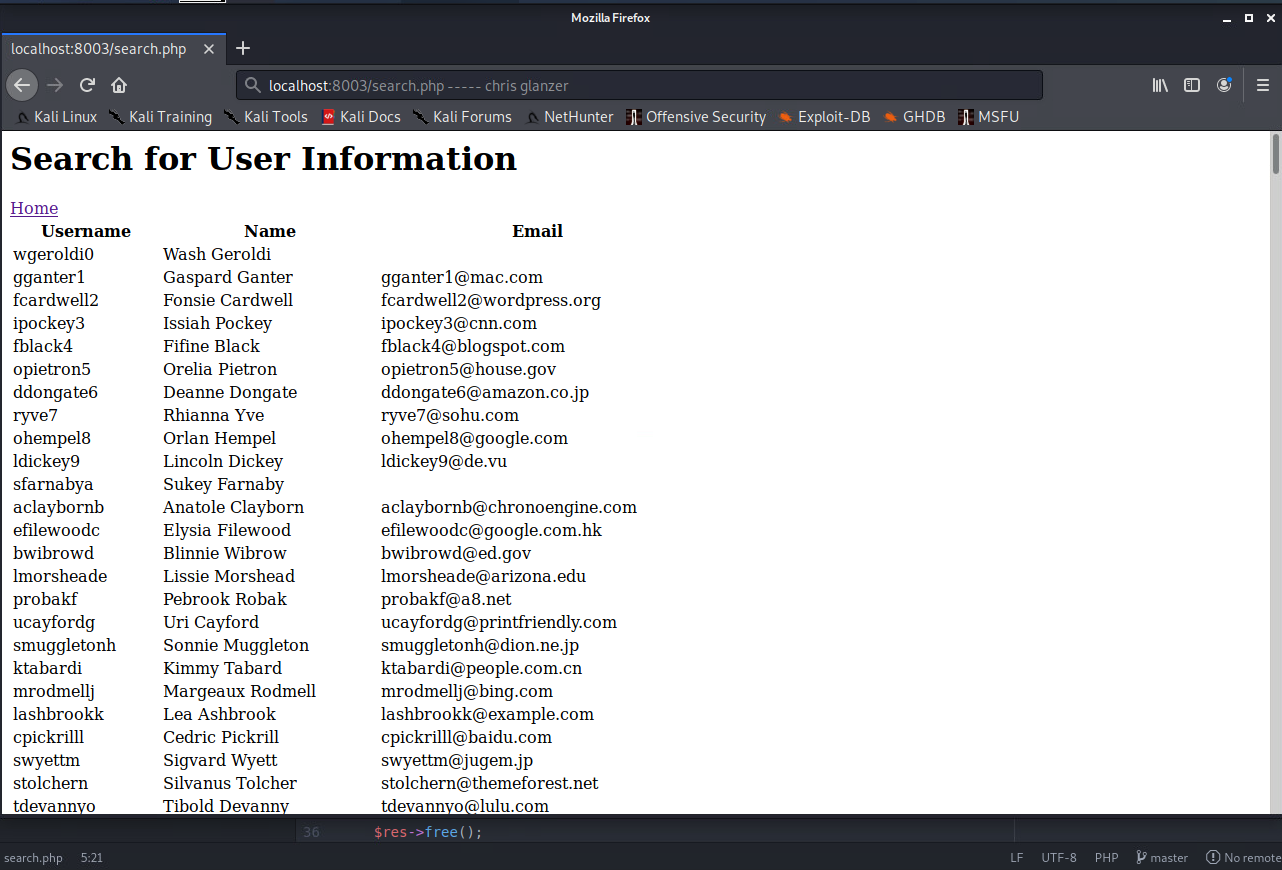
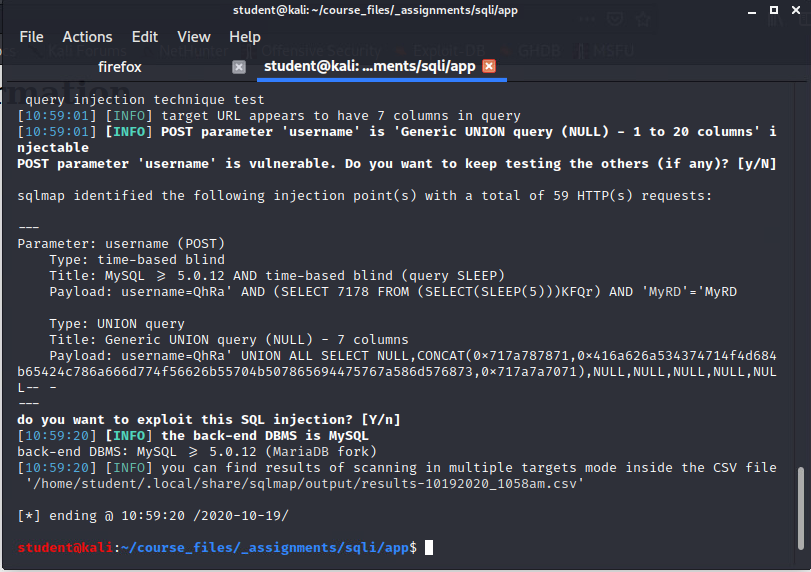
Discovery  
  
1.

