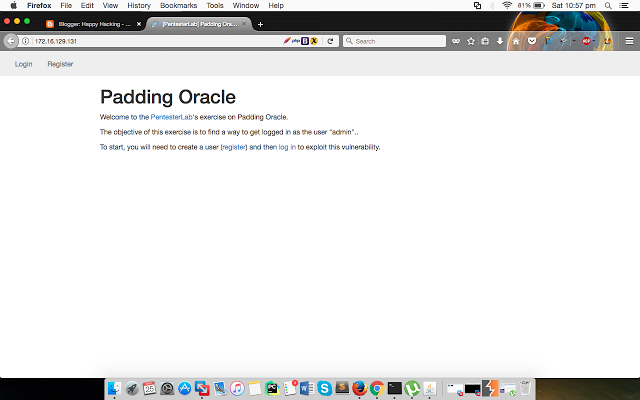
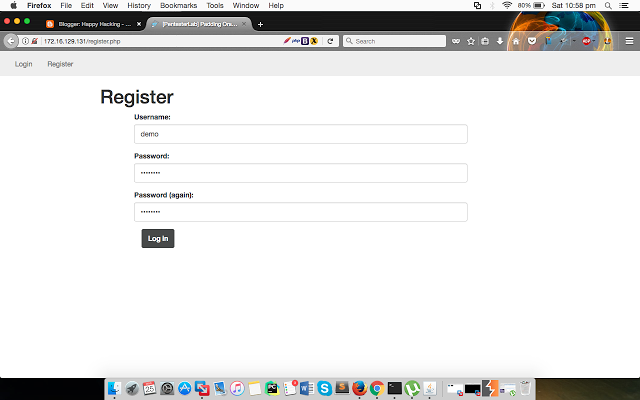
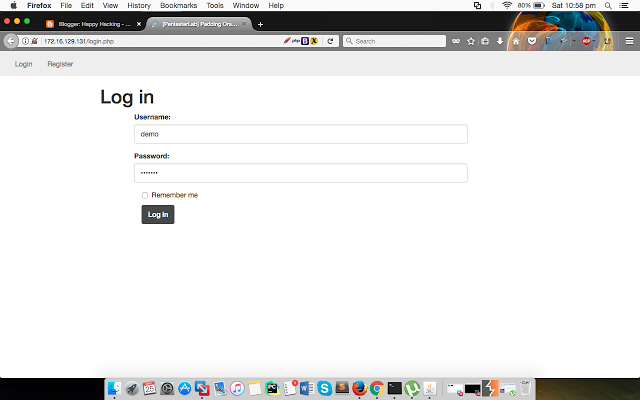
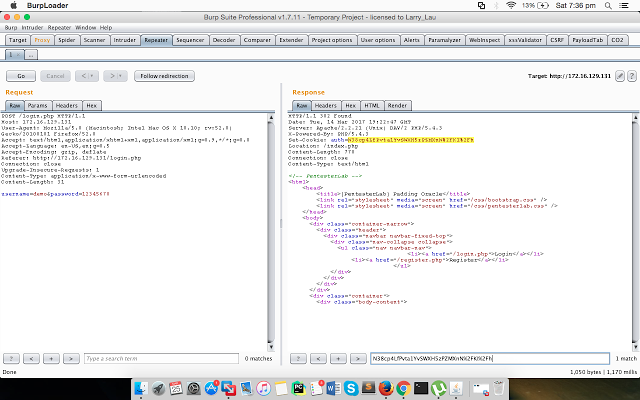
[March 25, 2017](https://dhamuharker.blogspot.co.id/2017/03/hack-padding-oracle.html" \o "permanent link)

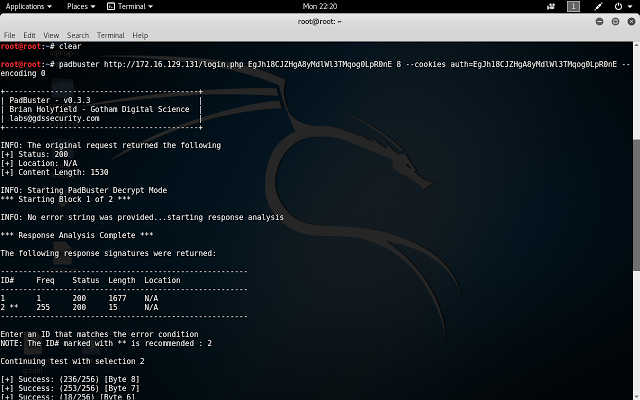
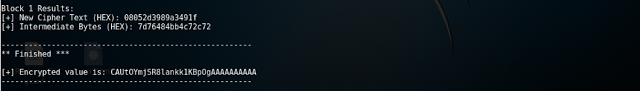
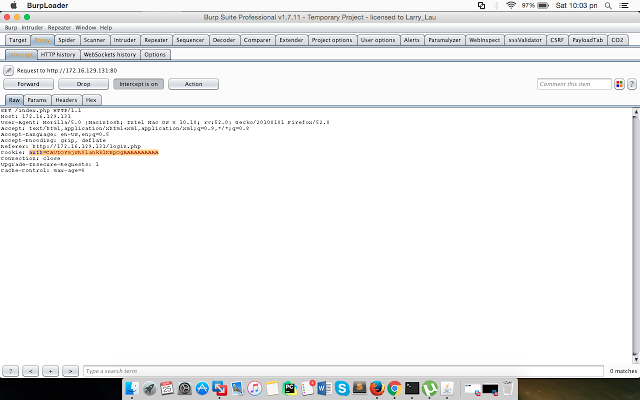
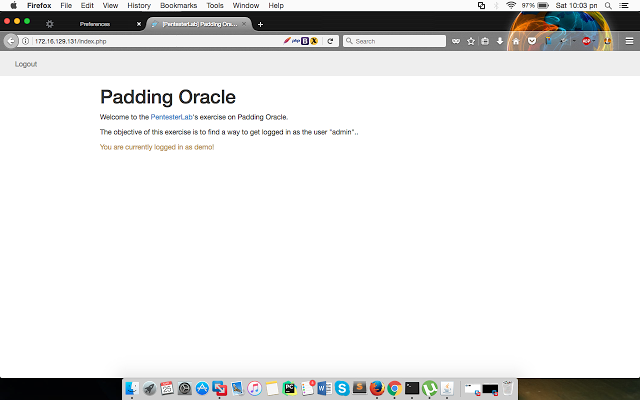
This VM, Provided by Pentester Lab, has a website vulnerable to padding oracle attack .   
Our goal is to exploit this vulnerability and login as user and admin .    
  
