مسابقة الإمارات للتكنولوجيا والابتكار
EMIRATES TECHNOLOGY & INNOVATION COMPETITION

Technical Description

Cyber Security

Contents

1. INTRODUCTION

This contest is a great opportunity for students that would like to major in or currently majoring in computer science, computer engineering, information technology, or any IT security related subjects to measure their skills in cyber security, and to acquire valuable experience. Furthermore, this contest prepares students to work as groups where each participant has a dedicated task such as designing a secure website, analyzing a website's structure, assessing the website's vulnerabilities, and finally planning and performing attacks.

The competition will allow students to interact with other students from different institutes where they will have the opportunity to test their security skills and knowledge by detecting different security flaws. The main objective of the competition is for students to work as a group to develop a secure website, exploit the vulnerabilities in each other's websites, and eventually harden their developed websites. An example of possible security threats and attacks: URL manipulation, SQL injection, and Cross Site Scripting.

2. COMPETENCY SPECIFICATION

The contest will run on three days where the first two days will have morning and afternoon sessions and the third day will run a morning session only. Students compete in teams against other teams from the same or other institutions. Each team has to analyze given specifications to develop a secure website and ensure its security by testing different vulnerabilities on it. In addition, each team will assess the security of websites developed by opponent teams. This will be done using one computer per team. Possible attacks to consider are SQL Injections, Cross-Site Scripting, etc. Denial of service attack is not allowed and teams who perform them are not qualified anymore to continue the contest. Teams are ranked based on the level of security for their website and their ability to attack other team's websites. The use of internet is not allowed during the competition; however, hard copy reference materials such as books and manuals are allowed on the third day.

3. OBJECTIVES

For the Participants:

- To measure their skills against those of their peers from other institutes.

- To acquire valuable experience.
- To compete for valuable prizes.
- To be seen by potential employers.
- To attend, free of charge, trainings on information security delivered by experts.

For Institutes:

- To promote their IT programs and particularly those in information security.
- To gain visibility.

For IT related Companies:

- To recognize and recruit potential employees.

For Emirates skills:

- To contribute on enhancing the community's knowledge about information security and its importance.
- To facilitate the networking and collaboration among institutes and companies.

4. RULES & REGULATIONS

4.1. Teams

1. Teams must register before the deadline.
2. Each team can register for two members.
3. Contestant must be a UAE national and registered either as a high school student (G12) or undergraduate student.
4. School students who participated in emirates skills can participate in Emirates Science and Technology Competition only if they are registered as university students.
5. Each institute may have one or more teams.
6. Each team must adopt a name and appoint a representative (Coach).

4.2. Competition

1. The main language of the contest is English and all the provided systems and materials are in English.
2. The contest lasts for three days where the first two days have two sessions, morning and afternoon sessions, and the third day have morning session only. Contestants should not

leave the competition during the contest time. Otherwise, the team will be considered withdrawing from the competition.

3. **PHP development skills** are needed and essential for all days.
4. Vulnerabilities are considered as detected once they have been exploited and used.
5. Contestants may bring published reference books only, except for e-books in either paper or electronic format; Manuals, listings and any hand written material are not allowed in the contest room.
6. Machine-readable versions/devices (computers, pocket calculators, mobile phones, CDs, flash memories, floppy disks …) are not allowed in the contest hall.
7. Rebooting the computers under any special circumstances during the contest must be done with the presence of an invigilator.
8. The contestants are free to choose the attacks that they want to achieve the breach. However, no tools or software codes can be used other than the provided (if any).
9. The contestants are not to inject viruses into the server.
10. During the contest days, the source code is not to be changed by any way.
11. Denial of Service attack and DDOS attack will be tolerated. Such an attack could result in the team's disqualification by judges.
12. Solutions are judged by reviewing the level of attacks performed from the judges' server.
13. Judges are solely responsible for determining the correctness of the submitted solutions; their decision is final.
14. Contestants requiring any kind of help should remain seated while being assisted by an invigilator.

4.3. General Rules

1. The organizing committee has the right to update these regulations as it sees suitable. The participants are not to complain about these regulations. It is the contestant responsibility to check the contest's website for any updates regarding the competition.
2. Any team attempting to communicate with another team, to tamper with the machines, or disrupt the contest environment in any way will be disqualified.
3. The participants shall agree to allow the organizers to publish their names as well as photos and videos in which they appear.
4. Smoking is not allowed in the competition room.
5. No visitors will be allowed in the competition room.

