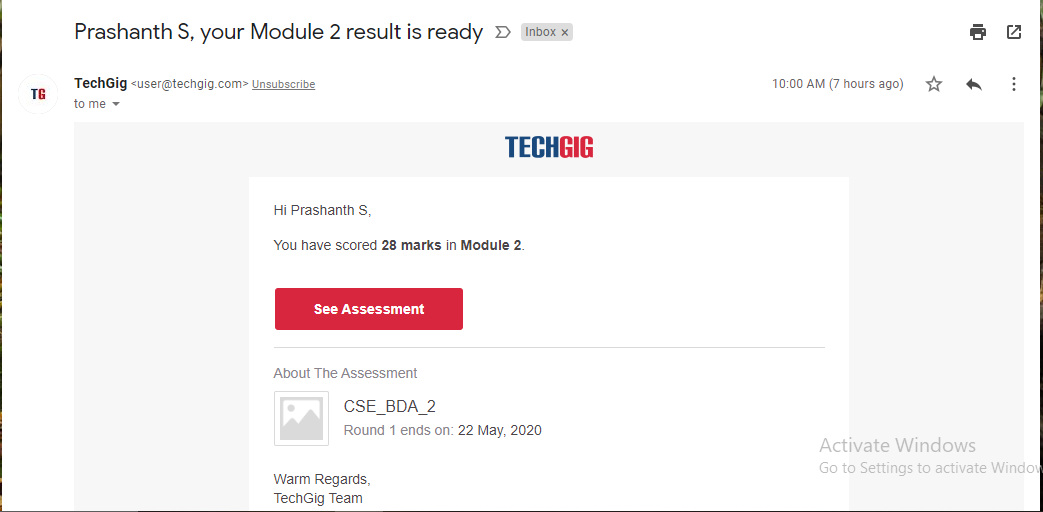
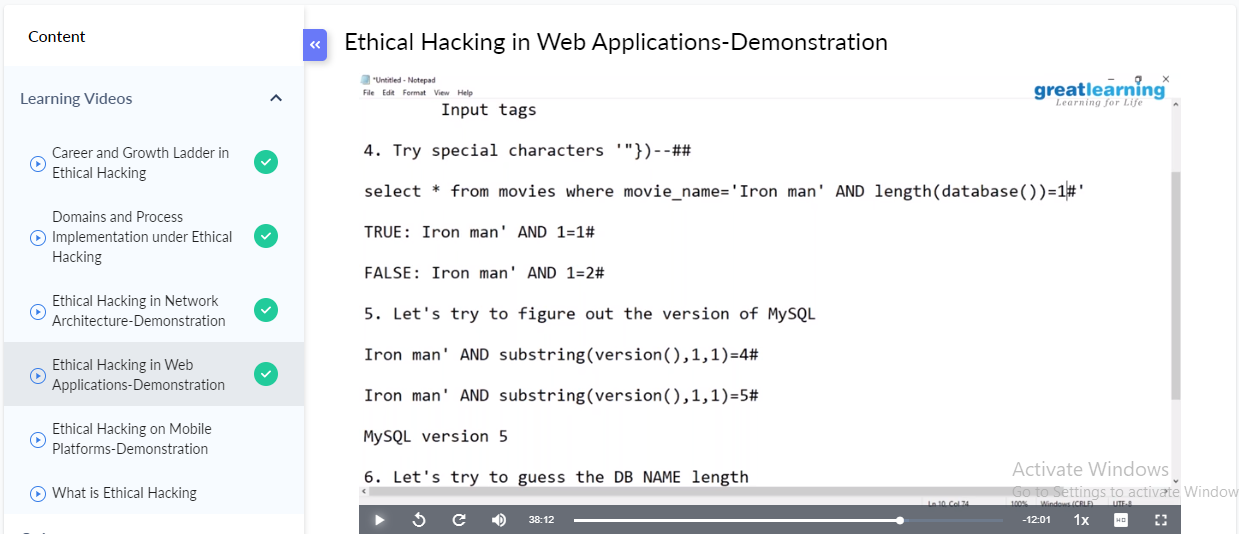
**DAILY ONLINE ACTIVITIES SUMMARY**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Date:** | **22-05-2020** | | | | | **Name:** | **Prashanth S** | |
| **Sem & Sec** | **8th sem B sec** | | | | | **USN:** | **4AL16CS069** | |
| **Online Test Summary** | | | | | | | | |
| **Subject** | | **BDA** | | | | | | |
| **Max. Marks** | | **40** | | **Score** | | | **28** | |
| **Certification Course Summary** | | | | | | | | |
| **Course** | **Introduction to Ethical hacking** | | | | | | | |
| **Certificate Provider** | | | **Great learning website** | | **Duration** | | | **6hr** |
| **Coding Challenges** | | | | | | | | |
| **Problem Statement: missing number in array** | | | | | | | | |
| **Status: completed** | | | | | | | | |
| **Uploaded the report in Github** | | | | | **yes** | | | |
| **If yes Repository name** | | | | | **prashanth** | | | |
| **Uploaded the report in slack** | | | | | **yes** | | | |

Online Test Details: (Attach the snapshot and briefly write the report for the same)



Certification Course Details: (Attach the snapshot and briefly write the report for the same)



Web application provides an interface between the web server and the client to communicate. Web pages are generated at the server, and browsers present them at the client side. The data is passed between client and server in the form of HTML pages through HTTP protocol.

There are client-side vulnerabilities and server-side vulnerabilities which lead to a web application

**Parameter Tampering:**

This involves modifying parameters exchanged between client and server, which may lead to XSS attack and SQL injection attack. Usually, HTML data goes as a name-value pair; if the attacker is able to modify the values of the parameter during transfer, it may lead to many other attacks.

**Directory traversal Attack:**

This is a type of vulnerability where an attacker is able to access beyond the web root directory, into the restricted directories on the web server. Then an attacker will be able to access system files, run OS commands, access configuration information, etc.

Coding Challenges Details: (Attach the snapshot and briefly write the report for the same)

Coding was given n it was uploaded for github and slack

PROGRAM1

|  |  |
| --- | --- |
| def MissingNo(A): | |
|  | n = len(A) | |
|  | total = (n + 1)\*(n + 2)/2 | |
|  | calsum = sum(A) | |
|  | return total - calsum | |
|  | |  |
|  | l=[] | |
|  | l=int(input("Enter the array")) | |
|  | miss = MissingNo(l) | |
|  | print(miss) | |