1.1 소프트웨어 개발 생명주기 모델 중 폭포수 모델에 대해 서술하시오.

폭포수 모델이란 소프트웨어 개발 방법론 중 하나로 각 단계가 순차적으로 진행되고, 다음 단계로 넘어가기 전에 이전 단계가 모두 끝나야 하는 특징이 있다.

단계로는

요구사항 분석 단계 (사용자의 요구를 명확히 정의함)

설계 단계 (요구사항을 바탕으로 시스템의 구조를 설계함)

구현 단계 (설계한 내용을 실제 코드로 개발함)

테스트 단계 (구현한 시스템이 요구사항대로 동작하는지 확인함)

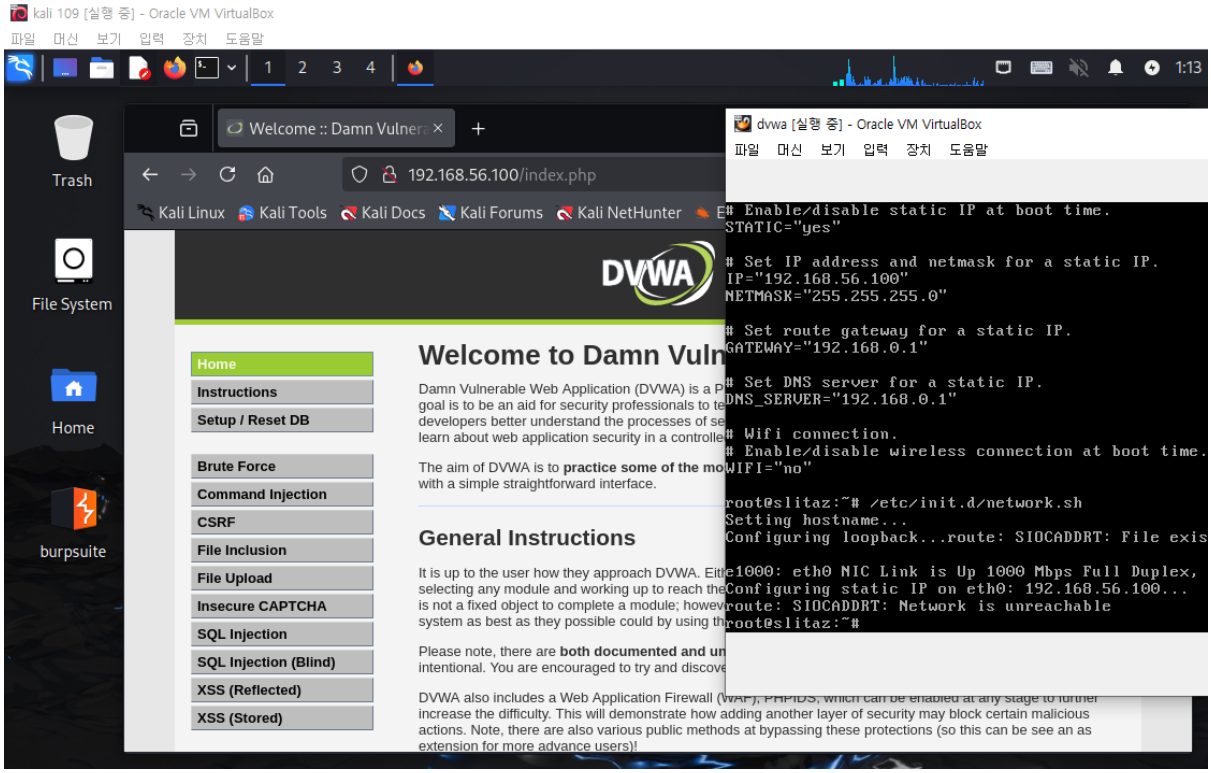
유지보수 단계 (배포 후 발생하는 문제를 해결하거나 기능을 개선함)

이 있으며 단계가 폭포수처럼 위에서 아래로 진행된다.

