

2022 오픈소스 컨트리뷰션 아카데미

Open Source
Contribution
Academy



Project Discovery



Project Guide



주최



과학기술정보통신부

주관



정보통신산업진흥원





프로젝트 개요

프로젝트 분야 · 활용 언어 · Repository · 난이도 · 참가자 모집
유형 및 우대사항 등



1 프로젝트 개요

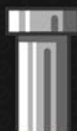
프로젝트 명 : Project Discovery

프로젝트 분야 : Security

프로젝트 저장소 : <https://github.com/projectdiscovery>

활용 언어 : Go, YAML

프로젝트 난이도 : 중~상





프로젝트 개요

참가자 모집 유형

- 보안 도구들을 사용해보신 경험이 있는 분
- 보안 분야에 관심이 많은 분
- Go언어로 개발 프로젝트 경험이 있는 분
- 자기주도적 학습이 가능하신 분

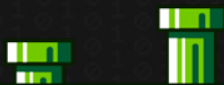
우대 사항

- CVE(Common Vulnerabilities and Exposures) 사례를 분석해보신 분
- 모의해킹 및 취약점 분석 경험이 있는 분
- 해킹대회 참여, CVE 보유, 버그바운티 참여 경험이 있는 분
- 개발 경험이 있는 분



프로젝트 소개

프로젝트 상세 소개 내용



2 프로젝트 소개

주요내용 1

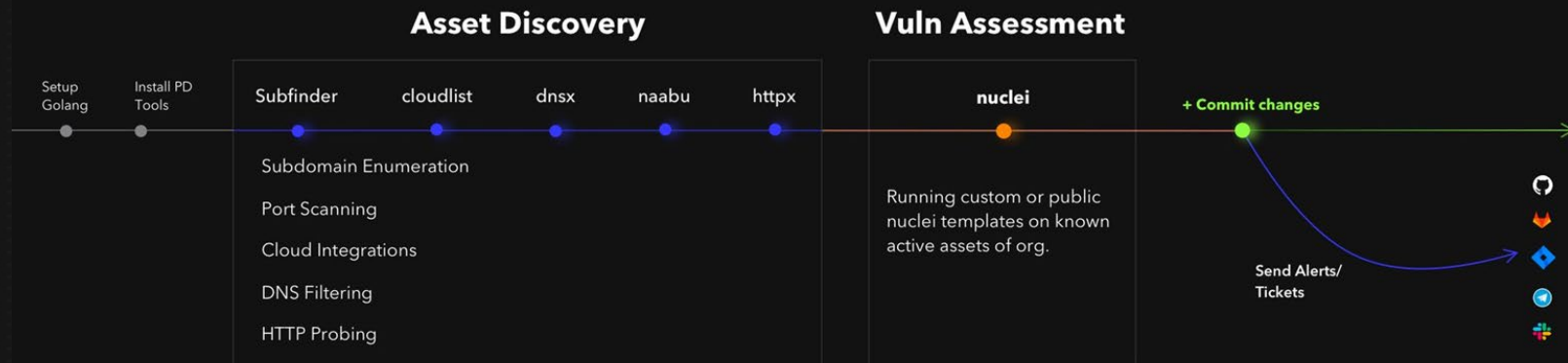
사이버 공격은 시간이 지날수록 고도화되어 증가하는 추세로 최근에는 주요 공격 대상을 스타트업으로 확장하면서 많은 스타트업에서 개인정보 유출 사례가 급증하고 있다. 이로 인한 정보보안 강화의 중요성은 날이갈수록 증가하고 있지만 예산과 인력 문제 등으로 어려움을 겪고 있다. 이러한 문제를 해결하기 위해 Project Discovery에서 개발한 도구들을 활용할 수 있다.

주요내용 2

Project Discovery는 IT 자산을 식별하고 보안 취약점을 찾아주는 오픈소스 프로젝트로 안전한 IT 서비스를 구축하고 유지하는데 활용할 수 있다. 본 프로젝트는 Go 언어로 개발되어 크로스 플랫폼 (Windows, Linux, macOS)에서 사용이 가능하고 명령어들을 파이프라인으로 연결시켜 한 줄의 명령어로 자산 식별과 보안 취약점 스캔이 가능하다.

