

DAILY ONLINE ACTIVITIES SUMMARY

Date:	22-05-2020	Name:	PRASANNA
Sem & Sec	8 th ,B	USN:	4AL16CS068
Online Test Summary			
Subject	Big Data analytics		
Max. Marks	40	Score	33
Certification Course Summary			
Course	Introduction to ethical hacking		
Certificate Provider	Great learner academy	Duration	6 Hrs
Coding Challenges			
Problem Statement: prob1- Find out missing number in an array			
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:

[prasannapatla16@gmail.com](#) [Logout](#)

Test Completed!

You have successfully participated in CSE_BDA_2.

Rate this Test

Your Rating: ★★★★★ [Click to Rate](#)

[Results](#) [Analytics](#)

✓ Module 2

Your Score **33**_{/40}

[Activate Windows](#)
Go to PC settings to activate Windows.

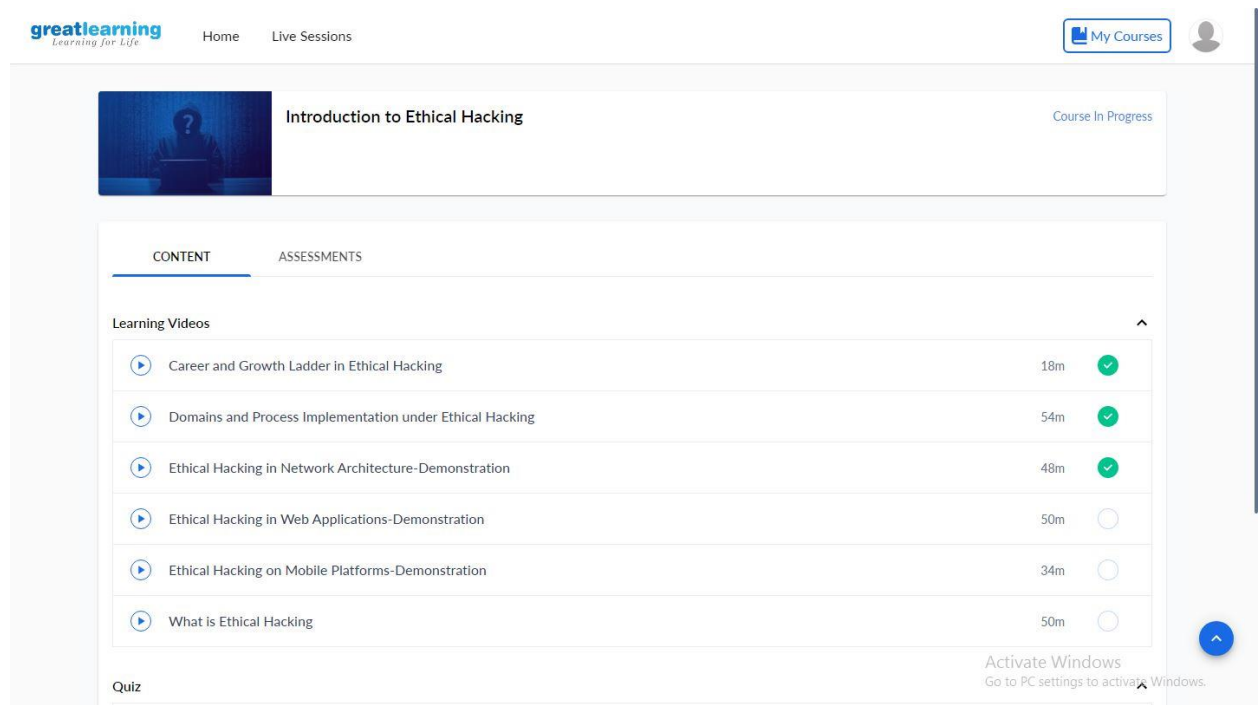
2) Certification Course Details:

Ethical Hacking in web application:

As we start doing web application testing, there's actually a number of things you can do inside your browser without having to rely on external tools. And there's actually a lot of use here because you're going to end up needing to do a lot of manual checking And maybe doing some follow up tests in addition to some of the automated tools.

Firefox has a long history of add-ons, they've been doing them for quite a while. And there's a pretty rich set of Add-on, a capability that exists from various developers around the world. So I need to go to, you saw I went to tools and add-ons, and now I am at the page that shows the add-ons manager.

