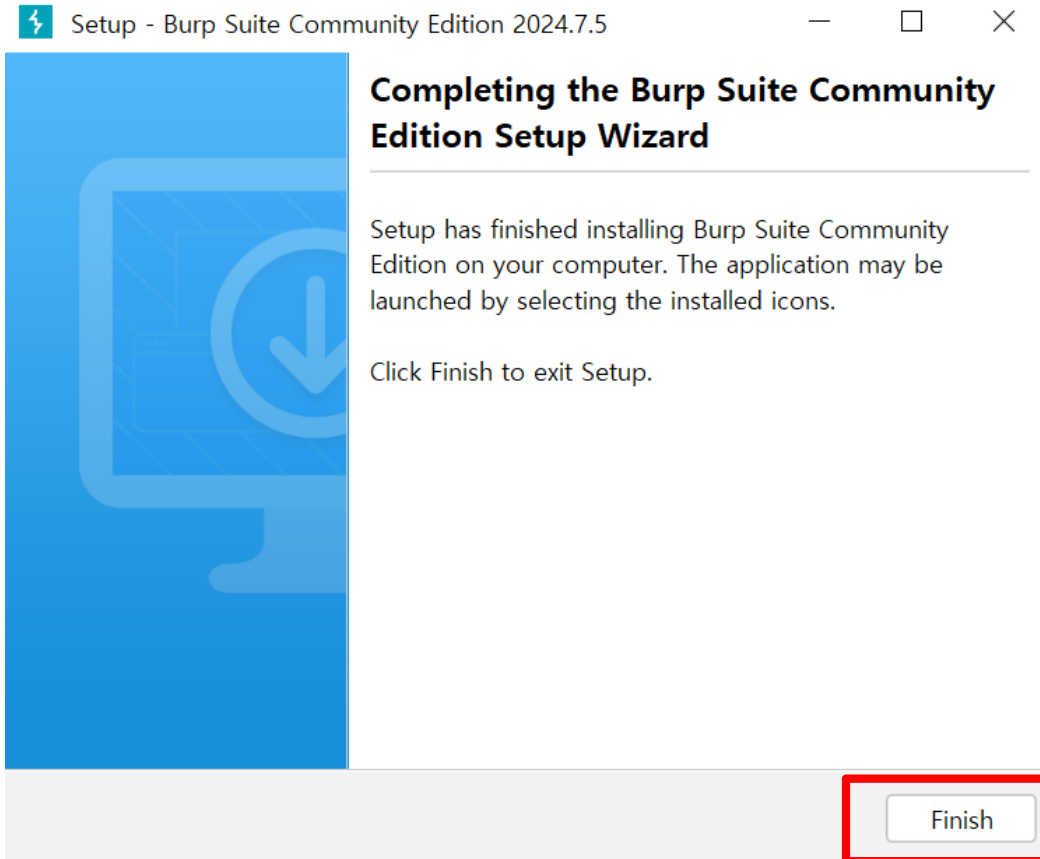






# 버프스위트 설치

## ■ Burp suite



Finish 누르면 설치 완료!





# 버프스위트 설치

## ■ Burp suite

Burp Suite Community Edition v2024.7.5

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

*Note: Disk-based projects are only supported on Burp Suite Professional.*

☒ Temporary project in memory

☐ New project on disk

Name:

File:

☐ Open existing project

Name	File
------	------

File:

☒ Trust this project file

☒ Pause Automated Tasks

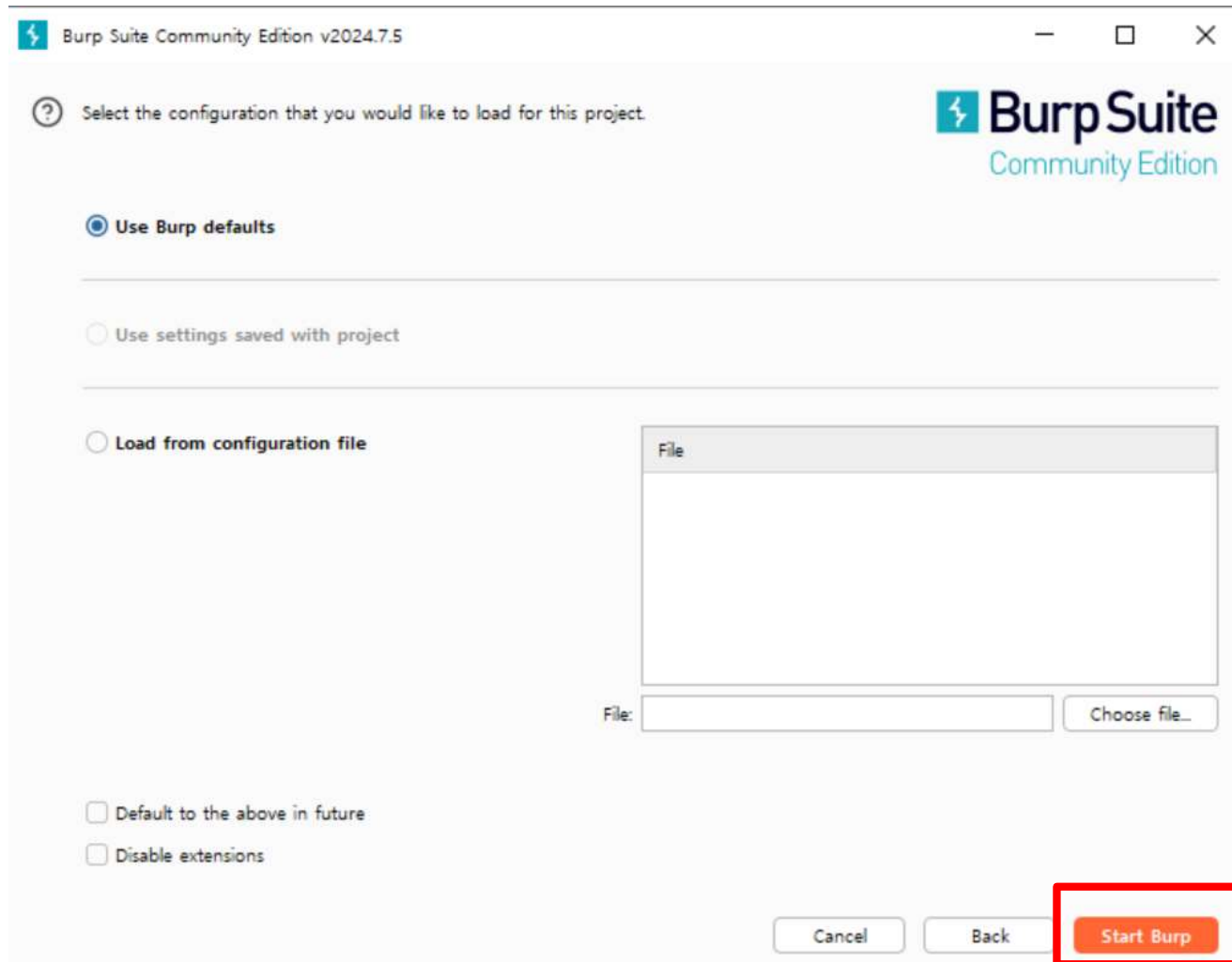
프로젝트 저장에 관한 내용인데 **next** 누르면 됩니다!





# 버프스위트 설치

## ■ Burp suite



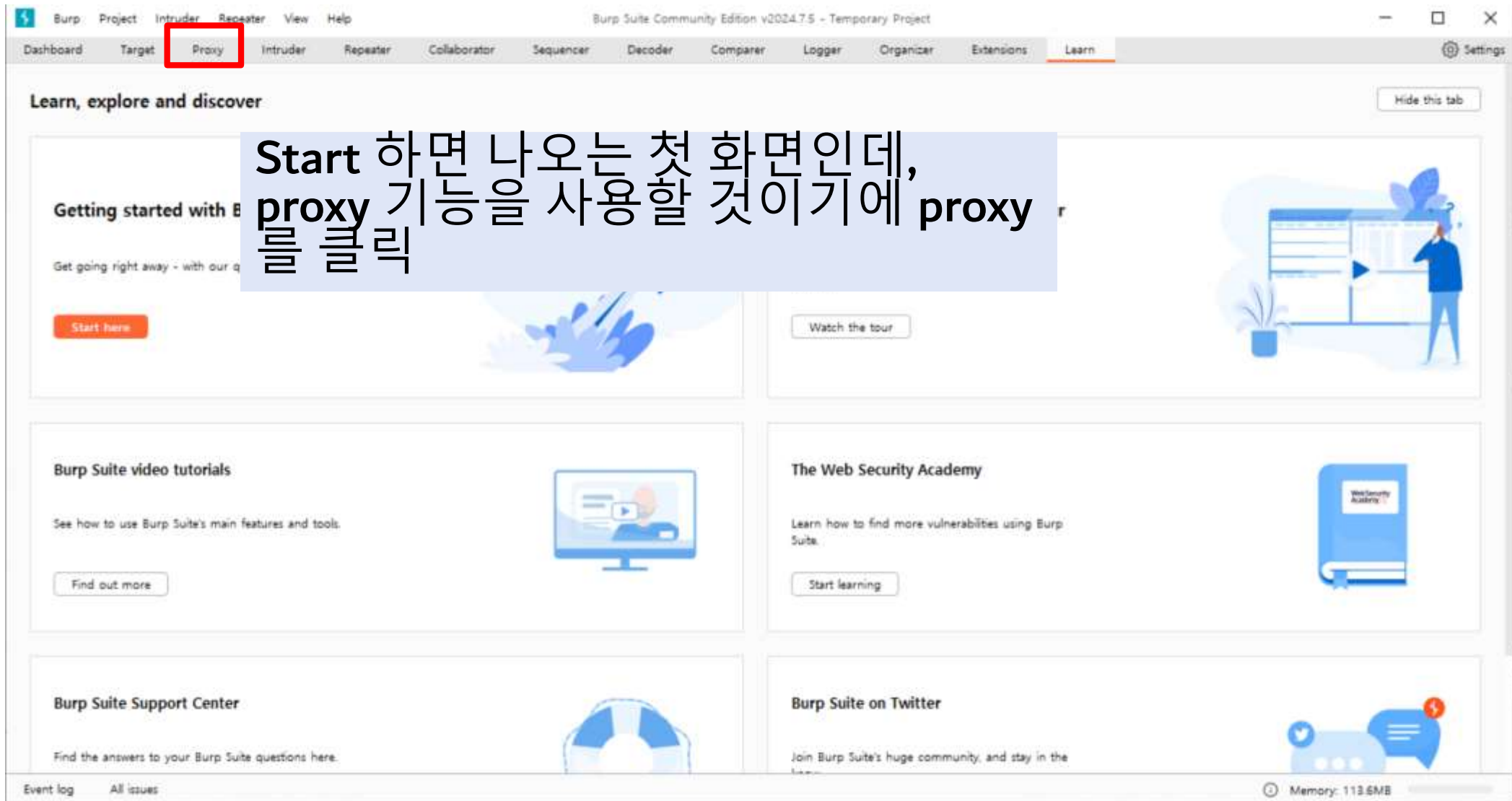
Start Burp 클릭!