1. php
2. search.php
3. a2user / changeme
4. search.php
5. 

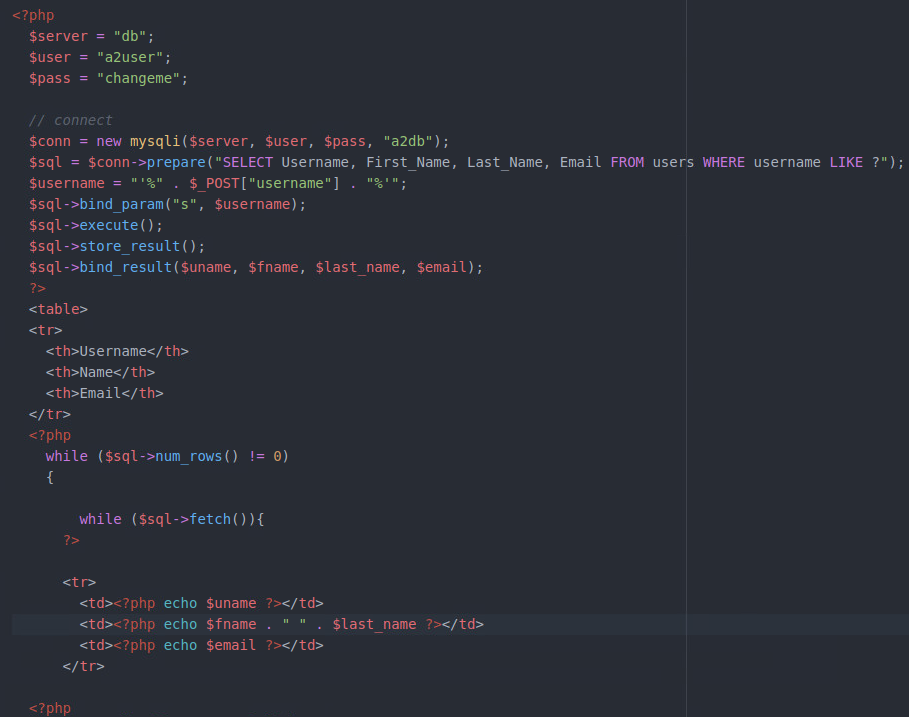
2.

a. 7  
 b. username: bill  
 c. ‘;# or ‘ OR 1=1 ;#  
 d. 

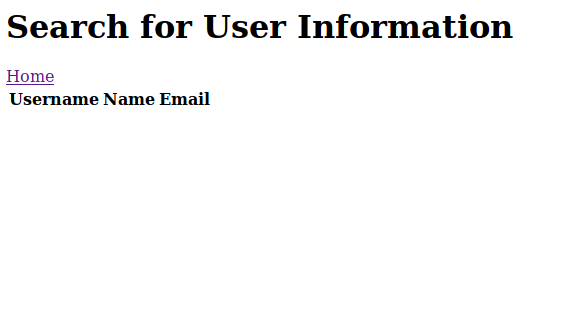
Testing

3.  
 a.   
 b. confused if the banner means something different in this context, but I’m thinking it’s this?:  
  
 c. tacked –count to the end of the previous command  
  
 d. 855

4.

a. 

b. 1) changed the SELECT \* to select only the specific columns from the table that are necessary (I didn’t check if there were any other columns to find)  
 . 2) we used native object functions to concatenate the user-provided search term with the prepared statement.   
  
I relied pretty heavily on the video / guide for this part as I am not familiar with PHP. I got it working, however I am not sure if the mysqli object is native to php or if it is something in from bwapp / the lab. I couldn’t find any includes in the assignment, so I’m lead to believe that it is native to PHP. I thought sqli meant sql injection, which seems like an odd object name for native PHP objects (mysqli) unless it means something different in this context.   
  
also I’m not 100% sure what is happening that this manages to filter out the dangerous string – whether we are escaping the dangerous characters? Or does the bind\_param() function somehow further abstract the input another level, similar to using a %s in printf ensuring that the input is interpreted as a string?

5.  
 a. response from “ ’;#” is blank, and so is “ ’; OR 1=1”  
 

b.   
  
