**Task 1 – Katie**

**Task 2 – Derek**

**Task 3a – Katie**

**Task 3b - George**

**Task 1:** The main purpose of this task is to provide you with a strong knowledgebase in web security. Your answers should not exceed a single sentence. Terseness is the key to successfully completing this section. [8 points]

**Q. Do some research on these items and then answer the following questions.**

|  |  |  |  |
| --- | --- | --- | --- |
| Input validation | Adware | Browser hijacking | Payload |
| Race condition | Spam | Checksum | Variant |
| Privilege confusion | Spyware | Sniffer | Firewall |
| Privilege escalation | Hacker | Password sniffing | Antivirus |
| Zero-day attack | Backdoor | Proxy | Retrovirus |
| Phishing | Denial of Service (DoS) | Man-in-middle | Intrusion Detection System |
| Logic/time bomb | Brute-force attack | Pharming | Sandboxing |

**1. Pick out 4 terms that belong to attack techniques and explain each of them.**

**2. Pick out 4 terms that belong to defense techniques and explain each of them.**

**Task 2:** In sections “Injection Attacks” and “WebGoat,” there are questions marked in red (also in *italics*). Under this task, answer all those questions. [16 points]

**Q. List any four malicious objectives that an attacker can achieve using SQL injection attack**? [2 points]

**Q. Briefly answer the following questions about SQL injection.** [4 points]

* ***Can you see a full list of all the employees in the database? Explain your answer and write down the SQL queries involved, if any.***
* ***Can you add a new employee to the database? Explain your answer and write down the SQL queries involved, if any.***

**Q. Briefly describe and demonstrate the various prevention measures that can be taken against SQL injection attacks (no implementations necessary).** [4 points]

**Q. Because WebGoat is a vulnerable web application, it will make your system insecure while you work on this project. How can an attacker attack your system if you are using WebGoat without taking any precautions?** [2 points]

**Q. How do you fix the above-mentioned problem? (Hint: There are multiple ways to fix this problem. You get points for mentioning the solution that does not hamper other system functionalities.)** [2 points]

**Q. What is the principle of least privilege? How can you manage access privileges for using WebGoat?** [2 points]

**Task 3a):**

**Run WebGoat and execute all the lessons under ‘Injection flaws’ (leave out the ones that require development version of WebGoat) and write a summary of your experience in one paragraph.**

**Task 3b):**

**From the lessons you learned (Task 3a), implement and demonstrate**

**1) string SQL injection and**

**2) Cross-Site Scripting attack (XSS attack).**

**For each of these attacks, summarize your understanding including:** [24 points]

** *SQL statements used.***

** *Modified SQL statement used for the SQL injection. How did it work?***

** *How did WebGoat fix the vulnerability (Hint: See ‘Show Java’ tab)?***

** Screenshots.**

**Part II - Block Ciphers: Symmetric Key Crypto Systems [52 points]**