COMPUTER ENGINEERING DEPARTMENT

SUBMISSION REPORT

SUB: Cryptography and System Security

COURSE: T.E. **Year: 2020-2021** **Semester: VI**

DEPT: Computer Engineering

SUBJECT CODE: CSC604 **SUBMISSION DATE: 14/05/2021**

==========

Name: Amey Thakur **Roll No.: 50**

Class: TE Comps B **ID: TU3F1819127**

INDEX

Sr. No.	Particulars	Submitted/Not Submitted or Enter Marks received
	Experiments	
1	Design and Implementation of a product cipher using Substitution and Transposition ciphers.	9/10
2	Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA/El Gamal.	9/10
3	For varying message sizes, test the integrity of the message using MD-5, SHA-1, and analyze the performance of the two protocols. Use crypt APIs.	9/10
4	Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.	9/10
5	Design a network and implement packet sniffing on telnet traffic using Wireshark.	9/10
6	Implement ARP spoofing using Ettercap.	9/10
7	Download and install Nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, TCP port scan, UDP port scan, Xmas scan etc.	9/10
8	Perform SQL injection on a vulnerable website.	9/10
9	Simulate DOS attack using Hoping, hping3 and other tools.	9/10
10	Explore the GPGwin tool and implement email security.	8/10

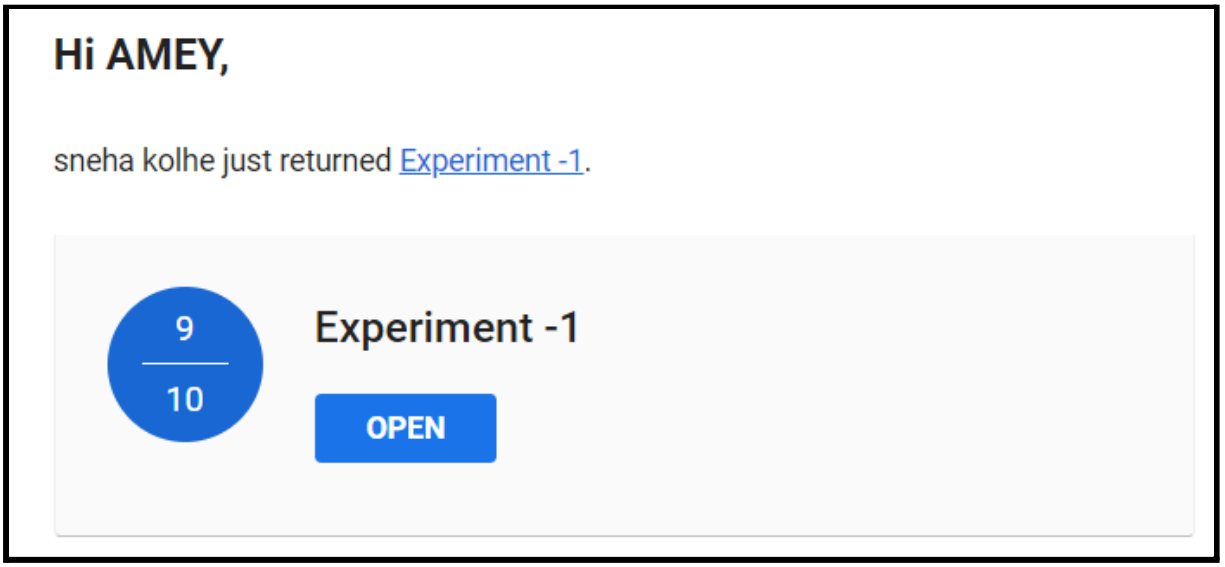
Assignments		
13	Assignment No. 1	9/10
14	Assignment No. 2	9/10
15	Assignment No. 3	Submitted
Quizzes		
16	CSS Quiz 1	10/10
17	CSS Quiz 2	10/10
18	CSS Quiz 3	10/10
19	CSS Quiz 4	10/10
20	CSS Quiz 5	10/10
21	CSS Quiz 6	10/10
IAT		
22	IAT-1	18/20
23	IAT-2	Submitted
Exit Survey		
24	Course Exit Survey	Submitted
25	Laboratory Exit Survey	Submitted

Signature:

Experiments

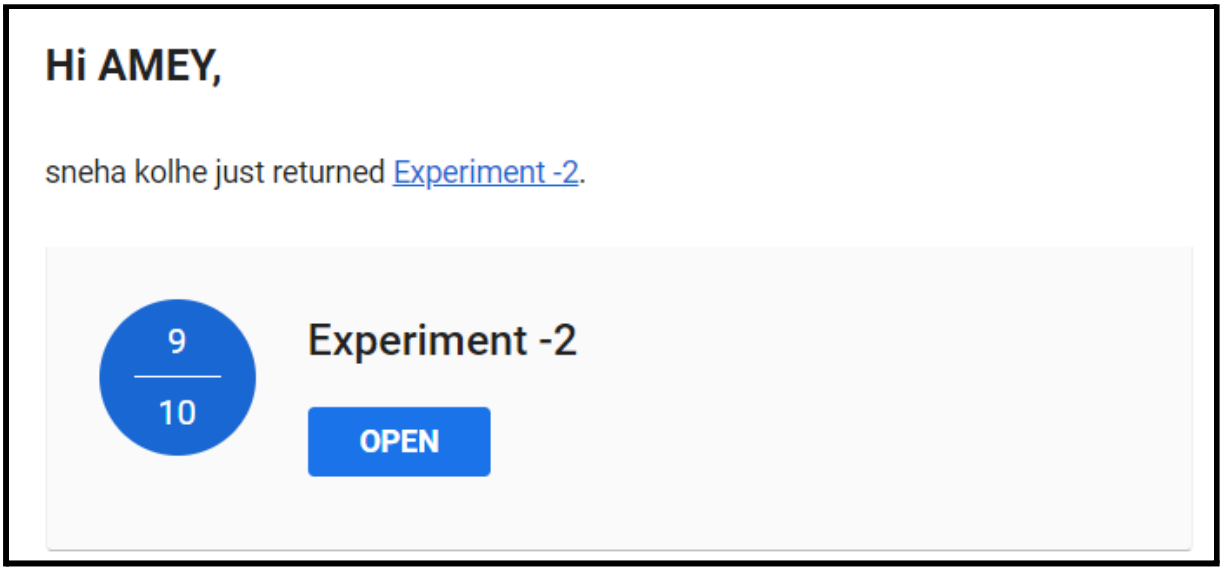
CSS Experiment 1

Marks: (9/10)



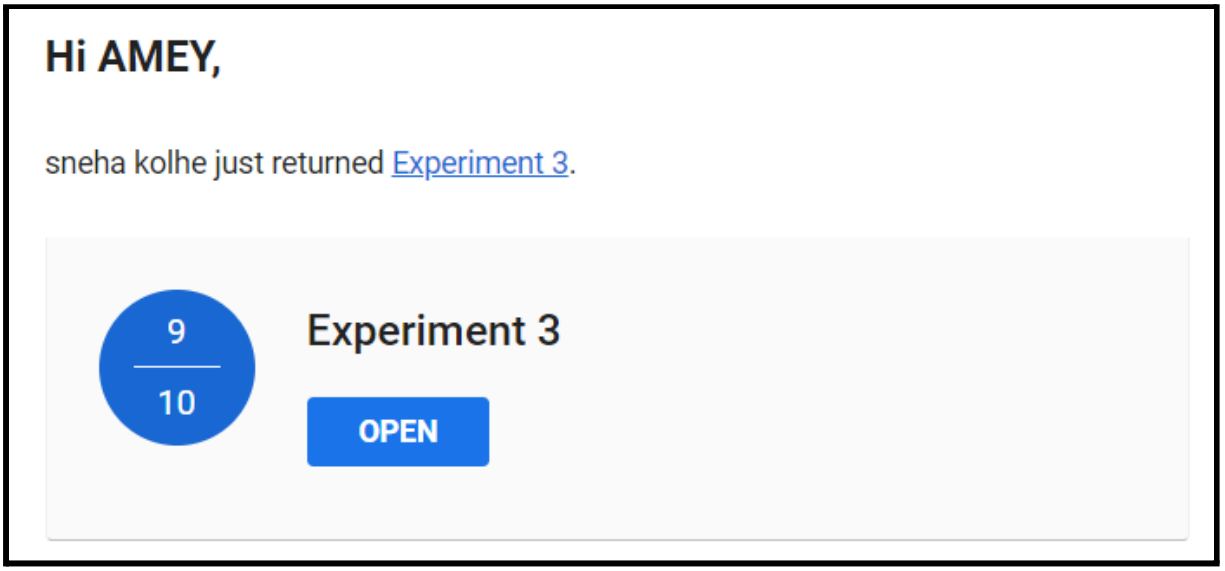
CSS Experiment 2

Marks: (9/10)



