Web Security

Exam checklist

Version: September 6, 2019, 11:07

- The teachers take the liberty to update this list as needed, but updates will only be applied to content relating to lectures that have not yet taken place.
- This list can be used as a tool when studying for the exam. It is a collection of topics that have been presented and discussed during the lectures. The topics are listed (roughly) in order of appearance in the lecture slides. The topics have been divided into two classes; *most important* and *less important*.
- There is no guarantee that *all* exam problems are covered by the information given in this document. Exam questions can often be based on the fact that you understand some concept rather than you just remembering it. These questions are hard to relate to a specific topic from the lectures since they may cover several lectures. However, studying the topics below will make you well prepared for these questions as well.

Several of the following topics WILL show up on the exam. Consider these to be the most important topics:

Cryptography

Exam question may assume that you know the underlying cryptography. Explicit cryptography questions may also appear on the exam, but not in abundance. Only the high profile topics are listed here.

□ How does the birthday paradox apply to finding collisions?
□ How TMTO and rainbow tables work.
  □ How to build the tables.
  □ How to perform lookups.
  □ How to use the TMTO-curve.
  □ When is it better to use brute-force?
□ How digital signatures work in general, and for RSA.
□ The purpose of digital certificates.

HTTP Security, Apache Security

□ The basic principles of HTTP communication.
□ HTTP methods GET, HEAD and POST. Safe and Idempotent methods.
□ Similarities and differences regarding POST and GET.
□ What cookies are and how and when they are sent/received.
□ First- vs. third party cookies. User tracking with both kinds.
□ Review the cookie attack terminology.
□ The relationship between httpd.conf and .htaccess-files.
□ You should be able to encode to and decode from Base64 encoding. You do not need to remember the Base64 alphabet or ASCII codes for letters and numbers.
□ Why is Base64 used at all, since it is just a way of expanding text?

□ HTTP Authentication:
  - □ How Basic Authentication works.
  - □ How Digest Authentication (RFC2069, 1997) works. The digest formula will be given if you need it.
  - □ How Digest Authentication (RFC2617, 1999) works. The digest formula will be given if you need it.
  - □ What problems with RFC2069 were discovered and fixed? Which problems remain?

Web applications and PHP security

□ What is the purpose of the same-origin policy, and how does it work?

□ Explain the ways in which the same-origin policy can be bypassed; proxy, iFrames, JSONP and DNS rebinding.

□ How CORS works.

□ The principles of PHP.

□ Usage of php.ini, securing operation and limiting information.

□ Be able to discuss pros and cons of register_globals.

□ Be able to illustrate how failure to validate input may lead to execution of code or JavaScript.

□ How remote file inclusion works.

□ Be able to read given and construct your own simple regular expressions.

□ Compare the two ways of handling sessions in PHP.

□ Explain how session fixation attacks work.
  - □ What are the requirements for it to work?
  - □ What are its limitations?
  - □ How can session fixation attacks be prevented?

□ What is session hijacking?

□ Explain how session prediction works.
  - □ What are the requirements for it to work?
  - □ What are its limitations?
  - □ How can session prediction attacks be prevented?

□ Explain how session sniffing works
  - □ What are the requirements for it to work?
  - □ What are its limitations?
  - □ How can session sniffing be prevented?

□ Explain how XSS attacks work.
  - □ What are the requirements for it to work?
  - □ What are its limitations?
  - □ How can XSS attacks be prevented?

□ How does CSP work?

□ Explain how CSRF attacks work.
  - □ What are the requirements for it to work?
  - □ What are its limitations?
  - □ How can CSRF attacks be prevented?

□ Explain how CRLF attacks and HTTP response splitting work.

□ Explain how an SQL injection attack works.
  - □ What are the requirements for it to work?
  - □ What are its limitations?
  - □ Show a few ways of preventing SQL-injections. Best method?

DNS

□ The principles of DNS.

□ How DNS amplification works.

□ The principles of DNS cache poisoning and how this attack can be made more efficient.

□ Explain how a DNS cache poisoning attack can realize a man-in-the-middle attack.
□ Explain how DNS rebinding attacks work.
□ What is DNS pinning and DNS anti-pinning?
□ Explain the principles of DNSSEC. Which services are provided and at what cost?
□ Explain the usage of the following records in DNSSEC:
  □ DNSKEY
  □ RRSIG
  □ NSEC and NSEC3
  □ DS
□ When are DNSSEC signatures calculated (and re-calculated)?
□ How are DNSSEC signatures and keys verified?
  □ Compare key verification functionality to usage of digital certificates.
□ How NSEC and zone enumeration works.
  □ How is the zone enumeration problem avoided in NSEC3?
□ Name one attack type that is prevented by DNSSEC, and name one that becomes more efficient.

Email security
□ The principles of SMTP.
□ Be able to read and interpret common mail headers in general and the Received header in particular. Distinguishing forged emails from genuine ones.
□ Usage of MX-records.
□ DKIM functionality.
  □ How are signatures created and verified?
  □ How and to what extent is integrity protection provided?
□ Explain how DNSBL can be used to fight spam. Pros and cons?
□ Explain how URI DNSBL works.
□ Explain how Greylisting can be used to fight spam. Pros and cons?
□ Explain how Nolisting can be used to fight spam. Pros and cons?
□ Usage of SPF-records and their relation to MX-records.
□ How DMARC works.
□ The principles of Hashcash.
□ In a sentence or two, describe how hybrid filters work.

Very few of the following topics will show up on the exam. These should be studied after you know everything above. The list is sorted but not divided into chapters. Consider these as less important:
□ Desired hash function properties:
  □ Pre-image resistance,
  □ 2^{nd} pre-image resistance,
  □ Collision resistance.
□ URL encoding.
□ How to use httpd.conf to limit
  □ access to directories,
  □ information to adversaries.
□ Explain how statistical filtering can be used to fight spam. Pros and cons? Given Bayes law, derive the formulas for the log-likelihood ratio and interpret the threshold value 0 (zero).