Hands-on A2: Looking for vulnerabilities

1. Table:

Environment	CVE identifier	Description of Summary	Date (dd/mm/yy)	CVSS base score	CVSS impact score	CVS exploitability score	CVSS attack vector	CVSS attack complexity	Status of Fix
Apple	CVE-2020-6528	Incorrect security UI in basic auth in Google Chrome on iOS prior to 84.0.4147.89 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	07/22/2020	4.3	1.4	2.8	Network	LOW	This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.
Microsoft	CVE-2019-1111	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1110.	07/15/2019	8.8	5.9	2.8	Network	LOW	The security update addresses the vulnerability by correcting how Microsoft Excel handles objects in memory.

Huawei	CVE-2020-9102	There is a information leak vulnerability in some Huawei products, and it could allow a local attacker to get information. The vulnerability is due to the improper management of the username. An attacker with the ability to access the device and cause the username information leak.	07/17/2020	3.3	1.4	1.8	Local	LOW	Huawei has released software updates to fix this vulnerability.
Google	CVE-2020-6527	Insufficient policy enforcement in CSP in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass content security policy via a crafted HTML page.	07/22/2020	4.3	1.4	2.8	Network	LOW	This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.
Facebook	CVE-2019-3563	Wangle's LineBasedFrameDecoder contains logic for identifying newlines which incorrectly advances a buffer, leading to a potential underflow. This affects versions of Wangle prior to v2019.04.22.00	04/29/2019	9.8	5.9	3.9	Network	LOW	This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further

									changes to the information provided.

2. Explain the meaning of CVSS base score, impact score, exploitability score, attack vector, attack complexity.

CVSS base score:

CVSS base score is an inherent characteristic of a vulnerability that remains constant over time and across user environments.

impact score:

The impact score reflects the immediate consequences of the successful exploitation of the vulnerability. It indicates that the affected of Impacted component.

exploitability score:

The exploitability score reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component.

attack vector:

The attack vector reflects the environmental potential to attack vulnerable components. The larger the metric, the higher the distance from which an attacker can attack a vulnerable component.

attack complexity:

Attack complexity is a condition beyond the control of the attacker that must exist to attack vulnerable components.

3. In your opinion, which vulnerability is most severe and why?

Microsoft Excel has been a very widely applied spreadsheet for all platforms. Almost all companies use Excel for daily tasks on this day. So the vulnerability affects the crowd significantly.

If the current user is logged on with administrative user rights, an attacker could control the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

The exploitation of the vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Excel. In an email attack scenario, an attacker could exploit the vulnerability by sending the specially crafted file to the user and convincing the user to open the file. In a web-based attack scenario, an attacker could host a website (or leverage a compromised website that accepts or hosts user-provided content) containing a specially crafted file designed to exploit the vulnerability. An attacker would have no way to force users to visit the website. Instead, an attacker would have to convince users to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file.