5. CONTEST ENVIROMENT

- The contest operating system is Microsoft Windows 7.
- The website will be developed using **PHP**, the database will be ran by **MySQL** on Apache Server.
- No wireless connection will be allowed.
- Development tools will not be provided and only **text editors can be used**.
- Participants can use the preinstalled Browser extensions (if needed).

6. COMPETITION STRUCTURE

The teams will have to (develop/modify) a secure website that has specific functionalities. For example: If adding a new topic has vulnerability then they have to secure it by adding the needed code to harden the security.

1. The teams should submit their web forum to be tested.
2. User names, Table names, Column names, and the database structure should not be changed. The web forums will be checked against the database. If a web forum has errors, penalties will be deducted.

The competition days:

The competition will run over three days. The winning team is the one who gets the highest total number of points from the three days with the least time needed.

- Day One and Two:

1. All teams will be given specifications to develop a secure website.
2. The teams should design secure sites by preventing them from having vulnerabilities.

- Day three:

1. The teams will be given each other's websites to detect the vulnerabilities through penetration testing.
2. The teams will be given the chance to harden their own websites.
3. A team will gain points if they can attack the forums for the other teams.
4. A team will lose points if other teams manage to attack their forum.

- Scoring:

1. The final score will be calculated from all days.

7. TRAINING

- For training use the following website: http://www.hackerskills.com/
- The paper titled Top Ten Hacks adapted from Black Hat conference gives examples of different attacks.
- To be trained you have to practice performing some attacks. An excellent site for security attacks is OWASP WebGoat project. Samples are provided below.

