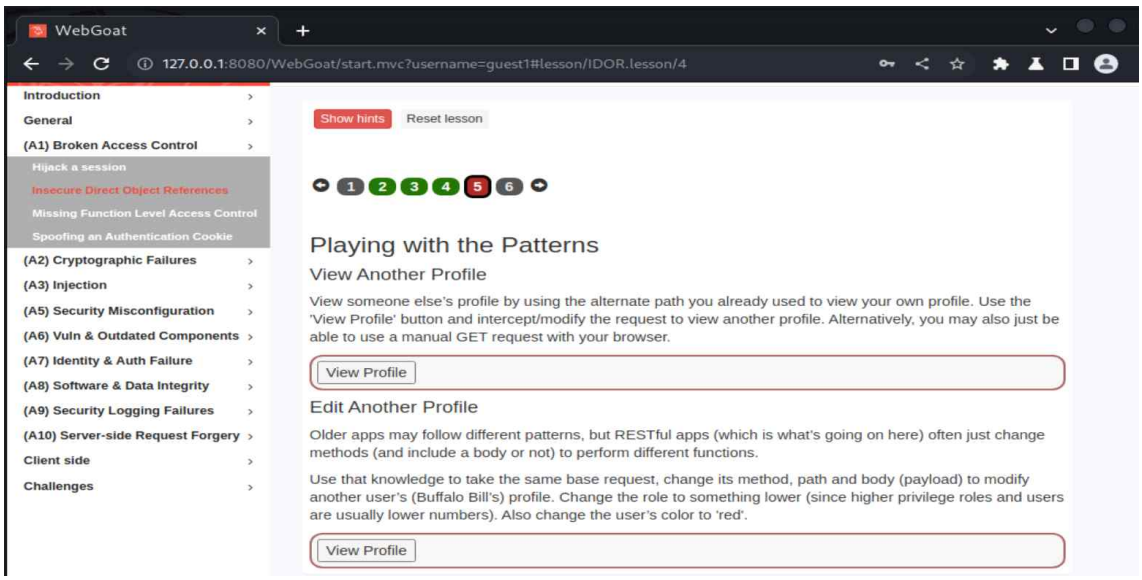
컴퓨터 보안 : 기말고사 공지

※ 기말고사 일시 및 장소: 12월 17일 화요일 오후 2시~2시50분
※ 기말고사 시험 유형: 주관식, 단답형, 서술형
※ 기말고사 시험 범위: 웹 보안
- 1장(인터넷과 웹의 이해), 2장(웹 해킹의 기초), 3장(인증 기술과 접근 통제),
- 4장(SQL 인젝션 공격), 5장(XSS 공격)
- 6장(소스코드의취약점), 7장(웹해커의 도구)
※ Take Home Exam 답안지 제출:
- cyber 캠퍼스 "Take Home Exam"에 업로드하기
- 답안지 : 학번_이름.hwp

※ Take Home Exam(10점) : WebGoat와 Burp Suite를 사용한 접근 통제 실습

WebGoat 환경에서 (A1) Broken Access Control - Insecure Direct Object References - 숫자 5 클릭 : Playing with the Patterns 학습에서 접근 통제를 학습하기 위해 다음 과정을 수행한다:



문제 1. View Another Profile (수평적 접근 통제 확인)

step 1: WebGoat의 **View Another Profile** 섹션에서 **View Profile** 버튼을 클릭하기.

step 2: Burp Suite를 사용하여 해당 요청을 가로채고, **userId** 파라미터의 값(2342388)을 이용하여 다른 사용자 userID을 찾기.
- url : /WebGoat/IDOR/profile/%7BuserId%7D HTTP/1.1
- Repeater 탭을 이용
- Intruder 탭을 이용

step 3: userid 값을 변경한 후 Forward를 클릭하여 서버 응답을 확인했을 때 나타날 수 있는 결과를 기록하시오(이미지 캡쳐).

문제 2: Edit Another Profile (권한 상승 공격 시도)
step 1: WebGoat의 Edit Another Profile 섹션에서 View Profile 버튼을 클릭
step 2: Burp Suite의 Proxy > Intercept 기능을 활성화한 상태에서 요청을 가로채기
step 3: Burp Suite에서 가로챈 요청의 URL과 파라미터를 기록하고, 이를 변경하여 다른 사용자의 프로필에 성공적으로 접근할 수 있는지 기록하시오(이미지 캡쳐).

