Grade 11 Computing

Unit 7 · Cybersecurity in Practice

WORKSHEET

Full marks 32

Name _____ Class _____ Roll no. ____ Date _____ Marks _____ / 32

1 Key words [4]

Fill in the blanks with words from the box. Two words in the box are not needed. Each blank carries 0.5 mark.

allow-list	**assets**	**attack surface**	**blocklist**	**escaping**	**firewall**	**parameterized query**	
responsible disclosure	**salt**	**trust boundary**					

The things a system must protect, such as data, money and a service people rely on, are its _____. The line between what we control and what we don't is a _____, and all the places where outside data enters, together, are the _____. A query with ? where each value goes, the values sent separately, is a _____. A list of the only values a program accepts is an _____. Replacing < with `<`, so that the browser shows the character instead of reading it as HTML, is _____. A random value mixed into each password before it is hashed is a _____. Telling the owner of a flaw privately, and describing it in public only after it is fixed, is _____.

2 Which kind of threat? [2]

Match each thing that could go wrong with the lost-and-found board, in Column A, with its kind of threat from STRIDE, in Column B. Two items in Column B are not needed. Each carries 0.5 mark.

	Column A		Column B
1.	A student signs in as a member of staff with a password he guessed.	☐	a. tampering
2.	Someone changes the date on a report that somebody else made.	☐	b. spoofing
3.	A program sends thousands of fake reports, and the board stops answering.	☐	c. elevation of privilege
4.	A student deletes items, which only staff are allowed to do.	☐	d. information disclosure
			e. denial of service
			f. repudiation

3 Multiple choice [5]

Choose the correct option for each of the following questions.

i. Which of these is a **physical** security measure? [1]

a. a slow, salted password hash
b. a Content-Security-Policy header
c. keeping the backup drive in a locked drawer
d. two-step login

ii. A program runs `db.execute("SELECT * FROM items WHERE id = " + item_id)`, where item_id came from the address. What is the best fix? [1]

a. check that item_id has no quote marks in it

b. put quote marks round item_id

c. `db.execute("SELECT * FROM items WHERE id = ?", (item_id,))`

d. make the address hard to guess

iii. Without salt, why does a thief's work not grow with the number of users? [1]

a. Unsalted hashes are shorter.

b. Each guess is hashed once and looked up among all the stored hashes at once.

c. The thief needs only the first user's password.

d. Without salt, the hash can be undone.

iv. The Twitter breach of 2020 is best classified as: [1]

a. SQL injection

b. a denial of service

c. social engineering, using staff tools that gave one person too much power

d. a stolen table of password hashes

v. While using your school's results website, you notice that changing one number in the address shows another student's marks. What should you do? [1]

a. Check a few more numbers to make sure it really is a flaw.

b. Post it in the class group so everyone knows to be careful.

c. Stop, write down what you saw, and tell the school's office or a teacher privately.

d. Ask the school for a reward before telling them how.

4 What does it print? [5]

Write exactly what each program prints, in the box under it.

a. [3]

```
1  import html
2
3  notice = 'Fees due <b>Friday</b> & "today"'
4  print("<li>" + notice + "</li>")
5  print("<li>" + html.escape(notice) + "</li>")
```

```
OUTPUT
```

Which of the two lines can a notice board safely put into its page? Why?

b. [2]

```
SORTABLE = {"what", "place", "found_on"}

def list_query(order_by):
    if order_by not in SORTABLE:
        raise ValueError("Can't sort by " + repr(order_by))
    return "SELECT what FROM items ORDER BY " + order_by

for column in ["place", "Place", "found_on"]:
    try:
        print(list_query(column))
    except ValueError as e:
        print("Refused:", e)
```

```
OUTPUT
```

5 Trace the program [3]

Fill in the trace table: one row for each time round the loop, then what the program prints after the loop.

To stop a flood of fake reports, the board refuses more than 2 reports from one address.

```
LIMIT = 2
counts = {}
for address in ["10.0.0.5", "10.0.0.7", "10.0.0.5", "10.0.0.5", "10.0.0.7"]:
    counts[address] = counts.get(address, 0) + 1
    if counts[address] > LIMIT:
        print("refused:", address)
print(counts)
```

address	counts[address]	Output

6 Review the code [4]

Read the program, then answer.

Here is part of a beginner's lost-and-found board. Each function has one flaw. For each, write the line, what harm it could allow (in words), and the fixed line.

```
1  import hashlib
2  import random
3
4  def store_password(password):
5      return hashlib.sha256(password.encode()).hexdigest()
6
7  def new_session():
8      return str(random.randint(1000, 9999))
9
10 def search(place):
11     return db.execute("SELECT what FROM items WHERE place = '" + place +
   "'").fetchall()
12
13 def item_html(item):
14     return "<li>" + item["what"] + "</li>"
```

7 The thief's work [3]

Work it out in the space below.

A website's table of 2,000 users is stolen. Each password is stored with its own salt and a slow hash that costs 100,000 fast hashes a guess. The thief's computer works out 10^{10} fast hashes a second. How long does it take to try a list of 1 million passwords against every user? How long would it take if the passwords had been stored with a fast hash and no salt?

Answer: _____

8 Long answer [4]

Write a long answer to the following question.

Your friend finds that the website of a shop in your town shows every customer's phone number if you add a word to its address. He wants to download the list "to prove it", then post about it. What does the law say, and what should he do instead?

9 Think [2]

Think, then answer.

A programmer says: "Nobody will find the Delete request: there's no button for it, and the address isn't written anywhere on the page." Why is this not a defense?

10 Activity: A threat model of your own (not marked)

Work in a group, on paper. Choose a system you know: the school library's borrowing register, a canteen's order book, or your class's chat group. For each kind of threat, write one thing that could go wrong, a defense, and who pays its price (users, data or devices) and how.

Threat	What could go wrong	Defense	Its price, and who pays
Spoofing			
Tampering			
Information disclosure			
Denial of service			