



캡스톤 디자인이 계획 발표

클라우드 기반 가상 머신 네트워크 및 보안 아키텍처 설계



#2025-09-10

#계획 발표

#태훈 업고 튀어

#20201738 서민재

#20222517 한하영

#20222021 김주령



서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

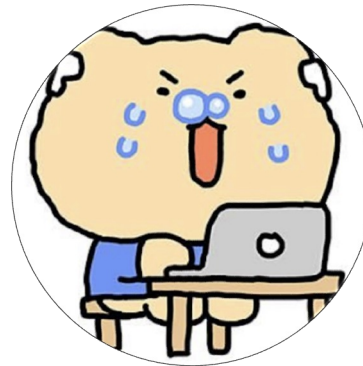
참고자료



한하영

프론트엔드

React, WebSocket,
Docker



김주령

백엔드

Spring Boot, Redis,
MySQL



서민재

가상머신 서버
Spring Boot,
Docker, K8S

무엇을 도와드릴까요?



서론

개요

주제 변경

구조도

주요 기능

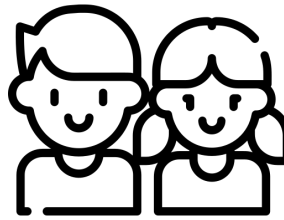
방학기간

계획

참고자료

📌 현재 발생하는 불편 사항

- 사용자가 어떠한 **프로그램을 사용**하기 위해서 해당 프로그램을 지원하는 **운영체제를 설치**해야 하는 과정 **필연적**.
(예시 : gdb, pwndbg → 리눅스에서 작동)
- 비전공자/초보자들에게는 해당 프로그램을 사용하기 위한 운영체제 **설치 과정**에서 오류 등의 **어려움** 발생
- 주니어 개발자 / 시니어 개발자들 또한 개발환경과 운영환경 간의 차이로 인하여 서버/운영체제 학습 별도 필요
- 잠깐 사용 후 사용하지 않을 경우 **컴퓨터 자원 낭비**



비전공자, 초보자



gdb: GNU debugger, 리눅스의 대표적인 디버거
pwndbg : gdb의 플러그인



서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

참고자료

위 문제를 해결하기 위한 다른 도구들이 다수 존재하지 않은가?



가상화 기술
QEMU(Quick Emulator)

하드웨어 및 운영체제를
가상화하여 실행할 수 있는 도구

속도가 느리고 어려움



컨테이너 기술
Docker

하드웨어 리소스를 적게 사용하여
애플리케이션과 필요한 환경을 컨테이너로
독립적인 실행시켜 배포하는 도구

사전 지식 학습 필요 및 보안 위협



클라우드 기술
AWS

사용자가 하드웨어 구매/유지보수 필요 없이
필요한 만큼만 IT 자원을 빌려서 사용
인터넷을 통한 IT 인프라 제공 기술

사전 지식 요구 및 비용부담

각각 단점들이 존재

서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

참고자료

📌 현재 발생하는 불편 사항

하드웨어 적 한계, 기술의 어려움의 한계, 비용의 한계로 인하여, 새로운 초보 개발자, 비전공자 들의 프로그램 이용의 **진입장벽**이 높아지고 있음



저게 다 뭐지...? 저거를 알아야 해당 서비스를 이용할 수 있는 건가..? 뭘 팔아서 사용해야하네..

서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

참고자료

프로젝트 목표 및 비전

No Hardware Restrictions

Supports multiple OS

Unlimited space

People who use Computer

No time constraints



Secure and Reliable

사용자가 요청하는 **운영체제**를 짧은 기간동안 **1회용**으로 생성
편리하게 이용할 수 있는 웹 기반 서비스

서론

개요

주제 변경

구조도

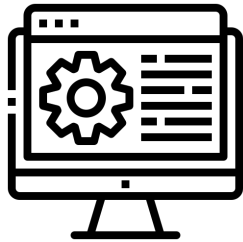
주요 기능

방학기간

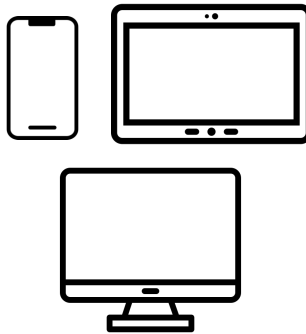
계획

참고자료

기대 효과는?