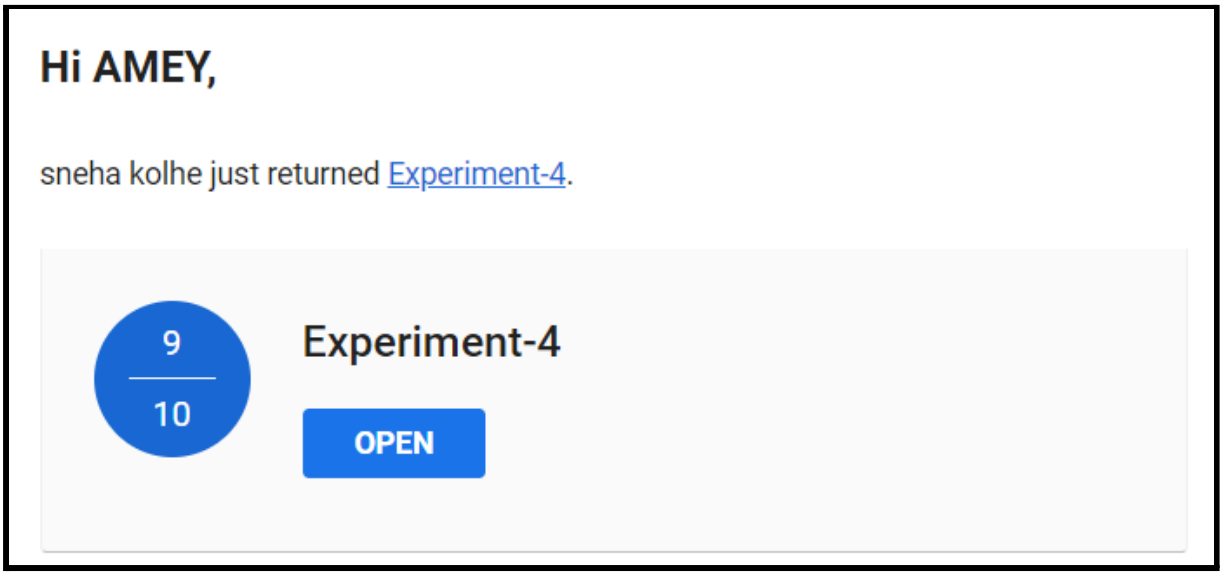
CSS Experiment 3

Marks: (9/10)



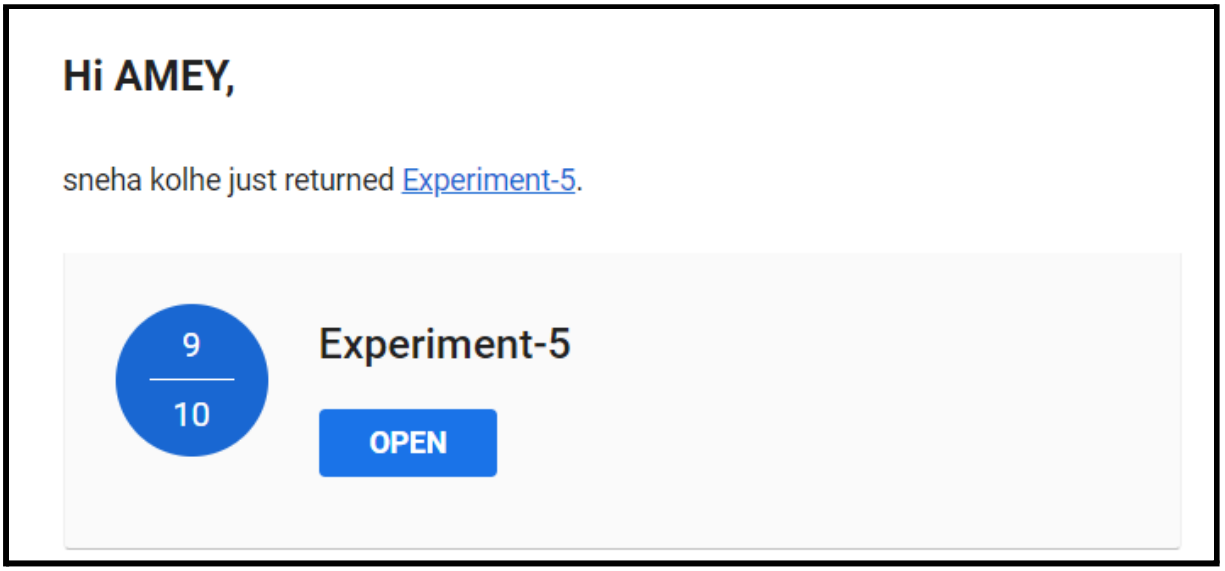
CSS Experiment 4

Marks: (9/10)



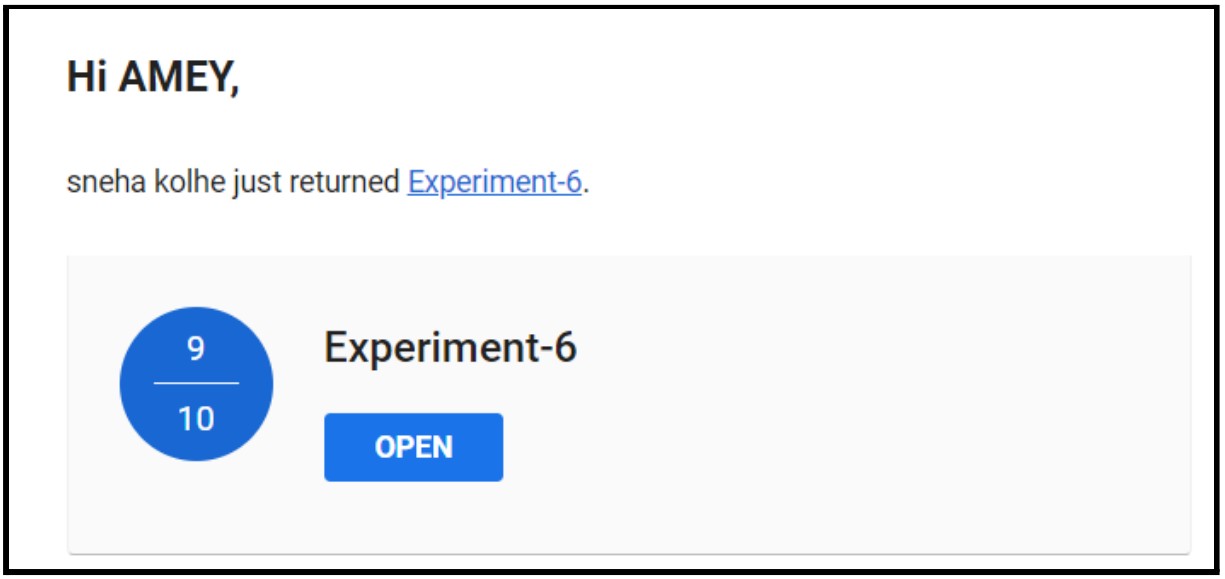
CSS Experiment 5

Marks: (9/10)



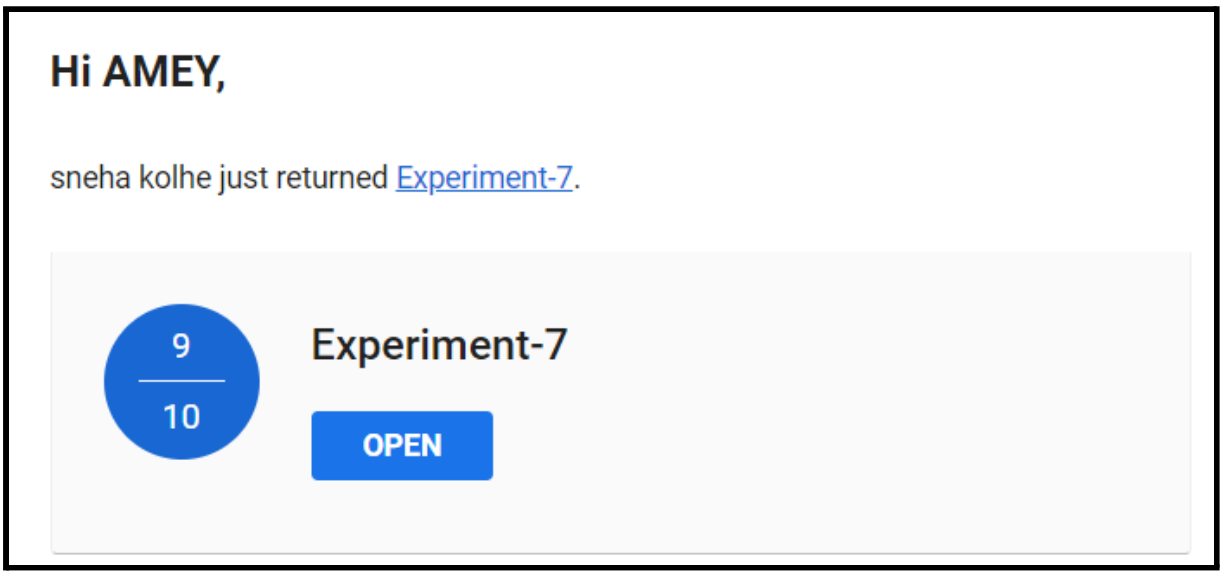
CSS Experiment 6

Marks: (9/10)



