

# Penetration Testing Report

Target Team: Team 8

Website url: <http://neu-csy6225-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](mailto:yalinli0312@gmail.com), try this email address after logout in “forget password” link, there throw an exception:

← → ↻ ⓘ neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/forgetpassword.htm ☆ ⓘ

**HTTP Status 500 - Request processing failed; nested exception is com.amazonaws.services.simpleemail.model.MessageRejectedException: Email address is not verified. The following identities failed the check in region US-EAST-1: yalinli0312@gmail.com (Service: AmazonSimpleEmailService; Status Code: 400; Error Code: MessageRejected; Request ID: eb916186-1b26-11e7-b1ba-cdd3370ca426)**

**type** Exception report

**message** Request processing failed; nested exception is com.amazonaws.services.simpleemail.model.MessageRejectedException: Email address is not verified. The following identities failed the check in region US-EAST-1: yalinli0312@gmail.com (Service: AmazonSimpleEmailService; Status Code: 400; Error Code: MessageRejected; Request ID: eb916186-1b26-11e7-b1ba-cdd3370ca426)

**description** The server encountered an internal error that prevented it from fulfilling this request.

**exception**

```
org.springframework.web.util.NestedServletException: Request processing failed; nested exception is com.amazonaws.services.simpleemail.model.MessageRejectedException: Email address is not verified. The following id
org.springframework.web.servlet.FrameworkServlet.processRequest (FrameworkServlet.java:894)
org.springframework.web.servlet.FrameworkServlet.doPost (FrameworkServlet.java:789)
javax.servlet.http.HttpServlet.service (HttpServlet.java:648)
javax.servlet.http.HttpServlet.service (HttpServlet.java:729)
org.apache.tomcat.websocket.server.WsFilter.doFilter (WsFilter.java:52)
```

**root cause**

```
com.amazonaws.services.simpleemail.model.MessageRejectedException: Email address is not verified. The following identities failed the check in region US-EAST-1: yalinli0312@gmail.com (Service: AmazonSimpleEmailServ
com.amazonaws.http.AmazonHttpClient$RequestExecutor.handleErrorResponse (AmazonHttpClient.java:1579)
com.amazonaws.http.AmazonHttpClient$RequestExecutor.executeOneRequest (AmazonHttpClient.java:1249)
com.amazonaws.http.AmazonHttpClient$RequestExecutor.execute (AmazonHttpClient.java:1030)
com.amazonaws.http.AmazonHttpClient$RequestExecutor.doExecute (AmazonHttpClient.java:742)
com.amazonaws.http.AmazonHttpClient$RequestExecutor.executeWithTimer (AmazonHttpClient.java:716)
com.amazonaws.http.AmazonHttpClient$RequestExecutor.execute (AmazonHttpClient.java:699)
com.amazonaws.http.AmazonHttpClient$RequestExecutor.access$500 (AmazonHttpClient.java:667)
com.amazonaws.http.AmazonHttpClient$RequestExecutor.execute (AmazonHttpClient.java:649)
com.amazonaws.http.AmazonHttpClient.execute (AmazonHttpClient.java:513)
com.amazonaws.services.simpleemail.AmazonSimpleEmailServiceClient.doInvoke (AmazonSimpleEmailServiceClient.java:3367)
com.amazonaws.services.simpleemail.AmazonSimpleEmailServiceClient.invoke (AmazonSimpleEmailServiceClient.java:3343)
com.amazonaws.services.simpleemail.AmazonSimpleEmailServiceClient.sendEmail (AmazonSimpleEmailServiceClient.java:2372)
com.ens.mailexchange.AWSPostMan.send (AWSPostMan.java:52)
com.ens.mailexchange.SendMail.sendTestEmail (SendMail.java:33)
com.ens.controllers.PasswordController.doSubmitAction (PasswordController.java:28)
sun.reflect.GeneratedMethodAccessor$5.invoke (Unknown Source)
sun.reflect.DelegatingMethodAccessorImpl.invoke (DelegatingMethodAccessorImpl.java:43)
java.lang.reflect.Method.invoke (Method.java:498)
```

2. RDS MySQL should not be publicly accessible

Endpoint: [csye6225.c94rmrccksz1.us-east-1.rds.amazonaws.com:3306](https://csye6225.c94rmrccksz1.us-east-1.rds.amazonaws.com:3306) ( **authorized** ) ⓘ