# 버프스위트 설치

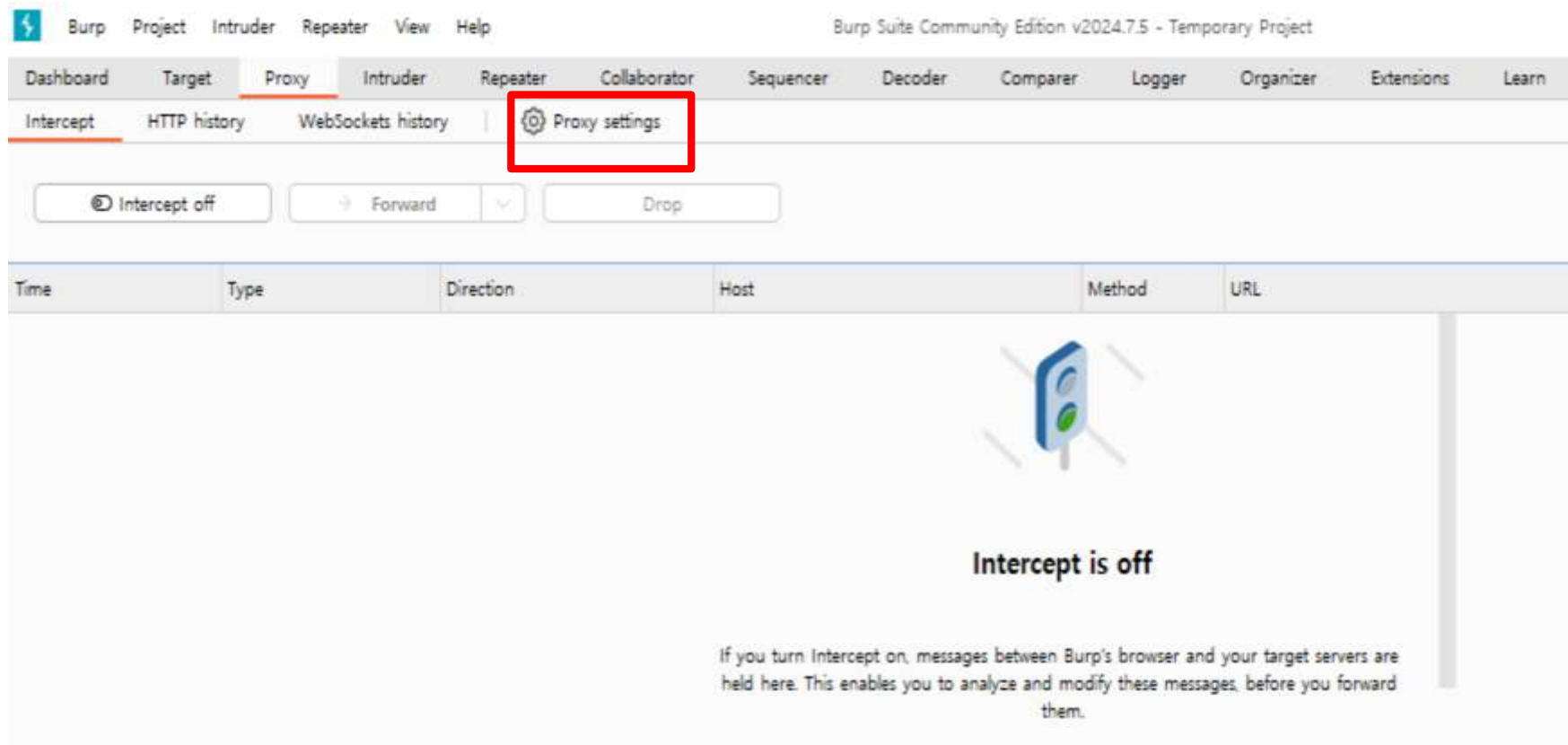
## ■ Burp suite





# 버프스위트 설치

## ■ Burp suite



환경설정 변경을 위해 **Proxy settings** 클릭





# 버프스위트 설치

## ■ Burp suite

The screenshot shows the Burp Suite Settings window, specifically the Proxy tab. The left sidebar lists various tools, with 'Proxy' selected. The main area is divided into two sections: 'Request interception rules' and 'Response interception rules'. Both sections have a checkbox to 'Intercept requests/responses based on the following rules', which is checked in both. The 'Response interception rules' section is highlighted with a red rectangle. Below each section is a table of rules.

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>	And	File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$...
<input type="checkbox"/>	Or	Request	Contains parameters	(get post)
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="checkbox"/>	And	URL	Is in target scope	

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>	And	Content type head...	Matches	text
<input type="checkbox"/>	Or	Request	Was modified	
<input type="checkbox"/>	Or	Request	Was intercepted	
<input type="checkbox"/>	And	Status code	Does not match	^304\$
<input type="checkbox"/>	And	URL	Is in target scope	

Response interception rules 에서  
Intercept responses based on the following rules 옵션 선택





# 버프스위트 설치 (필요시)

## ■ Burp suite

Settings

Tools > Proxy

### Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export

Import / export CA certificate   Regenerate CA certificate

### Request interception rules

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☒ Intercept requests based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$ ...
<input type="checkbox"/>	Or	Request	Contains parameters	
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="checkbox"/>	And	URL	Is in target scope	

Tools > Proxy > Proxy listeners > interface에서  
IP:PORT 세팅을 확인하기 (기본값: 127.0.0.1:8080)





# 버프스위트 설치 (필요시)

## ■ Burp suite

설정

홈

설정 검색

네트워크 및 인터넷

상태

Wi-Fi

이더넷

전화 접속

VPN

비행기 모드

모바일 핫스팟

프록시

프록시

본문에 적용되지 않습니다.

자동으로 설정 검색

☒ 끄

설정 스크립트 사용

☐ 끄

스크립트 주소

저장

수동 프록시 설정

이더넷 또는 Wi-Fi 연결에 프록시 서버를 사용합니다. 이 설정은 VPN 연결에 적용되지 않습니다.

프록시 서버 사용

☒ 켜

주소

127.0.0.1

포트

8080

다음 항목으로 시작하는 주소를 제외하고 프록시 서버를 사용합니다. 여러 항목은 세미콜론(;)으로 구분합니다.

저장

☐ 로컬(인트라넷) 주소에 프록시 서버 사용 안 함

설정 > 네트워크 및 인터넷  
> 프록시

수동 프록시 설정 메뉴에서  
주소와 포트를 **burp** 설정과  
동일하게 설정하기

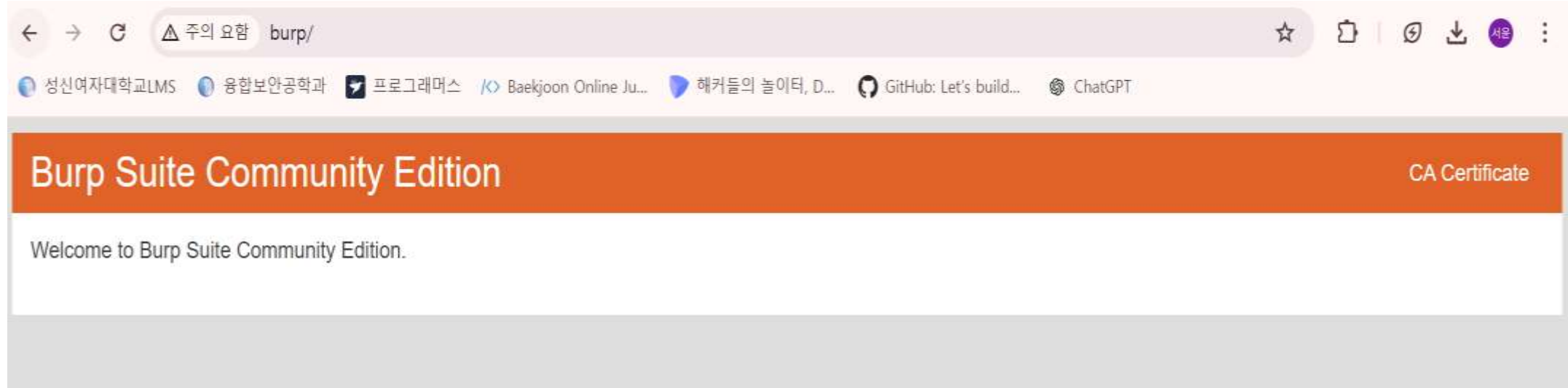






# 버프스위트 설치 (필요시)

- Burp suite



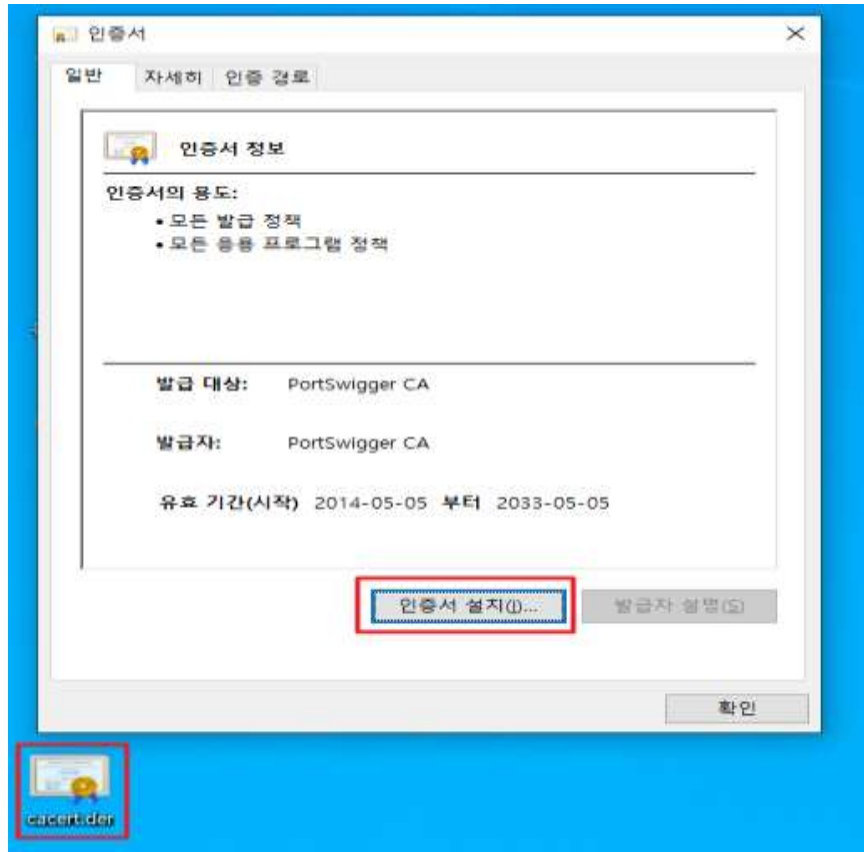
인터넷 브라우저에서 **http://burp/** 입력한 뒤,  
접속된 페이지에서 **CA Certificate** 선택 후 인증서 다운로드





# 버프스위트 설치 (필요시)

## ■ Burp suite



← 인증서 가져오기 마법사

### 인증서 가져오기 마법사 시작

이 마법사를 사용하면 인증서, 인증서 신뢰 목록, 인증서 해지 목록을 디스크에서 인증서 저장소로 복사할 수 있습니다.

인증서는 인증 기관이 발급하는 것으로 사용자 신분을 확인합니다. 인증서에는 데이터를 보호하거나 보안된 네트워크 연결을 하는 데 필요한 정보가 들어 있습니다. 인증서 저장소는 인증서를 저장하는 시스템 영역입니다.

저장소 위치

☐ 현재 사용자(U)

☒ 로컬 컴퓨터(L)

계속하려면 [다음]을 클릭하십시오.

