모의해킹 1주차 보고서

**1주차 진단 유형 및 기준+ 간단한 HTTP 메서드 설명**

1. 기술적 진단 유형

a. 업무서버, 네트워크 장비, 보안장비 취약점 점검

-장비들의 데몬들 혹은 권한들의 취약점을 점검

b. 주요 홈페이지 모의해킹 수행및 내,외부망 모의해킹 및 D.Dos공격

-초기의 모의해킹, 현재의 모의해킹의 차이

c. 소스코드 전수검사, 육안검사

-툴을 이용한 1차 점검 이후 확인된 결과물을 전문 보안 컨설턴트가 재검토하는 방식

1. 웹 모의 진단
2. 툴진단(웹 스캐너)

-자동으로 구조수집,취약점을 분석해준다 단,

오탐이나 탐지가 불가능한 부분도 있다. -> 모의진단으로 보완

1. 모의진단

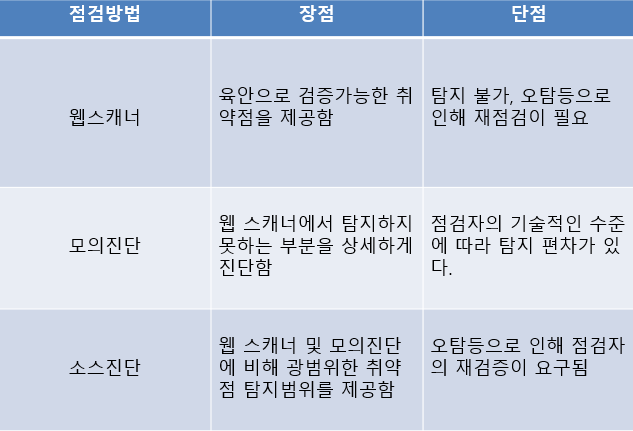
-각 이벤트 발생시 취약점을 검증하고 점검

ex)sql인잭션,쿠키번호,파라미터 변조, xss등

1. 소스진단

-소스코드를 분석하여 취약점 발생가능한 위치를 확인하는 기법.

-툴을 이용후 점검자가 검증하여 정상탐지 혹은 오탐을 분류한다



1. **진단기준**
   1. CVE(Common Vulnerabilities and Exposures)

-국가기관 및 벤더사 등이 함께 발생된 치약점을 번호화시켜 취약점을 관리하는 데이터베이스

* 1. CWE(Common Weakness Enumeration)

-미국방성 산하의 mitre라는 기관에서 정의해 놓은 C,Java를 포함한 여러 개발언어에 대한 취약점 데이터베이스

* 1. OWASP(Open Web Application Security Project)

-전 세계 기업, 교육기관 및 개인이 만들어가는 오픈소스 어플리케이션 보안 프로젝트

-2016년 8월에 새로 릴리즈 됨.

1. 간단한 HTTP 메서드 설명
   1. get

-웹에서 정보를 보낼 때 사용하는 프로토콜로 url상에 파라미터가 보여 ID,password 가 보일 수 있다.

* 1. post

-get과 마찬가지로 웹에서 정보를 보낼 때 사용하는 프로토콜이지만 url상에 파라미터가 보이지 않아 자주 쓰인다.

get과 post 둘다 form 형태의 태그안에서 action=“보낼곳“ 으로 보내며

받는곳 에서는 request.getParameter 형식으로 받는다.

* 1. put

-put 방식은 get/post방식과 비슷하게 쓰이나

get/post는 서버에 존재하는 스크립트나 파일을 요청하는데 비해

put방식은 새로 업로드할 방식을 알려준다는점이다.