IMPERIAL COLLEGE LONDON

TIMED REMOTE ASSESSMENTS 2020-2021

BEng Honours Degree in Computing Part III
BEng Honours Degree in Electronic and Information Engineering Part III
MEng Honours Degree in Electronic and Information Engineering Part III
MEng Honours Degree in Mathematics and Computer Science Part IV
BEng Honours Degree in Mathematics and Computer Science Part III
MEng Honours Degree in Mathematics and Computer Science Part III
MEng Honours Degrees in Computing Part III
MSc Advanced Computing
MSc Computing
MSc in Computing (Specialism)
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant assessments for the Associateship of the City and Guilds of London Institute

PAPER COMP60015=COMP96015=COMP96016

NETWORK AND WEB SECURITY

Thursday 18 March 2021, 10:00
Duration: 120 minutes
Includes 0 minutes for access and submission

Answer ALL TWO questions
Open book assessment

This time-limited remote assessment has been designed to be open book. You may use resources which have been identified by the examiner to complete the assessment and are included in the instructions for the examination. You must not use any additional resources when completing this assessment.

The use of the work of another student, past or present, constitutes plagiarism. Giving your work to another student to use constitutes an offence. Collusion is a form of plagiarism and will be treated in a similar manner. This is an individual assessment and thus should be completed solely by you. The College will investigate all instances where an examination or assessment offence is reported or suspected, using plagiarism software, vivas and other tools, and apply appropriate penalties to students. In all examinations we will analyse exam performance against previous performance and against data from previous years and use an evidence-based approach to maintain a fair and robust examination. As with all exams, the best strategy is to read the question carefully and answer as fully as possible, taking account of the time and number of marks available.

Paper contains 2 questions

1 **Pentesting a server**

a i) Briefly describe the *SQL injection*, *Command injection* and *Remote file inclusion* vulnerabilities. Specify what capabilities each vulnerability provides to an attacker when it is exploited on a given server.

ii) Suppose you are not allowed to access the code of a web application deployed on a server. Explain how you could use an Intrusion Detection System (IDS) to mitigate the 3 vulnerabilities from section (a.i). Discuss specific limitations of this approach relevant to the vulnerabilities considered here.

b You are tasked with a black-box pentesting exercise against cybersec.fun. The rules of engagement specify that: you should not use automated tools; you should not attempt to modify data on the server; you should not cause denial of service on the server. The goal is to demonstrate access to a hidden database.

i) Gather information about cybersec.fun, and find the URL for a web page that provides access to the hidden database. Report the flag that you see displayed on that page. Briefly describe the steps taken.

ii) Use SQL injection to read the *secret* of the record with *id = 331* from the *items* table of the database. Report the secret value as a flag. Briefly describe the steps taken.

iii) Find a way to login as database administrator, and report the flag you discover when you manage to do so. Briefly describe the steps taken.

The two parts carry equal marks.

2 Attacks and defenses

a i) The file ssl-access.log contains web logs from a server. Identify 3 malicious entries. For each entry, describe the attack attempt and propose the mitigation to be deployed in the server-side code of the web application itself that you consider most effective and relevant, justifying your answer.

b In this part you analyse malicious scripts and websites. These are realistic examples but are designed not to cause any harm or other side effect to your computer.

i) Download the obfuscated JavaScript malware sample jquery-v331.js. Identify what kind of attack it is trying to perform, and report the flag you discover in the process.

ii) You are tasked to analyse the malicious website nah.fun. The site uses the browser of innocent visitors to attack a third party server. Analyse the attack, with the goal of tricking the attacker into thinking that the attack was successful. Report the 2 flags that you discover during this process, and briefly describe the steps you have taken.

The two parts carry, respectively, 60% and 40% of the marks.