※ 기말 고사 예상 문제:

1. Burp Suite에서 프록시 설정을 활성화한 후, Intercept 설정을 끄기 위해 어떤 작업을 해야 합니까?
정답: Burp Suite의 Proxy 탭에서 "Intercept" 버튼을 클릭하여 "Intercept is off" 상태로 변경.

2. SQL 인젝션 공격은 어떤 상황에서 발생하며, 주로 어떤 입력 필드에서 취약점을 탐지할 수 있습니까?
정답: SQL 인젝션은 사용자 입력이 데이터베이스 쿼리에 직접 포함될 때 발생한다. 주로 검색창, 로그인 필드, URL 파라미터 등에서 취약점을 탐지할 수 있다.

3. robots.txt 파일의 역할은 무엇이며, 이 파일에 어떤 설정을 포함하면 검색 엔진의 크롤링을 막을 수 있습니까?
정답: robots.txt 파일은 검색 엔진의 크롤링 규칙을 정의한다. 크롤링을 막으려면 Disallow: /를 포함시킨다.

4. OWASP Top 10 중 "A3. 인젝션" 취약점은 주로 어떤 기술에 의해 발생하며, 이를 방지하기 위해 무엇을 해야 합니까?
정답: SQL 명령어 등과 같은 입력값이 제대로 검증되지 않을 때 발생한다. 이를 방지하기 위해 입력값을 검증하고, Prepared Statements를 사용한다.

5. Google 해킹에서 filetype 연산자를 사용하여 특정 파일 형식을 검색하려면 어떤 명령어를 사용합니까? 예를 들어 작성하시오.
정답: site:openai.com filetype:pdf

6. 웹 애플리케이션에서 권한 상승 공격이 발생하는 이유를 설명하고, 이를 방지하기 위한 접근 방식을 서술하시오.
정답: 권한 상승 공격은 애플리케이션에서 적절한 권한 검증 없이 다른 사용자 또는 관리자 권한에 접근할 때 발생한다. 이를 방지하려면 서버 측에서 역할 기반 접근 제어를 구현하고, 모든 요청에 대해 사용자의 권한을 확인해야 한다.

7. OWASP Top 10의 "A7. 식별 및 인증 실패"에 대해 설명하고, 이를 예방하기 위한 보안 조치를 제시하시오.
정답: 식별 및 인증 실패는 약한 비밀번호, 인증 토큰의 노출, 세션 관리 실패 등으로 발생한

다. 이를 예방하기 위해 강력한 암호 정책을 적용하고, 세션 타임아웃, 다중 인증, 암호화된 쿠키를 사용해야 한다.

8. SQL 인젝션 공격의 원리와 이를 탐지하기 위한 일반적인 방법을 서술하시오. 또한, 이를 방지하기 위한 구체적인 개발 전략을 설명하시오.
정답: SQL 인젝션은 입력값이 데이터베이스 쿼리에 그대로 포함되어 실행될 때 발생한다. 예를 들어, "' OR '1'='1"과 같은 입력값이 인증을 우회한다. 이를 탐지하기 위해 Burp Suite와 같은 도구를 사용하여 다양한 페이로드를 테스트한다. 방지 방법으로는 사용자 입력값 검증, Prepared Statements을 사용한다.

9. 디렉터리 인덱싱이 활성화된 경우 발생할 수 있는 보안 위협을 설명하고, 이를 방지하기 위한 설정 방법을 제안하시오.
정답: 디렉터리 인덱싱이 활성화되면 디렉터리 내 파일 목록이 공개되어 민감한 정보가 노출될 수 있다. 이를 방지하려면 디렉터리 내 index.html 파일을 추가하여 기본 파일을 제공해야 한다.

10. XSS 공격의 주요 목적은 무엇이며, 이를 방지하기 위한 일반적인 방어 방법은 무엇입니까?
정답: XSS의 목적은 사용자 브라우저에서 악성 스크립트를 실행하는 것이다. 이를 방지하려면 입력값 필터링, HTML 인코딩, CSP(Content Security Policy)를 사용한다.

