## Grade Value

32% of total grade

## Guidelines

* You are allowed to reference the course materials and online content to complete the assignment.
* AI tools may be used to support research, enhance understanding, and assist the configuration of the environment. However, they must not serve as the primary source of information or comprehension of the vulnerability or exploit.
  + Use of AI on either the presentation or recording will nullify the submission and earn a grade of 0 for all group members.

## Requirements

* The presentation must have a slide deck as a component of it.
  + The presentation must not be longer than 15 slides, not including title or reference slides.
* The presentation must have proof of concept as a component of it, which will need to be presented live.
  + If unable to demonstrate, the recording made may be used for a maximum of 50% of the demonstration grade.
* Presentation and PoC demonstration must be no longer than a total of 25 minutes.
  + Presentations may be terminated by the instructor if they go beyond this limit.
  + The presentation time limit will be adjusted depending on number of groups.
* This assignment will be completed in **group sizes between 3 and 4.**
  + Once you have decided on your group members, provide your instructor with a list of the group members.
  + The instructor reserves the right to reassign group members at their discretion.
* This assignment should take an estimated 8 to 10 hours to complete.

## Assignment

* Choose a recent software vulnerability which was disclosed within the last 5 years.
  + Presentations utilizing vulnerabilities disclosed more than 5 years prior to the assignment will receive a maximum of 50% of the possible grade.
* Presentation on the chosen software vulnerability which must contain
  + Definition of technical terminology used in the presentation.
  + A description of the vulnerability, including any details on why it exists (buffer overflow, security misconfiguration, etc.).
  + Details of the exploit.
  + Details on remediation or mitigation of the vulnerability. -> **if the mitigation takes long, there must be another machine for demo and another machine to show what is expected after running the mitigation**
  + Presentation and PoC demonstration must be no longer than 25 minutes.
* Proof of concept recording must contain
  + The code used is to be demonstrated prior to executing.
  + The execution of the code.
  + Remediation/mitigation of the vulnerability and proof of mitigation/remediation.
* Live demonstration of proof of concept must contain
  + The code used is to be demonstrated prior to executing.
  + The execution of the code.
  + Remediation/mitigation of the vulnerability and proof of mitigation/remediation.
  + If it cannot be demonstrated live, the recording can be played, for up to a maximum of 50% of the demonstration grade.
* References used must be provided at the end of the PPTX file. 🡪 **reference slide at the end**
  + Inaccessible references may cause loss of marks.
* Target audience for the presentation are technical and non-technical.

## Resources

* <https://www.cve.org/>
* <https://exploit-db.com/>
* <https://www.cyber.gc.ca/en/alerts-advisories>
* <https://www.cvedetails.com/>
* <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
* Other online resources as identified in the course and through your groups research

**POSSIBLE SOURCES!!!**

[**https://www.cse-cst.gc.ca/en**](https://www.cse-cst.gc.ca/en) **-🡪>> they are hiring, Clay applied here and security is really tough coz they contacted his parents, teachers, etc…**

* [**https://www.cyber.gc.ca/en/alerts-advisories**](https://www.cyber.gc.ca/en/alerts-advisories)
* <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
* <https://www.cvedetails.com/>

## Submission

* Presentation must be saved in PPTX format
* Video must be saved in a format which is natively playable in VLC Media Player
* PoC/exploit code should be saved in its native format (.c, .py, etc.)
* Upload the presentation, recorded video and proof of concept code prior to the due date listed in Brightspace
  + Do not zip the submission, unless it reports the PoC cannot be uploaded. Then zip ONLY the PoC
* Due date for the assignment will be posted in Brightspace
* Presentations will be performed the week after the due date

**Keep Powerpoint and video unzipped**

**Calyton suggested to use HandBrake (handbrake.fr) for vids**

## Grading Rubric

Marking rubric is attached to the assignment in Brightspace

## Due Date

Assignment due date is posted in Brightspace.