# 188.959 Software Security VU 2,0h

# Midterm Exam

May $6^{th}$, 2020

## Instructions

Please read the instructions BEFORE you start writing!

1. For calculations, write the complete calculation. Your solution needs to be comprehensible.
2. Read the questions carefully. Your answer should include only relevant information.
3. Try to keep your answers short.
4. You may answer in either English or German.
5. You can get up to **25 points** for this exam.
6. Whenever you answer a question, you are not allowed to copy text from websites, lecture slides or other students verbatim. Please always use your own words for your answers.
7. Screenshots or images of answers are not allowed as submission.
8. Upload your questions as pdf file to TUWEL and include your name and student ID on the first page of the document.
9. Make sure that you reference the question numbers in your answers.
10. You have 2 and a half hours to upload your answers, i.e. until 17:30.

1. **(1pt) Give a definition of "vulnerability" with its source and explain the reasoning behind it.**

2. **(2pt) Describe the main design goals of the CVE list in detail.**

3. **(1pt) Give the definition and main properties of a CWE.**

4. **(2pt) List two properties of the National Vulnerabilites Database (NVD) and describe its design goal and relationship to other security databases in detail.**

5. **(1pt) Give the definition of CERTS and list three of their main tasks.**

6. **(1pt) What type of software application does the OWASP list target? List five security threats from the OWASP Top 10.**

7. **(2pt) What is Postel's law? Describe a situation where following this principle is desirable. Name and describe one example where it leads to vulnerabilities. Then describe the patch to Postel's law.**

8. **(2pt) Describe the principles of a packet-in-packet attack. Is such an attack feasible against a WiFi network encrypted using WPA? Explain why or why not.**

9. **(2pt) Open the specification for the ID3 v2 tagging scheme used in MP3 files under https://id3.org/id3v2.3.0 and explain why this grammar is not context-free. Is input recognition decidable for this class of grammar? What about endpoint equivalence?**

10. **(8pt) Write a ABNF specification for "ID3v3": A context-free variant of ID3v2 (https://id3.org/id3v2.3.0), according to the following rules:**

    a) **Your "ID3v3" grammar should include the *ID3v3 header* (modeled after the ID3v2 header), at least three different *Text information frames*, the *Unique file identifier* frame (with the identifier having a fixed length of 64 bytes) and the *Comment* frame. These frames may appear in any order, and every frame has to appear exactly once. Your frame specifications should be as strict as the ID3v2 specification allows; only one of your chosen text information frames may be "free-form" (e.g. the `TPUB` frame), the other two (or three, if you're feeling brave) frames must have format restrictions (e.g. the `TDAT` frame must be "a numeric string in the DDMM format containing the date for the recording").**

    b) **You do not have to support any additional frames (but you're free to do so).**

    c) **Ignore any field that includes the word "flags", in particular *ID3v2 flags* and *Frame Header Flags*.**

    d) **Ignore the ID3v2 extended header.**

    e) **Text is always encoded in UTF-8. Ignore any fields that specify character encodings. Unless the ID3v2 specification imposes tighter restrictions, text content may contain any byte value (i.e. 0-255), although you may require escaping of certain characters - your grammar should make it clear if there are such characters.**

    f) **Ignore MPEG synchronization issues. (if you don't know what that is, do not bother looking it up)**

    g) **All languages shall be specified using ISO-639-2 codes.**

    **After you have completed your grammar, describe for every field how it could be validated (e.g. dates, language codes, ...) before using it.**

    **Finally, write a valid ID3v3 tag. For binary data, you may simply use ABNF syntax.**

**11. (2pt) What is a binary polyglot? Describe an example of such a polyglot for at least two different file formats.**

**12. (1pt) Describe how dead storage elimination may reduce security.**