ICT2214 Web Security (AY24/25 Tri 2 Jan 2025)

Assignment: Develop an Offensive or Defensive Solution for Web Security

---

1 Introduction

Web security is about applying technology, processes, and controls to protect online entities and assets. There are many tools and technologies out there that exist to support web security, such as secure protocols, web application firewalls, monitoring systems, hardened servers, code checkers and obfuscators, etc., which helps create a more secure web environment. On the other, there are also tools and technologies to help in surfacing weaknesses and vulnerabilities on the web, such as web proxies, protocol analyzers, vulnerability scanners, exploitation toolkits, security evasion tools, intelligence gatherers, code analyzers, browser extensions, etc., that are typically used in offensive and red team operations to uncover findings that could later be addressed by stakeholders.

Nevertheless, the fast-changing pace of web technologies often introduce new things that have to be catered for or render what was previously learnt or developed obsolete. Hence it is imperative that practitioners keep themselves, and their arsenal, updated with the current trends in the industry.

2 Task

Form your own teams of 5 pax (default) and **report** your team members **during Week 1 lab session** to your lab tutor on a first-come-first-serve basis. If there are any disputes, we will ballot using https://wheelofnames.com/.

There are 2 lab sessions, i.e. P1 on Tues, 2pm to 4pm; and P2 on Tues, 4pm to 6pm. P1 has 95 pax while P2 has 94 pax. Both are sub-divided into the following classes:

Main Session	Sub-session	Tutor	No. of Pax	No. of Groups
P1	P1A	Hee Meng	35	7
	P1B	Harminder	30	6
	P1C	Ben Tan	30	6
P2	P2A	Hee Meng	30	6
	P2B	Harminder	35	7
	P2C	Ben Tan	29	6*

* One of the groups in P2C will have 4 pax while the rest has 5 pax.

Please see the class lists in the **Assignment** folder under the **Content** tab in LMS.

You are required to design and implement a novel technical solution (software) that is broadly applicable to web security. You are free to choose any specific use-case, being on the offensive or defensive side of web security.

When considering possible ideas, you may want to address the following questions:

- What **exactly** do you want to develop and how does it **relate** to web security?
- Is it sufficiently **novel** and **complex**?
- What are the existing technologies, tools, or solutions out there that can already be used as an alternative to your proposed solution, and how would they compare against your proposed solution? This requires some sort of **literature review**.
- Does **development** of your solution allow you to demonstrate **technical** competency in web security?
- Can the proposed solution be implemented **within 8 weeks** (by a team of 4-students) and be of **reasonably high quality**?
- Does the solution have **potential** to be showcased to the public, such as through cybersecurity/ academic conferences or community meetups?

You will be assessed based on your technical competency, the novelty, complexity, and correctness of the solution, the comprehensiveness of the literature review, and the quality of your submissions.

3 Deliverables

The total weightage for the assignment is **35%**. There are 2 sets of deliverables – see Table 1 below:

Deliverable	Deadline	Remarks*
Project Proposal Document (5% Group Mark)	**19 Jan 2025 Sun 2359 hours,** end of Week 2	You are also to discuss and confirm with your lab tutor your project proposal during the **Week 3 lab session**.
Final Presentation Slides and Video (10% Group Mark & 20% Individual Mark)	**9 Mar 2025 Sun 2359 hours,** end of Week 9	You are also to show your draft project demo and report the status of your project during **Week 8 lab session**.

** Failure to attend the lab session in Weeks 3 and 8 will result in marks being deducted.*

Table 1

Week 6 Finish must

3.1 Project Proposal (5% Group Mark)

As indicated in the Table 1 above, although you are free to decide on what your solution does, you are required to consult the instructor before embarking further on the assignment. To do this, firstly, you are required to submit a recommended two-page (maximum of three pages) document following the template *proposal-template-a4.docx* provided to you at the LMS Dropbox. The detailed requirements of this project proposal document are in the template *proposal-template-a4.docx*.