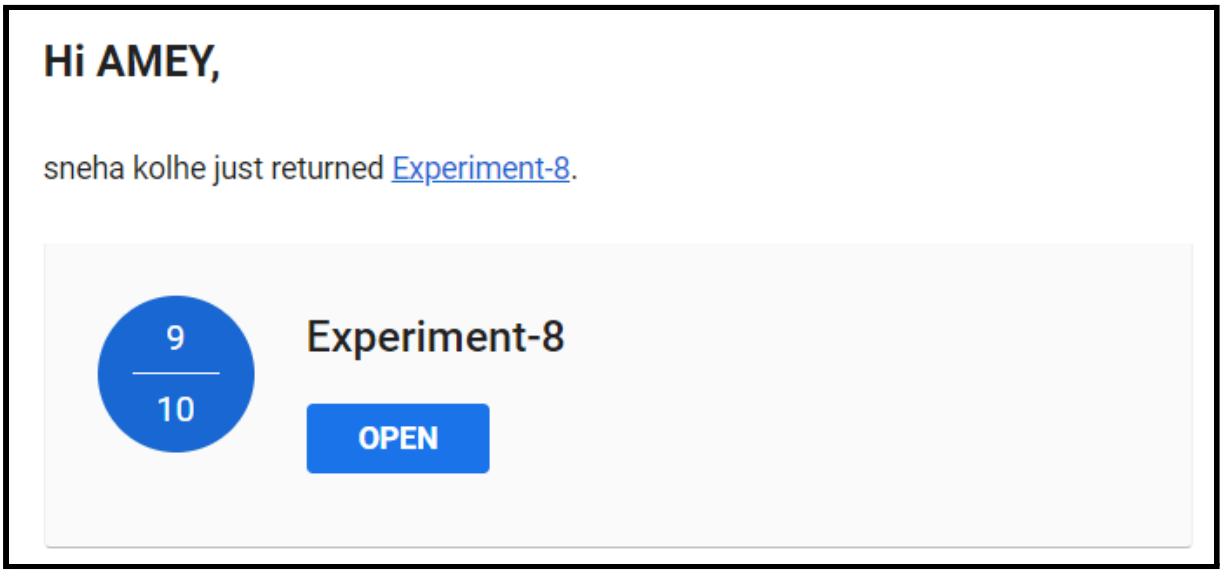
CSS Experiment 7

Marks: (9/10)



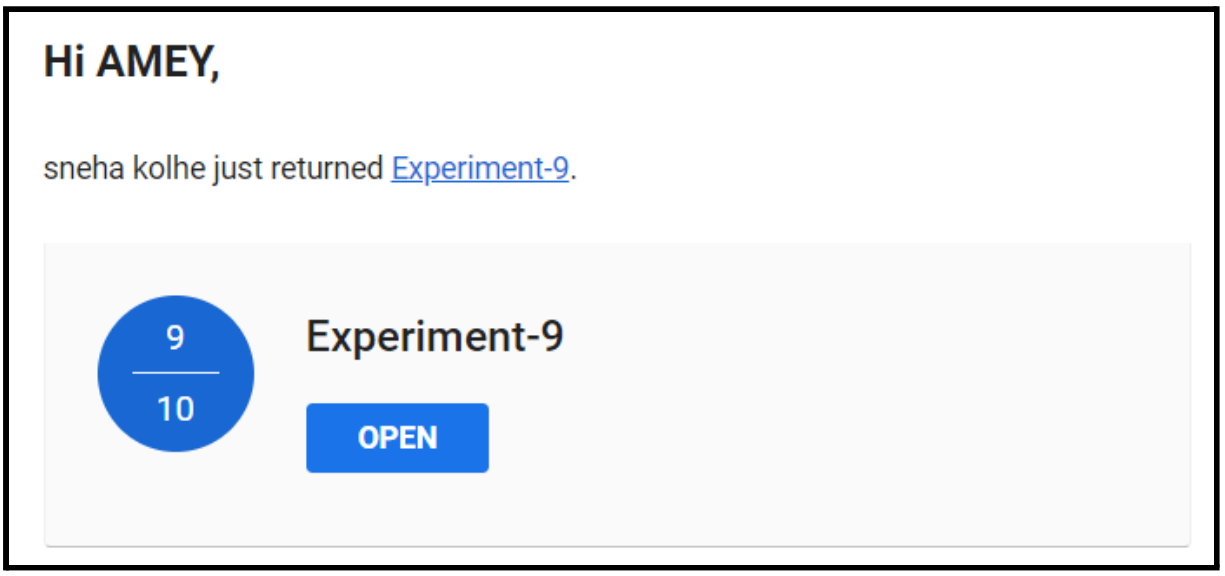
CSS Experiment 8

Marks: (9/10)



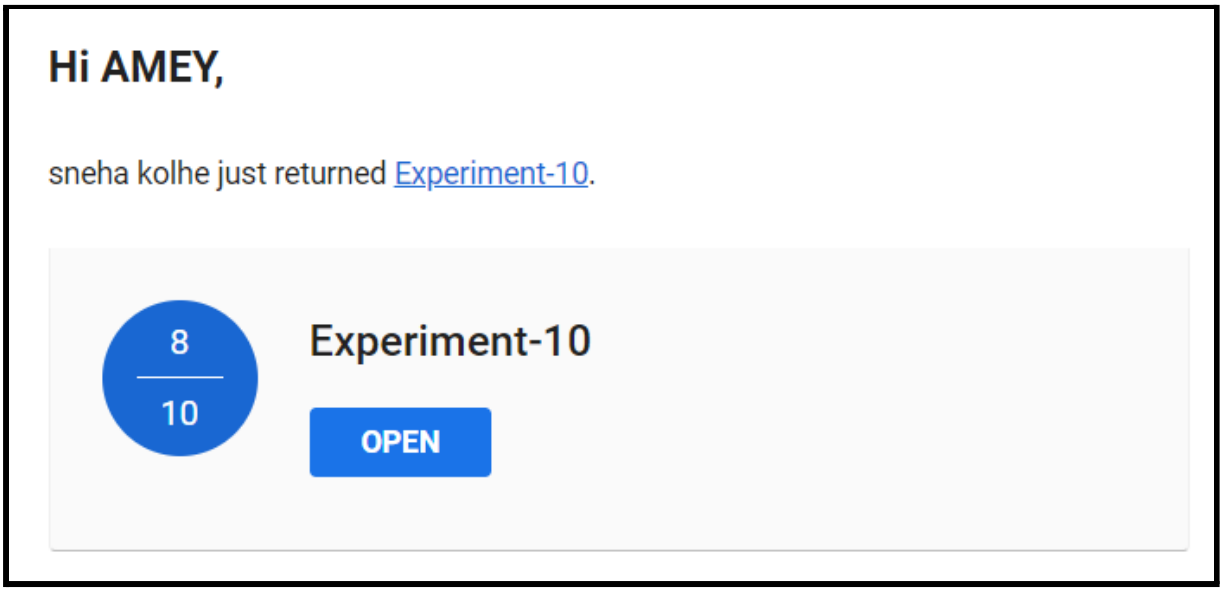
CSS Experiment 9

Marks: (9/10)



CSS Experiment 10

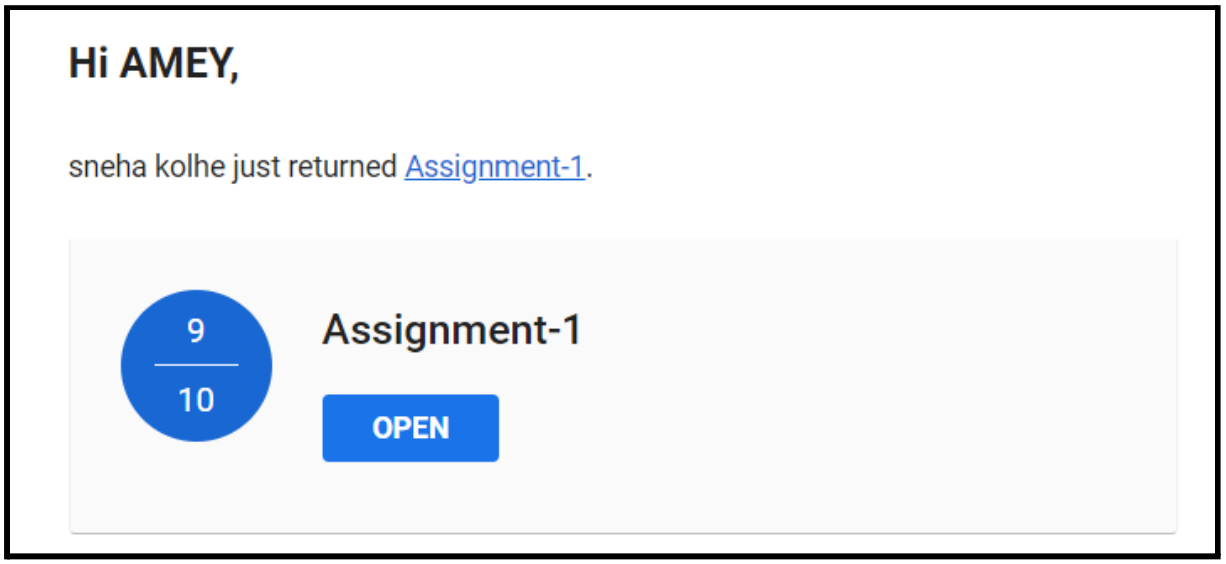
Marks: (8/10)



