|  |  |
| --- | --- |
| 2노드 간 상호 연결을 최초로 성공시킨 연도와 인물을 바르게 나열한 것은 무엇인가? | 1969년, 레너드 클라인록 |
| 프로토콜에 대한 상세한 내용을 담고 있는 문서는 무엇인가? | RFC |
| DNS와 IP주소, 프로토콜 번호와 매개변수 배정 등을 관리하며, DNS루트 네임 서버 시스템의 개선 및 운영을 담당하는 기관은 무엇인가? | 국제 인터넷 관리 기구(ICANN) |
| 인터넷에 영향을 미칠 수 있는 관세 문제를 다루고, 정보통신 네트워크에 대한 기술적인 표준과 운영 표준을 발행하는 기관은 무엇인가? | 국제 전기 통합 연합(ITU) |
| 월드 와이드 웹을 최초로 개발한 사람은 누구인가? | 팀 버너스 리 |
| 웹 서버에 데이터를 보낼 때 인수를 이용하여 보내는 메소드는? | GET |
| 클라이언트 측의 에러를 나타내는 HTTP 상태 코드느 무엇인가? | 400번대 |
| 동적인 웹 페이지를 위한 서버측 스크립트 언어 아닌 것은 무엇인가? | 자바스크립트 |
| 시스템에 침투하는 일반적인 해킹 과정을 바르게 나열한 것은 무엇인가? | 공격 대상 선정 > 정보 수집 > 취약점 분석 > 공격 |
| 구글의 고급 검색 기능 중 특정 도메인으로 지정한 사이트에서 검색 결과를 얻을 수 있는 검색 인수는 무엇인가? | site: |
| Hankuk.ac.kr이라는 사이트에서 admin 문자열을 찾는 구글 검색 키워드는 무엇인가? | site: hankuk.ac.kr admin |
| 다음 중 ‘가지고 있는 것’을 사용한 인증 방법이 아닌 것은 무엇인가? | i-PIN |
| 다음 중 가장 안전한 패스워드는 무엇인가? | Ab3D#f |
| 접근 통제 유형 중에서 일반 사용자가 접근할 수 있는 정보와 상위 관리자가 접근할 수 있는 정보에 각기 다른 접근 권한을 부여하는 것은 무엇인가? | 수직적 접근 통제 |
| 다음 중 SQL DML(데이터 조작 언어)이 아닌 것은 무엇인가? | CREATE DATABASE(DDL) |
| 다음 중 SQL DDL(데이터 정의 언어)이 아닌 것은 무엇인가? | DELETE(DML) |
| 한번에 두 갱의 테이블에서 데이터를 조회할 때 사용하며, 특히 SQL 인젝션 공격에서 다른 테이블의 내용을 조회할 때 사용하는 명령어는 무엇인가. | UNION |
| Microsoft SQL Server 환경에서 로그인 부분을 SQL 인젝션 공격으로 우회하려고 할 때 사용하는 특수문자는 무엇인가 | ‘(쿼레이션) |
| 다음 중 오라클에서 사용자 정의 테이블을 가져오는 SQL 구문은 무엇인가? | select tname from sys.tab |
| 웹 사이트에서 각각의 개인을 구별하기 위해 만들어 클라이언트에 저장해두는 것은 무엇인가? | 쿠키 |
| 다음 중 쿠키의 일반적인 용도가 아닌 것은 무엇인가? | 바이러스 전파 |
| XSS는 무엇을 줄여서 부르는 말인가? | Cross - site scripting |
| XSS공격을 통해 공격자가 일차적으로 얻고자 하는 정보는 무엇인가? | 사용자의 쿠키정보 |
| XSS 공격을 할 때 기본적으로 사용하는 태그는 무엇인가? | <script> |
| 웹 애플리케이션의 외부 구조나 인터페이스를 보는 것이 아니라 개발된 소스코드를 살펴봄으로써 코딩의 취약점을 찾는 방식은 무엇인가? | Whtie Box Testing |
| 웹 애플리케이션에서 발생하는 취약졈의 유형을 체계적으로 정리하여 가장 흔히 발생하는 취약점 열 개를 발표하는 공개 조직은 무엇인가? | OWASP |
| 소스코드 취약점의 대표적인 유형이 아닌 것은 무엇인가? | 패스워드 설정 취약점 |
| 소스코드 내에 패스워드와 같은 민감한 정보가 포함된 취약점 유형은 무엇인가? | 코드 내 중요 정보 노출 취약점 |
| 최근 사용자가 급격하게 늘어난 구글의 웹 브라우저는 ? | 크롬 |
| 최근에 가장 많이 사용하는 새 개의 웹 브라우저에 포함되지 않는 것은 무엇인가? |  |
| Burp Suite에서 수작업으로 확인되지 않은 페이지까지 자동으로 접속하여 추가 정보를 수집하는 기능은 무엇인가? | Spider 기능 |
| Burp Suite에서 특정 요청을 계속해서 전달할 수 있는 기능은 무엇인가 | Repeater 기능 |
| 웹 어플리케이션의 보안 취약점을 찾는 두 가지 방법을 밝히고 각각의 장단점을 설명하시오. |  |

