Formative Assignment

Question 1:

1. There is no sanitisation of input meaning it is open to a user entering program arguments or database queries in the form of an SQL injection. This could lead to a threat actor gaining access to other sections of the database that contain private or security information.
2.
Prepared Statements – These are statements that have been written and checked by experts in the field, you can follow the template given and bind a query to a specific value, negating the chance of an attacker adding extra queries to the end of a legitimate one
Stored procedures – Keeping SQL queries stored within the database server so that new queries don't need to be generated, when implimented correctly this can mean that user input can't affect the generated queries.
3.

```
$author = $_GET['author'];
$query = "SELECT (*) FROM books WHERE author = :author";
$stmt = $dbh → prepare($query)
$stmt → bindParam(':author', $author);
$stmt → execute();
```

Question 2:

1.
A HttpOnly cookie is sent to a browser in an attempt to stop XSS attacks by not allowing the cookie to be accessed by anything other than HTTP/S requests, preventing scripts from being run to collect it.
2.
Implimenting HttpOnly cookies can make it harder to perform XSS attacks but can't stop them all together as if an attacker can circumvent collecting the cookies from the browser, they can be accessed in several other locations such as querying the web server that the website is hosted on.

Question 3:

1.
A UID is a set of permissions that the user has, they can be subdivided into
Effective UID: The privileges of the user at the time
Real UID: The actual privileges of the user
Saved UID: Used to store the effective UID when changing priveleges
2. The First call of testfile will be effective as the user is root and only root can access etc/shadow, the priveleges are then set to that of a normal user and so the opening attempt will fail. Finally when trying to set the UID back to root, the setuid will fail, this is because once you drop priveleges they are dropped throughout.

Question 4:

1. Setting up several layers of security between sensitive data and outside connections. An example of this is using a white list to validate a prepared statement, even though a prepared statement is relatively secure, extra can be added.

Question 5:

1.

Consequences -

Access to/Ability to change Name, All other given profile information, Current grades, Released lecture slides, messages sent via canvas, Groups within modules and they are also able to upload assignments

Largest Personal affect -

Uploading assignments as this could have an enormous affect on grades and personal achievement

Largest University affect -

Sending messages via canvas, released data from one account is manageable but if the attacker can use the messaging system to infect more users then it could become a very large data breach