Assignments

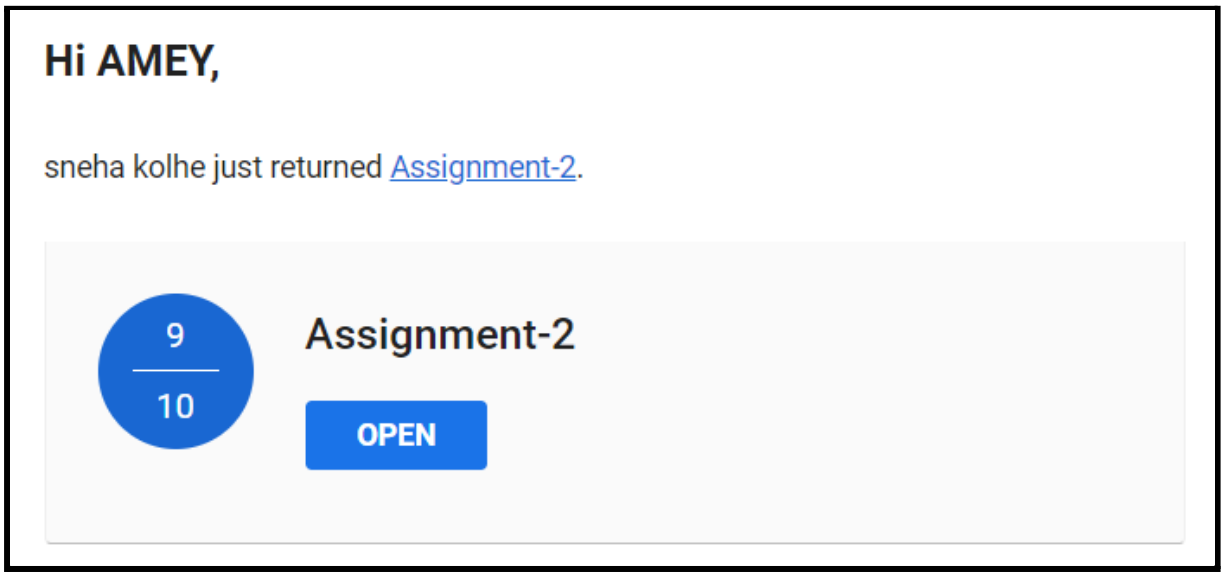
CSS Assignment 1

Marks: (9/10)



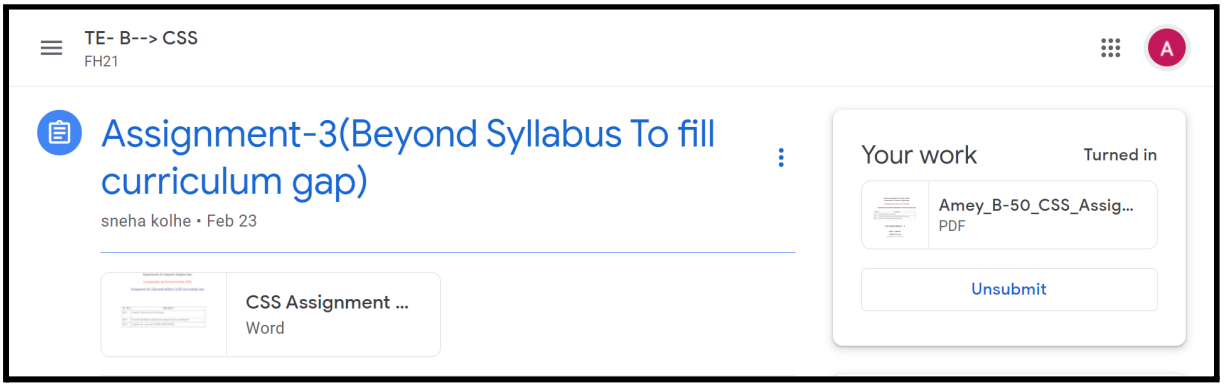
CSS Assignment 2

Marks: (9/10)



CSS Assignment 3

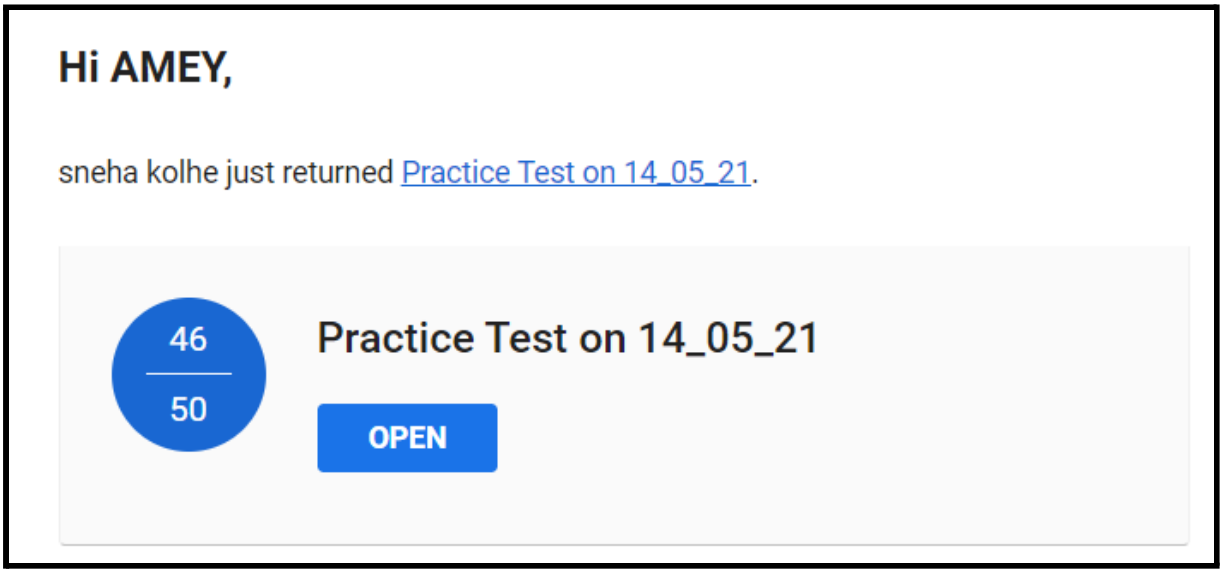
Marks: Not Received



CSS Practice Test

Date: 14/05/2021

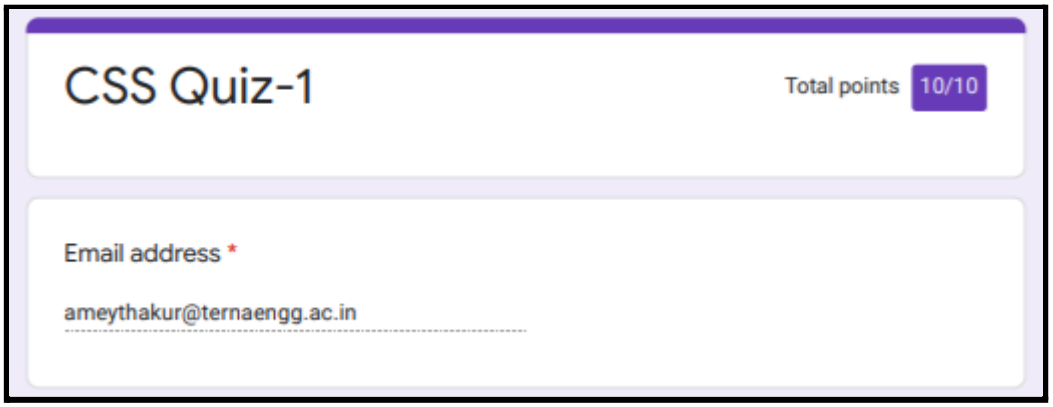
Marks: (46/50)