단점으로는 한 번 결정된 요구사항을 나중에 변경하기 어렵다는 점이 있다.

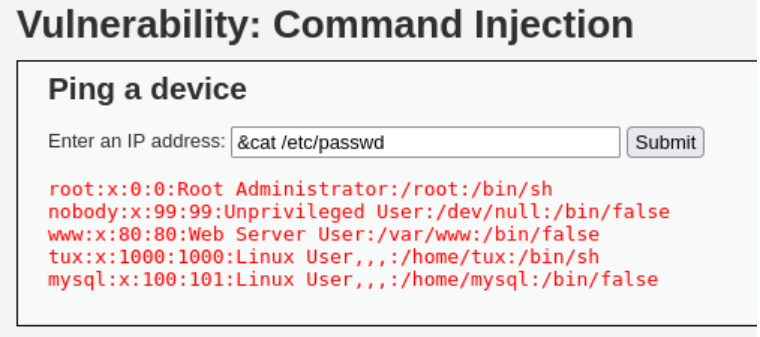
1.2 ~ 1.4 소프트웨어 개발 보안 환경을 테스트가 가능하도록 설계하여 구축하고 정상적으로 동작이 되도록 가능하도록 설정하시오.

- Kali, Metasploitable2(dvwa)



Kali linux에서 dvwa에 접속한 상태이다

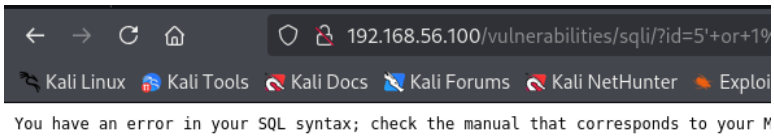
2.1 실습 도구에서 PHP 코드의 취약점을 통해 공격을 실행하고 대응 방안에 대해 실습을 진행하시오. (Command Injection)



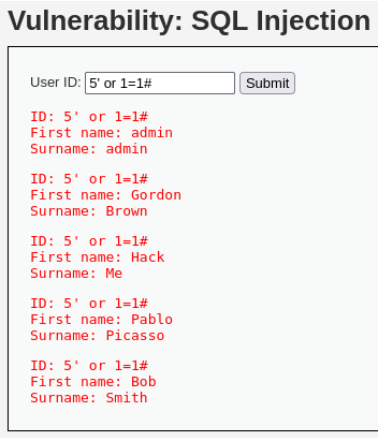
IP address 를 넣어야 하는 입력 칸에 Command Injection 공격 코드를 넣어보니 곧바로 명령어가 실행되어 중요한 정보가 노출되는 것을 확인

대응 방안으로는 화이트 리스트(정해진 패턴이나 값만 포함하도록 제한함)를 사용하거나 입력값 길이를 제한하고, 입력값 필터링을 통해 특수문자가 포함되지 않도록 하여 악의적인 코드가 들어가는 것을 방지할 수 있다.

2.2 실습 도구에서 PHP / MySQL 의 취약점을 통해 공격을 실행하고 대응 방안에 대해 실습을 진행하시오. (SQL Injection -> 사용자 계정 정보 획득)



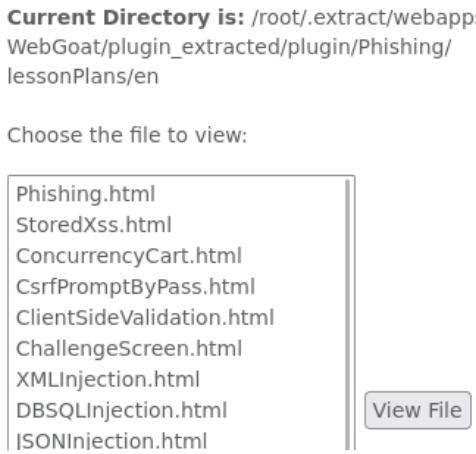
SQL Injection 공격이 통하는지 보기 위해 5' or 1=1 을 입력하니 구문 오류가 뜬다는 것을 확인