불필요한 프로그램 설치
관리 미필요



어떤 디바이스 환경에서도
쉽고 빠른 접근



손 쉬운 서버 관리 및
편리한 서버 상태 확인



실시간 악의적 이용
빠른 대응

서론

개요

주제 변경

구조도

주요 기능

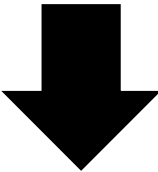
방학기간

계획

참고자료

📌 주제 변경 사유

AWS 활용 가상 머신 네트워크 시스템 구축 및 취약점 분석과 대응 솔루션 개발



클라우드 기반 가상 머신 네트워크 및 보안 아키텍처 설계

AWS에 한정하지 않는 아키텍처

클라우드에 맞는 보안 시스템 구축을 위한
아키텍처 설계

조금 더 확장되고 클라우드에 맞춰진 주제 이름 변경

서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

참고자료

왜 이렇게 변경하였는가?

기존 환경

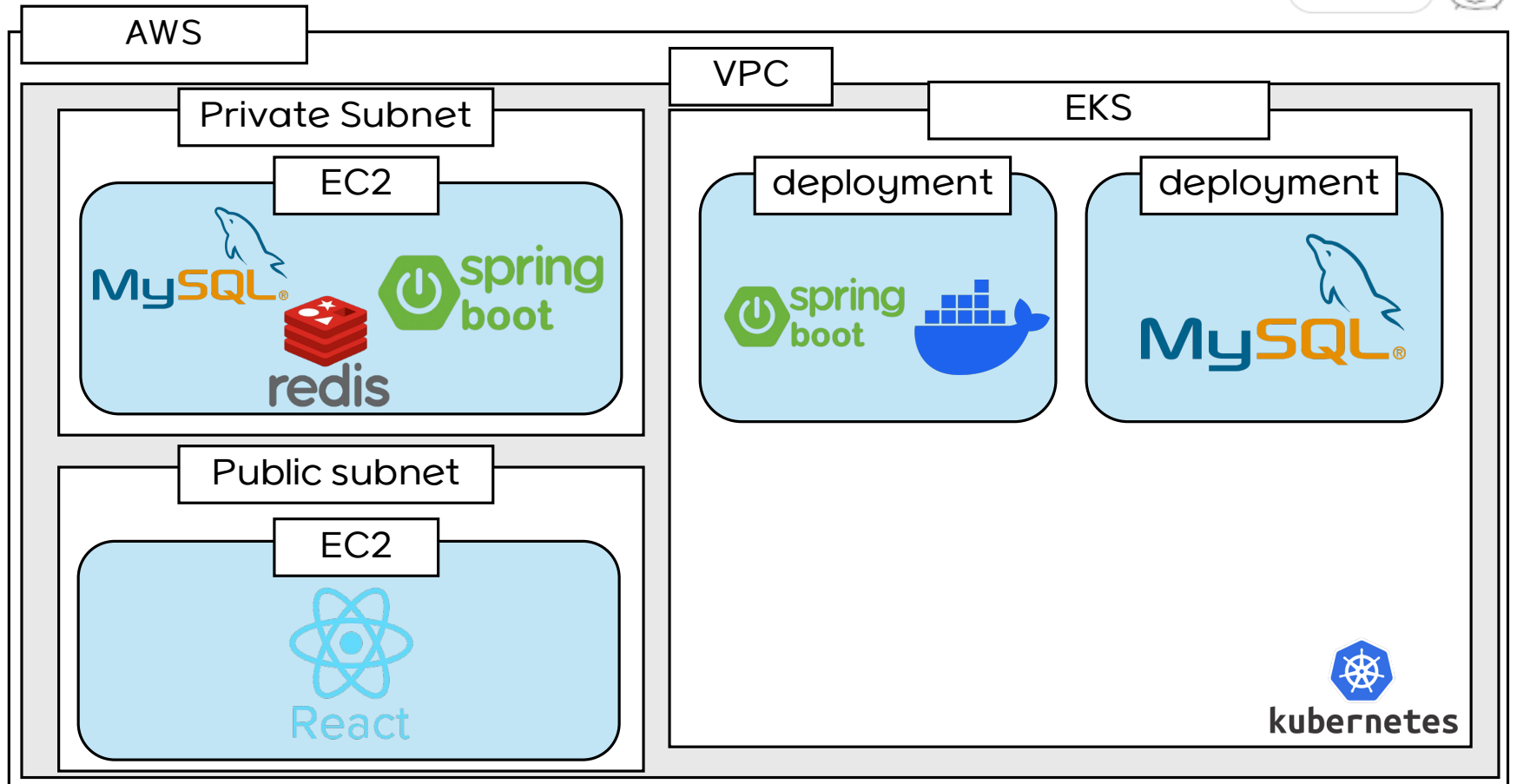
- 사후 대응 중심 (침해 발생 후 분석 및 패치)
- 직접 보안 솔루션 구축(방화벽, IDS, IPS...)
- 직접 유지보수, 패치, 로그 수집
- 보안 책임 → 사용자가 직접 모든 책임 부담