**Step 1 :** Now A look at Website  
 **[](https://4.bp.blogspot.com/-0_U5QG2404E/WNaozw6cCFI/AAAAAAAADtw/QaSRhIKlx84-zF3SES6BB0fCPK_C32NegCK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B10.57.34%2Bpm.png)**  
  
The Website said that we should create an account first. This is because key only appears when you are logged in .   
  
[](https://3.bp.blogspot.com/-5mF1Gbfoz2E/WNapCpvokII/AAAAAAAADt8/-xXI5yQvXxsnAIw6TnERNd-0-v2PDWoewCK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B10.58.06%2Bpm.png)  
  
[](https://3.bp.blogspot.com/-RPsDyAmsTFA/WNapH9nL_MI/AAAAAAAADuI/KrEgAtjquZwSj7b999nTnqhVRgjyTcyxwCK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B10.58.19%2Bpm.png)  
  
**Step 2 :** Using Burpsuite , We can Intercept the server's response  and see how it's look like .

[[](https://3.bp.blogspot.com/-lMdIr0iZWBk/WNafdEPS4nI/AAAAAAAADs4/1uamr72p_R4Dsd5QXhkXV9u6TWbyGlxbgCK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B7.36.16%2Bpm.png)](https://3.bp.blogspot.com/-lMdIr0iZWBk/WNafdEPS4nI/AAAAAAAADs4/1uamr72p_R4Dsd5QXhkXV9u6TWbyGlxbgCK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B7.36.16%2Bpm.png)

**Step 3 :**  Now We have Auth  Key       EgJh18CJZHgA8yMdlWl3TMqog0LpR0nE

**Step 4 :** Kali has an  Padbuster  Tool .

Where URL = The target URL (and query string if applicable)                                                            EncryptedSample = The encrypted value you want to test.                                                                   Must also be present in the URL, PostData or a Cookie   
BlockSize = The block size being used by the algorithm

[[](https://3.bp.blogspot.com/-513BfZt4fiE/WNah9Fee8jI/AAAAAAAADtE/NYxu9QafUwY9i5tFOJMWCMv22rfQpOqQACK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B8.29.07%2Bpm.png)](https://3.bp.blogspot.com/-513BfZt4fiE/WNah9Fee8jI/AAAAAAAADtE/NYxu9QafUwY9i5tFOJMWCMv22rfQpOqQACK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B8.29.07%2Bpm.png)  
  
  
**Step 5 :**  Now Decrypt Value Of Auth key is user = hacker . We Can Simply Reencrypt Using the String User = demo    
  
padbuster http://172.16.129.131/login.php EgJh18CJZHgA8yMdlWl3TMqog0LpR0nE 8 --cookies auth=EgJh18CJZHgA8yMdlWl3TMqog0LpR0nE --encoding 0  -plaintext user=demo    
  
  
[[](https://2.bp.blogspot.com/-4OwPp7P3jM0/WNajad5c0UI/AAAAAAAADtQ/ajYCq2vQ75kX2HMappwFvyYNSFgrh7jEwCK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B10.35.05%2Bpm.png)](https://2.bp.blogspot.com/-4OwPp7P3jM0/WNajad5c0UI/AAAAAAAADtQ/ajYCq2vQ75kX2HMappwFvyYNSFgrh7jEwCK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B10.35.05%2Bpm.png)  
  
**Step 6 :** Using Burpsuite , Intercept the Request and Change the Auth Cookie Value With the New Encrypted value     
  
 [[](https://2.bp.blogspot.com/-JFBXBS0PT4c/WNalSnfLiuI/AAAAAAAADtc/SosftYot3DEx5cUen00Igw0T2GFeTT7CACK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B10.03.26%2Bpm.png)](https://2.bp.blogspot.com/-JFBXBS0PT4c/WNalSnfLiuI/AAAAAAAADtc/SosftYot3DEx5cUen00Igw0T2GFeTT7CACK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B10.03.26%2Bpm.png)  
  
  
**Step 7 :** Click Forward and You Got Logged in User Account .   
  
  
 [](https://4.bp.blogspot.com/-7LkOf_NP52E/WNalXSB6T5I/AAAAAAAADtk/W8M_DU7bJ0AmFvvoXAwChYsujmWbjca2ACK4B/s1600/Screen%2BShot%2B2017-03-25%2Bat%2B10.03.50%2Bpm.png)  
  
  
Thank You Pentester Lab .