You must focus your solution on accomplishing specific things within a reasonable scope, so that you can produce an output that is of high quality and depth. Care must be taken not to choose a scope or set of tasks that is trivial, of which there may be nothing much to develop for, nor too broad, for which there may be too much to possibly develop leaving insufficient time to produce work of high quality/depth.

Avoid using generic references, such as Wikipedia, since the content is not peer-reviewed (i.e., anyone can write an article there or edit them). Rather, search from reputable research databases such as ACM Library: https://dl-acm-org.singaporetech.remotexs.co/, IEEE Xplore: https://ieeexplore-ieee-org.singaporetech.remotexs.co/Xplore/home.jsp, Google Scholar: https://scholar.google.com.sg/ or top-tier cybersecurity conferences, such as Black Hat and USENIX. GitHub repositories of existing solutions are also acceptable. You should have between 7 to 14 references.

You must upload your project proposal document to the LMS Dropbox – see deadline in Table 1 above. Indicate your team number in files following the convention below:

PxTy-ProjectName where Px refers to your lab sessions, Tx refers to your team number and ProjectName refers to your project title/name. Please refer to your introductory/overview lecture slides on your lab sessions.

E.g., P1T1-SuperWebDefender.pdf; P1T1-SuperWebDefender.docx

Upload a **Word** and a **PDF** version. One reason is so that if one of the files are erroneous, we can still see the other file. Marks can be deducted if (i) you upload to the wrong folder, (ii) do not name your files properly, or (iii) do not upload both type of files.

Secondly, you must be present during the Week 3 lab session to discuss and confirm the project proposal with your lab tutor. We want to avoid a scenario where there are teams doing a project that are too similar which can likely lead to plagiarism.

3.2 Final Presentation Slides & Video (10% Group Mark and 20% Individual Mark)

See submission deadline in the Table 1 above.

Presentation Slides:

- There is no limit on the number of slides in your presentation slides.
- A template *presentation-template.pptx* is available at LMS which has the following sections:
  - **(i) Mandatory:** Project Team & Links – indicate **full name** of your students, email addresses and which section is done by them and the links to the GitHub repository and presentation videos.

Name/Email	**Section Responsible**	**Group Mark (10%)**	**Individual Mark (20%)**
James Bond 2901001@sit.singaporetech.edu.sg	Introduction, Findings		
Peter Parker 2901002@sit.singaporetech.edu.sg	Analysis, Conclusion		
…	…		
The above is just a sample…			

Table 2

Mandatory: In Table 2 above and at the start of each presentation slide section, indicate the name of the student who is **responsible** for writing/presenting the section. We will allocate individual marks based on this section. See Section 4 Assessment Weightage for more information.

  - (ii) Introduction/Background/Problem Statement – introduces your project giving the background, motivation and problem your project is trying to solve.
  - (iii) Related Works/Literature Review – provides more information on the latest trends and knowledge related to your project, e.g., what is presently happening in your project/subject area by other researchers/developers, etc.
  - (iv) Objective/Purpose/Research Question – highlights/summarizes concisely the actual purpose and objective of your project.
  - (v) Methodology/Approach – discusses how you intend to develop your solution/approach to solve the problem you highlighted. E.g., your algorithms, pseudocodes, design solution, flowcharts, etc.
  - (vi) Findings/Results/Demo – presents the results of your developed solution and show your

