수행프로젝트	항목	주요내용
	프로젝트 명	CTF 제작
	수행기간	2025/3/20 ~ 2025/4/18
	목표	- 시스템 및 웹 취약점을 통해 최종적으로 루트(root) 권한 획득 - 실전 해킹 기법 구현을 통한 역량 강화 - 팀원 간 상호 테스트를 통해 보안 실무 역량 강화
	내용	본 프로젝트는 보안 실습 과정의 일환으로, 팀별로 CTF 문제를 제작하고 다른 팀이 이를 풀이하는 방식으로 진행되었습니다. 우리 팀은 Rocky Linux 가상 머신을 기반으로 WordPress, FTP(vsftpd), SSH 환경을 구축하고, 다음과 같은 해킹 경로를 기반으로 문제를 설계했습니다: 정보 수집 → FTP 취약점 이용 → 웹 분석(Base64) → 인증 우회 → 리버스 쉘 획득 → SSH 접근 → 권한 상승(root) 실전 공격 흐름을 반영하여 다양한 보안 기술을 종합적으로 요구하도록 구성하였으며, 워크스루 문서를 통해 풀이 가이드를 함께 제공하였습니다.
	설계/프로세스	- 기획: 취약점 흐름 설계(FTP → 웹 → 인증 우회 → 리버스 쉘 → SSH → sudo) - 환경 구축: Rocky Linux VM에 Apache, PHP, MySQL, WordPress 취약 플러그인,vsftpd설정 - 테스트: 팀원 간 교차 풀이 후 힌트/난이도 조정, 오류 수정 및 최종 워크스루 문서화
	담당 역할	- FTP 취약점 기반 파일 힌트 구성(Base64 인코딩 - 전체 해킹 흐름에 대한 테스트 및 난이도 밸런싱 - 워크스루 문서화 과정 지원 (명령어, 스크린샷, 설명 정리 등)
	느낀점/성장점	- 익명 FTP 서비스의 보안 위험성을 직접 구성하며 시스템 보안 설정의 중요성을 체감 - 실전 해킹 흐름에 따라 리버스 쉘, 권한 상승 과정을 직접 수행하며 공격자의 시점에서 사고하는 역량 강화 - 문제 설계 및 테스트 과정에서 디버깅 능력 향상, 팀원 간 협업을 통한 기술적 커뮤니케이션 능력 향상