11. 세션 하이재킹(Session Hijacking)이란 무엇이며, 이를 방지하기 위한 대표적인 기술은 무엇입니까?
정답: 세션 하이재킹은 공격자가 사용자의 세션 ID를 탈취하여 세션을 가로채는 공격이다. 이를 방지하려면 HTTPS와 Secure 속성을 가진 쿠키를 사용해야 한다.

12. CSRF 공격은 어떤 방식으로 수행되며, 이를 예방하기 위한 가장 일반적인 방법은 무엇입니까?
정답: CSRF는 사용자의 인증된 세션을 악용하여 의도치 않은 요청을 서버에 보낸다. 이를 예방하려면 CSRF 토큰을 사용해야 한다.

13. HTTPS는 HTTP에 어떤 보안 계층을 추가하며, 이를 통해 어떤 종류의 보안을 제공합니까?
정답: HTTPS는 SSL/TLS 계층을 추가하여 데이터 암호화, 서버 인증, 데이터 무결성을 제공한다.

14. SQL 인젝션 공격 방지를 위해 Prepared Statements를 사용하는 이유는 무엇입니까?
정답: Prepared Statements는 쿼리 구조와 사용자 입력을 분리하여 SQL 인젝션 공격을 방지한다.

15. 브라우저에서 쿠키(Cookie)의 Secure와 HttpOnly 속성은 각각 어떤 역할을 하며, 이를

설정하지 않았을 때 발생할 수 있는 보안 위협을 설명하시오.
정답:
Secure: 쿠키를 HTTPS 연결에서만 전송하도록 제한한다. 이를 설정하지 않으면 중간자 공격으로 쿠키가 탈취될 수 있다.
HttpOnly: 클라이언트 측 스크립트에서 쿠키에 접근하지 못하게 한다. 이를 설정하지 않으면 XSS 공격에 취약해진다.

16. 브루트포스 공격(Brute Force Attack)이란 무엇인지 설명하고, 이를 완화하기 위한 구체적인 보안 조치를 제안하시오.
정답: 브루트포스 공격은 가능한 모든 암호 조합을 시도하여 인증을 우회하는 공격이다.
방지 조치는 계정 잠금(로그인 실패 횟수 제한)이다.

17. Burp Suite를 사용하여 HTTP 요청에 포함된 민감한 데이터(예: 쿠키, 세션 토큰)를 검사하는 방법을 설명하고, 민감한 데이터가 노출되지 않도록 하기 위한 서버 측 조치를 제안하시오.
정답: Burp Suite의 Proxy 탭에서 HTTP 요청을 캡처하여 요청 헤더에서 민감한 데이터를 확인한다. 방지 방법은 쿠키에 Secure와 HttpOnly 설정 추가, 세션 토큰 암호화, 세션 만료 시간 설정.

18. Google 해킹을 사용하여 특정 사이트에서 디렉토리 인덱싱이 활성화된 페이지를 찾으려면 어떤 명령어를 사용합니까?
정답: site:<도메인> "index of" (예: site:example.com "index of")

19. 사이트 내부의 로그인 페이지를 찾기 위해 Google에서 사용할 수 있는 명령어는 무엇입니까?
정답: site:<도메인> inurl:login (예: site:example.com inurl:login)

20. Google 해킹에서 intitle 연산자는 어떤 용도로 사용되며, 예시로 사이트 제목에 "Admin Login"을 포함하는 페이지를 찾는 명령어를 작성하세요.
정답: intitle:"Admin Login“

21. Google 해킹에서 site, filetype, 그리고 inurl 연산자를 조합하여 특정 도메인의 Word 문서를 검색하는 명령어를 작성하고, 이 명령어가 어떻게 동작하는지 설명하시오.
정답: site:<도메인> filetype:docx inurl:documents
이 명령어는 특정 도메인에서 documents라는 경로를 포함하며 Word 문서(.docx) 파일만 검색한다. site는 특정 사이트를 필터링하고, filetype은 파일 형식을 지정하며, inurl은 특정 경로를 포함한 URL만 검색한다.

22. 다중 인증에서 사용되는 인증 요소의 세 가지 주요 유형을 설명하시오.
정답:
알고 있는 것(Something you know): 비밀번호, 주민등록번호, PIN 등.

가지고 있는 것(Something you have): 스마트카드, 인증서, 여권, 카카오톡, 보안 토큰.
생체 기반(Something you are): 지문, 홍채, 얼굴 인식 등.

