CS628A - CTF 2
Deepanshu Bansal (150219)
Securing the VIHS

General approach to secure the VIHS platform is to prevents two types of major attacks that are

SQL Injection

To prevent SQLI attacks on VHIS we can :

1. **Parameterized Queries** : Use Prepared Statements with Parameterized Queries. Since VIHS is php based we should use PDO with strongly typed parameterized queries.
2. **Validation of user input** : We should do an input validation first to make sure the value is of the accepted type, length, format, etc. Only the input which passed the validation can be processed to the database.
3. **Object Relational Mapping (ORM) :** We can also use ORM frameworks to make the translation of SQL result sets into code objects more seamless.

File Inclusion

To prevent file inclusion based attacks on VIHS :

1. In this also first step would be to validate the url given as input.
2. We should save the file paths in a database and assign an ID to each of them so that users only see the ID and are not able to view or change the path.
3. We should also use a whitelist of filenames and ignore every other filename and path.
4. We should store the content of files in databases whereever possible instead of including files on the web server.

Games

To prevent vulnerabilities like in the Game of collision we should we should sanitize the urls and validate them so that the type of parameter specified doesn't change in the request as done on the server.

References :

1. https://tableplus.io/blog/2018/08/best-practices-to-prevent-sql-injection-attacks.html
2. https://dzone.com/articles/local-file-inclusion-vulnerability-1