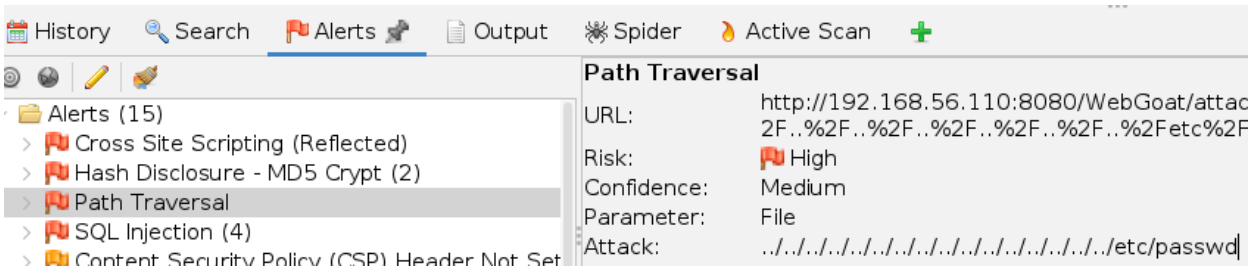
명령어를 변형하여 뒤쪽 주석 처리를 하니 항상 참이 되어 중요 정보들이 노출되는 것을 확인

대응 방안으로는 화이트리스트 방식으로 입력값 검증을 통해 특수문자를 제한하거나 최소 권한 원칙을 적용하여 애플리케이션이 데이터베이스와 상호작용할 때 필요한 최소한의 권한을 적용시킬 수 있다.

2.3 OWASP ZAP 도구를 활용하여 취약점을 스캐닝하고 발견된 취약점 중 하나를 선택하여 테스트 진행과 결함을 해결하기 위한 방안에 대해 서술하시오.



예시로 Webgoat Bypass a Path Based Access Control Scheme로 테스트하였다



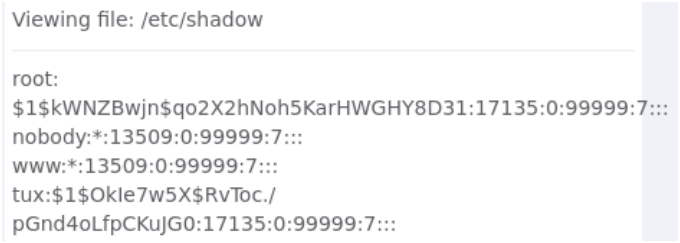
Zaproxy로 스캔결과 경로 조작 취약점 있는 것을 확인

```
GET
http://192.168.56.110:8080/WebGoat/attack?Screen=294&menu=200&File=Phishing.html&SUBMIT=View+F
ile HTTP/1.1
Host: 192.168.56.110:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://192.168.56.110:8080/WebGoat/start.mvc
```

Zaproxy On 후 Phising.html -> View File 을 잡아두고 파라미터를 확인

```
GET
http://192.168.56.110:8080/WebGoat/attack?Screen=294&menu=200&File=../../../../../../../../../../
etc/shadow&SUBMIT=View+File HTTP/1.1
Host: 192.168.56.110:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://192.168.56.110:8080/WebGoat/start.mvc
```

파라미터를 변경하고 넘긴 후 웹페이지 확인



/etc/shadow의 정보가 뜨는 것을 확인할 수 있다.

이런 경로 기반 접근 제어를 우회하는 취약점을 해결하기 위한 방안은 파일 경로가 루트 디렉토리를 벗어나지 않도록 경로를 제한하거나 허용된 파일명이나 경로만 접근 가능하도록 설정하기, WAF를 사용하여 룰을 적용시키는 방법 등이 있다.