Quizzes

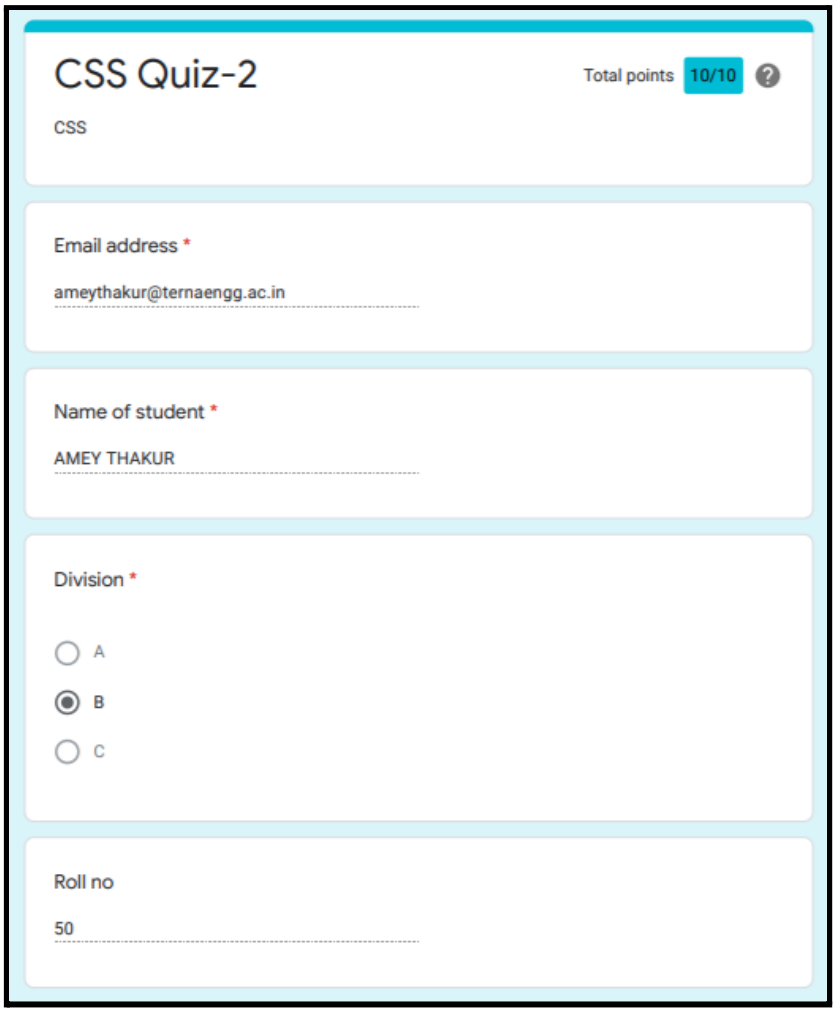
CSS Quiz 1

Marks: (10/10)



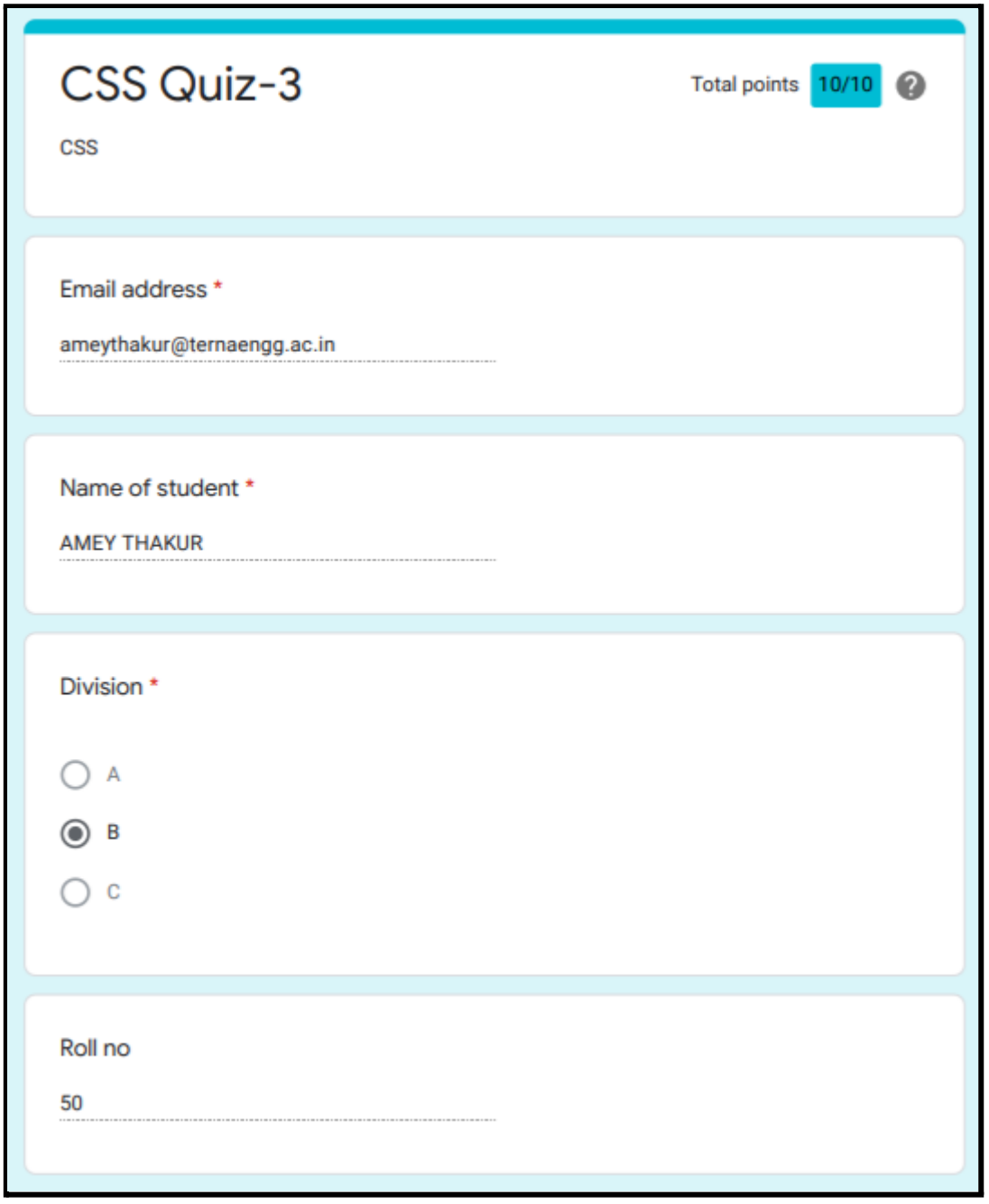
CSS Quiz 2

Marks: (10/10)



CSS Quiz 3

Marks: (10/10)



CSS Quiz-3

Total points 10/10

CSS

Email address *

ameythakur@ternaengg.ac.in

Name of student *

AMEY THAKUR

Division *

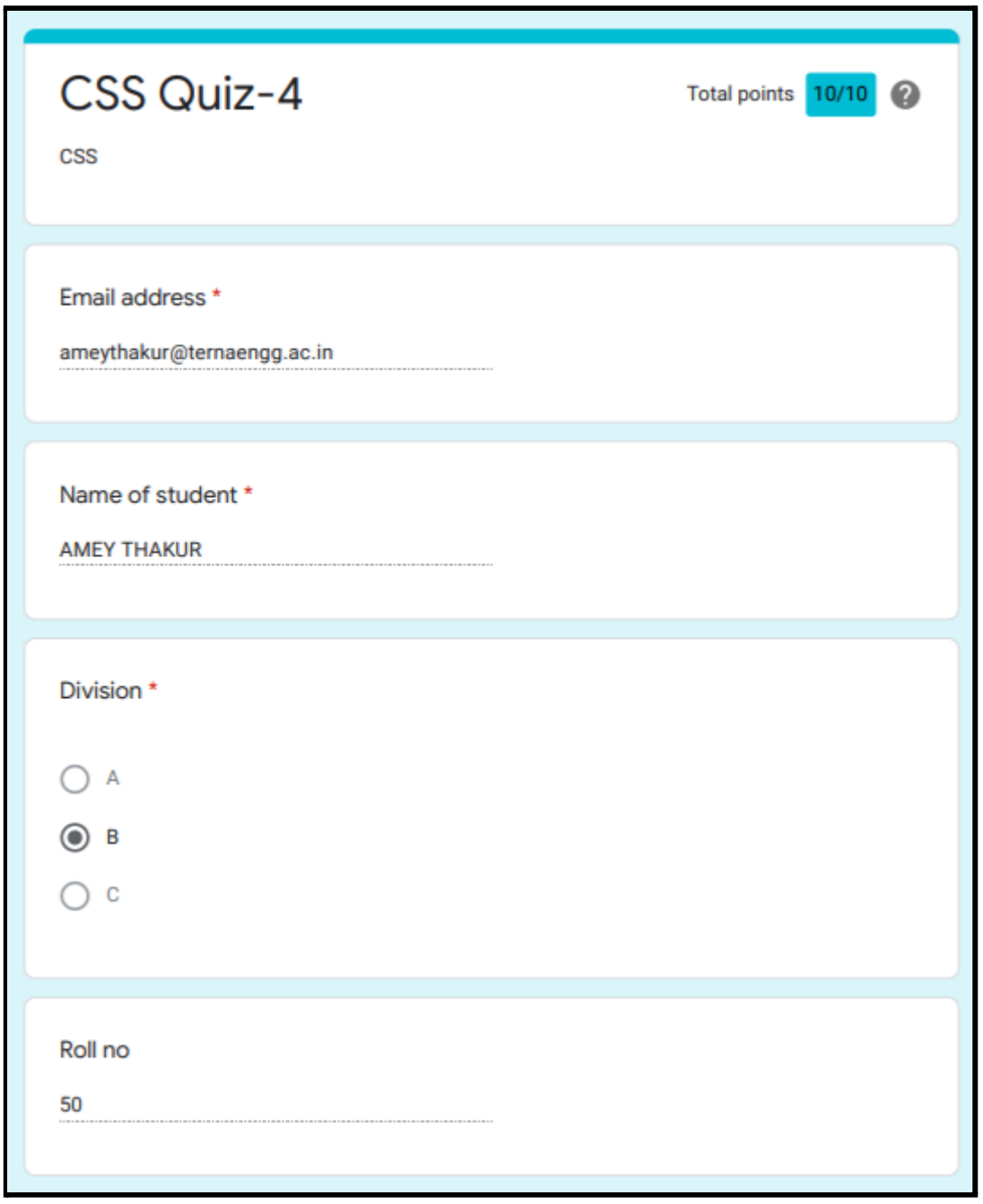
- A
- B
- C

Roll no

50

CSS Quiz 4

Marks: (10/10)