다음(N)

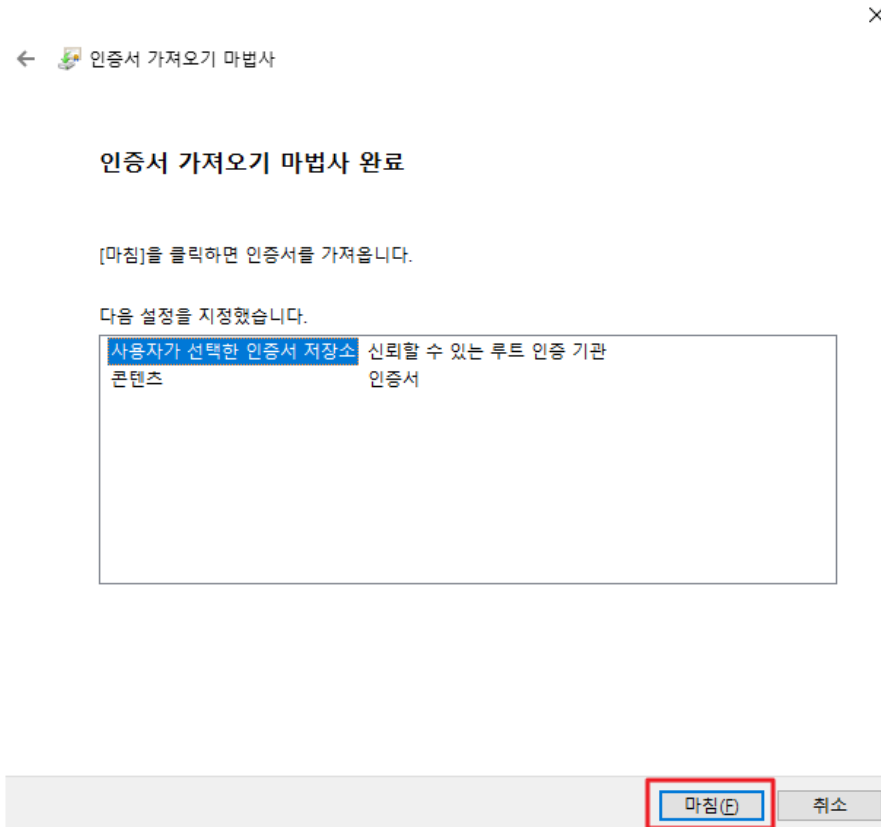
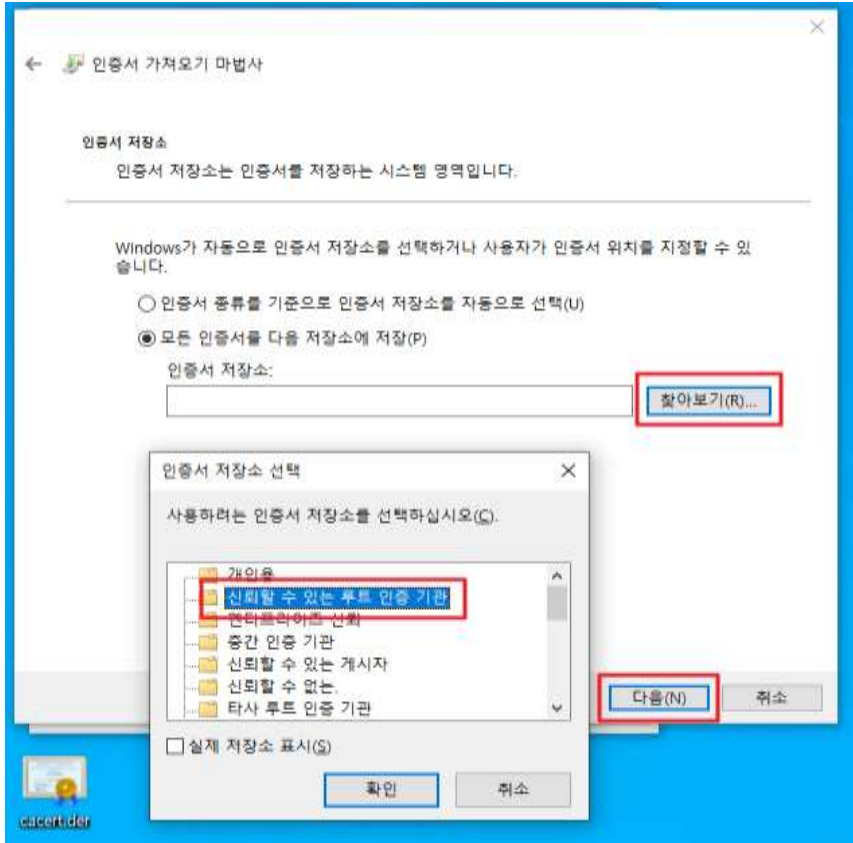
취소

인증서 설치 > 로컬 컴퓨터 선택





- Burp suite



모든 인증서를 다음 저장소에 저장 > 신뢰할 수 있는 루트 인증 기관 > 사용자가 선택한 인증서 저장소 > 마침까지 하면 인증서 설치까지 완료!





화학하고 오래 성하는 지키는 장인들  
融保工

## 버프 스위트 기능 소개

-기획부-



# 버프스위트 기능 둘러보기



- **Proxy** – burp suite는 proxy와 함께 사용되는데 default로 8080 포트에서 실행 proxy를 사용하여 클라이언트에서 웹 서버로 흐르는 트래픽을 가로채서 수정
- **Intruder** – 무차별 대입 공격이나 사전 공격을 수행
- **Repeater** – 같은 요청을 많은 횟수로 수정해서 보내서, 응답을 분석할 때 사용





# 버프스위트 기능 둘러보기



- **Sequencer** – 주로 웹 응용 프로그램에서 제공하는 세션 토큰의 임의성을 확인 할 때 사용
- **Decoder** – 암호화된 데이터를 다시 원래 형태로 해독하거나, 데이터를 암호화 하기 위하여 사용
- **Comparer** – 두 개의 요청, 응답 또는 다른 형태의 데이터 비교를 수행하는 데 사용  
다른 입력에 대한 응답을 비교하는 경우에 유용





# 버프스위트 기능 둘러보기

## ■ Proxy 기능

### □ Intercept

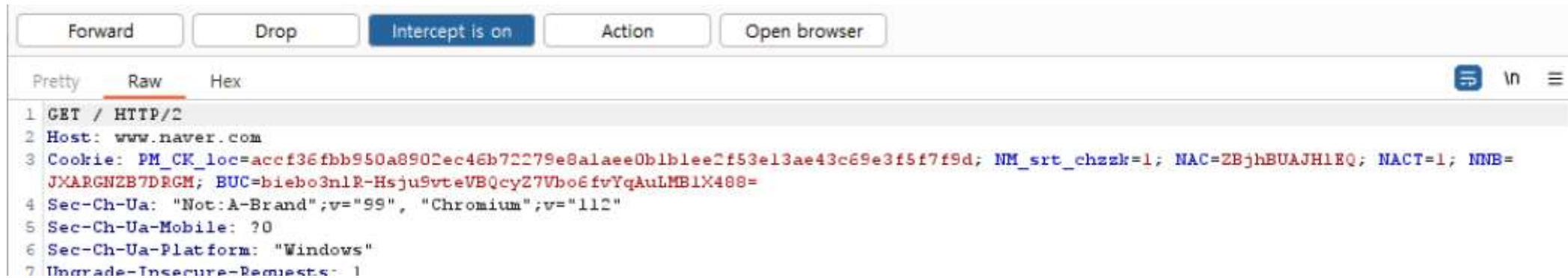
- 브라우저와 웹 서버 간에 전달되는 HTTP 및 web socket 메시지를 표시하고 모든 메시지를 모니터링, 가로채기 및 수정하는 기능을 가지고 있는 항목





# 버프스위트 기능 둘러보기

## ■ Proxy 기능



- **Forward** – 서버에게 메시지를 보낼 수 있음
- **Drop** – 메시지가 전달되지 않도록 중간에 차단할 때 사용
- **Intercept is on/off** – 차단에 대하여 켜고 끄는데 사용
  - **on** – 구성된 옵션에 따라 메시지가 차단되어 패널에 출력
  - **off** – 모든 메시지가 자동으로 전달
- **Action** – 현재 표시된 메시지에서 수행 가능한 동작 메뉴를 보여줌







# 버프스위트 기능 둘러보기

## ■ Proxy 기능

### □ HTTP History

- 프록시를 통과한 **HTTP** 메시지 기록들을 모두 저장하여 기록
- 리스트에 대한 필터링 및 주석을 설정하여 정보 관리 가능

[테이블에서 알 수 있는 정보]

요청 색인 번호, 프로토콜 및 서버 호스트 이름, HTTP 메소드, URL 파일 경로 및 쿼리 문자열, HTTP 상태 코드, 응답 길이, MIME 유형, URL 파일 확장자, 페이지 제목, TLS 사용 여부, 대상 서버의 IP 주소, 응답에 설정된 쿠키, 요청한 시간, 요청이 수신된 포트 등





# 버프스위트 기능 둘러보기

Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
1	https://sb-ssl.google.com	POST	/safebrowsing/clientreport/download?...	✓		400	765	JSON				✓	142.250.199.110
2	https://www.naver.com	GET	/			200	244986	HTML		NAVER		✓	223.130.192.248
4	https://ssl.pstatic.net	GET	/tveta/libs/ndpsdk/prod/ndp-loader.js			200	1638	script	js			✓	61.247.194.133
6	https://ssl.pstatic.net	GET	/tveta/libs/assets/js/pc/main/min/pc.ve...			200	31787	script	js			✓	61.247.194.133
7	https://ssl.pstatic.net	GET	/tveta/libs/ndpsdk/prod/ndp-core.js			200	97683	script	js			✓	61.247.194.133
8	https://ssl.pstatic.net	GET	/tveta/libs/glad/prod/gfp-core.js			200	48652	script	js			✓	61.247.194.133
9	https://pm.pstatic.net	GET	/resources/js/search.ab2d8d96.js?o=w...	✓		200	288422	script	js			✓	183.111.26.110
10	https://pm.pstatic.net	GET	/resources/js/main.faaf4442.js?o=www	✓		200	760609	script	js			✓	183.111.26.110
11	https://pm.pstatic.net	GET	/resources/js/preload.33507660.js?o=w...	✓		200	156669	script	js			✓	183.111.26.110
12	https://pm.pstatic.net	GET	/resources/js/polyfill.a163af38.js?o=www	✓		200	207734	script	js			✓	183.111.26.110
13	https://ssl.pstatic.net	GET	/tveta/libs/glad/prod/2.30.2/gfp-sdk.js			200	266065	script	js			✓	61.247.194.133

**Request**

Pretty Raw Hex

```
1 POST /safebrowsing/clientreport/download?key=dummytoken
2 HTTP/1.1
3 Host: sb-ssl.google.com
4 Content-Length: 349
5 Content-Type: application/octet-stream
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: no-cors
8 Sec-Fetch-Dest: empty
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
  Safari/537.36
10 Accept-Encoding: gzip, deflate
11 Connection: close
12
13 http://burp/cert"
14 )Å&@YU$ =N305DiDugU-a
15 jy\*NW--
16 http://burp/cert 127.0.0.1"http://burp/"
17 http://burp/*0J
18 cacert.derP2koQÅ3(08@JChrome/112.0.5615.50/WindowsPX`DBâe<
19 http://burp/cert 127.0.0.1"http://burp/09DëoiyBPXpe.
20 http://burp/ 127.0.0.1"09PüliyBPXp00 "e**
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/2 400 Bad Request
2 Vary: Origin
3 Vary: X-Origin
4 Vary: Referer
5 Content-Type: application/json; charset=UTF-8
6 Date: Thu, 12 Sep 2024 14:16:42 GMT
7 Server: ESF
8 Cache-Control: private
9 Content-Length: 412
10 X-Xss-Protection: 0
11 X-Frame-Options: SAMEORIGIN
12 X-Content-Type-Options: nosniff
13 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
14
15 {
16   "error": {
17     "code": 400,
18     "message":
19       "API key not valid. Please pass a valid API key.",
20     "status": "INVALID_ARGUMENT",
21     "details": [
22       {
23         "@type": "type.googleapis.com/google.rpc.ErrorInfo",
24         "reason": "API_KEY_INVALID".
```

