2021. 3

주제 선정을 위한 리서치 수행.

Shodan을 이용하여 국내 취약점 사례를 검색하고, 가장 많이 노출되는 취약점을 조사 후 ligttpd에 대한 취약점을 분석하기로 주제 선정.

2021. 4 – 2021. 6

개인 학습을 통해 보안에 대한 지식 획득.

Cali-linux 설치 후 beebox, msfv2, metasploitable과 같은 취약점 환경 설치 후 모의 실습 진행.

2021. 7 – 2021. 8

Path Traversal과 SQL injection에 대한 학습과 선행 연구에 대한 조사.

CVE-2018-19052와 CVE-2014-2323에 대한 취약점 테스트를 하기 위해 ubuntu linux 13.10 버전을 설치하고 lighttpd 1.4.34 버전과 mysql 설치.

Conf 파일을 열어 mod_alias 모듈 적용 및 dir-listing 활성화 후 lighttpd를 이용하여 서버 구동.

2021. 9

CVE-2018-19052 환경 테스트를 위해 여러 폴더 계층을 만들고 다양한 이미지 파일, 텍스트 파일, 스크립트 파일 등을 넣어 환경 구축 후 lighttpd 서버를 구동하여 path traversal 취약점 테스트를 수행.

Lighttpd conf파일에서 mod_mysql_vhost 모듈 적용 후 mysql-vhost 관련 db 세팅 환경 설정 완료

2021. 10

CVE-2014-2323 환경 테스트를 위해 Mysql 내부 테이블 생성.

Ligttpd 서버 구동 후 curl 명령어 등을 통해 SQL injection 공격 수행.

Ubuntu linux 20.04 LTS 버전 설치 및 lighttpd 1.4.34 재설치 후 conf 파일 안에 지금까지 했던 환경 설정 그대로 다시 설정 후 ligttpd 서버 구동.

취약점 테스트 재 진행 후 CVE-2018-19052와 CVE-2014-2323 각각에 대한 시큐어 코딩 진행.

CVE-2018-19052의 경우 주소에 '..'이나 '../'가 들어가는 지 확인 후 오류 처리를 하게 함.

CVE-2014-2323의 경우 '(따옴표)와 같은 문자가 있으면 ₩를 추가하여 이스케이프 처리하여 보안 강화.

시큐어 코딩 후 다양한 방법으로 재 공격 실습.

해당 취약점 분석에 대한 논문 작성 후 한국정보과학회에 논문 제출.

2021. 11.

발표를 위한 ppt 작성, 동영상 제작.

한국정보과학회로부터 논문 승인.