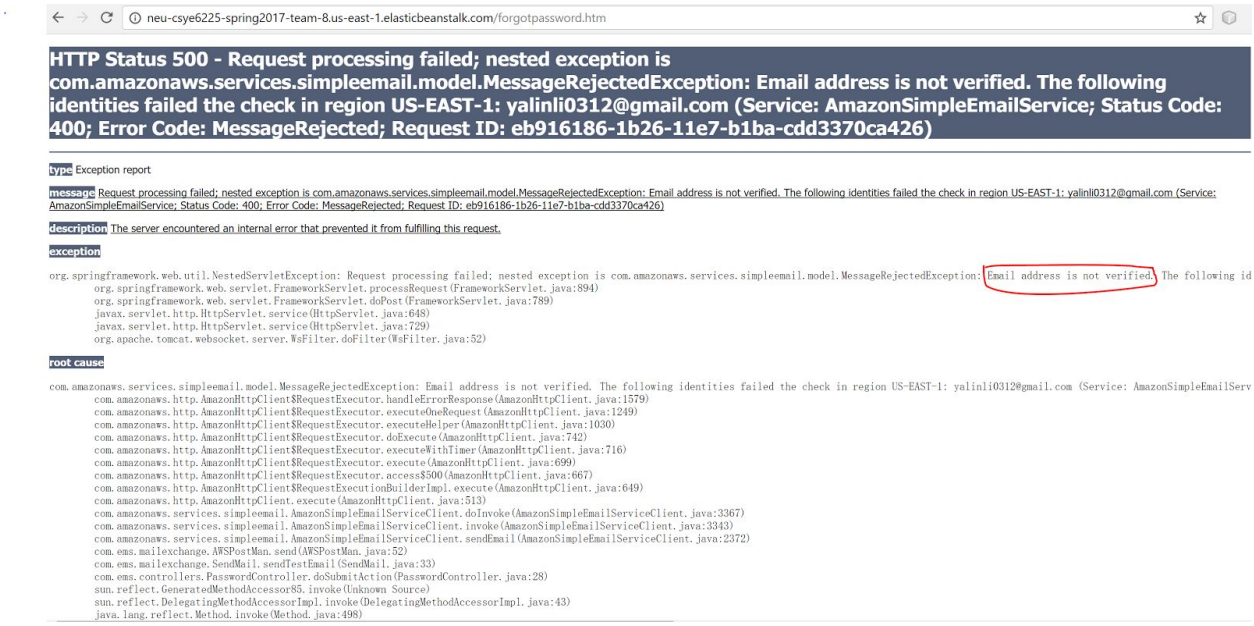
Penetration Testing Report

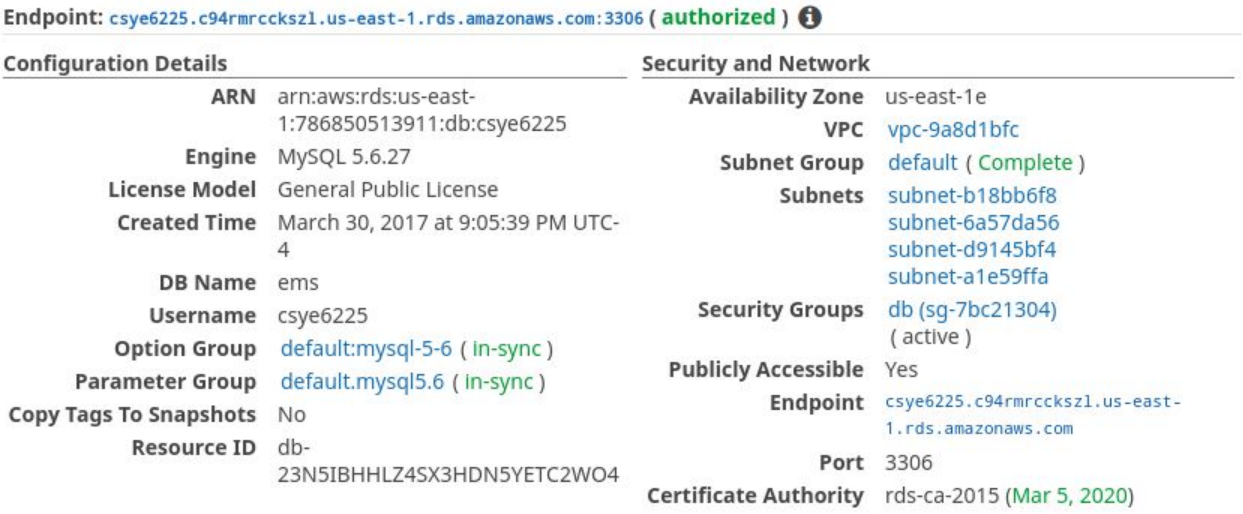
Target Team: Team 8
Website url: http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/