**Inspector**

Request attributes 2

Request query parameters 1

Request body parameters 59

Request headers 9

Response headers 12





# 버프스위트 기능 둘러보기

- Proxy 기능

- WebSockets History

- 프록시를 통과한 WebSockets 메시지 기록들을 모두 저장하여 기록
- 리스트에 대한 필터링 및 주석을 설정하여 정보 관리 가능

[테이블에서 알 수 있는 정보]

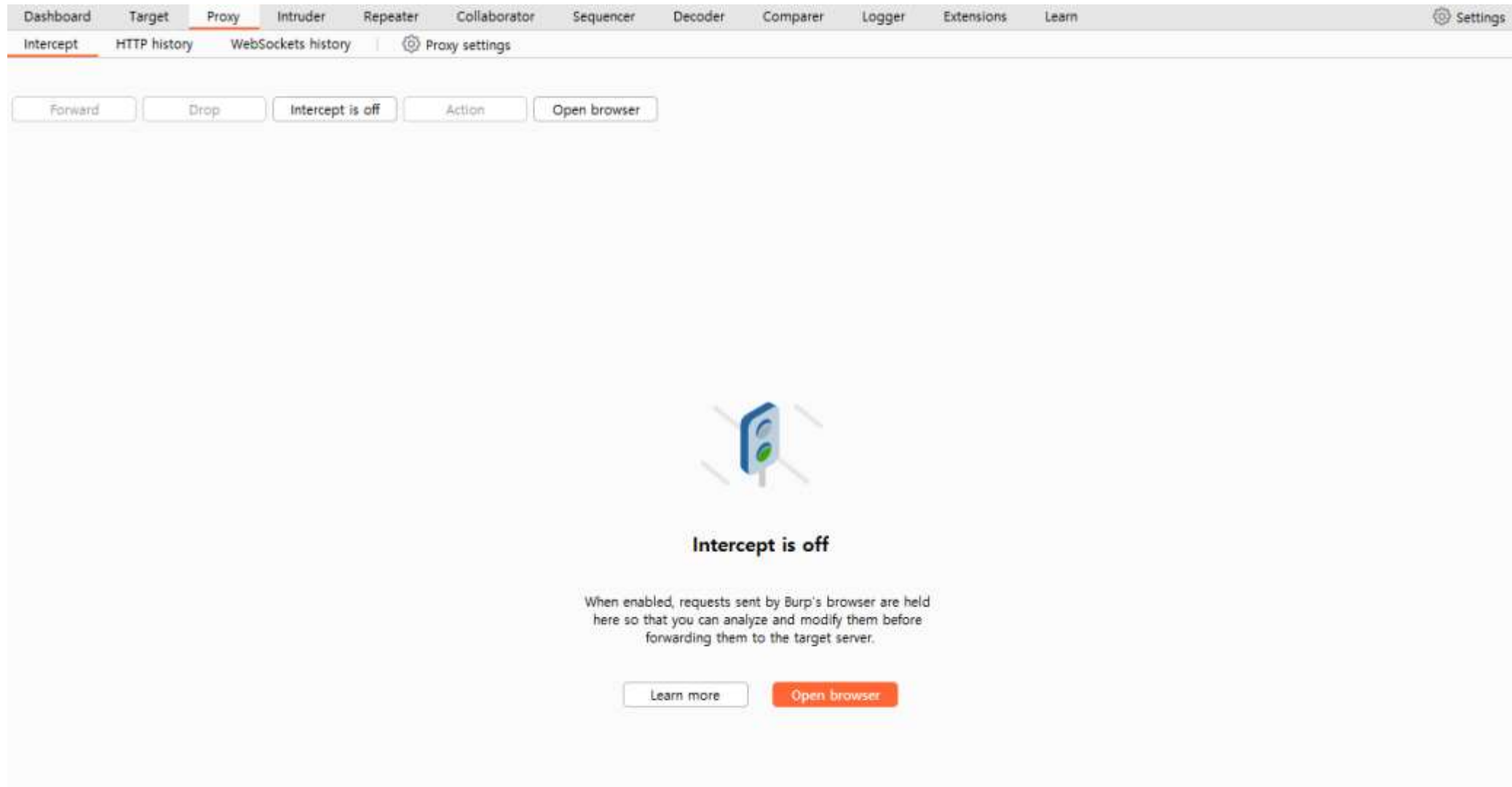
요청 색인 번호, WebSocket 연결의 URL, 메시지의 방향, 사용자가 메시지를 수정했는지 표시, 응답 길이, TLS 사용 여부 플래그, 메시지가 수신된 시간, 메시지가 수신된 포트 등





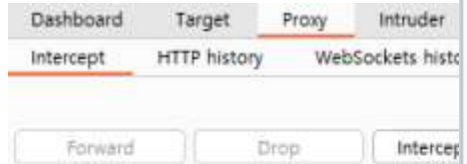
# 버프스위트 간단 실습

## ■ Proxy 실습해보기





## ■ Proxy 실습해보기



← → ↻ sugang.sungshin.ac.kr/logon.do?timestamp=1... ☆ ★ ⚙️ ⬇️ □ 👤 ⋮

# LOGIN

Please select a language 한국어 ▾

Settings

성신인(재학생, 교직원)은 성신 포탈 시스템 ID/PW로 로그인해 주세요.  
예비학부생 ID는 수험번호이며 비밀번호는 주민등록번호 뒤 7자리입니다.

아이디를 입력하세요.

비밀번호를 입력하세요.

로그인

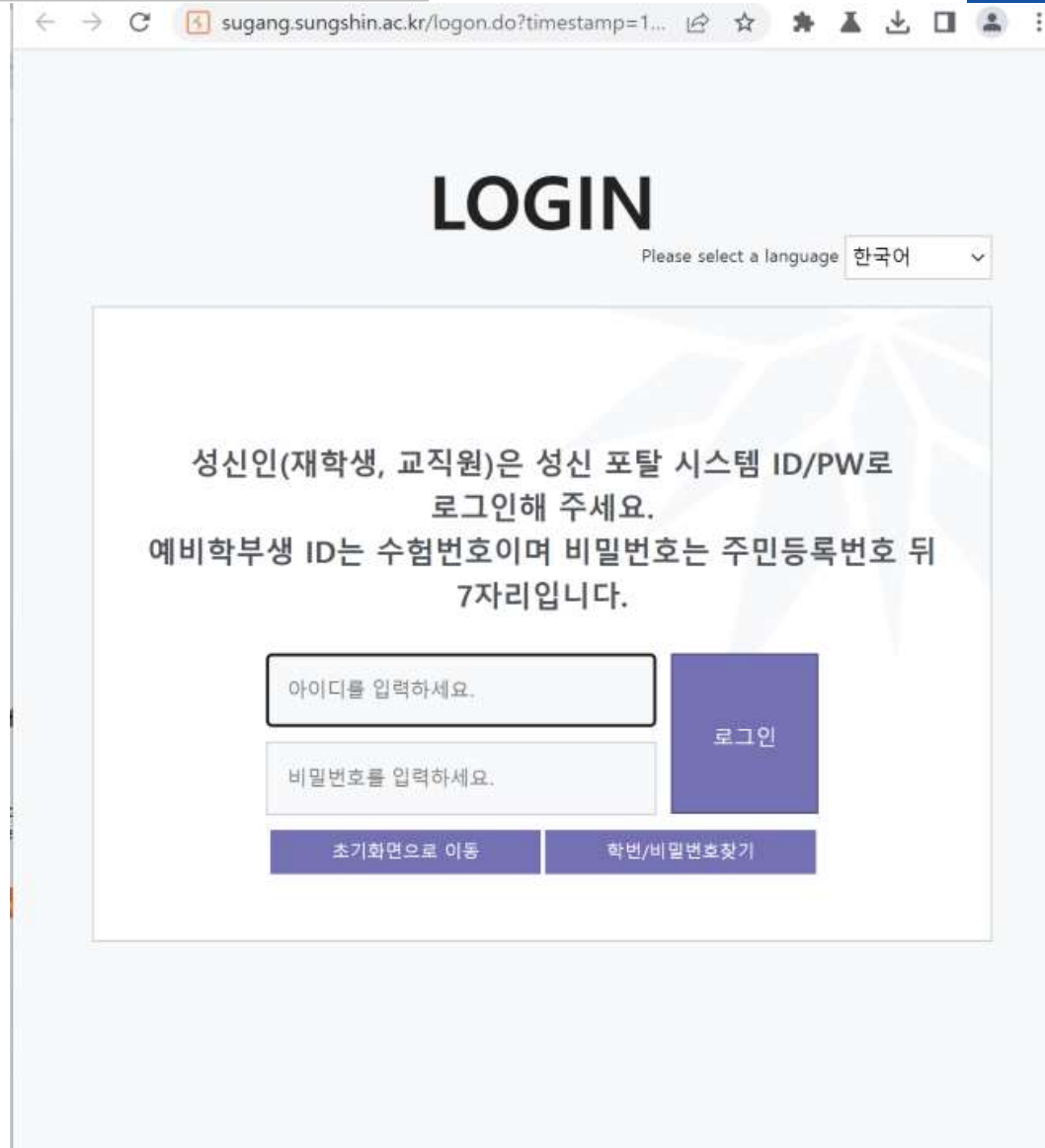
초기화면으로 이동 학번/비밀번호찾기





# 버프스위트 간단 실습

- 성신여대 사이트 -> 수강신청탭



The screenshot shows a web browser window with the URL `sugang.sungshin.ac.kr/login.do?timestamp=1...`. The page title is "LOGIN". Below the title, there is a language selection dropdown menu with "한국어" (Korean) selected. The main content area contains the following text:

성신인(재학생, 교직원)은 성신 포탈 시스템 ID/PW로  
로그인해 주세요.  
예비학부생 ID는 수험번호이며 비밀번호는 주민등록번호 뒤  
7자리입니다.

Below the text, there are two input fields:

- 아이디를 입력하세요. (Enter your ID)
- 비밀번호를 입력하세요. (Enter your password)

To the right of the input fields is a blue "로그인" (Login) button. Below the input fields are two buttons:

- 초기화면으로 이동 (Move to initial screen)
- 학번/비밀번호찾기 (Find student ID/password)





# 버프스위트 간단 실습

- 잘못된 아이디와 비밀번호를 작성
- Intercept on으로 변경
- 잠시 대기
- Forward 버튼 계속 클릭(3-4번정도)

## LOGIN

Please select a language 한국어

성신인(재학생, 교직원)은 성신 포탈 시스템 ID/PW로  
로그인해 주세요.  
예비학부생 ID는 수험번호이며 비밀번호는 주민등록번호 뒤  
7자리입니다.

