SE 421: Project: Vulnerability Assessment

Due on November 16, 2018 at 12:00 PM (noon)

Instructor: Ben Holland

Student Name:

Problem 1

(10 points - Professionalism)
Your report will be graded on its professional quality. At a minimum your report should:

- Clearly document the names of each team member and their roles in the vulnerability assessment. Note that you should discuss with your team how to best balance the workload among all team members. Allowing team members to specialize on tasks that suit each team member's strengths may be one way to divide the workload, but is not required.
- Provide a table of contents
- Include page headers and page numbers
- Be single spaced with 1 inch margins
- Use an appropriate font (no Comic Sans)
- Be professionally typed (see Syllabus and Piazza clarifications for details)
- Use complete and grammatically correct sentences (run a spell checker)
- Include captions and identifiers for figures (Example: "Figure 2 - Shows XYZ")
- Include appropriate references and citations if needed
- Be complete in the sense that the report would enable a business executive to make an informed decision with the information contained in the report. To provide additional completeness you may wish to include citations to additional references.
- Be targeted at a professional audience. Present ideas clearly and succinctly. You may assume that your audience is vaguely familiar with the original project source code and with the basic concepts presented in this course (i.e. use the appropriate technical terminology, but also provide concise definitions of the concepts in laymen's terms). If you have difficulty writing, you may wish to seek advice from one of the Writing Media Centers on campus.

Problem 2

(10 points - Threat Modeling)
Using the STRIDE methodology, model the threat environment for the *Vulnerable Video Service* as completely as you can. At a minimum your report threat modeling section should:

- Include a diagram of your threat model.
- Include written explanations of the key components in your threat model.
- Consider:
  - Client user privacy
  - Client user security
  - Server-side security
  - Reliability of services that could impact business operations

Problem 3

(15 points - Audit Methodology)
Describe your audit strategy. Use all means available to you to audit the application for security vulnerabilities. At a minimum your report audit methodology section should:

- Provide an executive summary (no more than one page in length) of how you will systematically audit the *Vulnerable Video Service*. Think of this as a sales pitch. How will you convince your client you will be successful? How will you be systematic? Can you make any guarantees about certain classes of vulnerabilities that you find? Can you show that you can prove any classes of vulnerabilities do not exist? Your approach should not simply consist of running automatic analysis tools. You may use any tools you want, but your process must include some human reasoning.
- List the categories of vulnerabilities you intend to audit. There is no set number of categories that you need to include, but you should strive for completeness. In the spirit of completeness you may wish to add a section that includes a justification for why certain categories are irrelevant to your analysis. At a minimum include as many categories as it takes to cover the space of your threat model. Do not include categories that are irrelevant to your threat model. Since this is a web application you may also want to consider whether or not any of the OWASP Top 10 lists are applicable to your threat model.
  - For each category provide and link to the MITRE CWE (Common Weakness Enumeration) category. For example an SQL Injection vulnerability is specifically listed as "CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')" at `https://cwe.mitre.org/data/definitions/943.html`.
  - For each category provide traceability to your threat model. That is your report should contain some sort of reference system that indicates what parts of the threat model correspond to a given category. If there is no traceability to the threat model then be sure to include special justification for why a category is being included.
  - For each category elaborate on what proof your audit will produce. What program artifacts (APIs, code patterns, etc.) would be identified for a detection of a vulnerability? What sort of evidence of correctness will be produced if a vulnerability is not identified?
- If you plan to use additional tools (for example AFL [1] or any tools from the Kali Linux Penetration Testing Distribution [2]) be sure to include a section that clearly identifies the tool and where the tool is available. For each tool, you should compare and contrast the features of the tool with similar tools available. Consider elements such as tool features, ease-of-use, accuracy, overhead costs, reliability, and types of tool outputs or measurements.

[1] `http://lcamtuf.coredump.cx/afl`
[2] `https://www.kali.org`

Problem 4

(30 points - Vulnerability Audit Findings) Describe your audit findings. Use all means available to you to audit the application for security vulnerabilities. At a minimum your report audit methodology section should:

- Provide a finding identifier (Example: Finding 1).
- Provide a traceability from the vulnerability category to the finding.
- Provide a short description of the vulnerability.
- Classify the finding as Low, Medium, or High impact to the *Vulnerable Video Service* business.
- Classify the finding as Low, Medium, or High risk. Be sure to include how you are defining risk. Risk could be define as the difficulty to exploit or probability of success of exploiting the vulnerability.
- Provide a security patch in the form of one or more commits to your group project repository on GitHub. Be sure to link the commit directly in your report!

Problem 5

(15 points - Security Recommendations) Describe any security recommendations you would like to make to the system in addition to fixing the previously reported audit findings. Security recommendations should cover the full software stack and not just the *Vulnerable Video Service* application. At a minimum your report audit methodology section should:

- Provide enough detail for the reader to make an informed security decision about the recommendation. What would be the impacts or tradeoffs to deploying the recommendation?
- You should consider security recommendations that will enable you to understand the attacks and exploits that might be tried against you.
- Provide enough detail for the reader to deploy the security recommendation.
  - If the security recommendation includes changes to the code, provide a link to the commits on GitHub that implement the security recommendation.
  - If the security recommendation includes additional software then include a link to the tool and a summary of the service that the tool performs.