23. 사용자 인증 시스템에서 세션 관리의 중요성을 설명하고, 세션 하이재킹을 방지하기 위한 방법을 3가지 이상 서술하시오.
정답:
- 중요성 : 사용자의 인증 상태를 유지하며, 올바른 사용자인지 확인하는 데 중요하다.
- 세션 하이재킹 방지 방법: HTTPS를 사용하여 세션 토큰을 암호화. 세션 타임아웃 설정으로 비활성 세션 종료. Secure 및 HttpOnly 속성을 사용한 쿠키 보호. 세션 ID를 주기적으로 갱신하여 고정 공격을 방지.

24. 접근 통제 시스템에서 최소 권한의 원칙을 설명하고, 이를 구현하기 위한 실질적인 방법을 제시하시오.
정답: 최소 권한의 원칙은 사용자가 작업 수행에 필요한 최소한의 권한만 가지도록 설정.
구현 방법: 역할 기반 접근 제어로 필요한 권한만 할당. 주기적인 권한 검토 및 불필요한 권한 제거. 관리자 계정을 분리하고 중요한 작업에만 사용. 시스템 로그를 통해 권한 사용을 모니터링.

25. 웹 해킹 과정에서 "정보 수집" 단계의 주요 목표는 무엇입니까?
정답: 공격 대상의 외부 접점, 웹 애플리케이션 취약점, 웹 서버의 종류 및 구조를 파악하여 공격 가능한 표면을 식별하는 것.

26. Burp Suite를 활용한 웹 사이트의 디렉터리 구조 확인 방법을 단계별로 서술하시오.
정답:
1. Burp Suite 실행: Burp Suite를 실행하고 브라우저의 프록시 설정을 활성화.
2. 웹 사이트 접속: 브라우저를 통해 웹 사이트에 접속.
3. Target 탭 이동: Burp Suite에서 [Target] 탭으로 이동하고 [Site map]을 클릭.
4. 디렉터리 탐색: 웹 사이트 메뉴를 클릭하면서 Burp Suite가 탐지한 디렉터리 구조, 파일 목록, HTML 소스코드 등을 확인

27. OWASP Top 10에서 "A01. Broken Access Control"이란 무엇인지 서술하시오.
정답: Broken Access Control은 적절한 인증 및 권한 검증 없이 사용자가 비인가된 데이터나 기능에 접근할 수 있는 취약점이다.

28. 접근 통제에서 수직적 접근 통제와 수평적 접근 통제의 차이점을 설명하고, 각각의 예시를 하나씩 제시하시오.
정답:
(1) 수직적 접근 통제: 특정 정보에 대한 접근 권한을 수준별로 상이하게 설정한 통제을 의미.
예: 일반 사용자와 관리자가 접근 가능한 데이터가 다름. 관리자 계정으로만 특정 대시보드에 접근 가능.
(2) 수평적 접근 통제: 같은 권한을 가진 사용자 간에 데이터 접근을 제한.

예: 사용자 A가 사용자 B의 데이터에 접근하지 못하도록 제한. 사용자 A가 다른 사용자의 주문 기록에 접근하지 못하도록 제한.

29. 수직적 접근 통제에서 "권한 상승"이란 무엇이며, 이를 방지하기 위한 세 가지 방법을 제시하시오.
정답: 권한 상승은 낮은 권한의 사용자가 관리자 권한이나 높은 권한으로 불법적으로 접근하는 행위.
방지 방법: 역할 기반 접근 제어 적용. 서버 측에서 모든 요청에 대해 권한 검증을 수행. 민감한 작업에 대해 이중 인증을 도입.

30. 소스코드의 입력값 검증 미비로 인해 발생할 수 있는 대표적인 취약점 3가지를 설명하고, 각 취약점을 방지하기 위한 방법을 서술하시오.
정답:
(1) SQL 인젝션: 데이터베이스 쿼리에 사용자 입력값을 직접 포함할 경우 발생.
- 방지 방법: Prepared Statements 사용.
(2) XSS: 입력값을 필터링하지 않고 HTML 출력에 포함할 경우 발생.
- 방지 방법: 사용자 입력을 HTML 이스케이핑 및 콘텐츠 보안 정책(CSP) 적용.
(3) 파일 업로드 취약점: 파일 확장자나 형식을 검증하지 않아 악성 스크립트가 업로드될 경우
- 방지 방법: 파일 이름과 확장자를 엄격히 필터링하고, 업로드 디렉터리를 격리.