로그인

[초기화면으로 이동](#)[학번/비밀번호찾기](#)







# 버프스위트 간단 실습

- 사이트로 가서 로그인 버튼을 누르기
- **Forward** 몇 번 눌러보면 아래와 같이 나타남(내가 입력한 값)
- 올바른 아이디와 비밀번호로 수정

```
retty  Raw  Hex
POST /logonAjax.do HTTP/1.1
Host: sugang.sungshin.ac.kr
Cookie: __fwb=156f3fed0FB2U2R0Fw9QYyY.1726162686298; __ga=GA1.1.1353336950.1726162687; __smVisitorID=mdeKY2_OPi0; JSESSION_SUGANG=7F5E8ghNLyV2m80Qkff10rrNQA0TAaLAbfKVgN6vFPDT1idp2ql94UuxyX0J46AU.amVlc19kb2lhaW4vdGtjMw==; __ga_9WF3HXQYB6=GS1.1.1726165219.2.1.1726167293.0.0.0; NetFunnel_ID=500213A20013Akey13Dconnection_timeout
Content-Length: 36
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; 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/112.0.5615.50 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://sugang.sungshin.ac.kr
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://sugang.sungshin.ac.kr/logon.do?timestamp=1726167636173
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

```
{
  "id": "20221140",
  "password": "12345"
}
```







# 버프스위트 간단 실습

- Forward 버튼 계속 누르기
- 사이트로 돌아와 로그인이 되어있는 것을 확인

**성신여자대학교**  
SUNGSHIN WOMEN'S UNIVERSITY

최선영(20221140) - 로그아웃

수강신청일정 >

수강신청안내 >

교양수강안내 >

사이버대학수강안내 >

개설강좌조회 >

관심강좌신청 >

수강신청 >

강의시간편성표 >

 **수강신청일정**

**2024학년도 2학기 수강신청 일정**

구분	기간
강의시간표 조회	2024. 7. 9.(화) 이후
관심강좌신청	2024. 7. 30.(화) 10:00 ~ 8. 5.(월) 17:00
수강신청	2024. 8. 13.(화) 10:00 ~ 8. 16.(금) 17:00 *8. 15.(목) 광복절: 수강신청 기간에 포함. 단 질의 응답
수강정정	2024. 9. 2.(월) 13:00 ~ 9. 9.(월) 11:00
수강철회	2024. 9. 23.(월) 10:00 ~ 9. 27.(금) 17:00





확실히하고 오래 성하는 지키는 장인들  
融保工

# 버프 스위트(Burp Suite) 실습

-기획부-



# 목차

---

- 활동 일정

- Docker 설치하기

- Docker란?

- DVWB 호스팅하기

- DVWB 실습하기

- Brute force

- 워게임 문제 풀어보기

- 쿠키 조작하기





# Docker 설치하기

---

- WSL, Docker Desktop 설치

설치 참고 링크

[Windows에 Docker Desktop 설치하기 \(tistory.com\)](https://tistory.com/entry/Windows에-Docker-Desktop-설치하기)

Docker Desktop 설치 후 명령어 입력

Docker --version

- 버전이 무사히 뜨면 설치완료!

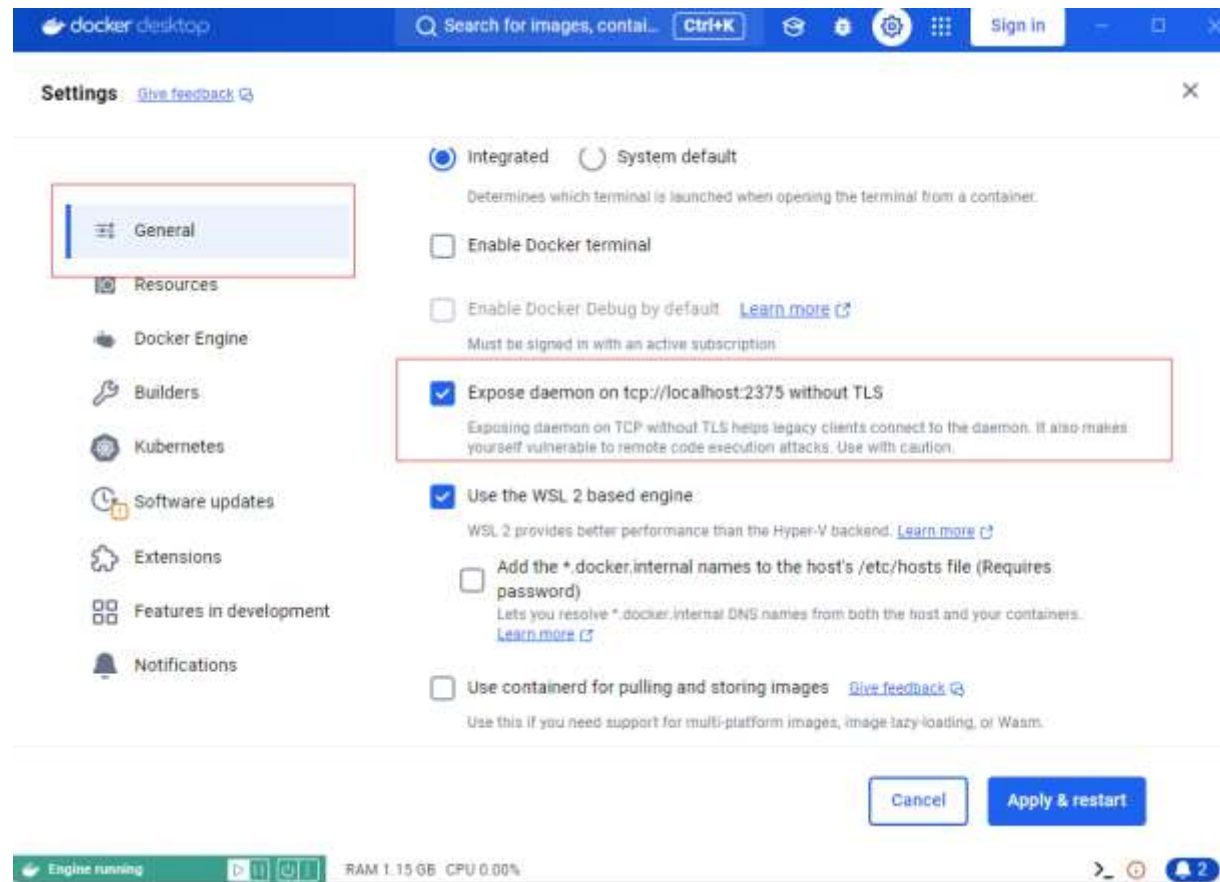




# Docker 설치하기

- 혹시 오류가 날 경우에는....

## ❑ Expose daemon on tcp://localhost:2375 옵션 활성화





# Docker가 뭐지?

- 컨테이너 기반의 오픈소스 가상화 플랫폼

## □ 컨테이너 기술의 혁명

- 애플리케이션과 그 종속성을 하나의 패키지로 묶어 실행
- 컨테이너'라는 격리된 환경에서 애플리케이션 실행

## □ 도커의 주요 개념

- 이미지: 애플리케이션과 그 실행 환경을 포함한 패키지애플리케이션 배포 및 확장 용이성
- 컨테이너: 이미지의 실행 가능한 인스턴스
- Dockerfile: 이미지 생성을 위한 명령어 집합
- Docker Hub: 이미지 저장소





# 그래서 Docker를 왜 쓰는데?

- 배포와 호스팅을 위해서

- 배포는 개발된 애플리케이션을 사용자가 접근할 수 있는 환경(예: 호스팅 서버)에 설치하고 구성하는 과정
  - 비유: 배포는 상품을 매장에 진열하는 것과 같음. 개발된 애플리케이션(상품)을 서버(매장)에 올리고 설정하는 과정
  - 과정: 코드 업로드, 환경 설정, 데이터베이스 마이그레이션, 테스트, 서비스 시작 등을 포함.
  - 도구: Jenkins, GitLab CI, Docker, Kubernetes 등 다양한 도구가 사용됨
- 예시: 내가 열심히 만든 떡볶이(프로그램)를 사람들이 먹을 수 있게 접시에 담고 포장하는 과정





# 그래서 Docker를 왜 쓰는데?

- 배포와 호스팅을 위해서

□ 호스팅은 웹사이트나 애플리케이션을 인터넷에서 접근 가능하게 만드는 서비스

□ 비유: 내가 만든 떡볶이(프로그램)을 포장한 후(배포) 가판대를 빌려서 파는 것(호스팅)

□ 종류: 공유 호스팅, VPS(가상 사설 서버), 전용 서버, 클라우드 호스팅

□ 특징: 24/7 가용성, 보안, 백업, 기술 지원 등을 제공







# 그래서 Docker를 왜 쓰는데?

## ■ Docker의 장점

- ❑ 일관성: 개발, 테스트, 운영 환경이 동일해져 "내 컴퓨터에서는 작동했는데..."라는 문제를 해결
- ❑ 이식성: 어떤 시스템에서도 동일하게 실행할 수 있어, 클라우드 환경으로의 이전이 쉬움
- ❑ 효율성: 가상 머신보다 자원을 덜 사용하면서 더 많은 애플리케이션을 실행할 수 있음
- ❑ 빠른 배포: 컨테이너는 빠르게 시작되고 중지되어, 빠른 스케일링과 업데이트가 가능
- ❑ 격리: 각 애플리케이션이 독립적으로 실행되어 보안과 자원 관리가 용이





# 그래서 Docker를 왜 쓰는데?

- 도커는 떡볶이 밀키트와 같다

## 앱 개발 = 떡볶이 만들기

- 1. 재료 준비 (코드 작성)
  - 떡, 어묵, 고추장 등의 재료 = 프로그래밍 언어, 라이브러리, 프레임워크
- 2. 조리 과정 (앱 개발)
  - 재료를 씻고, 썰고, 볶는 과정 = 코딩, 디버깅, 테스트
- 3. 레시피 (개발 문서)
  - 조리 순서와 방법 = 개발 가이드, 주석, README 파일

## 배포 = 포장 (패키징)

- 1. 밀키트 패키지 (도커 컨테이너)
  - 모든 재료와 소스를 정확한 양으로 담은 패키지 = 앱과 모든 종속성을 포함한 컨테이너
- 2. 패키지 설명서 (Dockerfile)
  - 밀키트 조리 방법 = 컨테이너 빌드 및 실행 지침
- 3. 진공 포장 (이미지 생성)
  - 신선도 유지를 위한 포장 = 앱의 현재 상태를 이미지로 저장





# 그래서 Docker를 왜 쓰는데?

- 도커는 떡볶이 밀키트와 같다

## 호스팅 = 판매 (서빙)

1. 편의점 진열대 (클라우드 서버)
  - 밀키트를 진열하는 공간 = 앱을 실행하는 서버 환경
2. 구매 및 조리 (배포 및 실행)
  - 고객이 밀키트를 사서 조리 = 사용자가 앱에 접근하여 사용
3. 프랜차이즈 (스케일링)
  - 여러 지점에서 동일한 밀키트 판매 = 여러 서버에서 동일한 앱 실행

## 도커의 장점 (밀키트 비유)

1. 일관성
  - 어느 주방에서 조리해도 동일한 맛 = 어느 환경에서 실행해도 동일한 동작
2. 이식성
  - 어느 편의점에서도 동일한 밀키트 판매 가능 = 어느 서버에서도 동일하게 실행 가능
3. 효율성
  - 필요한 양만큼만 재료 제공 = 필요한 리소스만 사용
4. 확장성
  - 수요에 따라 밀키트 수량 조절 용이 = 트래픽에 따른 컨테이너 수 조절 용이





# DVWB 호스팅하기

- DVWB 설치하기

1. 터미널 창을 연다. (CMD 혹은 git bash)

2. 하단의 명령어를 입력한다

```
git clone https://github.com/ethicalhack3r/DVWA
```

3. 클론받은 후, 해당 폴더로 들어가서 터미널 창을 연다 (CMD)

4. 하단의 명령어를 입력한다

