Network Security Question 답안

[Lab2]

1. Alice는 aliceDetails.txt를 열고 몇 가지 사항을 변경했습니다. 그녀는 변경한 사항을 저장할 수 있는지에 대해 설명하세요.
   A. 가능하다. 파일의 소유권이 있으며 접근 권한 또한 충분하기 때문이다.

2. Bob은 자신의 파일 bobDetails.txt에 접근하려고 하지만 접근할 수가 없었습니다. 접근할 수 없었던 이유를 설명하고 Bob은 이 파일에 접근하려면 어떻게 해야 하는지 설명하세요.
   A. 해당 파일의 접근 권한이 지정되어 있지 않으므로 접근하기 위해서는 R권한을 부여하면 된다. (chmod u+r bobdetails.txt)

3. Trudy가 ls –l 명령어를 사용하여 Alice의 홈 디렉토리에 있는 aliceFolder의 내용을 표시하려고 하면 파일과 디렉토리를 볼 수 있습니다. Trudy는 cd 명령어를 통해 디렉토리에 접근할 수 있는지에 대한 여부와 그 이유를 설명하세요.
   A. 접근이 불가하다. 해당 디렉토리에 대한 실행 권한이 지정되어 있지 않기 때문이다.

4. UNIX 권한 구조가 열 접근인지 행 접근인지 설명하세요.
   A. 열 접근 방식이다. 사용자 당 파일 권한을 나열한 것이 아닌 각 개별 파일에 대한 사용자 권한을 나열하기 때문이다.

5. /usr/bin/passwd는 시스템에서 비밀번호를 변경하는 데 사용되는 파일입니다. 이 파일은 다음과 같은 권한 설정이 되어있습니다.
   -rwsr-xr-x 1 root root 41292 2009-07-31 09:55 /usr/bin/passwd
   여기서 s는 무엇이며, 그 역할을 설명하세요.
   A. S는 setUID가 root로 설정되었음을 의미한다. 즉, passwd 파일은 파일의 소유자와 동일한 권한으로 실행되므로 다른 사용자가 해당 파일을 실행할 때마다 root의 권한을 가지고 파일을 실행하게 된다.

6. public_html (Alice의 홈 디렉토리 중)에는 index.html이라는 파일이 있으며 다음과 같은 권한이 설정되어 있습니다.
   -rw-r--r-- 2 alice alice 4096 2010-01-17 18:46 index.html
   Trudy는 index.html 파일의 내용을 표시하도록 요청된 웹 서버를 호스팅 할 때 그 내용이 표시되는지에 대한 여부와 그 이유를 설명하세요.
   A. 내용이 표시된다. Trudy는 그 외(other) 사용자로 읽기 권한이 없는 디렉토리의 파일 목록을 읽을 수는 없으나, 읽기 권한이 있는 파일을 사용하기 때문에 디렉토리의 내용을 읽을 수 있다.

7. Documents (Alice의 홈 디렉토리 중) 디렉토리와 관련하여 각 사용자들의 권한을 나열하세요.
   A. Alice는 디렉토리의 소유자이며, 읽기/쓰기/실행 권한을 모두 가지고 있다. Bob은 소유자는 아니지만 동일한 group에 소속되어 있으므로 읽기와 실행 권한을 가지고 있다. Trudy는 소유자도 아니고, 동일한 group에 소속되어 있지 않으므로 아무런 권한이 없다.

[Lab3]

1. [SQL Injection 취약점 찾기]에서 어떤 문자열을 입력하여 해결했는지 기술하세요. 그리고 왜 가능했는지에 대해 이유를 서술하세요.
   A. ID';# 이와 같이 쓸 경우에는 where에서 ID만 확인하고 Password는 확인하지 않고 True값을 반환함. 그 외에도 ' or '1'='1'# 이나 'or 'x'='x'#와 같이 ID를 검증하지 않고 True값을 만들어서 반환하는 것 또한 가능함.