CSS Quiz-4

Total points 10/10

CSS

Email address *

ameythakur@ternaengg.ac.in

Name of student *

AMEY THAKUR

Division *

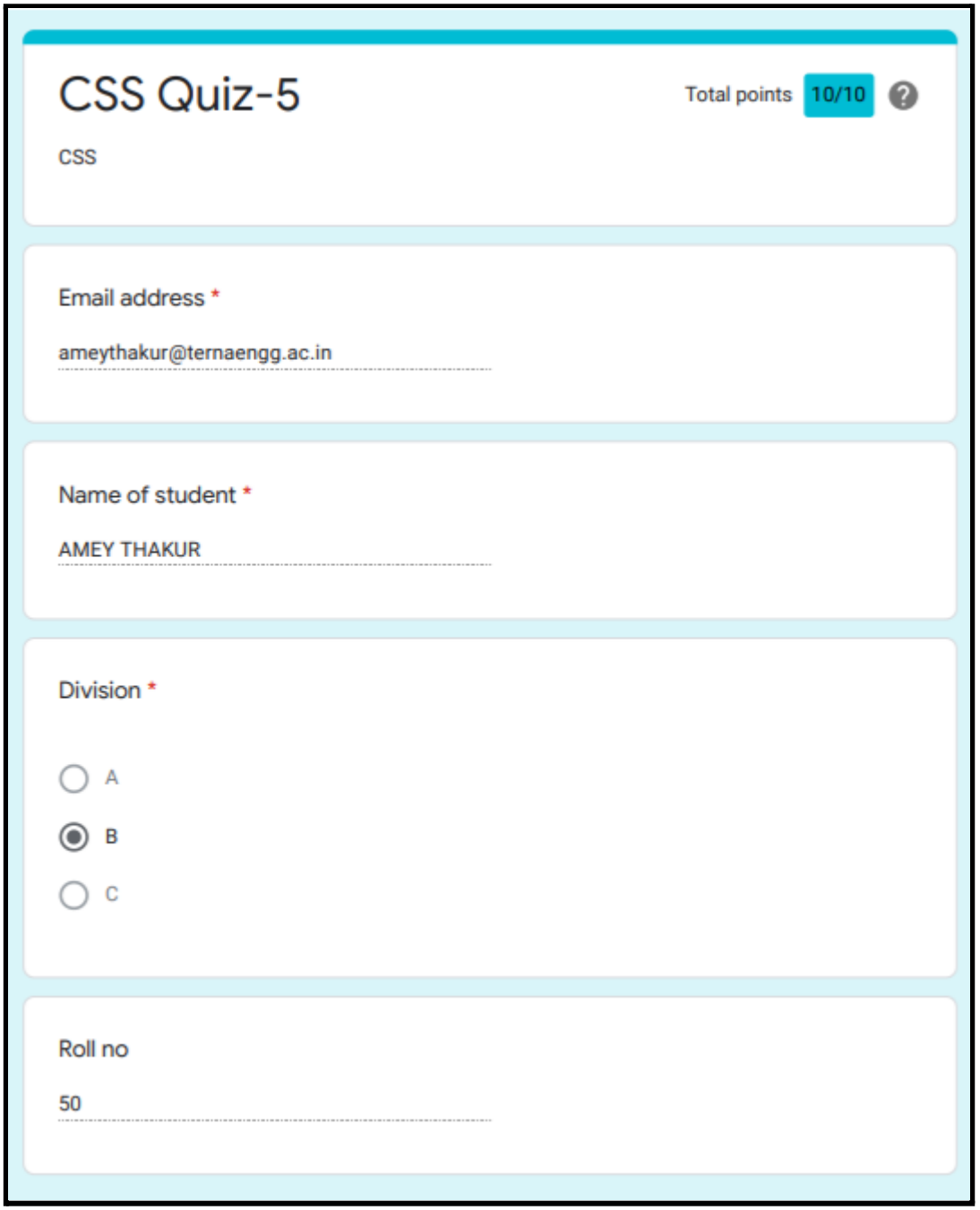
- A
- B
- C

Roll no

50

CSS Quiz 5

Marks: (10/10)



CSS Quiz-5

Total points 10/10

CSS

Email address *

ameythakur@ternaengg.ac.in

Name of student *

AMEY THAKUR

Division *

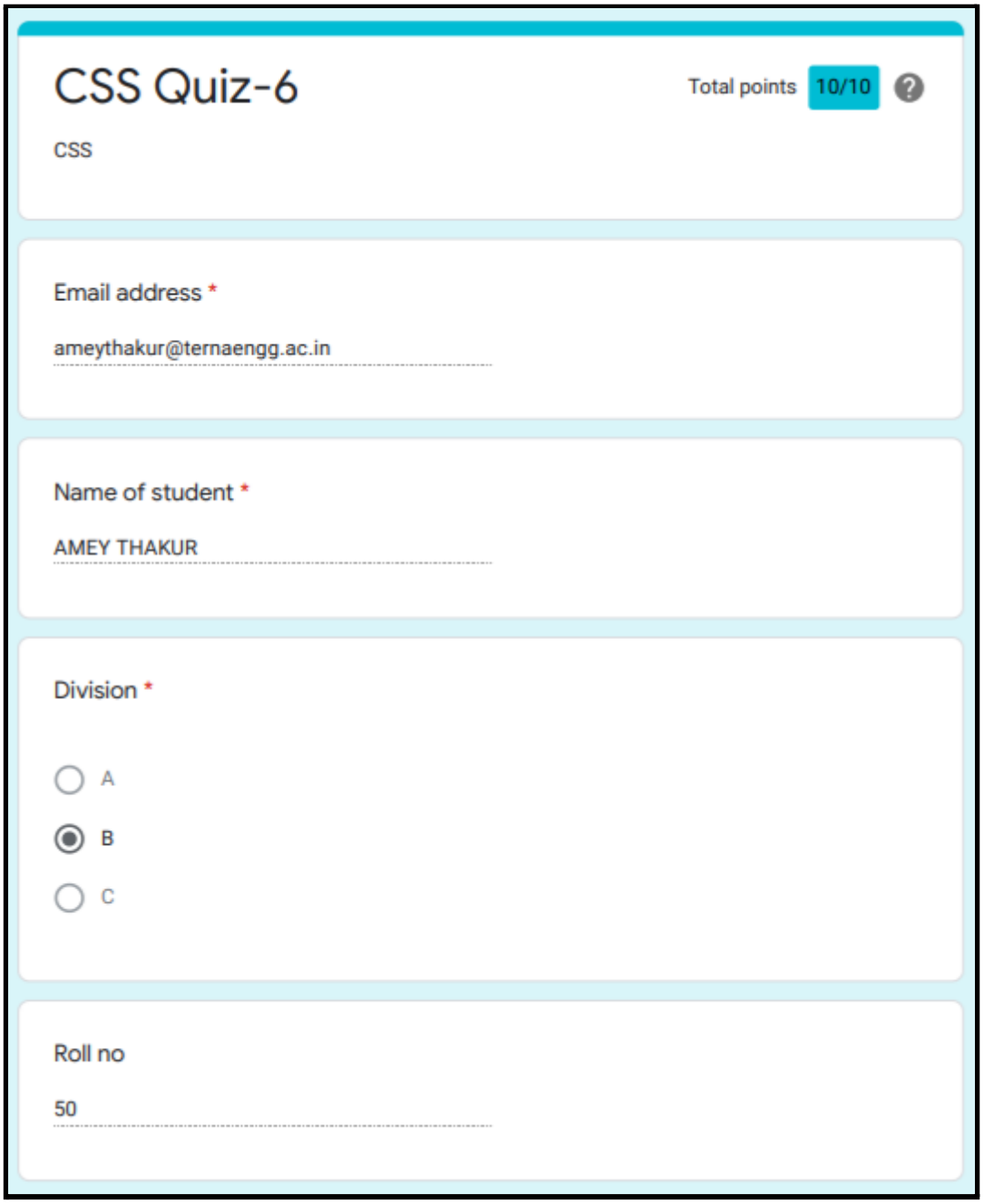
- A
- B
- C

Roll no

50

CSS Quiz 6

Marks: (10/10)