```
docker compose up -d
```

5. 브라우저에 주소창에 localhost:4820 을 쳐서 들어간다.

6. admin/password로 로그인해준다.





# DVWB란?

- 취약점이 가득한 펜테스팅용 웹

## □ DVWA란?

- PHP/MySQL 기반의 의도적으로 취약한 웹 애플리케이션
- 웹 보안 학습 및 테스트를 위해 설계됨

## □ DVWA의 목적

- 보안 전문가, 개발자, 학생들의 실습 환경 제공
- 다양한 웹 취약점 탐지 및 해결 방법 학습
- 보안 도구 테스트 플랫폼

## □ DVWA에 포함된 주요 취약점

- SQL 인젝션
- 크로스 사이트 스크립팅(XSS)
- 불안정한 파일 업로드
- 크로스 사이트 요청 위조(CSRF)
- 명령어 실행
- 기타 다양한 웹 보안 취약점

## □ DVWA 사용 시 주의사항

- 교육 및 학습 목적으로만 사용
- 실제 운영 환경에 배포 금지
- 법적, 윤리적 가이드라인 준수





## ■ 난이도 설정

□ 난이도가 초반에는 Impossible 로 되어 있을 텐데, 왼쪽 하단의 DVWA Security 페이지로 가서 Low 로 바꿔준다.





- Brute force 공격 실습

## □ Brute Force Attack이란?

- 시스템의 비밀번호나 암호키를 찾아내기 위해 가능한 모든 값을 대입해보는 공격 방식
- 단순하지만 시간이 많이 소요되는 공격 방법

## □ Brute Force Attack의 작동 원리

- 가능한 모든 문자 조합 생성
- 각 조합을 대상 시스템에 입력
- 성공할 때까지 반복





## ■ Brute force 공격 실습

### □ Brute Force Attack의 유형

- 단순 Brute Force: 모든 가능한 조합 시도
- 사전 공격: 미리 정의된 단어 목록 사용
- 하이브리드 공격: 사전 공격과 단순 Brute Force의 조합

### □ Brute Force Attack의 위험성

- 충분한 시간과 리소스가 있다면 거의 모든 암호 해독 가능
- 약한 암호나 짧은 암호에 특히 취약
- 계정 잠금, 시스템 과부하 등의 부작용 발생 가능

### □ Brute Force Attack 방어 방법

- 강력한 비밀번호 정책 시행 (길이, 복잡성)
- 계정 잠금 정책 구현
- 다중 인증(MFA) 사용
- CAPTCHA 등의 추가 보안 계층 도입
- 로그인 시도 모니터링 및 이상 징후 탐지







## ■ Brute force 공격 실습

Brute Force 탭에 들어가서 로그인해보기  
맞는 계정 : admin/password  
틀린 계정 : 그 외

[Home](#)  
[Instructions](#)  
[Setup / Reset DB](#)  
**Brute Force**  
[Command Injection](#)  
[CSRF](#)  
[File Inclusion](#)  
[File Upload](#)  
[Insecure CAPTCHA](#)  
[SQL Injection](#)  
[SQL Injection \(Blind\)](#)  
[Weak Session IDs](#)  
[XSS \(DOM\)](#)  
[XSS \(Reflected\)](#)  
[XSS \(Stored\)](#)

### Vulnerability: Brute Force

**Login**  
Username:  
  
Password:  
  
  
  

Username and/or password incorrect.

**More Information**

- [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](https://owasp.org/www-community/attacks/Brute_force_attack)
- <https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <https://www.golinuxcloud.com/brute-force-attack-web-forms>

[Home](#)  
[Instructions](#)  
[Setup / Reset DB](#)  
**Brute Force**  
[Command Injection](#)  
[CSRF](#)  
[File Inclusion](#)  
[File Upload](#)  
[Insecure CAPTCHA](#)  
[SQL Injection](#)  
[SQL Injection \(Blind\)](#)  
[Weak Session IDs](#)

### Vulnerability: Brute Force

**Login**  
Username:  
  
Password:  
  
  
  
Welcome to the password protected area admin  






# DVWB

## ■ Brute force 공격 실습

로그인을 할 때 proxy > interceptor를 켜고 실험해보자!

GET 요청으로 id와 pw를 보내는 걸 알 수 있다.

우클릭해서 send to Intruder

The screenshot shows the Burp Suite interface with the DVWA login page on the left. The login form has fields for Username (admin) and Password (\*\*\*\*\*), and a Login button. The right panel shows the HTTP history and the interceptor settings. The 'Intercept on' button is highlighted, and the 'Send to Intruder' option is selected in the context menu. The request details show a GET request to http://localhost:4280/vulnerability/ with query parameters username=admin&password=\*\*\*\*\*&login=Login.

**Request Details:**

- Time: 07:48:50.12
- Type: HTTP
- Direction: Request
- Host: localhost
- Method: GET
- URL: http://localhost:4280/vulnerability/
- Status code: 200
- Length: 1024

**Request Body:**

```
GET /vulnerabilities/brute/ HTTP/1.1
Host: localhost:4280
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
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=0.7
```



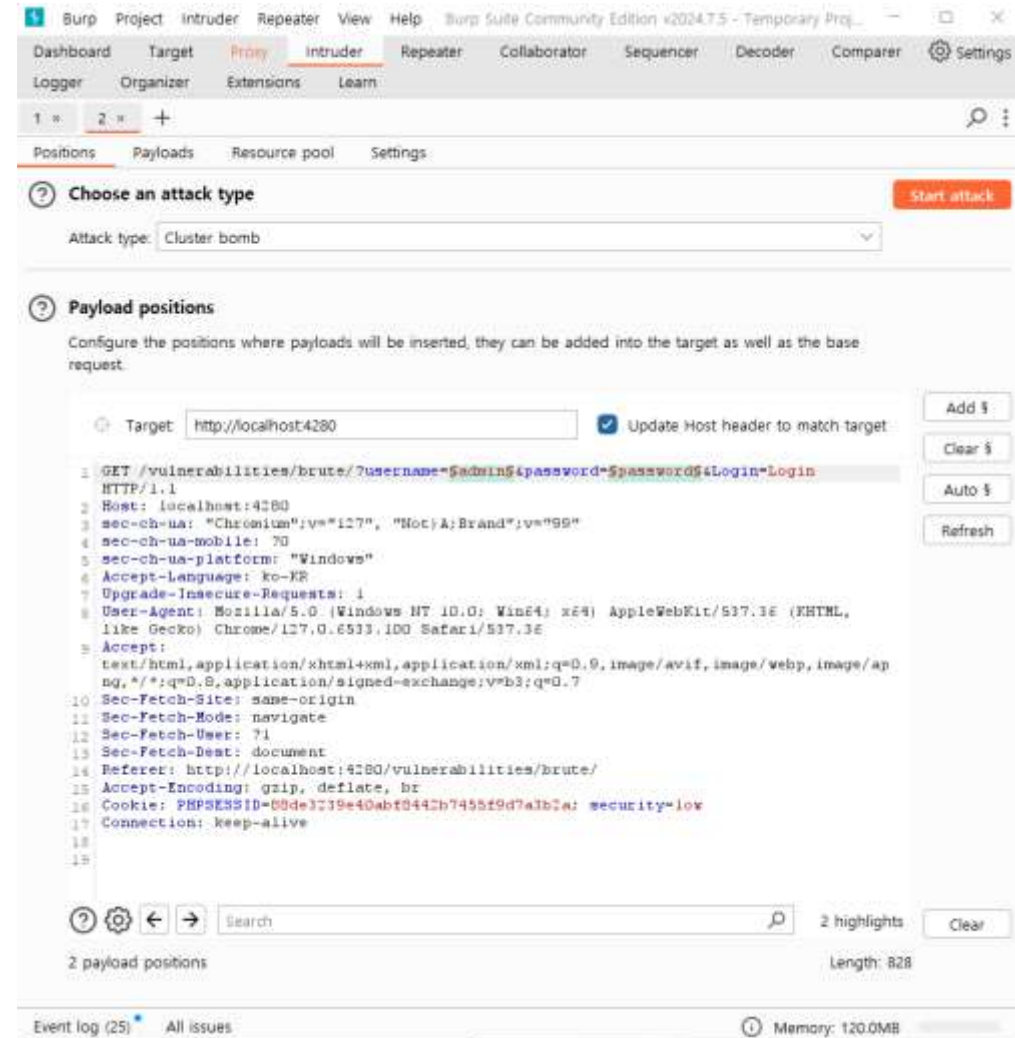


- Brute force 공격 실습

Introder로 와서,  
Attack type은 Cluster bomb로  
설정 (2개 이상일 때에는  
single이 아니라 cluster로 설  
정해줘야 함)

Payload positions에서 id 영역  
과 pw 영역에 드래그를 한 후,  
Add \$ 버튼을 눌러서 추가해  
주자.

(그림 안 보이면 키워서 확대)





## ■ Brute force 공격 실습

다음에는 Payloads에 들어간다.  
Payload sets 가 총 1개 있을 텐데,  
payload set 1(id)부터 세팅해준다.  
Enter a new item에 넣어보고 싶  
은 문자열을 넣은 후, Add를 해 주  
면 된다. 지우고 싶으면 클릭 후  
Remove

1 x 2 x +

Positions Payloads Resource pool Settings

**Payload sets** Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 6

Payload type: Simple list Request count: 30

**Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate Add Add from list ... [Pro version only]

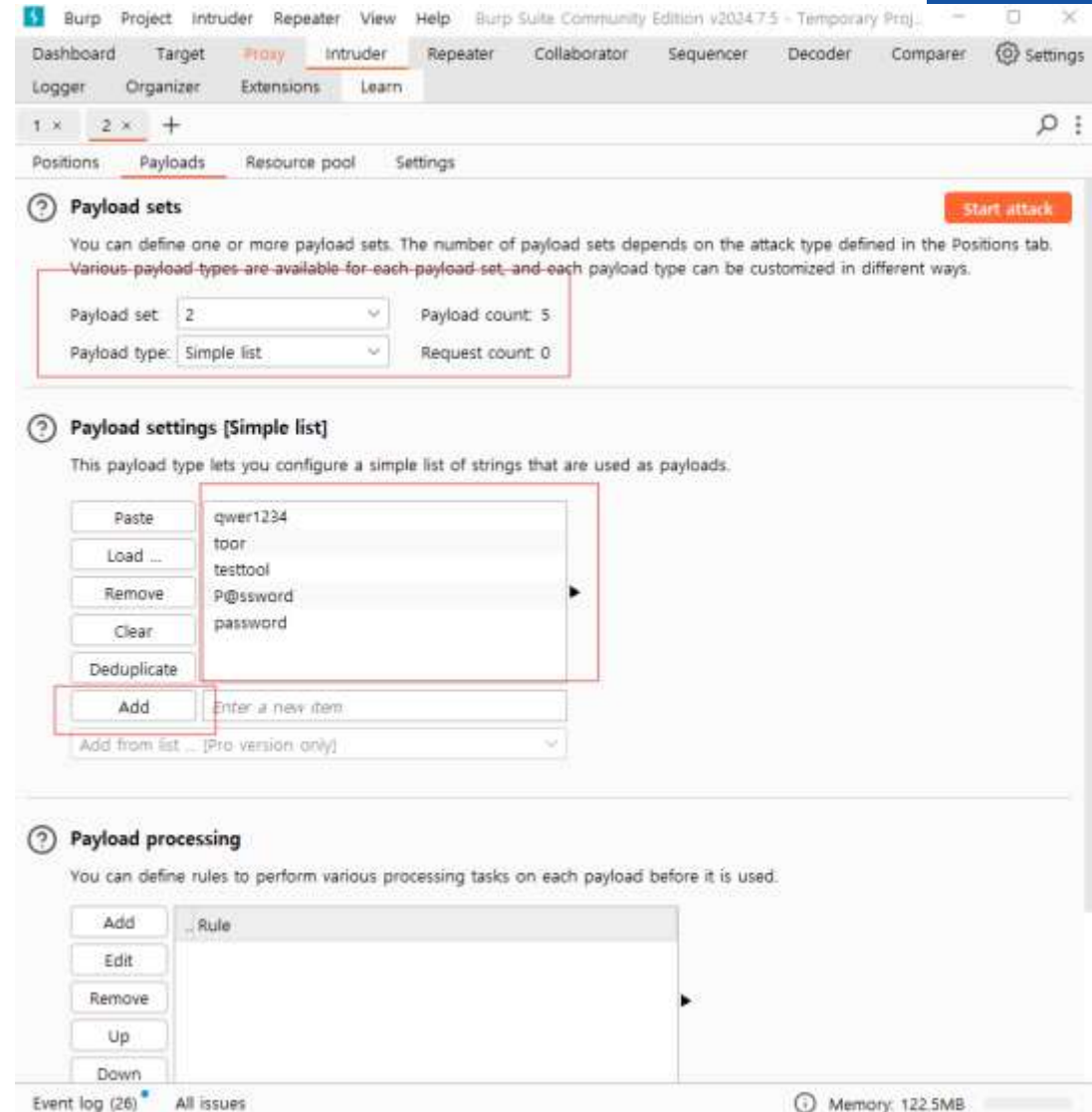
yeji  
security  
admin  
Administrator  
root





## ■ Brute force 공격 실습

다 설정했으면 Payload sets에서 Payload set 2(password)로 설정한 후, Payload settings에 비밀번호 후보들을 입력한다.





## ■ Brute force 공격 실습

다음은 settings > Grep – Match를 설정한다.

먼저 clear를 눌러서, 리스트에 있는 문자열을 다 지운 후, 성공했을 때 나타났던 문자열인 welcome to the password protected area admin을 입력해서 Add 해준다.

위에 있는체크박스인 Flag result items with responses matching these expressions:를 해준다.



### 3. Intruder attack of http://localhost:4280

Results

Positions

Payloads

Resource pool

Settings



#### Attack results



These settings control what information is captured in attack results.

- ☒ Store requests
- ☒ Store responses
- ☒ Make unmodified baseline request
- ☐ Use denial-of-service mode (no results)
- ☐ Store full payloads



#### Grep - Match



These settings can be used to flag result items containing specified expressions.

- ☒ Flag result items with responses matching these expressions:

Paste Load ... Remove Clear

welcome to the password protected area admin

Add Enter a new item

Match type: ☒ Simple string

☐ Regex

☐ Case sensitive match

☒ Exclude HTTP headers





- Brute force 공격 실습

다시 Payloads 탭으로  
돌아가서  
Start attack 버튼을 누른  
다.

1 x 2 x +

Positions Payloads Resource pool Settings

**Payload sets** Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 6

Payload type: Simple list Request count: 30

**Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate Add Add from list ... [Pro version only]

yeji  
security  
admin  
Administrator  
root







## ■ Brute force 공격 실습

로딩후에, 모든 조합을 시도해보며 맞는 조합을 찾는다. Welcome..탭에 보면 1이라고 되어 있는 조합이 있다! 눌러보면 해당 조합이 맞는 id/pw조합이 된다.

The screenshot shows the Burp Suite interface during an intruder attack. The top window displays the 'Intruder attack results filter: Showing all items' table, which lists the results of the brute force attack. The bottom window shows the 'Response' view for the selected request, displaying the HTML content of the response.

Request	Payload 1	Payload 2	Status code	Response	Error	Timeout	Length	welcom...	Comment
17	security	P@ssword	200	4			4645		
18	admin	P@ssword	200	5			4646		
19	Administrator	P@ssword	200	5			4646		
20	root	P@ssword	200	5			4646		
21	yeji	password	200	5			4646		
22	security	password	200	6			4646		
23	admin	password	200	4			4684	1	
24	Administrator	password	200	5			4646		
25	root	password	200	5			4646		

