**Team Name:** Noble Team

**Current Leader:** Lucas Scharf

**Members:** Melanie Brown, Marwan Elashry, Viren Kumar, Tanya Malik, Emily Nolan, and Lucas Scharf

**Melanie Brown:** I was able to recreate the CVE-2022-0337 browser exploit which leaks system environment variables using an html file and require the user to press enter for two second to run and accept the save dialog box. <https://github.com/Puliczek/CVE-2022-0337-PoC-Google-Chrome-Microsoft-Edge-Opera>

It took some time because this CVE has already been patched in current Microsoft Edge and Google Chrome versions. I was able to find a download for Google Chrome version 96 and recreate the exploit on that because the vulnerability was patched in version 97 and current version of Edge. I did try the exploit on the current version of Edge and it did return the system environment variable fields, however not the actual data. I found out that there is no longer a way to uninstall the edge browser on Windows 10. I think we could possible take the html file from this example of the exploit and modify to look like the gmu page or like a page that has the user press enter to continue to the webpage after clicking the link from the last year’s team exploit. I had also spent time attempting to recreate an exploit looking at a Microsoft Edge vulnerability to steal files. This vulnerability was patched in 2015 and I could not find a download for Edge version 40 or 41 before moving on to the Chrome exploit.

**Marwan Elashry:** I tried to recreate multiple CVEs, CVE-2020-15999 (Heap buffer overflow) , CVE-2022-0337 (System environment variables leak ) but I was not able to get any of them to actually work. After countless tries I found out that the reason they are not working is because I have a newer version of chrome (Viren is the one who made me notice). Then I downloaded a previous version of chrome to try to recreate CVE-2022-0337 and I got some success with it, but I ran out of time (before typing this work log, I will keep working on it today). I was able to successfully inject the code into a fake login page.

**Viren Kumar:** I was able to reproduce a CVE-2022-0337 (<https://github.com/Puliczek/CVE-2022-0337-PoC-Google-Chrome-Microsoft-Edge-Opera>) in a previous version of Google Chrome, I took the vulnerabilities code and injected it into a fake gmu login page. In there, instead of clicking login, it says “Hold Enter to Login”, doing this allows the page to submit a line of code that grabs the computer’s environmental variables. We can adjust the list of environmental variables as we desire. Next steps are to use this within the cortana breach itself.

**Tanya Malik:** I have not heard from Tanya all week despite reaching out to her multiple times -Lucas

**Emily Nolan:** I continued to research the CVE-2020-15999 (<https://nvd.nist.gov/vuln/detail/CVE-2020-15999>) which was remotely exploiting heap corruption using a crafted html page and took some time to learn/understand the python code that was used in the documents. I was able to successfully exploit it once but I think that it is going to be too unstable to reliably use this further in this project. I think that the 2022-0337 cve that the other members were working on will be what we end up using but I started researching other CVEs as well to find a more suitable and reliable one for this project. I also installed a certificate to the windows machine and continued to try recreating a mitm attack on the windows 10 machine but was able to view traffic only on the kali machine.

**Lucas Scharf:** This week I worked on recreating the Cortana response results from the previous group. I was successful in replacing the link in the Cortana answer. I explored the newer version of burpsuite. Combined with my research of burpsuite from last week I fully understand what it does and what all buttons do. Therefore, I no longer need the previous groups settings. An explanation of their Java code could be helpful though. Shortcuts were taken to achieve this result. Burpsuite was set up as a proxy server instead of a MITM. The ca cert was pre installed. I believe the ca cert may not be required for this exploit to work, but I have no definitive proof of this yet. It worked without it but it may have been cached. The proxy forward in windows allows me to push all packets to port 8080. Going forward I can duplicate their attack exactly by forwarding to port 8080. The cacert combined with the old version of burpsuite do not allow for access to all websites. Google.com will prevent connection with a privacy error.(Other tab below)