findings, e.g., present screencaps, outputs, performance charts, etc. It is **mandatory** to demo how your solution performs, and this can be an appropriate section to showcase the demo. However, you can decide where/when you want to demo your solution.
  - (vii) Analysis/Discussion – discusses/analyzes the results/findings/impact/benefits of your solution.
  - (viii) Limitations and Future Works – discusses the limitations of your solution and future research work/direction that can be done to improve it further.
  - (ix) Use of Generative AI – see Section 8 below. Like the section on (i) Project Team Composition, this section is **mandatory**.
  - (x) Conclusion – summarizes and concludes the key points of your project.
  - (xi) References – lists your references here using IEEE citation style. There must be at least 7 references from reputable sources, e.g., ACM Library, IEEE Xplore, etc. Ensure that the references are correctly cited at the relevant slides. E.g., you may have a reference [1] that is used to support a point in the Introduction section. If so, make sure that [1] appears next to the point in the Introduction section.
  - (xii) Others – put whatever else you think is necessary here. E.g., Appendix, Acknowledgements, etc.
- There is no hard and fixed rule on the number or type of sections mentioned above as it depends on the nature of your solution and how you want to report it. E.g., change name of sections, combine/add/delete sections, etc. However, do not frivolously ignore any of the sections above. Please take a look at the research papers in ACM Library, IEEE Xplore, USENIX, etc. on how authors structure/organize their papers. A few sample papers are uploaded in LMS for your reference.
- **Mandatory:** Your solution (codes, binaries, readme.txt, user manual, etc.) must be uploaded to a GitHub repository. *Indicate the link to your GitHub repository in your slides.*

Video Presentation

- While there is no limit on the number of presentation slides, you have a hard limit of keeping the video to 5 mins per team member, i.e., if the team comprises 5 pax, then the video duration limit is 25 mins. Tutors are instructed to **ignore** the beyond the video duration limit.
- Your video must be at the **minimum** of Full High-Definition (1920 x 1080) resolution and **subtitled**. Please upload your video to a suitable repository, e.g. YouTube, etc.
- It is **mandatory** to have the presenter's head shown in the video – this is so that we can validate that the section is presented by the actual student. The position/manner of the talking head is completely up to you. We recommend using Zoom or PowerPoint to record your presentation video.

You must upload your project presentation slides/video to the LMS Dropbox – see deadline in Table 1 above. Indicate your team number in your **files** following the convention below:

PxTy-ProjectName where Px refers to your lab sessions, Tx refers to your team number and ProjectName refers to your project title/name. Please refer to your introductory/overview lecture slides on your lab sessions.

E.g., P1T1-SuperWebDefender.pdf; P1T1-SuperWebDefender.pptx; P1T1-SuperWebDefender.txt

(A) Upload a **PPTX** and a **PDF** version of your presentation slides. One reason is so that if one of the files are erroneous, we can still see the other file.
(B) Upload a video recording of your presentation to YouTube and let us have the link to your YouTube presentation. Make sure that your YouTube link is working properly! You can upload a text file containing your YouTube link.

Marks can be deducted if (i) you upload to the wrong folder, (ii) do not name your files properly, (iii) do not upload the necessary type of files, or (iv) we cannot see your YouTube video!

4 Assessment Weightage

This assignment will constitute **35%** of your final grade. Your project will be marked by your lab tutor.

There are two components involved when marking your project:

- **[Group Mark: 15%]:**
  - *Project Proposal [5%]:* You will be assessed on clarity, format and completeness of your proposal.
    - Clarity: All sections are well written. E.g., Section 1's purpose and motivations for the project is clear, etc. The proposal is very easy to read and understand, and everything reads and flows logically and smoothly. There are no spelling/grammar errors.
    - Format: You follow the format of the proposal template closely. If there are changes, then changes are excellent, reasonable and further improve the proposal. The proposal is between 2 to 3 pages. The proposal uses IEEE citation style.
    - Completeness: All the sections in the template are complete. If there are any changes, the changes are excellent, reasonable and further improve the proposal. There are 7 to 14 relevant references (more are acceptable but not too excessive).
  - *For Final Presentation Slides & Video [10%]:*
  - Assess the **format** (e.g. professional looking, etc.) and **overall** quality (e.g., logical flow, structure, appropriate sections, novelty, value, complexity, etc.) of the project proposal and presentation slides. The whole idea for this section is to have a seamless feel of a project even though it is done by different individuals.
- **[Individual Mark: 20% - for Final Presentation only]:** Assess the **content quality**, **accuracy** and **ease of understanding and clarity** of each section as presented by the individual student. General guidelines:
  - As mentioned in the previous page, at Table 2 and at the start of each presentation slide section, indicate the **name** of student who is responsible for writing/presenting the section. E.g. Introduction-James Bond, Related Works-Peter Parker, Conclusion-Clark Kent, etc. Make sure too that the student's head is shown in the presentation video.
    - Put the student's name in the section ONLY if the student is truly contributing to the section. We will then mark accordingly. If you choose to put a free rider who is not contributing to the section/report, please do not complain of their non-contribution because we will mark based on the name of the student in the section. E.g., say that there are 25 slides and there is only 1 slide allocated to the student or that the student is only presenting 1 minute out of 25 minutes, we will mark down the student accordingly.
  - A complex (e.g., in terms of slides, amount of work done, etc.) section may comprise of up to two to three students only. E.g., Discussion-Peter Parker & Mary Jane & Gwen Stacy, etc.
  - A student's name can appear in more than one section. However, the student should not appear in more than 20% of the presentation slides or video presentation duration.
  - **Generally,** for a 5-person team, each student should be responsible for **roughly** 20% of the slides or video presentation duration. Likewise, for a 4-person team, each student should be responsible for roughly 25% of the slides or video presentation duration. As such, it is the **responsibility** of each student to ensure that they have sufficient work/presentation slides and video presentation duration. This is especially true from Week 3 onwards after your project is confirmed by your lab tutor.
  - There will **not** be any peer evaluation.
  - Basically, we are trying to ensure that each student is contributing and that there are no free riders or only one or two students doing all the heavy lifting. Speak to your lab tutor if you need guidance.

5 Late Submission

A penalty of 20% per day for each deliverable will be imposed for late submission unless extension has been granted prior to the submission date. Request for extension will be granted on a case-by-case basis. Any work submitted more than 4 days after the submission date will not be accepted and no mark will be awarded.

6 Plagiarism

SIT's policy on copying does **not** allow you to copy software as well as your assessment solutions from another person/student. It is **not** acceptable to copy other person/student's work. It is the students' responsibility to guarantee that their assessment solutions are their own work. Meanwhile, you must also ensure that others do **not** obtain access to your work. Where such plagiarism is detected, **both** assessments involved will receive **ZERO** mark.

We will publish the project titles of each team for the entire cohort at start of Week 3 in the LMS before your lab session. It is your **responsibility** to check that your project is **not similar** to another team. If it is, please speak to your lab tutor to change/modify the scope.

7 Use of Generative AI (gAI)

The use of generative AI is permitted for this assignment. These powerful tools can enhance your productivity and offer new perspectives and ideas. It is up to you to decide whether to use and the extent it is used. However, it is crucial to understand and adhere to the following guidelines to ensure the integrity and quality of your work.

- Understand the Tool's Limitations: Generative AI tools are an evolving technology with limitations. It is important to recognize that these tools may not always provide accurate or contextually appropriate content. You must critically **assess/validate** responsibly the information generated by these tools.
- Maintain Academic Integrity: While generative AI can assist in your work, the responsibility for the content's accuracy, originality, and relevance lies with you. You are required to **fact-check** and ensure the academic integrity of your submission. Plagiarism rules still apply, and it is your duty to use generative AI tools ethically. *Tip: ChatGPT is known for giving inaccurate references!*
- Appropriate Use and Attribution: Clearly understand how and to what extent you can use generative AI tools in your assignment. For instance, while such tools can assist in drafting or idea generation, they should not replace your analytical and critical thinking. Generative AI tools should be acknowledged as means of assistance in work but **not** as co-authors or cited sources.
- Reporting Use of Generative AI: We mandate transparency in the use of generative AI tools that you are using. In your presentation slide/video, you must have one section to explain how you utilized these tools in your assignment, focusing on the areas they helped you.

Any form of academic misconduct or plagiarism will be severely dealt with.

Wishing all the best to all students!

END OF DOCUMENT