```
<div id="main_body">
  <div class="body_padded">
    <h1>
      Vulnerability: Brute Force
    </h1>
    <div class="vulnerable_code_area">
      <h2>
        Login
      </h2>
      <form action="#" method="GET">
        Username:<br />
        <input type="text" name="username">
        <br />
        Password:<br />
        <input type="password" AUTOCOMPLETE="off" name="password">
        <br />
        <br />
        <input type="submit" value="Login" name="login">
      </form>
      <p>
        Welcome to the password protected area admin
      </p>
      
    </div>
    <h2>
      More Information
    </h2>
  </div>
</div>
```





# CTF 문제 풀어보기

쿠키 조작하기



- cookie

cookie | 워게임 | Dreamhack | 워게임 | Dreamhack



프로젝트를 기획하는 방법

# 팀 프로젝트



# 프로젝트 기획

- 정의

- 프로젝트 기획의 정의

- 목표 설정, 요구사항 분석, 자원 할당, 일정 수립 등을 포함하는 종합적 과정

- 기획의 중요성

- 명확한 방향 제시
  - 리스크 최소화
  - 효율적인 자원 활용
  - 이해관계자 간 의사소통 촉진





# 프로젝트 기획

## 2. 프로젝트 기획 과정 개요

- 전체 과정 도식화: 아이디어 정의 → 서비스 구체화 → 청사진 작성 → 시스템 설계 → UI/UX 설계 → 구현 계획 → 테스트 계획 → 배포 전략 → 유지보수 계획
- 각 단계별 핵심 목표:
  - 아이디어 정의: 문제 인식 및 해결책 구상
  - 서비스 구체화: 기능 및 요구사항 명세
  - 청사진 작성: 전체 프로젝트 로드맵 수립
  - 시스템 설계: 기술적 아키텍처 설계
  - UI/UX 설계: 사용자 중심의 인터페이스 설계
  - 구현 계획: 개발 전략 및 일정 수립
  - 테스트 계획: 품질 보증 전략 수립
  - 배포 전략: 서비스 출시 및 운영 계획
  - 유지보수 계획: 지속적인 개선 및 관리 방안





# 프로젝트 기획

## ■ 3. 소프트웨어 개발 방법론

### □ 워터폴 모델

- 특징: 순차적, 단계별 접근
- 장점: 명확한 단계 구분, 문서화 용이
- 단점: 변경에 대한 유연성 부족
- 적합한 프로젝트: 요구사항이 명확하고 변경이 적은 프로젝트

### □ 애자일 방법론

- 특징: 반복적, 점진적 개발
- 장점: 유연성, 빠른 피드백 반영
- 단점: 초기 계획의 불확실성
- 적합한 프로젝트: 요구사항 변경이 잦은 프로젝트

### □ 방법론 선택 기준

- 프로젝트 규모 및 복잡성
- 팀의 경험과 선호도
- 고객의 요구사항 변경 가능성





# 프로젝트 기획

## ■ 4. 아이디어 정의 방법

### □ 브레인스토밍 기법

- 자유로운 아이디어 제시
- 판단 유보, 양적 생산 강조 아이디어 결합 및 개선

### □ 문제 정의 방법

- 5Whys 기법: 근본 원인 파악
- 문제 명세서 작성: 현재 상태와 목표 상태 명확화

### □ 타겟 사용자 분석 기법

- 페르소나 생성: 가상의 대표 사용자 프로필 작성
- 사용자 조사: 설문, 인터뷰, 관찰 등

### □ 시장 조사 방법

- SWOT 분석: 강점, 약점, 기회, 위협 요인 분석
- 경쟁사 분석: 주요 경쟁사의 특징 및 차별점 파악





# 프로젝트 기획

## ■ 5. 서비스 구체화 기법

### □ 기능 명세서 작성법

- 사용자 스토리 작성: "사용자로서, 나는 [기능]을 원한다. 그 이유는 [가치]때문이다."
- 기능 분류: 핵심 기능, 부가 기능, 향후 개발 기능

### □ 우선순위 결정 방법

- MoSCoW 방법: Must have, Should have, Could have, Won't have
- 가치 vs 노력 매트릭스: 구현 난이도 대비 사용자 가치 평가

### □ 차별화 전략 수립 방법

- USP(Unique Selling Proposition) 정의
- 블루오션 전략: 가치 혁신을 통한 새로운 시장 창출

### □ 기술적 요구사항 분석

- 필요 기술 스택 선정
- 확장성 및 성능 요구사항 정의







# 프로젝트 기획

## ■ 6. 프로젝트 청사진 작성법

### □ 범위 설정 기법

- WBS(Work Breakdown Structure) 작성: 프로젝트를 작업 단위로 분할
- 범위 선언서 작성: 포함 사항과 제외 사항 명확화

### □ 일정 계획 수립 방법

- 간트 차트 작성: 작업별 일정을 시각화
- 크리티컬 패스 분석: 프로젝트 완료에 필수적인 작업 경로 식별

### □ 리소스 계획 방법

- 인력 자원 계획: 필요 인력 및 역할 정의
- 예산 계획: 비용 추정 및 예산 할당





# 프로젝트 기획

## 6. 프로젝트 청사진 작성법

### □ WBS, 간트 차트



제작 일정

(수행 기간 : 2019년 03월 15일 ~ 2019년 06월 10일)										
작품 제작 내용	3월 15일	3월 25일	4월 3일	4월 13일	4월 23일	5월 3일	5월 13일	5월 23일	6월 2일	6월 10일
자료 수집										
작품 설계										
모바일 어플리케이션 개발										
인공지능 학습										
관리자 웹 서버 개발										
테스트 및 디버깅										
최종 검증										





# 프로젝트 기획

## ■ 7. 시스템 설계 기법

### □ 시스템 아키텍처 설계 방법

- 3-tier 아키텍처: 프레젠테이션, 비즈니스 로직, 데이터 계층 구분
- 마이크로서비스 아키텍처: 기능별 독립적 서비스 구성

### □ UML 다이어그램 활용법

- 유스케이스 다이어그램: 사용자와 시스템 간 상호작용 표현
- 클래스 다이어그램: 시스템의 정적 구조 표현
- 시퀀스 다이어그램: 객체 간 상호작용의 시간적 흐름 표현

### □ 데이터 흐름 모델링 기법

- DFD(Data Flow Diagram) 작성: 데이터의 입력, 처리, 저장, 출력 과정 시각화
- ERD(Entity-Relationship Diagram) 작성: 데이터베이스 구조 설계

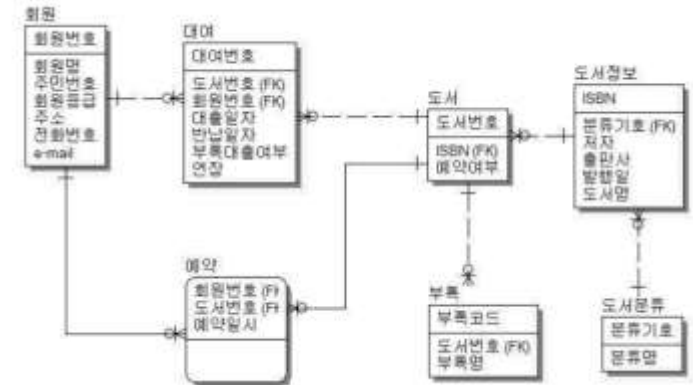
