DAILY ONLINE ACTIVITIES SUMMARY

Date:	**29-05-2020**	**Name:**	**PRASANNA**
Sem & Sec	**8th,B**	**USN:**	**4AL16CS068**

Online Test Summary

Subject	**BDA**		
Max. Marks	**30**	**Score**	**24**

Certification Course Summary

Course	**Introduction to ethical hacking**		
Certificate Provider	**Great learner academy**	**Duration**	**6 Hrs**

Coding Challenges

Problem Statement: prob1- ***To check whether the given year is leap year or not***

Status: Solved

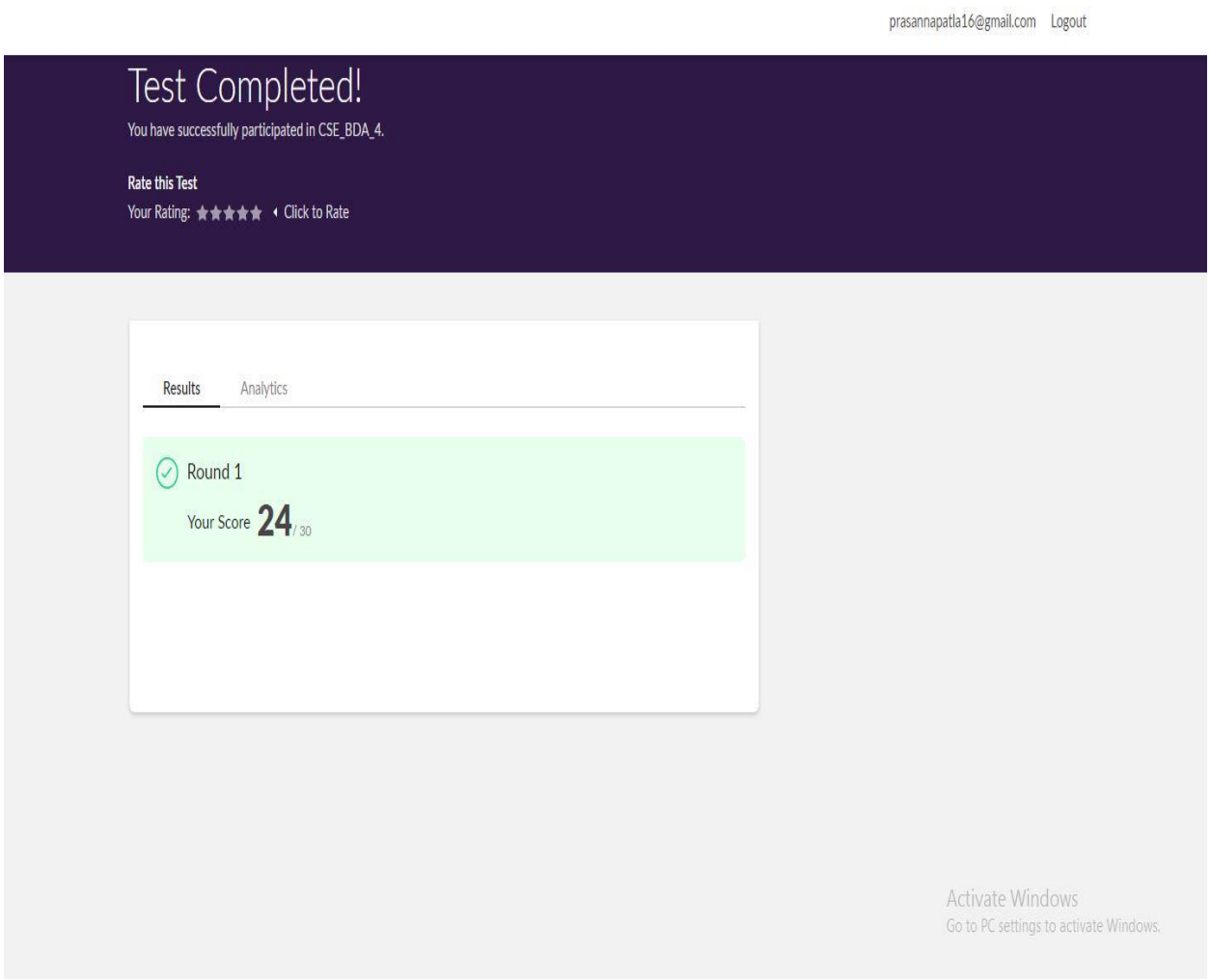
Uploaded the report in Github	**Yes**
If yes Repository name	**prasanna_p**
Uploaded the report in slack	**Yes**

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)

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

1) Online Test Details:

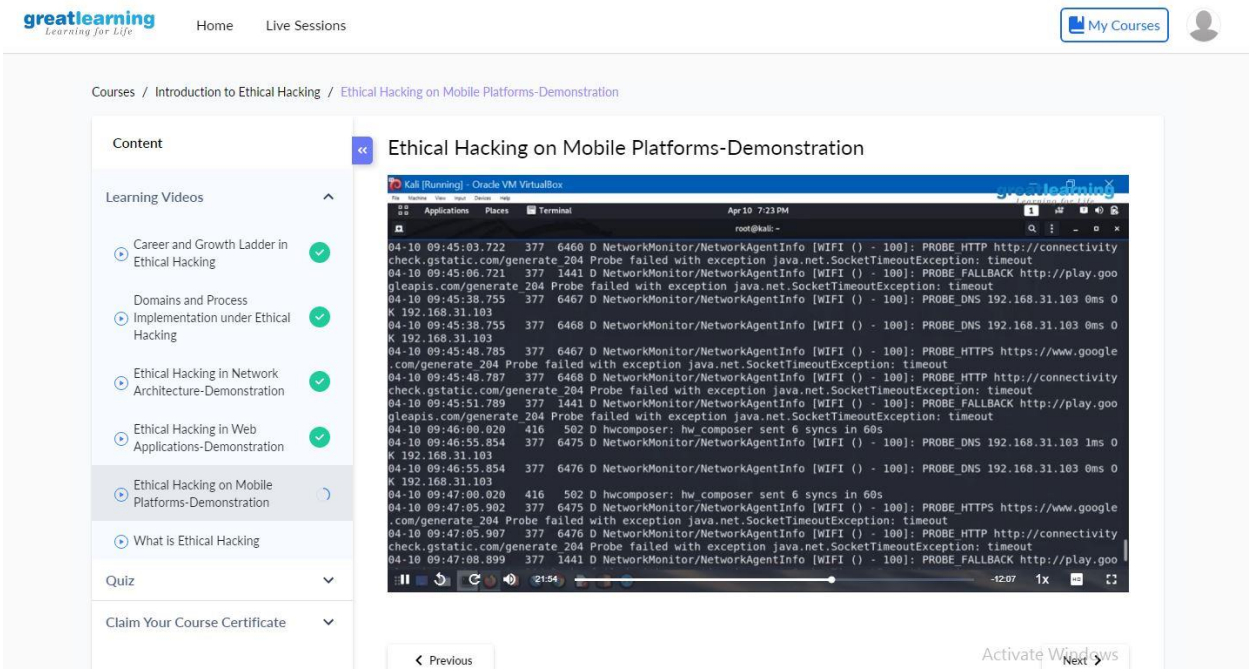


2) Certification Course Details:

Domains Under Ethical hacking

- Web application Domain
- Mobile
- Network Architecture Domain

Direct communication cannot be achieved across application domains. However, application domains can still talk to each other by passing objects via marshalling by value (unbound objects), marshalling by reference through a proxy (application-domain-bound objects). There is a third type of object called a context-bound object which can be marshalled by reference across domains and also within the context of its own application domain. Because of the verifiable type-safety of managed code, a CLI can provide fault isolation between domains at a much lower cost than an operating system process can. The static type verification used for isolation does not require the same process switches or hardware ring transitions that an operating system process requires.



Web application domain:

Two major categories:

- Client Side vulnerabilities
- Server side vulnerabilities

All the attacks can be categorized into 3 major attacks:

- Parameter tampering
- Unvalidated inputs
- Directory Traversal attacks

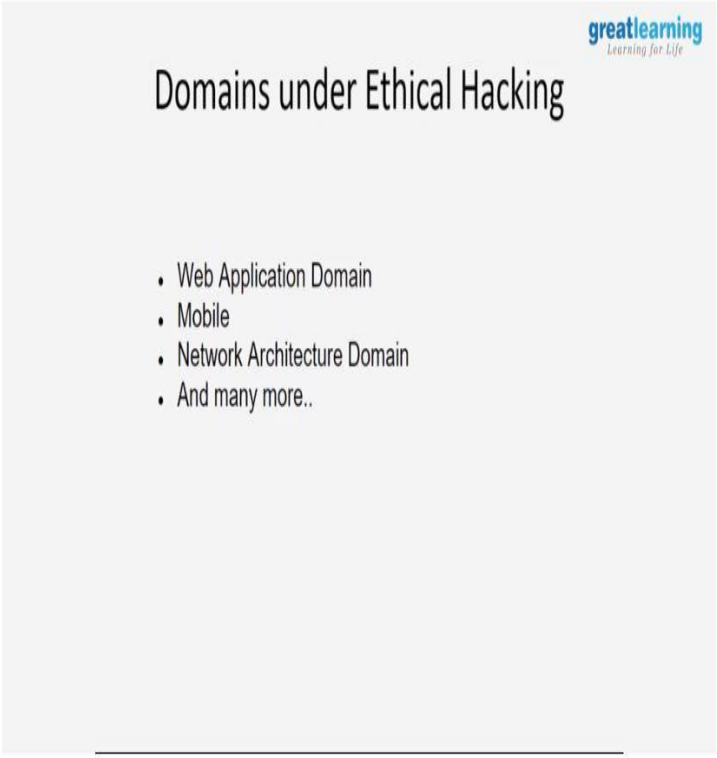
Common web application attacks:

- Injection Flaws eg.SQL injection ,HTML injection etc.
- Cross site , scripting
- Web services attacks eg.DNS cache poisoning, file uploads etc

Hacking methodology:

- Web Footprinting –gathering information
- Vulnerability Scanners –w3af,acunetix
- Identity Entry and attack surface

Domains and Process Implementation under Ethical Hacking



‹ Previous
Next ›

3) Coding Challenges:

1. To check whether the year is leap year or not

Pgrm1:

```
year = 2000

if (year % 4) == 0:
   if (year % 100) == 0:
      if (year % 400) == 0:
         print("{0} is a leap year".format(year))
      else:
         print("{0} is not a leap year".format(year))
   else:
      print("{0} is a leap year".format(year))
else:
   print("{0} is not a leap year".format(year))
```