CSS Quiz-6

Total points 10/10

CSS

Email address *

ameythakur@ternaengg.ac.in

Name of student *

AMEY THAKUR

Division *

- A
- B
- C

Roll no

50

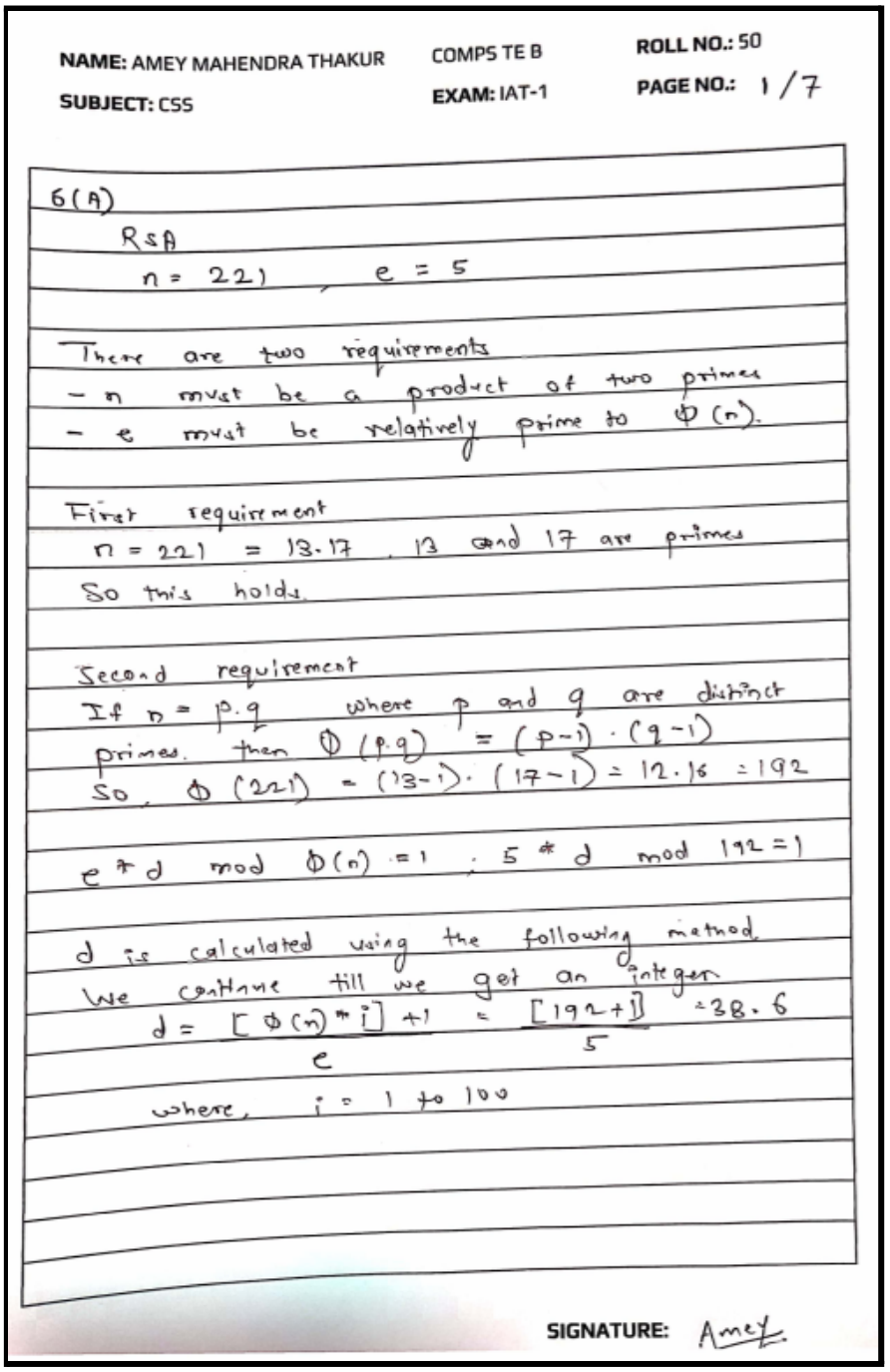
IAT

CSS IAT 1

Marks: (18/20)

IAT 1 Descriptive Answer Sheet

(First page attached)



NAME: AMEY MAHENDRA THAKUR COMPS TE B ROLL NO.: 50

SUBJECT: CSS EXAM: IAT-1 PAGE NO.: 1/7

6(A)

RSA

$n = 221$, $e = 5$

There are two requirements

- n must be a product of two primes
- e must be relatively prime to $\Phi(n)$.

First requirement

$n = 221 = 13 \cdot 17$. 13 and 17 are primes

So this holds.

Second requirement

If $n = p \cdot q$ where p and q are distinct primes. then $\Phi(p \cdot q) = (p-1) \cdot (q-1)$

So, $\Phi(221) = (13-1) \cdot (17-1) = 12 \cdot 16 = 192$

$e * d \bmod \Phi(n) = 1$ $\therefore 5 * d \bmod 192 = 1$

d is calculated using the following method.

We continue till we get an integer.

$d = \frac{[\Phi(n) * i] + 1}{e} = \frac{[192 * i] + 1}{5} = 38.6$

where, $i = 1$ to 100

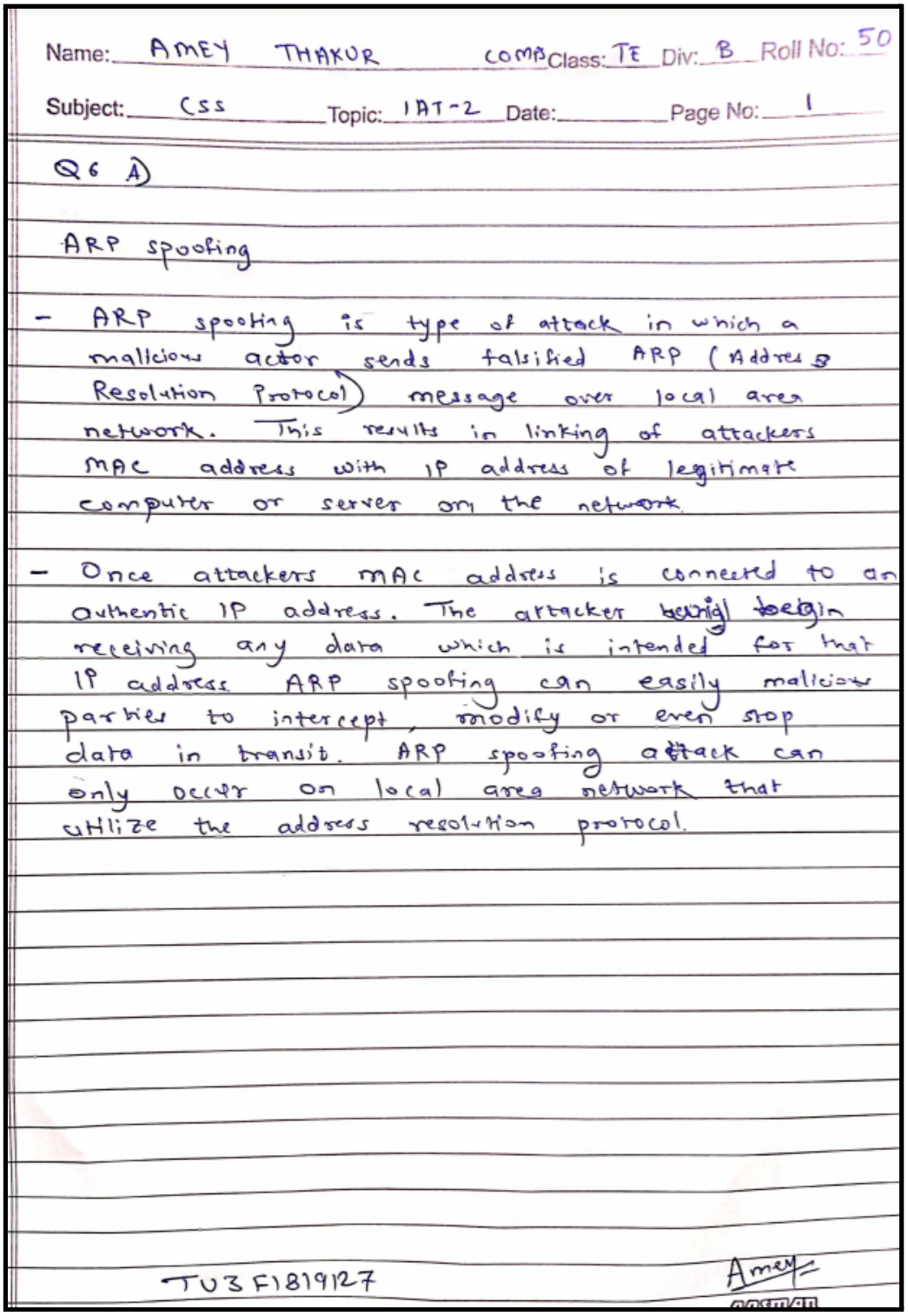
SIGNATURE: Amey

CSS IAT 2

Marks: Not Received

IAT 2 Descriptive Answer Sheet

(First page attached)