OWASP Top 10 에 대해 서술

OWASP는 온라인을 통한 오픈 프로젝트로서 2001년 12월 마크 커페이. 데니스 그로브스에 의해 처음 만들어졌고. 2004년에는 OWASP Top 10이라는 웹 애플리케이션상의 10대 주요 취약점을 발표하여 많은 보안 전문가에게 알려지게 되었다. OWASP Top 10에는 인젝션, 취약점 인증, 민감한 데이터 노출, XML 외부 개체, 취약한 접근 통제, 잘못된 보안구성, XSS, 안전하지 않은 역 직렬화, 알려진 취약점이 있는 구성요소 사용, 불충분한 로깅 및 모니터링이 있습니다.

SQL 인젝션 취약점이 발생하는 원인

SQL 인젝션은 응용 프로그램 보안 상의 허점을 의도적을 이용해, 개발자가 생각하지 못한 SQL 문을 실행되게 함으로써 데이터베이스를 비정상적으로 조작하는 기법으로 웹페이지의 로그인 창 등에 SQL 구문을 넣어 데이터베이스의 정보를 빼내거나 홈페이지를 변조해 악성코드를 유포하는 해킹 수법입니다. 이러한 SQL 인젝션 공격이 계속해서 일어나는 이유는 취약점을 이용해 공격하는 것이 매우 쉽고, 성공률이 높은 공격이기 때문입니다.기초적인 해킹 공격이지만 사이트의 정보 유출 및 숙주 서버 변조를 통한 악성코드 유포 등을 통해 큰 피해를 줄 수 있고, 소프트웨어 개발자나 기업에서 보안 패치에 크게 신경 쓰지 않는 경우 때문입니다.

XSS공격의 두가지 유형과 각각의 동작 원리에 대해 설명

XSS에는 대표적으로 Stored XSS 와 Reflected XXS 두가지 유형이 존재합니다. 첫번째로 Stored XSS는 웹 사이트의 게시판에 스크립트를 삽입하는 공격 방식으로 공격자는 게시판에 스크립트를 삽입한 후 공격 대상자가 해당 게시글을 클릭하도록 유도한다. 게시글이 클릭되면 서버가 악성 스크립트를 포함한 응답을 전송하여 공격자의 악성 스크립트가 실행되어 공격자가 의도한 동작이 실행되는것이다. 그리고 Reflected XSS는 웹 애플리케이션에 스크립트를 저장하는 것이 아니라 URL의 변수 부분처럼 스크립트 코드를 입력하는 동시에 결과가 바로 전해지는 공격 기법이다.

웹 애플리케이션의 보안 취약점을 찾는 두 가지 방법을 밝히고 각각의 장단점을 설명하시오.

웹 애플리케이션의 보안 취약점을 찾는 방법으로는 Black Box Testing 과 White Box Testing이 있다. 첫번째로 Black Box Testing은 소스코드를 보지 않고 웹 애플리케이션의 외부 인터페이스나 구조를 분석하여 취약점을 찾는 방식으로 취약점을 찾는 속도가 빠르다는 장점이 있지만, 테스터가 프로그래밍 지식이 부족하면 테스트할 시나리오가 줄어들어 모든 경우의 수를 테스트할 수 없어 취약점을 모두 찾아낼 수 없다는 단점이 존재한다. White Box Testing은 웹 애플리케이션의 내부 소스코드를 확인하기 때문에 취약점의 존재 유무를 정확하게 알 수 있지만. 최근에 개발되는 웹 애플리케이션들은 굉장히 많은 양의 소스코드가 존재하기 때문에 일일이 검토해서 취약점을 찾는데 너무 많은 시간이 소요된다는 단점이 존재한다.