변경 된 클라우드 환경

- 사전 대응 중심 (설계 단계 중심 대응)
- 관리형 서비스(WAF, Shield, GuardDuty)
- 자동화 기반 운영(IaC 로그 수집/ 분석)
- 공동 책임 모델

클라우드의 **공동 책임 모델** 및 **자동화 중심 운영** 철학과 맞지 않아,
클라우드에 적합한 보안 아키텍처 중심으로 주제 수정

- 서론
- 개요
- 주제 변경
- 구조도**
- 주요 기능
- 방학기간
- 계획
- 참고자료



서론

개요

주제 변경

구조도

주요 기능

방학기간

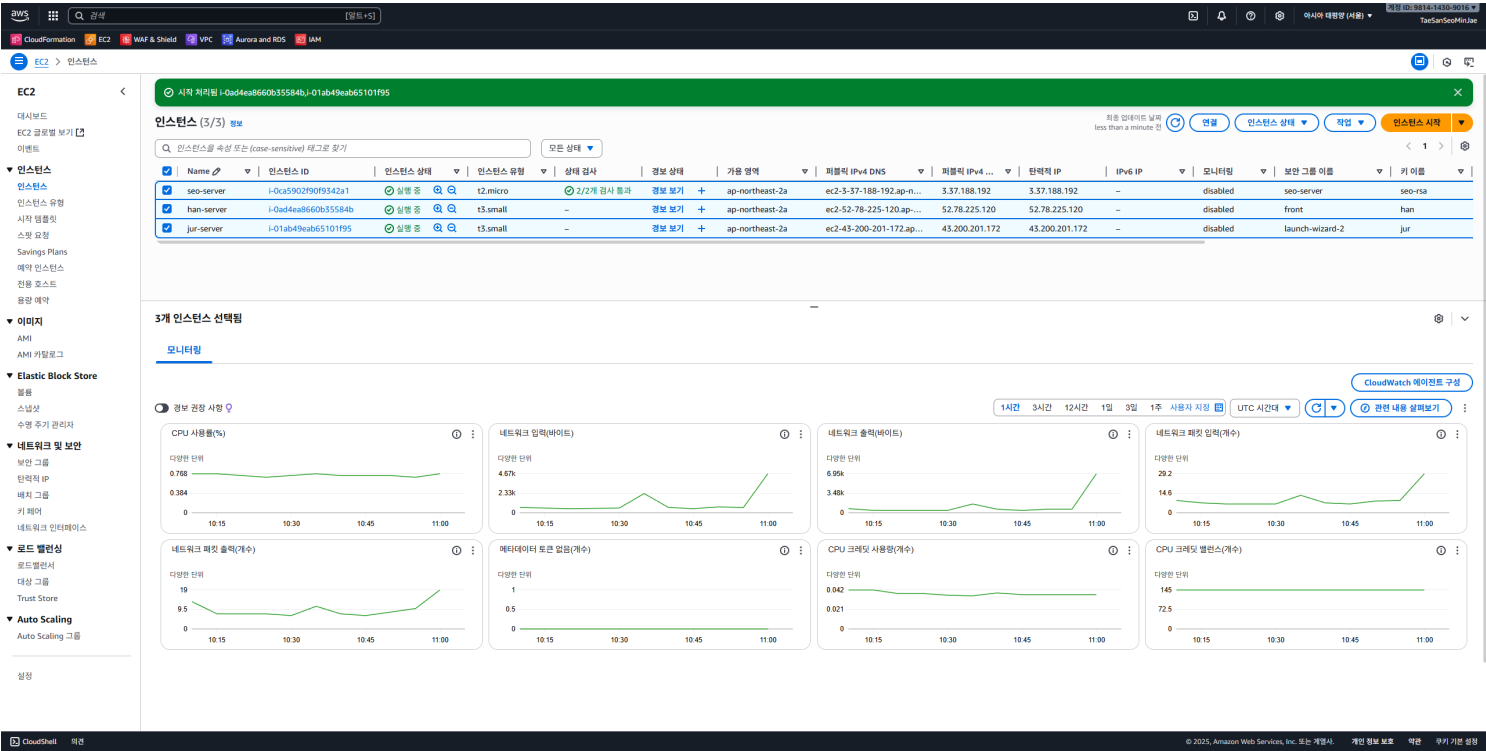
계획

참고자료

역할 이름	신뢰할 수 있는 개체	마지막 활동
AmazonEKSPodIdentityAmazonCloudWatchObservabilityRole	AWS 서비스: pods.eks	-
aws-elasticbeanstalk-service-role	AWS 서비스: elasticbeanstalk	-
AWSServiceRoleForAmazonEKS	AWS 서비스: eks (서비스 연결 역할)	15분 전
AWSServiceRoleForElasticLoadBalancing	AWS 서비스: elasticloadbalancing (서비스 연결 역할)	506일 전
AWSServiceRoleForRDS	AWS 서비스: rds (서비스 연결 역할)	42분 전
AWSServiceRoleForSupport	AWS 서비스: support (서비스 연결 역할)	314일 전
AWSServiceRoleForTrustedAdvisor	AWS 서비스: trustedadvisor (서비스 연결 역할)	-
eks-cluster-role	AWS 서비스: eks	18분 전
rds-monitoring-role	AWS 서비스: monitoring.rds	-

IAM 정책 및 권한 설정

AWS 서비스 구축 (VPC, 서브넷, EC2)



서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

참고자료

TCAR 마이페이지

이곳은 TCAR 사이트입니다.

양방향 소통이 가능한 공간, 지금 바로 가입해 보세요!

http://52.78.225.120:3000/main

- 서론
- 개요
- 주제 변경
- 구조도
- 주요 기능
- 방학기간
- 계획
- 참고자료

백엔드 서버 구축 / CI/CD 환경 구축

```
version: '3.8'

services:
  mysql:
    image: mysql:8
    container_name: mysql
    restart: always
    environment:
      MYSQL_ROOT_PASSWORD: 2301
      MYSQL_DATABASE: tcar
      MYSQL_USER: appuser
      MYSQL_PASSWORD: appuserpass
    ports:
      - "3306:3306"
    volumes:
      - mysql_data:/var/lib/mysql

  app:
    build:
      context: ./app
    container_name: springboot
    restart: always
    environment:
      SPRING_DATASOURCE_URL: jdbc:mysql://mysql:3306/tcar?serverTimezone=UTC
      SPRING_DATASOURCE_USERNAME: appuser
      SPRING_DATASOURCE_PASSWORD: appuserpass
      # 필요 시 Redis, 기타 변수도 추가
    depends_on:
      - mysql
    ports:
      - "8080:8080"

  nginx:
    image: nginx:latest
    container_name: nginx
    restart: always
    ports:
      - "80:80"
    volumes:
      - ./nginx/nginx.conf:/etc/nginx/nginx.conf:ro
    depends_on:
      - app

volumes:
  mysql_data:
```

Swagger UI interface showing the OpenAPI definition for the application. The endpoints are categorized as follows:

- 댓글 좋아요 (comment likes):**
 - GET /comments/{commentId}/like: 댓글 좋아요 수 조회
 - POST /comments/{commentId}/like: 댓글 좋아요 토글
- 게시글 (posts):**
 - GET /posts/{postId}: 게시글 상세 조회
 - PUT /posts/{postId}: 게시글 수정
 - DELETE /posts/{postId}: 게시글 삭제