Name: AMEY THAKUR COMPS Class: TE Div: B Roll No: 50

Subject: CSS Topic: IAT-2 Date: Page No: 1

Q6 A)

ARP spoofing

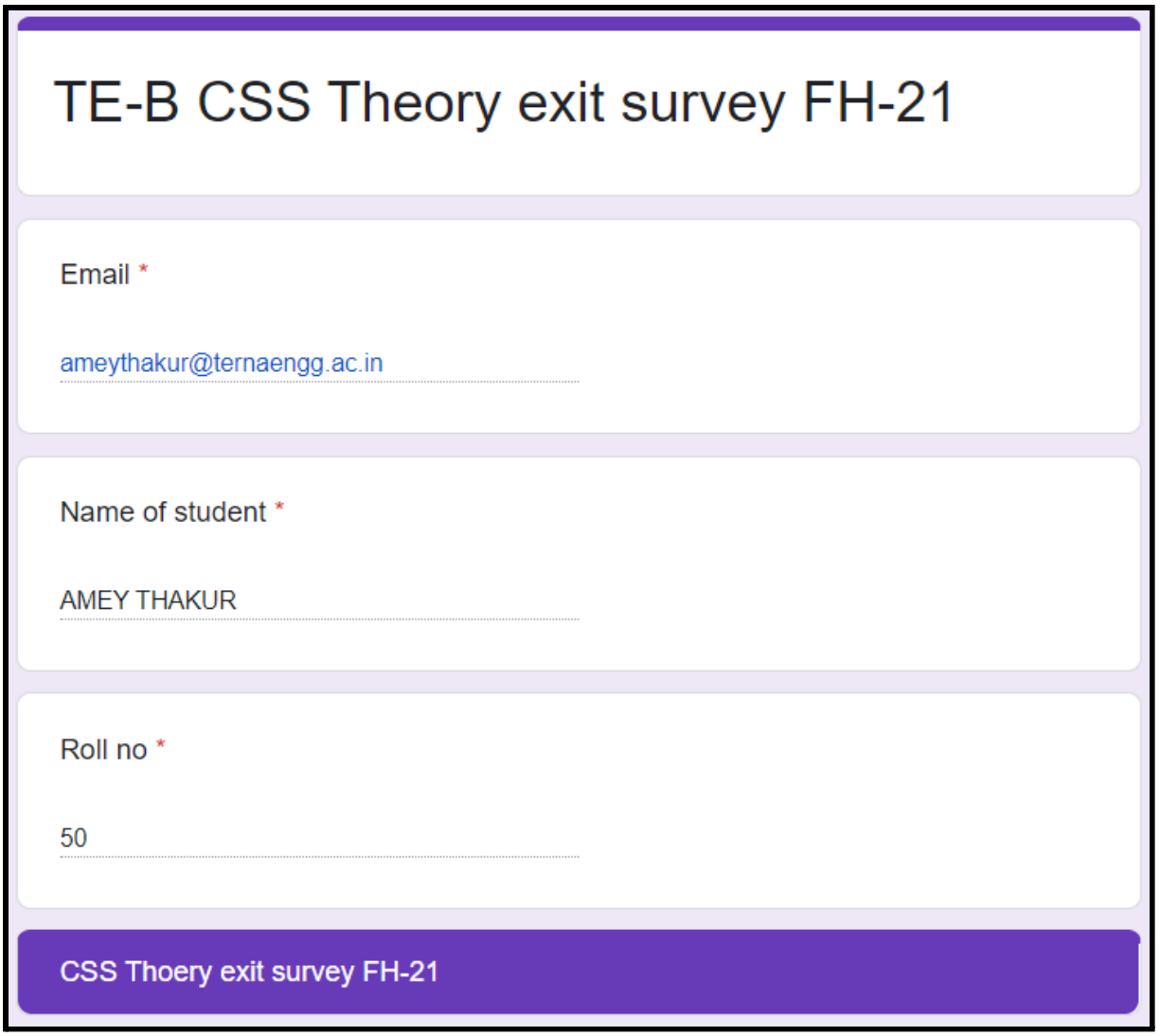
- ARP spoofing is type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) message over local area network. This results in linking of attackers MAC address with IP address of legitimate computer or server on the network.

- Once attackers MAC address is connected to an authentic IP address. The attacker begin receiving any data which is intended for that IP address. ARP spoofing can easily malicious parties to intercept, modify or even stop data in transit. ARP spoofing attack can only occur on local area network that utilize the address resolution protocol.

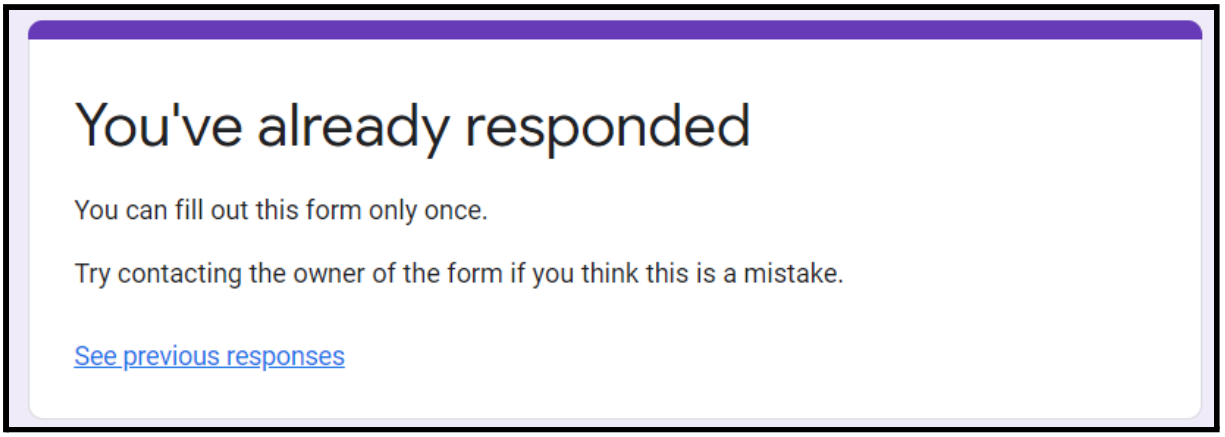
TU3F1819127 Amey

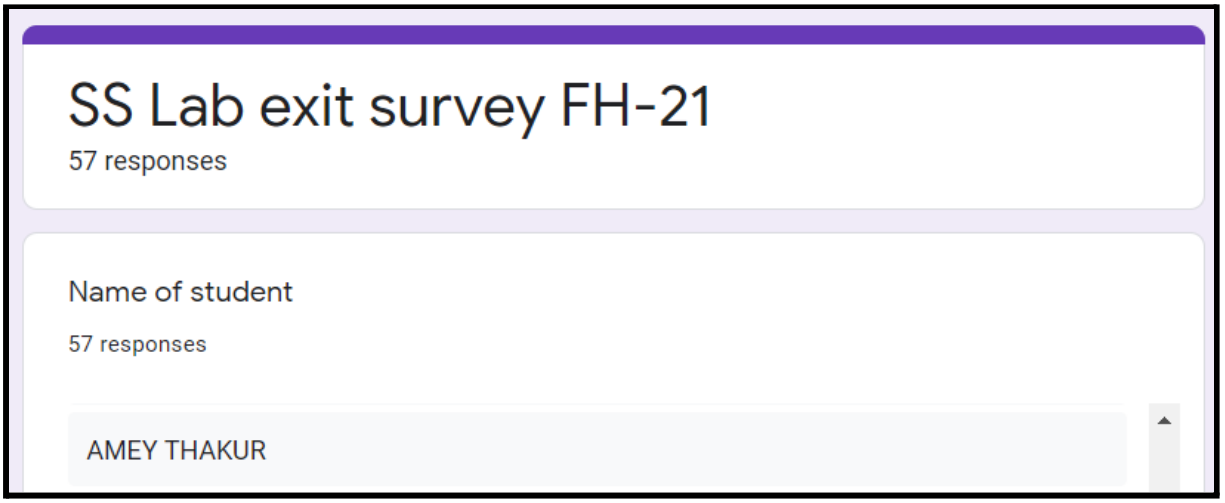
Exit Survey

CSS Course Exit survey



CSS Laboratory Exit Survey





Google Classroom Submission Report

AMEY THAKUR

Submission Report 1	No due date	Turned in
Practice Test on 14_05_21 1	No due date	46/50
Experiment-10 1	No due date	8/10
Experiment-9 1	No due date	9/10
Experiment-8 1	No due date	9/10
Experiment-7 1	No due date	9/10
Experiment-6 1	No due date	9/10
Experiment-5 1	No due date	9/10
Experiment-4 1	No due date	9/10
Assignment-3(Beyond Syllabus To fill curriculu... 1	No due date	Turned in
Assignment-2 1	No due date	9/10
Assignment-1 1	No due date	9/10
Experiment 3 1	No due date	9/10
Experiment -2 1	No due date	9/10
Experiment -1 1	No due date	9/10