This type of hacking targets applications that require the use of the internet on your browser. It includes email programs, Google apps, shopping carts, online forms, etc



The screenshot displays the 'Introduction to Ethical Hacking' course page on the Great Learning platform. The page features a header with the Great Learning logo, navigation links for 'Home' and 'Live Sessions', and a 'My Courses' button. The course title 'Introduction to Ethical Hacking' is prominently displayed, along with a 'Course In Progress' status. Below the title, there are tabs for 'CONTENT' and 'ASSESSMENTS'. The 'CONTENT' tab is active, showing a list of learning videos. Each video entry includes a play button icon, the video title, its duration, and a completion status indicator (a green checkmark for completed videos and a blue circle for incomplete ones). The videos listed are: 'Career and Growth Ladder in Ethical Hacking' (18m, completed), 'Domains and Process Implementation under Ethical Hacking' (54m, completed), 'Ethical Hacking in Network Architecture-Demonstration' (48m, completed), 'Ethical Hacking in Web Applications-Demonstration' (50m, incomplete), 'Ethical Hacking on Mobile Platforms-Demonstration' (34m, incomplete), and 'What is Ethical Hacking' (50m, incomplete). At the bottom of the page, there is a 'Quiz' section and a Windows activation watermark.

Video Title	Duration	Status
Career and Growth Ladder in Ethical Hacking	18m	Completed
Domains and Process Implementation under Ethical Hacking	54m	Completed
Ethical Hacking in Network Architecture-Demonstration	48m	Completed
Ethical Hacking in Web Applications-Demonstration	50m	Incomplete
Ethical Hacking on Mobile Platforms-Demonstration	34m	Incomplete
What is Ethical Hacking	50m	Incomplete

bWAPP :

bWAPP, or a *buggy web application*, is a free and open source deliberately insecure web application.

It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.

bWAPP prepares one to conduct successful penetration testing and ethical hacking projects.

bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux/Windows with Apache/IIS and MySQL. It can also be installed with WAMP or XAMPP.

Why are web applications an attractive target?

- Easily available via the Internet (24/7)
- Mission-critical business applications with sensitive data
- Often direct access to backend data
- Traditional firewalls and SSL provide no protection
- Many applications are custom-made == vulnerable

OWASP :

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

The OWASP Mobile Security Testing Guide (MSTG) is a comprehensive manual for mobile app security testing and reverse engineering for the iOS and Android platform, describing technical processes for verifying the controls listed in the MSTG's co-project Mobile Application Verification Standard (MASVS).

The MASVS defines a mobile app security model and lists generic security requirements for mobile apps while the MSTG serves as a baseline for manual security testing and as a

template for automated security tests during or after development. Included with the MSTG, the Mobile Security Hacking Playground is a collection of iOS and Android mobile apps, that are intentionally built insecure.

The screenshot shows the Great Learning website interface. At the top, there's a navigation bar with the Great Learning logo, 'Home', 'Live Sessions', a 'My Courses' button, and a user profile icon. Below this, a breadcrumb trail reads 'Courses / Introduction to Ethical Hacking / Ethical Hacking in Web Applications-Demonstration'. The main content area is split into two columns. The left column, titled 'Content', contains a 'Learning Videos' section with a list of videos: 'Career and Growth Ladder in Ethical Hacking', 'Domains and Process Implementation under Ethical Hacking', 'Ethical Hacking in Network Architecture-Demonstration', 'Ethical Hacking In Web Applications-Demonstration' (which is highlighted with a blue bar and a play icon), 'Ethical Hacking on Mobile Platforms-Demonstration', and 'What is Ethical Hacking'. Below the videos are sections for 'Quiz' and 'Claim Your Course Certificate'. The right column displays the video player for 'Ethical Hacking in Web Applications-Demonstration'. The video shows a web browser window displaying the OWASP Broken Web Applications Project (owaspbwa) homepage. The page includes a warning message: '!!! This VM has many serious security issues. We strongly recommend that you run it only on the "test only" or "NAT" network in the virtual machine settings !!!'. Below the warning is a section titled 'TRAINING APPLICATIONS'. The video player has a progress bar at 10:40 and a volume icon. At the bottom of the video player, there are 'Previous' and 'Next' navigation buttons. A watermark 'Activate Windows. Go to PC settings to activate Windows.' is visible in the bottom right corner of the video player area.

Hosted at some of most iconic technology companies in the world, the Bay Area chapter is one of the Foundation's largest and most active. This month they are hosting a Hacker Day and monthly meetups in San Francisco at Insight Engines and in South Bay at EBay. Usually the agenda includes three proactive and interesting talks, lots of interesting people to meet, and great food. The Bay Area Chapter also participates in planning AppSec California

3) Coding Challenges:

1. Given an array containing n distinct numbers taken from 0, 1, 2, ..., n, find the one that is missing from the array.

Example 1:

Input: [3,0,1]

Output: 2

Example 2:

Input: [9,6,4,2,3,5,7,0,1]

Output: 8

Program :

```
def missNo(x):  
    l=len(x)  
  
    maxs=max(x)  
  
    mins=min(x)  
  
    for i in range(0,l):  
        if mins not in x and mins<=maxs:  
            return mins  
        else:  
            mins+=1  
  
y=[9,8,7,6,5,3]  
  
m=(missNo(y))  
  
print("missing number is",m)
```