Configuration Details		Security and Network	
ARN	arn:aws:rds:us-east-1:786850513911:db:csye6225	Availability Zone	us-east-1e
Engine	MySQL 5.6.27	VPC	vpc-9a8d1bfc
License Model	General Public License	Subnet Group	default ( <b>Complete</b> )
Created Time	March 30, 2017 at 9:05:39 PM UTC-4	Subnets	subnet-b18bb6f8 subnet-6a57da56 subnet-d9145bf4 subnet-a1e59ffa
DB Name	ems	Security Groups	db (sg-7bc21304) ( active )
Username	csye6225	Publicly Accessible	Yes
Option Group	default:mysql-5-6 ( <b>In-sync</b> )	Endpoint	csye6225.c94rmrccksz1.us-east-1.rds.amazonaws.com
Parameter Group	default:mysql5.6 ( <b>In-sync</b> )	Port	3306
Copy Tags To Snapshots	No	Certificate Authority	rds-ca-2015 ( <b>Mar 5, 2020</b> )
Resource ID	db-23N5IBHHLZ4SX3HDN5YETC2WO4		

### 3. *No DKIM setup*

There is no DKIM setup for verified email address in Amazon SES

#### ▼ DKIM

**DKIM is not enabled for this email address.**

Enabling DKIM for an email address is a 3 step process.

1. Your DKIM DNS setting must be generated using the button below.
2. You must update your DNS settings with the records provided by AWS.
3. Once these records are verified, you can enable DKIM for this email address. You can then disable/enable DKIM at any time.

[Learn more about DKIM](#)

**Generate DKIM Settings**

## 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-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/>

Result:

```
root@kali:~# grabber --spider 1 --sql --xss --url http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/
Start scanning... http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/
runSpiderScan @ http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/ | #
1
runSpiderScan @ http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//forgotPassword.jsp | # 0
runSpiderScan @ http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//testJSP.jsp | # 0
Start investigation...
Method = GET http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//forgotPassword.jsp
Method = GET http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/
Method = GET http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//testJSP.jsp
[Cookie] 0 : <Cookie JSESSIONID=DCEA36C7DDA9E21AEC58011473228413 for neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/>
Method = GET http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//forgotPassword.jsp
Method = GET http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/
Method = GET http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com//testJSP.jsp
[Cookie] 0 : <Cookie JSESSIONID=DCEA36C7DDA9E21AEC58011473228413 for neu-csy6225-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-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/>

Result:

```
root@kali:~# xsser --gtk http://neu-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/
/usr/share/xsser/core/gtkcontroller.py:62: GtkWarning: IA_gtk_text_buffer_get_insert: assertion 'GTK_IS_TEXT_BUFFER (buffer)' failed
  wTree.add_from_file(os.path.join(path, uifile))
/usr/share/xsser/core/gtkcontroller.py:62: GtkWarning: IA_gtk_text_buffer_get_iter_at_mark: assertion 'GTK_IS_TEXT_MARK (mark)' failed
  wTree.add_from_file(os.path.join(path, uifile))
/usr/share/xsser/core/gtkcontroller.py:62: GtkWarning: _gtk_text_layout_get_block_cursor: assertion 'layout != NULL' failed
  wTree.add_from_file(os.path.join(path, uifile))
/usr/share/xsser/core/gtkcontroller.py:62: GtkWarning: IA_gtk_text_layout_get_cursor_location: assertion 'layout != NULL' failed
  wTree.add_from_file(os.path.join(path, uifile))
/usr/share/xsser/core/gtkcontroller.py:62: GtkWarning: gdk_window_invalidate_rect_full: assertion 'GDK_IS_WINDOW (window)' failed
  wTree.add_from_file(os.path.join(path, uifile))
byeZZZZzzzz!
```

## 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-csy6225-spring2017-team-8.us-east-1.elasticbeanstalk.com/>

Result:

```
[*] starting at 20:41:59
[20:41:59] [INFO] testing connection to the target URL
[20:41:59] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[20:41:59] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS/IDS
do you want sqlmap to try to detect backend WAF/IPS/IDS? [y/N] y
[20:42:14] [WARNING] dropping timeout to 10 seconds (i.e. '--timeout=10')
[20:42:15] [INFO] using WAF scripts to detect backend WAF/IPS/IDS protection
[20:42:15] [CRITICAL] WAF/IDS/IPS identified as 'Generic (Unknown)'. Please consider usage of tamper scripts (option '--tamper')
are you sure that you want to continue with further target testing? [y/N] y
[20:42:31] [INFO] testing if the target URL is stable
[20:42:31] [INFO] target URL is stable
[20:42:31] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1')
[20:42:31] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times
[*] shutting down at 20:42:31
```

#### ***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.