7 Security (mgk25)

(a) An SQLite database set up with

```
CREATE TABLE users(name varchar(32), password varchar(32));
CREATE TABLE prices(commodity varchar(32), value varchar(32));
INSERT INTO users VALUES ('alice', 'SeCreT');
INSERT INTO prices VALUES ('gold', 1335.33);
```

is used by a Perl web application for looking up commodity prices. The
application receives a string in variable $metal from a user-provided HTML
form, forms an SQL statement to look up the corresponding price with

```
$sql = "SELECT value FROM prices WHERE commodity='$metal';";
```

and displays to the user the value it finds in the first column of the first row of
the table returned.

(i) What text could an attacker provide in $metal, such that

(A) the value displayed is the password of user alice? [3 marks]

(B) the password of user alice is changed to qwerty. [3 marks]

(ii) Briefly describe three measures that the designer of the web application can
take to reduce the risks created by the attack described in Part (a)(i)(A). [6 marks]

(iii) Describe how the TCB of the web application could be structured to reduce
the risk of the attack described in Part (a)(i)(B). [2 marks]

(b) The WikiHash web application stores for each registered user $U$ in its user table
the tuple $(U, V)$ with $V = H(P)$, where $H$ is a collision-resistant hash function
and $P$ is $U$’s password. When an HTTP request arrives, it applies the following
authentication procedure:

- if the request arrives without a session cookie, the user is presented with a
password login form
- when the user submits username $U$ and password $P$ via that form, the web
application checks the user table for entry $(U, H(P))$ and if it exists sets
the session cookie to $(U, H(H(P)))$
- if the request arrives with a session cookie $(U, C)$, the web application loads
the user’s user-table entry $(U, V)$ and checks if $H(V) = C$ before granting
access to pages restricted to user $U$

(i) What risk does storing $H(P)$ (as opposed to storing $P$) in a user table aim
to mitigate? [2 marks]

(ii) Show that this risk isn’t actually mitigated by the above procedure and
suggest a fix. [4 marks]