Github ci/cd, docker 이용

서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

참고자료

EKS 구축

클러스터 (1) 정보

클러스터 필터링

삭제

클러스터 생성

<

1

>

클러스터 이름	상태	Kubernetes 버전	지원 기간	정책 업그레이드	생성됨	공급자
TCAR_VM	활성	1.33	2026년 7월 29일까지 표준 지원	표준	42분 전	EKS

해당에 VM 서비스 구축 예정(CI/CD)

서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

참고자료

클라우드 / DVWA , AWS WAF, Endpoint 등 클라우드 보안 지식 학습

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module, however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users!)

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

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)

CSP Bypass

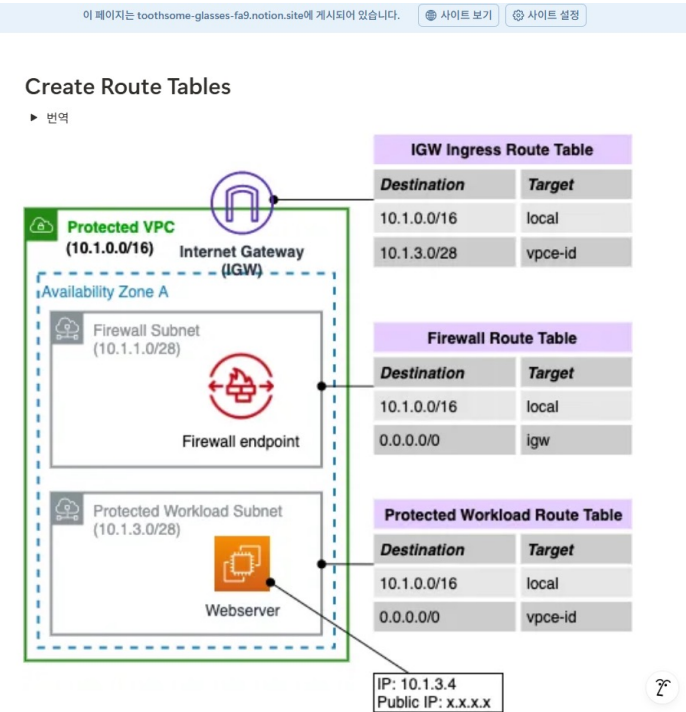
JavaScript

DVWA Security

PHP Info

About

Logout



이를 토대로 한 클라우드 서비스 재구축 필요(로드밸런스)

서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

참고자료

2학기 계획

월	세부 계획
7월	웹 취약점, 네트워크 취약점, 데이터 보호 취약점 사전 지식 학습(XSS, 포트 스캐닝..)
8월	클라우드에 대한 지식 학습, 이해 / 온프레미스 환경이 아닌 클라우드 환경으로 서비스 재정의 및 구축 필요
9월	클라우드에 맞는 보안 서비스 구축
10월	
11월	
12월	캡스톤디자인2 최종 발표
12월	-

클라우드 보안 아키텍처로 1학기 때 개발한 서비스 보안 위협으로부터 지키기

서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

참고자료

참고자료

홈페이지 해킹을 통한 내부망 장악 사례 분석
<https://www.lawtimes.co.kr/LawFirm-NewsLetter/182204>

보안 취약한 리눅스 SSH 서버에 ‘스캐너 악성코드’ 설치 주의
<https://www.boannews.com/media/view.asp?idx=125039>

중국 해커, 국내 90개 웹 사이트 DB 계정 정보 노출 등 추가 공격... 설날 공격 예고
<https://m.boannews.com/html/detail.html?idx=126317>

구름
<https://ide.goorm.io/my/dashboard>

리플릿
<https://replit.com/~>

Aws
<https://ap-northeast-2.console.aws.amazon.com/console/home?region=ap-northeast-2#>

ctf-d
<https://ctfd.io/>

서론

개요

주제 변경

구조도

주요 기능

방학기간

계획

참고자료

⚠️ **Thank you** ⚠️

발표가 종료되었습니다. 감사합니다.

ANY QUESTION?

태훈 업고 투어(TCAR) – 한하영, 서민재, 김주령