2 프로젝트 소개

주요내용 3





컨트리뷰션 가이드

단계별 컨트리뷰션 커리큘럼



3. 컨트리뷰션 가이드

컨트리뷰션 코스 1

코스 1. 웹 구조 및 웹 취약점 이해하기

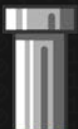
- 웹 구조 및 OWASP 10 웹 취약점에 대한 설명이 진행됩니다.
- 대표적인 CVE(Common Vulnerabilities and Exposures) 취약점 사례에 대해 학습합니다.
- 버그바운티 사례를 찾아 학습합니다.
- 팀별 CVE (Common Vulnerabilities and Exposures) 취약점 들을 찾아보고 원인 분석을 진행하고 팀별 발표를 진행합니다.

3 컨트리뷰션 가이드

컨트리뷰션 코스 2

코스 2. 개발환경 구성

- Project Discovery 프로젝트 도구 실습 및 이해하기
- Git 개발 환경 구성, local, fork, remote repo, upstream 구조 잡기
- 각 Repository 별 컴파일 및 실행 테스트
- 팀별 관심 분야에 대해 생각해보기



3 컨트리뷰션 가이드

컨트리뷰션 코스 3

코스 3. 프로젝트 분석 및 기여방향성 정하기

- Project Discovery 제공 소스코드 주요 기능 분석
- 이슈 선정: repository 에 'bug' or 'good first issue' 라벨링 되어 있는 이슈 선정
- 이슈 분석: 이슈에 해당하는 코드 분석, 동작 과정에 대한 이해 및 분석
- 이슈 설계: 이슈 코멘트와 Discord를 이용해서 이슈 해결에 대해서 논의

3 컨트리뷰션 가이드

컨트리뷰션 코스 4

코스 4. 프로젝트 기여하기

- 구현 및 테스트: 기능 추가, 취약점 템플릿 추가, 리팩토링, 버그 수정 등의 구현 작업을 진행
- Pull Request 제출 및 코드 리뷰
- 문서화: 기존 영문으로 작성된 문서를 한글화로 번역 작업 진행
- 그 외 이슈 댓글 토론 참여, 새로운 기능 제안, 버그 리포트, 블로그 포스팅, 컨퍼런스 발표



컨트리뷰션 운영 방안

컨트리뷰션 단계별 상세 운영 방안



4. 컨트리뷰션 운영 방안

1주차

웹 취약점 소개

- OWASP TOP10, CVE, 버그바운티 이해하기

2주차

CVE 취약점 사례 학습

- 보안 취약점 실습
(* 노트북 지참 필수, 취약한 환경 VM 제공)

4. 컨트리뷰션 운영 방안

3주차

프로젝트 소개 및 실습

- Project Discovery 주요 도구

4주차

개발 파트 선택

- 자산 식별
- 보안 취약점 스캔

4. 컨트리뷰션 운영 방안

5주차

- 개발 파트별 학습 활동 및 현황 공유
- 자산 식별 파트
 - 보안 취약점 스캔 파트

6주차

기여 브레인스토밍 실시



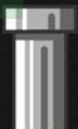
4. 컨트리뷰션 운영 방안

7주차

이슈 검토 및 선정

8주차

컨트리뷰션 진행 및 피드백



4. 컨트리뷰션 운영 방안

9주차

컨트리뷰션 진행 및 피드백

10주차

컨트리뷰션 진행 및 피드백



4. 컨트리뷰션 운영 방안

11주차

컨트리뷰션 진행 및 피드백

12주차

컨트리뷰션 진행 및 피드백



4. 컨트리뷰션 운영 방안

13주차

컨트리뷰션 진행 및 피드백

마무리

결과 정리 및 리뷰



4. 컨트리뷰션 운영 방안

ONLINE



- Slack, Discord, Kakao 등을 이용한 커뮤니케이션
- Google Meet을 이용한 화상회의 실시

OFFLINE



- Open UP 사무실 또는 토즈에서 오프라인 모임 실시



멘토 소개

컨트리뷰션 프로젝트팀 멘토단 소개



5 멘토 소개

최관호 멘토



- 시큐아이

김관영 멘토

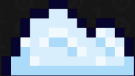


- 공개 소프트웨어
- 오픈 프런티어
- 한화시스템
- 삼성전자



2022 오픈소스 컨트리뷰션 아카데미

Open Source
Contribution
Academy



Project Discovery

컨트리뷰션에 도전해 보세요!



THANK YOU



주최



과학기술정보통신부

주관



정보통신산업진흥원