2. [SQL Injection 취약점 찾기(심화)]에서 어떤 문자열을 입력하여 해결했는지 기술하세요. 그리고 간략하게 공격을 진행했던 과정을 서술하세요.
   A. ' or 1=1;# 을 입력할 경우 현재 등록되어 있는 e-mail을 확인할 수 있다. 원래 있던 email주소의 정보를 확인한 후에는 table명과 attribute명을 찾아야 하며, browser의 개발자 도구를 통해 유추할 수 있는 정보 중 emailaddress라는 속성명을 통해 attribute명을 검증하고자 x' AND emailaddress is null;#을 입력하여 attribute 이름이 emailaddress임을 확인한다. 마지막으로 x' AND 1=(SELECT COUNT(*) FROM users);#를 통해 table의 이름까지 확인하였으며, 이 정보들을 토대로 최종적으로 작성하는 Query는 다음과 같다.

   x'; UPDATE users SET emailaddress = '본인email' WHERE emailaddress='기존email';#

3. 1개의 테이블이 가질 수 있는 Primary Key와 Foreign Key는 총 몇 개입니까?
   A. PK는 오직 1개의 테이블에 1개만 있어야 하며, FK는 몇 개를 가져도 상관이 없다.

4. 다음은 버스 운행과 관련된 테이블입니다.

Driver-ID	Bus-ID	Route-ID	Start-Time	Stop-Time
44	67	6	2019/10/01-14:00:00	2019/10/01-22:00:00
44	62	6	2019/10/02-12:00:00	2019/10/02-16:00:00
54	63	9	2019/10/01-16:00:00	2019/10/01-21:00:00
54	63	8	2019/10/02-09:00:00	2019/10/02-17:00:00

Primary Key로 가장 적합한 필드 또는 필드 조합은 무엇인지, 왜 그런지 설명하세요.

A. 현재 주어진 Table에서는 단일 Attribute로 PK를 지정할 수 없는 상황이며, 복합된 속성들이 Unique할 수 있는 조합을 통해 PK를 지정해야 한다. 여기서 가장 이상적인 것은 Driver-ID와 Start-Time의 조합이다. 한 버스기사가 다른 시간에 똑같이 출발할 수는 없기 때문이다.

5. 다음은 어느 산악회의 테이블 구조입니다.

Climber-ID	Name	Skill Level	Age
123	Edmund	Experienced	80
214	Arnold	Beginner	25
313	Bridgett	Experienced	33
212	James	Medium	27

Primary Key가 Climber-ID라고 했을 때, 다음 각 행들을 테이블에 추가할 수 있는지에 대한 여부를 설명하세요.

Climber-ID	Name	Skill Level	Age
214	Abbot	Medium	40
	John	Experienced	19
15	Jeff	Medium	42

A. 첫 번째 레코드는 PK가 중복이므로 추가할 수 없다. 두 번째 레코드는 PK는 NULL값을 취할 수 없기 때문에 이 또한 추가할 수 없다. 마지막 레코드는 PK가 중복되지 않으므로 추가할 수 있다.

[Lab4]

1. 사용자 입력단에서 SQL을 주석처리하는 '--을 제거한다면 모든 SQL Injection을 방지할 수 있습니까? 이에 대한 답과 이유를 서술하세요.
   A. 불가능하다. 주석처리는 -- 뿐만이 아닌 #이나 /*와 같은 형식으로 코드를 주석처리 할 수 있으므로 모든 SQL Injection을 방지하는 것은 가능하지 않다.

2. 단순히 Addslashes() 또는 mysql_real_escape_string()을 사용하여 SQL Injection 방어를 하면 어떤 문제가 있습니까?
   A. 특수문자만 처리하기 때문에 특수문자를 사용하지 않고도 Injection을 하는 경우는 막을 수 없으며, 또한 인코딩 방식의 차이를 이용하여 이를 우회하는 것 또한 가능하다.

3. DB에 대한 보안적 접근을 유지하는데 있어서 UNIX 계열 OS의 접근 제어 메커니즘이 충분하지 않은 이유는 무엇입니까?
   A. 파일은 사용자의 입력을 가져와서 실행하지만, 이를 누가 입력했는지는 따지지 않음. 따라서 DB를 편집하는 권한을 가진 로컬 파일을 통해 DB에 공격을 가해도 OS 단계에서는 이를 처리할 방법이 없음.

4. 기능적인 부분에 있어서 addslashes()와 htmlentities()의 차이는 무엇입니까?
   A. addslashes()는 \ 또는 NULL값과 같은 특정한 escape sequence에 대해서만 취급하지만 htmlentities()는 문자를 HTML entity로 그대로 보여주지만 DBMS에는 영향을 미치지 않도록 문자를 변환한다.