Used gobuster to find /blood directory.

Used *‘ OR 1=1;-- -* to bypass the authentication page.

Used Sqlmap to test the *id* parameter. Sqlmap identified that it was vulnerable to a:

* Error-based query injection.
* UNION query injection.
* Text

  Description automatically generatedTime-based query injection.

Using the information provided by Sqlmap, the format for injecting a query into the field of *id* is:

*{target\_url}/blood/view.php?id=’’UNION ALL SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL,CONCAT(table\_name) FROM information\_schema.tables;-- -*

Upon executing the above query, we find that ‘blood\_db’ is the returned database.

If we modify our query to reflect using the found database,

**Alternatively**, we could simply go to the /submit-info.php page, enter arbitrary values, and quickly identify that the site returns the database.

Text

Description automatically generated**Alternatively**, we could also invoke the --dbs switch in the Sqlmap command. Doing so will return the databases found in the site.

Text

Description automatically generated with low confidenceIf we check the -hh menu, we find that we can include the database that we found into Sqlmap using the -D switch. After doing so, we are presented with three tables we can enumerate.

Text

Description automatically generatedGoing one step further with Sqlmap and its switches, we find that we can also include a Table using -T, as well as return the data within one or all tables using the --dump / --dump-all switches.

The results above detail the information required to complete the room.