31. 하드 코딩(Hard Coding)의 정의를 설명하고, 소스코드에서 하드 코딩된 정보를 사용하면 발생할 수 있는 보안 위협을 두 가지 서술하시오.
정답: 하드 코딩은 소스코드 내에 민감한 정보(예: 비밀번호, API 키, 데이터베이스 접속 정보)를 직접 작성하는 것을 의미한다.
보안 위협:
(1) 소스코드가 유출되면 민감한 정보가 노출될 위험.
(2) 정보가 변경될 때마다 코드를 수정해야 하므로 유지보수성이 떨어지고, 무단 접근의 가능성이 높아짐.

32. Prepared Statements의 정의를 설명하고, Prepared Statements가 SQL 인젝션 방지에 효과적인 이유를 서술하시오.
정답: Prepared Statements는 데이터베이스 쿼리를 실행하기 전에 쿼리 구조를 미리 컴파일하고, 사용자 입력을 파라미터로 전달하여 실행하는 방식.
- SQL 인젝션 방지 효과는 입력값이 SQL 구문으로 실행되지 않고 데이터로 처리되므로 인젝션 공격이 차단된다. 쿼리와 입력값을 분리하여 실행하기 때문에 의도하지 않은 SQL 명령 실행을 방지한다.

33. 웹 사이트에서 개인을 구별하기 위해 만든 것으로 클라이언트 측에 저장해두는 것은?
정답: Cookie

34. XSS는 무엇을 줄여서 부르는 말인가요?

정답: Cross-site scripting

35. XSS 공격을 통해 공격자가 일차적으로 얻고자 하는 정보는 무엇인가요?
정답: 사용자의 Cookie 정보

36. CSRF는 무엇을 줄여서 부르는 말인가요?
정답: Cross-site Request Forgery

37. XSS 공격에 대해 설명하시오.
정답: 사용자가 입력한 악성 스크립트가 검증 없이 웹 페이지에 포함되어 다른 사용자의 브라우저에서 실행되어 정보를 탈취하는 공격.

38. XSS 공격 유형 중 Reflected XSS와 Stored XSS 방식의 차이점에 대해 설명하시오.
정답:
- Reflected XSS : 악성 스크립트가 요청에 포함되어 응답 시 즉시 실행되는 방식이며, 주로 URL 파라미터를 통해 전달된다.
- Stored XSS : 악성 스크립트가 서버에 저장되어 여러 사용자에게 지속적으로 실행된다.

39. CSRF 공격에 대해 설명하시오.
정답: 사용자가 인증된 상태에서 공격자가 위조된 요청을 전송하도록 유도해, 의도치 않은 작업을 수행하게 하는 공격이다.

40. 입력값 검증 취약점의 대표적인 예를 적으시오.
정답: SQL 인젝션, XSS, 위험한 형식의 파일 업로드, 디렉터리 경로 조작

41. Black Box Testing 방식이란 무엇이며, 이 방식의 주요 특징을 설명하시오.
정답: Black Box Testing은 애플리케이션의 내부 구조를 알지 못한 상태에서 외부 인터페이스와 동작을 기반으로 취약점을 테스트하는 방식.
특징:
- 내부 로직이나 코드를 보지 않고 입력과 출력만으로 취약점을 탐지.
- 실제 공격 시나리오와 유사한 환경에서 취약점 테스트 가능.

42. White Box Testing 방식의 정의와 이를 적용할 때 얻을 수 있는 장점을 두 가지 서술하시오.
정답: White Box Testing은 소스코드와 내부 구조를 완전히 이해하고 수행하는 테스트 방식.
장점:
- 내부 로직, 조건문 등 세부적인 취약점을 깊이 분석 가능.
- 모든 실행 경로와 로직을 테스트하여 숨겨진 취약점 탐지 가능.