AWS setup and identify security issues :

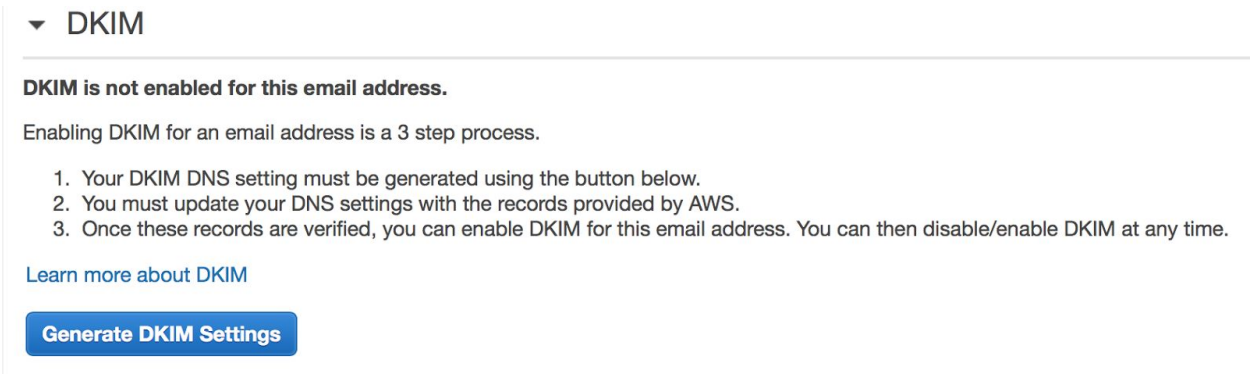
1. ***Try to find password of one new registered email when the recipient email address is not verified in Amazon SES***.
   Register new manager using the email of yalinli0312@gmail.com, try this email address after logout in "forget password" link, there throw an exception:



2. ***RDS MySQL should not be publicly accessible***



3. ***No DKIM setup***
   There is no DKIM setup for verified email address in Amazon SES



WebApp Hacking using Kali Linux Tools:

1. ***Grabber***
   Grabber is a web application scanner. Basically it detects some kind of vulnerabilities in your website.
   Attack Vector: Cross-Site Scripting/SQL Injection
   Command Line: grabber --spider 1 --sql --xss --url http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/
   Result:

```
root@kali:~# grabber --spider 1 --sql --xss --url http://neu-csye6225-spring2017-team-8.us-eas
t-1.elasticbeanstalk.com/
Start scanning... http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/
runSpiderScan @  http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/  |   #
1
runSpiderScan @  http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//forgotP
assword.jsp  |   # 0
runSpiderScan @  http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//testJSP
.jsp  |   # 0
Start investigation...
Method = GET  http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//forgotPass
word.jsp
Method = GET  http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/
Method = GET  http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//testJSP.js
p
[Cookie]        0       :       <Cookie JSESSIONID=DCEA36C7DDA9E21AEC58011473228413 for neu-cs
ye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/>
Method = GET  http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//forgotPass
word.jsp
Method = GET  http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/
Method = GET  http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//testJSP.js
p
[Cookie]        0       :       <Cookie JSESSIONID=DCEA36C7DDA9E21AEC58011473228413 for neu-cs
ye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/>
```