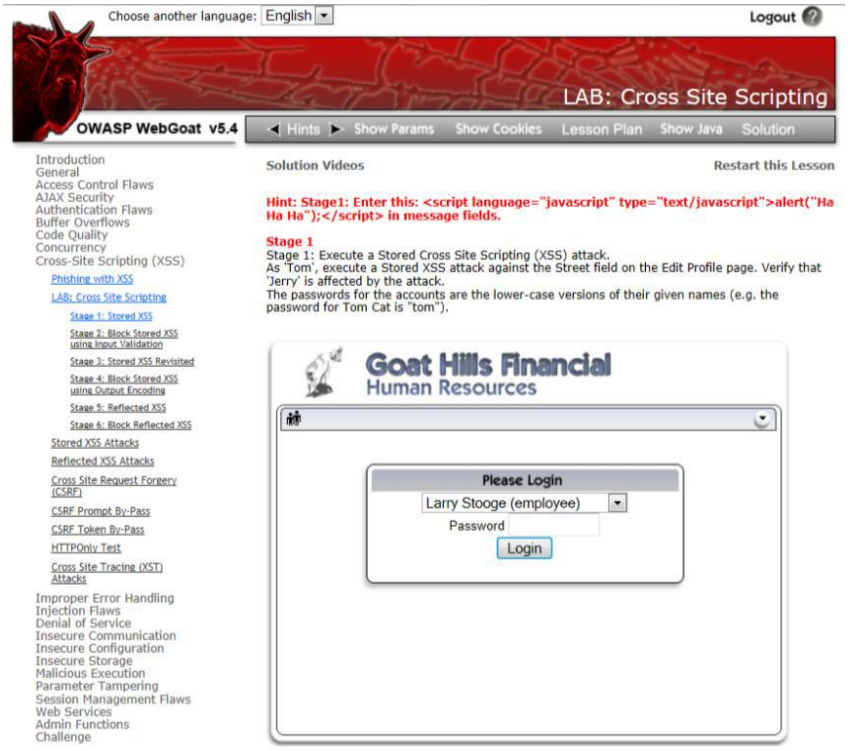

Figure 1: INDEX I - WebGoat Training

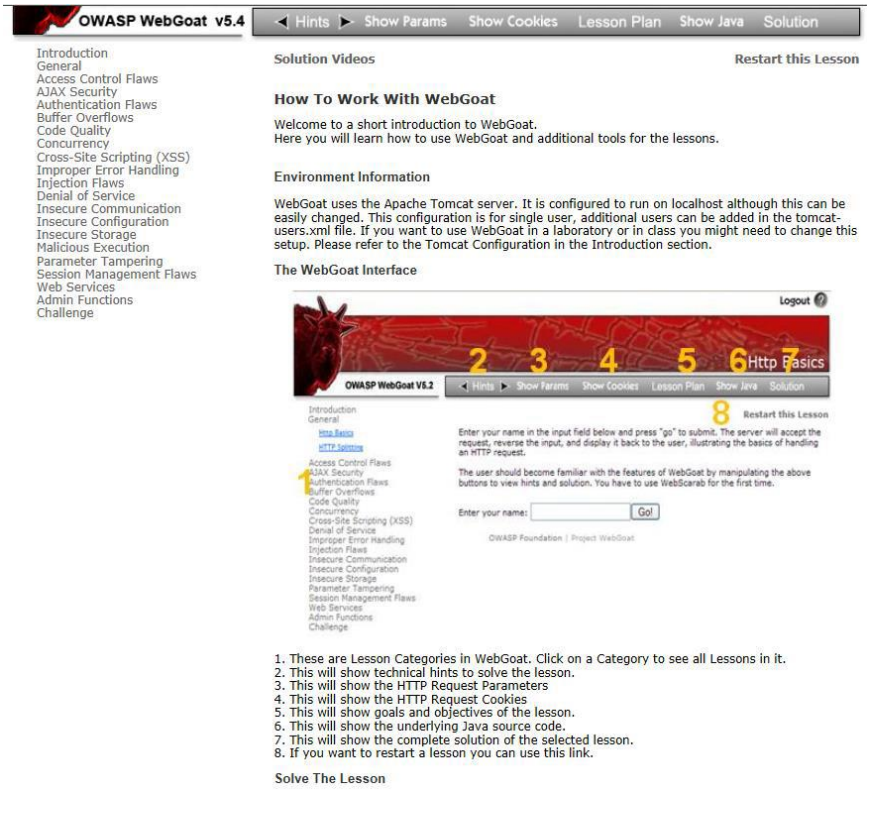

Figure 2: WebGoat Sample 2

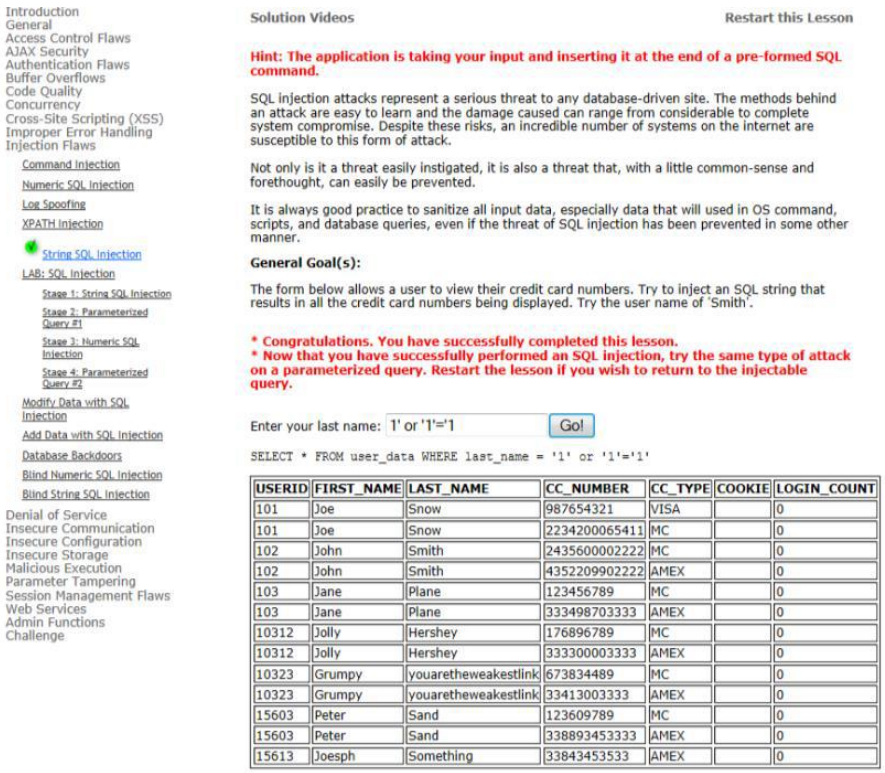

Figure 3: WebGoat Sample 3