CSIS 330 – Lab 6: Identifying Security Vulnerabilities

**Background:**

SANS (SysAdmin, Audit, Network, Security) is a site that provides information on defenses for threats against computers and networks.

In this assignment, you will utilize the SANS website to identify security threats and preventative measures that can be taken to secure a computer or network.

**Assignment Instructions:**

*[A Word template is provided for your answers.]*

1. Go to the <http://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html>

For example: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'). (updated 2021, September from <http://cwe.mitre.org/data/definitions/89.html>).

1. Select from the list shown by selecting the CWE number.
2. In the “Insecure Interaction Between Components” section, click the weakness **CWE ID** link (CWE-89 Improper Neutralization of Special element used in an SQL Command ‘SQL Injection’)
3. **Answer the following questions in one or two sentences each: (1 point each)**
4. What is the Weakness Prevalence of this issue?
5. Describe how attackers can exploit this vulnerability.
6. List one “Architecture and Design” Prevention and Mitigation strategy that can be used to defend against this threat.
7. What is one “Implementation” approach used to defend against this threat?
8. List 2 CWEs of your choice that are related to this issue.
9. Highlight five of the ***Potential Mitigations*** Phases in the link provided and write a brief explanation of each based on your research.

**Deliverables:**

Save your Answer Template using the convention of [your first initial] + [your last name] + “\_Lab6”.

For example: Joe Smith will save his file template as JSmith\_Lab6.doc .

Submit your **Word Template** to Blackboard by attaching it to the appropriate assignment link.