C331

Q1.a

This question was answered very well by most students.

Some points were lost mostly on the comparison part of the question, which in some cases lacked details or missed the most important points.

Q1.b

Students did well at describing and identifying malicious domains.

Most students struggled with the hardest task of identifying the compromised host from network traffic.

The key was to look for suspicious behaviour at the TCP protocol level in the pattern of communication between the different host pairs present in the trace, and relate it to a specific pattern (port knocking) seen in the lectures.

Q2.a

The vast majority of students correctly identified stride threats for the two scenarios.

Points were lost mostly by describing objectives that were not specific to the presented scenarios, or by repeating similar objectives within (or across) scenarios.

Q2.b

The vast majority answered well to the CSRF part of the questions.

The second part on security headers was answered ok, but several student failed to discuss the headers in relation to the specific threat model of Answerbook as opposed to any web application.

The last and hardest part on how to harden Answerbook was not answered correctly by the majority of students.

Points were given for providing a sensible CSP even if it was not addressing the main vulnerability.

Q3.a

Most students provided good descriptions of how to identify attacks from the logs.

Very few provided answers that were off topic, not relevant to the kind of logs described in the question.

The second part was open-ended, effectively asking to report as many attacks as possible with enough confidence to avoid false positives.

Very few false positives were submitted (less than 200 out of 7,000+ entries).

Students lost point for reporting too few attacks.

Q3.b

Most students answered well this question, but top marks were awarded only to exhaustive answers that provided complementary defenses rather that similar ones.

The practical part, harder by design, turned out to be perhaps too difficult.

Very few students identified the vulnerable line, whereas many students reported as vulnerable a safe line (probably based on assumptions on the behaviour of code that was missing from the provided file).

Q4.a

The vast majority of students answered well to the first three questions, demonstrating a good grasp of the scenario.

Yet the last part was not answered as well, because many answers were not specific to the scenario.

A good answer would consider a pharming/csrf attack leading to dns hijacking, as seen in the lectures.

Answers like malware infection (on a security conscious, fully patched user) were penalised.

Q4.b

In order to identify the tracking cookie it was necessary to do a few experiments reloading the page.

Since any cookie can be used to do at least a minimum of tracking, any of the 3 gave some points.

Fewer marks were given for the constant cookie that only relied the information "someone has visited this site before".

The vast majority of students correctly found the first flag, and most identified the kind of attack being delivered.

The last and hardest part on analysing further the attack proved to be too difficult.

No student reported the correct flag.

Points were still given to students who made some of the right steps towards getting the flag (even if they did not submit a flag!) when we could attribute a logged access to a relevant server to a specific student.