43. Gray Box Testing 방식의 개념을 설명하고, Black Box Testing과 White Box Testing의 장점을 어떻게 결합하는지 서술하시오.

정답: Gray Box Testing은 테스트 수행자가 일부 내부 구조를 알고 테스트를 수행하는 방식. 결합 방식: Black Box Testing의 외부 입력/출력을 기반으로 한 접근 방식과 White Box Testing의 코드와 구조 이해를 결합하여 더 폭넓은 취약점 탐지 가능.

44. 다음과 같은 소스코드에서 발견된 SQL 인젝션 취약점의 원인과 방지 방법을 설명하시오.

```
String query = "SELECT * FROM users WHERE username = '" + username + "' AND password = '" + password + "'";
```

정답:

(1) 취약점 원인:

- 사용자 입력값 username과 password가 그대로 SQL 쿼리에 포함되어 실행됨.
- 공격자가 아이디, 패스워드에 admin, 'or''='를 입력하면 만들어지는 취약한 쿼리문이 됨

(2) 방지 방법:

- Prepared Statements를 사용하여 입력값과 SQL 쿼리를 분리.
- 입력값을 정규 표현식으로 검증하여 유효하지 않은 문자 차단.

45. 다음과 같은 소스코드에서 발견된 XSS 취약점의 원인과 방지 방법을 설명하시오.

```
String message = request.getParameter("MESSAGE");
out.println("<h1>" + message + "</h1>");
```

정답:

(1) 취약점 원인:

- 사용자 입력값 MESSAGE가 검증 없이 HTML 응답에 출력되므로 악성 스크립트가 실행될 수 있음.

(2) 방지 방법:

- 사용자 입력값을 출력하기 전에 HTML 이스케이핑 적용.
- Content Security Policy(CSP)를 설정하여 허용된 스크립트만 실행되도록 제한.

46. 다음 코드에서 디렉토리 경로 조작 취약점이 발생하는 이유를 설명하시오.

```
String filePath = request.getParameter("path");
File file = new File("/uploads/" + filePath);
```

정답:

(1) 취약점 원인:

- 사용자가 ../ 등을 사용하여 경로를 조작하면 서버의 민감한 파일에 접근할 수 있음.

(2) 방지 방법:

- 경로 입력값을 검증하여 허용된 경로 외의 접근을 차단.
- 파일 경로를 고정된 디렉토리 내부로 제한하고, 외부 경로 접근을 방지.

47. 파일 업로드 기능에서 악성 파일이 업로드되는 취약점의 원인과 방지 방법을 설명하시오.

```
File userfile = new File(uploads_and_target_parent_directory + TARGET_RELATIVE_PATH + s.getUserName() + ".txt");
```

정답:

(1) 취약점 원인:
- 파일 확장자 타입을 검증하지 않아 실행 가능한 스크립트 파일이 업로드될 수 있음.
- File 객체를 생성할 때 s.getUserName()과 같은 사용자 입력값이 경로에 포함되어 있으며, 이 값이 검증 없이 사용됨.
(2) 방지 방법:
- 허용된 파일 확장자만 업로드를 허용하고, 서버 측에서 타입을 검증함.

```
if (!filename.endsWith(".txt")) {
    throw new SecurityException("Only .txt files are allowed.");
}
```

48. 일반적인 웹 해킹 과정을 적으시오.
정답: 공격 대상 선정 -> 정보 수집 -> 취약점 분석 -> 공격 -> Report/Defacement/흔적 제거 등

49. 웹 해킹 공격에 이용할 수 있는 도구를 적으시오.
정답: 프록시 도구 Burp Suite, 브라우저의 개발자 도구, 구글 검색 연산자.

50. 웹 애플리케이션에서 HTTP 프로토콜의 GET 방식과 POST 방식의 주요 차이점을 서술하고, 각각 적합한 상황을 한 가지씩 예를 들어 설명하시오.
정답:
(1) 데이터 전달 방식:
- GET: URL 쿼리 스트링을 통해 데이터를 전달하며, URL에 데이터가 노출된다.
- POST: HTTP 요청 본문(Body)을 통해 데이터를 전달하며, URL에는 데이터가 노출되지 않음.
(2) 예;
- GET : 검색어를 포함한 페이지 URL 공유가 필요한 경우.
예: https://example.com/search?q=web+security
- POST : 사용자 로그인과 같은 민감한 데이터 처리.
예: 로그인 폼에 입력한 사용자 ID와 비밀번호를 서버로 전송.