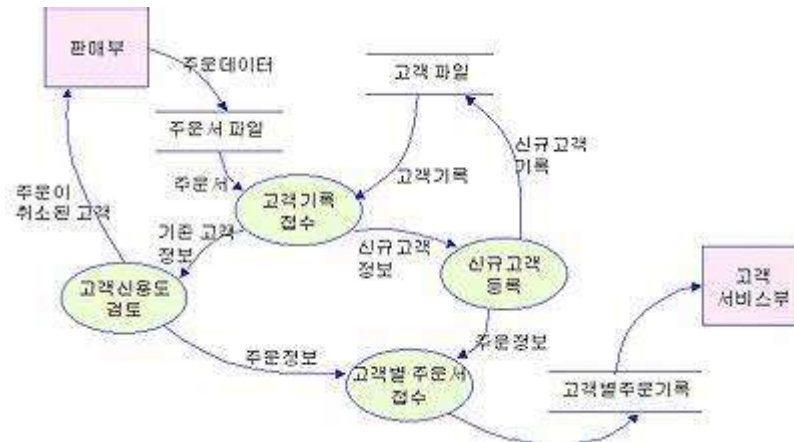
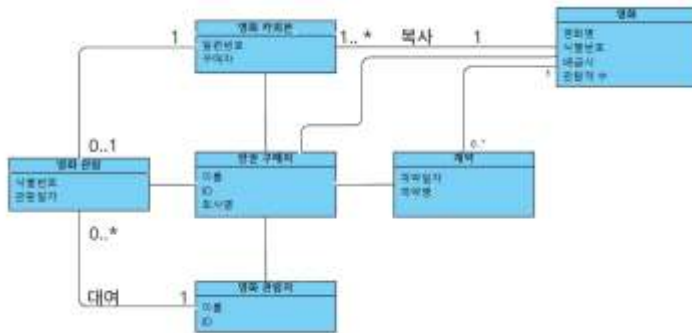




# 프로젝트 기획

## 7. 시스템 설계 기법

### UML, DFD, ERD





# 프로젝트 기획

## ■ 8. UI/UX 설계 방법

### □ 와이어프레임 작성법

- 로우 피델리티 와이어프레임: 기본 레이아웃 및 구조 설계
- 하이 피델리티 와이어프레임: 세부 디자인 요소 포함

### □ 프로토타입 제작 도구 소개

- Figma, Adobe XD, Sketch 등 툴 비교
- 인터랙티브 프로토타입 제작 방법

### □ 사용자 경험 설계 원칙

- 사용성 5대 원칙: 학습성, 효율성, 기억성, 오류, 만족도
- 정보 아키텍처 설계: 메뉴 구조 및 네비게이션 설계

### □ 사용자 테스트 방법

- A/B 테스트: 두 가지 버전 비교 테스트
- 사용성 테스트: 실제 사용자를 대상으로 한 관찰 및 피드백 수집

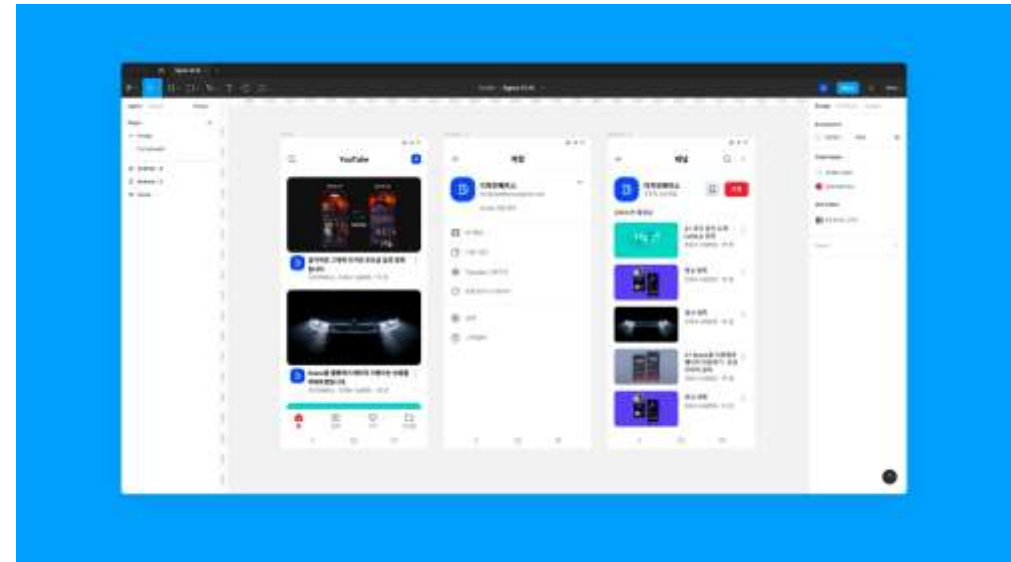
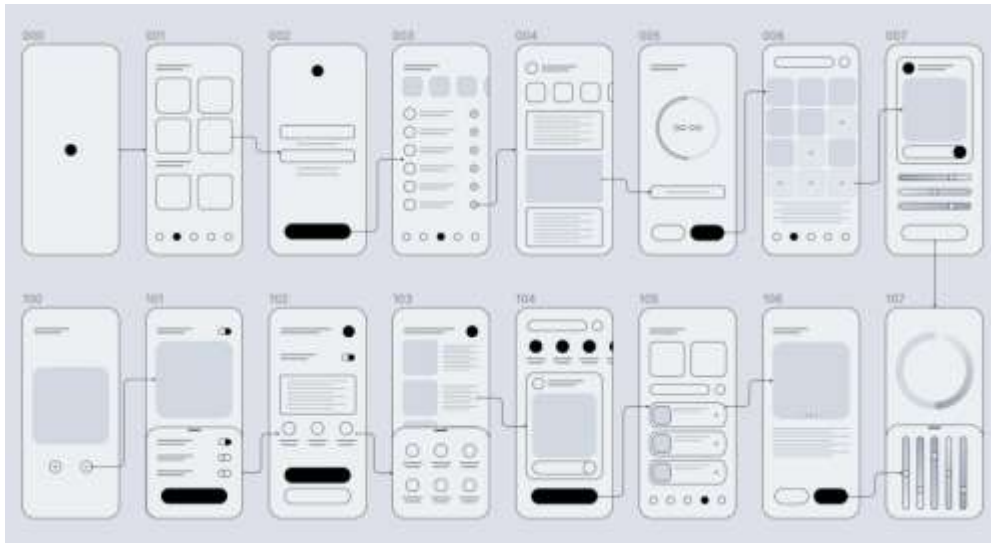




# 프로젝트 기획

## ■ 8. UI/UX 설계 방법

### □ 와이어프레임, 피그마





# 프로젝트 기획

## ■ 9. 구현 계획 수립 방법

### □ 개발 환경 설정 가이드

- 버전 관리 시스템 선택 (e.g., Git)
- 개발 프레임워크 및 라이브러리 선정
- CI/CD 파이프라인 구축 방안

### □ 코딩 표준 및 가이드라인 설정 방법

- 코드 스타일 가이드 작성
- 코드 리뷰 프로세스 설계
- 문서화 규칙 수립

### □ 버전 관리 전략 수립 방법

- Git-flow 또는 GitHub-flow 채택
- 브랜치 전략 수립
- 릴리스 관리 계획





# 프로젝트 기획

## ■ 10. 테스트 계획 수립 기법

### □ 테스트 케이스 작성법

- 기능 테스트: 각 기능의 정상 동작 확인
- 경계값 분석: 입력값의 경계 조건 테스트
- 예외 처리 테스트: 오류 상황에 대한 대응 확인

### □ 다양한 테스트 방법론 소개

- 단위 테스트: 개별 모듈/함수 테스트
- 통합 테스트: 모듈 간 상호작용 테스트
- 시스템 테스트: 전체 시스템 동작 테스트
- 성능 테스트: 부하 테스트, 스트레스 테스트

### □ 테스트 자동화 도구 소개

- 단위 테스트 프레임워크: JUnit, PyTest 등
- UI 테스트 도구: Selenium, Cypress 등  
성능 테스트 도구: JMeter, Gatling 등







# 프로젝트 기획

- 중요한 것

- 요구 사항(구현하고자 하는 것)이 명확할 것
- 역할과 기한이 명확할 것

-각 팀별로 공모전 준비 및 프로젝트 기획 시작-

-거창하게 할 필요 없고, 매 주차 목표 설정-





# 팀 구성 (10분)

## ■ 팀원

- 팀끼리 모여앉기
- 팀별 스터디 주제 및 공모전 정하기
- 일정 및 역할 기획하기

	4명	4명	5명	5명
기획부	최선영(22)	유예지(20)	정서윤(22)	문수연(new,23)
신입부원	강서윤(23)	김예원(24)	김서현(24)	
		박다연(23)		
6기				김선우(22)
7기(20)	이정연(20)		김민지(20)	
7기(21)		김하연(21)		한도희(21)
7기(22)			이연우(22)	김진서(22)
7기(23)			송윤경(23)	박유채(23)
7기(24)	경서연(24)			
평균	22.25	22	22.2	22.2



# 공지

행사 및 과제 안내



# 행사 안내

- 용보공 마스코트 그리기 컨테스트 연장
- 용보공 굿즈를 위한 마스코트 디자인 경진대회
  - 수룡이 + 용보공 로고 OR 자물쇠 모양
  - 뭐가 되었든 보안을 표현하면서도 굿즈로서의 가치가 있는 마스코트
  - 대동제 상품으로 걸릴 예정
  - 디자인에 관심있거나 그림이 취미이신 분들 가볍게 도전해주세요!
- 대회 안내
  - 9월 6일~9월 17일
  - 18일 투표 후 굿즈 제작
  - 화질은 선명하게, 그림은 크게! (PNG 혹은 일러스트 선호)
  - 유예지에게 개인 카톡으로 제출
- 상품
  - 설빙 1만원권 혹은 그에 준하는 상품





# 행사 안내

- 교수님 포토카드 디자인 경진대회
- 용보공 굿즈를 위한 이일구 교수님 포토카드 디자인 경진대회
  - 이일구 교수님의 공식적인 허락을 받은 공식 포토카드 굿즈 제작
  - 20매 한정 제작(같은 디자인)
  - 뉴스에 있는 이일구 교수님의 사진을 편집해서 유예지에게 개인 카톡으로 제출
- 대회 안내
  - 9월 6일~9월 17일
  - 18일 투표 후 굿즈 제작 (일정 앞당겨질 가능성 있습니다)
  - 포토카드 사이즈 : 59x89 (mm)
  - 고해상도 사진
  - 투명 포토카드도 제작 가능하니 png로 주셔도 됩니다.
- 상품
  - 상점, 본인이 디자인한 포토카드 1매





# 행사 안내

## ■ 대동제

### □ 용보공 대동제 부스 참여

- 용보공 부스는 [참여형 부스]로, 암호 퀴즈&미니게임&뽑기 등으로 진행
- 25일, 26일 15시~19시 부스 진행위원 모집 (김선우 회장님께 연락)

### □ 용보공 대동제 퀴즈 출제

- 암호 퀴즈 부스인 만큼 퀴즈가 필요합니다.
- 학생들이 가볍게 맞출 수 있고, 흥미를 느낄만한 퀴즈 3개 정도를 만 들어주세요. (객관식 가능)
- 각 팀별로 8문제 정도 제출
- 집에 미니게임 있으면 찬조 받습니다. 링 던지기 다트 등등





# 행사 안내

## ■ 재능기부 프로젝트

### □ 보안 관련 재능기부 활동

- 성북구 고등학생들을 대상으로 보안 이론,  
실습 수업을 통한 보안 인식 재고 및 보안 학과 진학 희망자 멘토링
- 활동 기간 : 한 학기 (24.9월 – 25.1월 / 5개월)
- 한 달에 한 번(금요일 or 토요일)
- 장소 : 프라임관 508호 예정
- 모든 일정에 참여하지 않아도 OK
- 재학생 우선, 휴학생 약간의 불이익(장학금 수혜 불가)
- 김선우 회장님께 자세한 사항 문의
- [링크](#)





# 이번주 과제

## ■ 회비 및 과제

### ☐ 대동제 퀴즈 제출

- ☐ 다음주까지

### ☐ 리뷰 작성

- ☐ 카페 리뷰 게시판에 리뷰 작성 (매주 리뷰 작성 필수/OT내용 및 피드백 작성)

### ☐ 과제

- ☐ 코딩테스트 1문제
- ☐ DVWA brute force(로그인 파트) medium or high (너무 어려우면 다른 문제 푸셔도 괜찮아요)

### ☐ 팀 프로젝트

- ☐ 팀별 계획서 과제게시판에 제출

### ☐ 개인발표 슬롯 작성

- ☐ 선착순(성신여자대학교 계정으로 접속)
- ☐ [링크](#)





**Thank you**