2. ***XSSer***

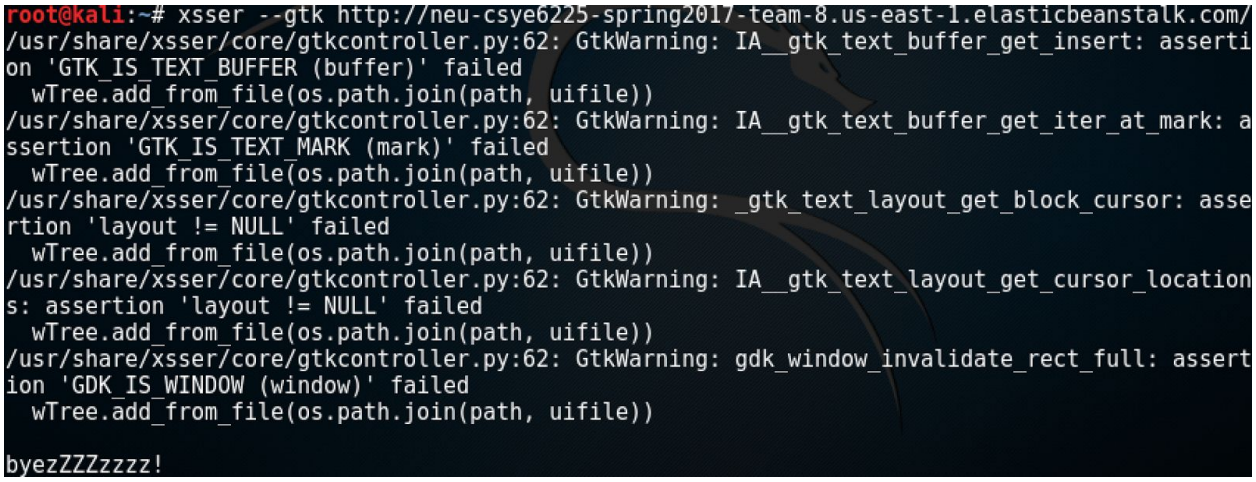
Cross Site "Scripter" (aka XSSer) is an automatic -framework- to detect, exploit and report XSS vulnerabilities in web-based applications. It contains several options to try to bypass certain filters, and various special techniques of code injection.

Attack Vector: Cross-Site Scripting

Command Line: xsser --gtk

http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/

Result:



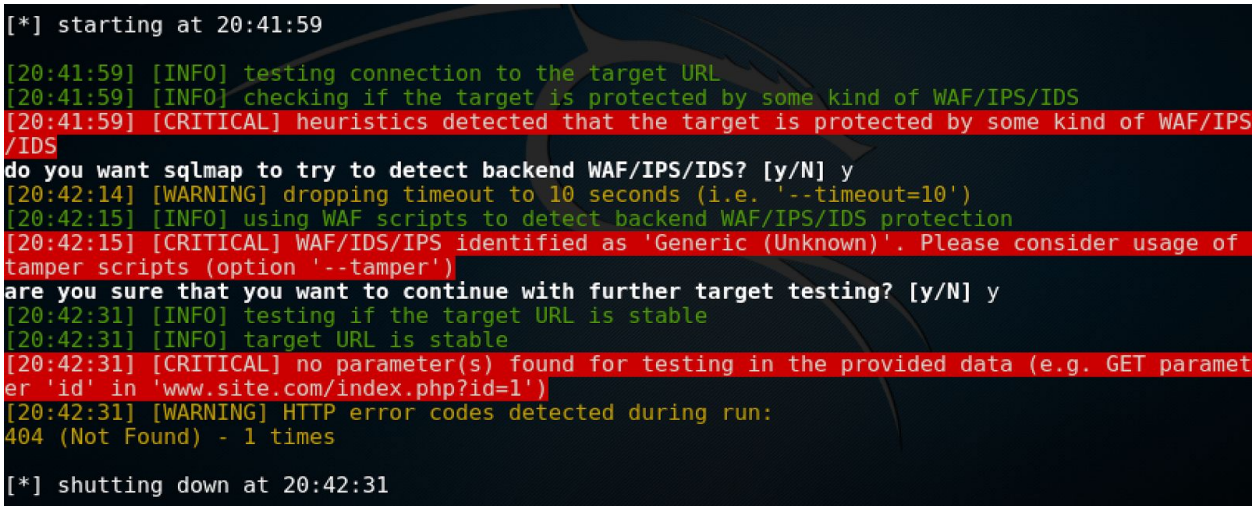
3. ***Sqlmap***

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

Attack Vector: SQL injection

Command Line: sqlmap -u http://neu-csye6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/

Result:



4. ***Manual Script Injection***

   Attack Vector: Search box script injection

   On loginuser.htm page, enter script: <script>alert(“Error!”);</script> in search box

   Result: Attack failed. The website prevented script injection successfully.