December 2, 2020

Mitigation of a Known Vulnerability Affecting the Creation of Official Employee Accounts of InstaNeTV

Ahmad Aryan
CSC 129

Introduction

On October 19, 2020, InstaNeTV's Secure Software Team discovered a vulnerability in one of our company's web pages. This vulnerability allowed employees to create official employee accounts based on their personal email accounts without proper screening. While the use of personal email addresses to create employee accounts is allowable per company policies (Policy # OP32-75), up to recently there hasn't been any policy certifying allowable personal email addresses for this purpose. This would have allowed employees to create official company accounts using email addresses that had been compromised in many data breaches.

The discovered vulnerability was reported to the Head of Operation Mr. Doug Lundin on October 20 and assigned problem report No. JSI-584. A joint investigation of the vulnerability by Development Team (DVT), Secure Software Team (SST) and Operations Office confirmed the severity of the issue and a priority level of 9 (out of 10) was assigned to the issue. Due to the severity of discovered vulnerability and lack of an appropriate policy to address the issue, another meeting was organized to discuss the development of a relevant policy and to find ways for mitigation of the problem. On October 21, the meeting was attended by the mentioned teams and a draft policy was developed to address the issue and was assigned No. OP35-92. The developed policy was approved by the Head of Operations on October 22 and took immediate effect. The main points of the policy are as follows:

- Any personal email accounts that are used to create company accounts shall not have been compromised in more than 3 data breaches.
- To prevent brute force attacks, at any one time, an employee shall be allowed up to three attempts to enter a valid and secure email address. If the employee fails to enter a valid and secure email address within 3 attempts, the employee shall be unable to try again before 30 minutes has passed.
- If the employee fails to provide an acceptable email address in the second round of attempts, he/she shall be locked out of the system. The event should be reported to Employee Services Office so that an account is created for the employee using a newly created email address. This shall be done by the Employee Services Office.

The full text of the policy can be found at:
https://instanetv.com/operations/policies/op35-92.

During the meeting it was suggested that the services of an IT security provider firm that specializes in keeping records of data spills should be purchased, so that potential email addresses that are intended to be used to create official company employee accounts, are checked against the database of known data spills. Such company has since been identified and the relevant service purchased after approval by the Head of Operations. Furthermore, during the meeting an agreement was reached that would lay down the process for immediate mitigation of the vulnerability. SST was tasked to find ways to mitigate the vulnerability upon approval of the policy and received official approval to work on the issue on October 22. This report discusses the details of mitigation of the vulnerability.
The full details and minutes of the meeting can be found at:
https://instanetv.com/operations/meetings/mt729fd.

Analysis of security vulnerability

The vulnerability allows new employees to create an official employee account based on their personal email accounts, regardless of how many times that email address may have been breached in known data spills. This would pose a significant security risk to our systems and services. Any email address that have been breached in numerous data spills could be used by attackers as a token to try breach the employee accounts. This type of attack is called credential stuffing attacks and is usually carried by automated tools using stolen usernames and passwords. Each years, millions of email addresses, usernames, and passwords are compromised in data breaches. Since InstaNeTV allows creation of employee accounts using personal email addresses per company policies, in case an email address is known to attackers, it could be used as a token to gain access to employees' accounts using password stuffing. Although InstaNeTV's software security infrastructure can discover and shut down any attempts of brute force attacks that may be used to carry out credential stuffing, our policy of defense in depth dictates securing our systems at all possible layers. These types of security threats are known as Broken Authentication which is number 2 on OWASP top ten's most recent security threats list. This can give an idea about the importance of mitigation of vulnerabilities that may lead to these types of threats or possible exploits. A successful attack of this type may result in exposure or loss of employee data or records, and jeopardize the security of our company's databases or services. Classified data that is exposed in this manner can be used by attackers to conduct further attacks which may have significant consequences to our services and/or the reputation of the company.

To address this vulnerability, each email address that may be used to create employee accounts has to be checked against a database of known data spills. There are some third- party companies that maintain a database of known data spills. InstaNeTV has purchased a license to use such a service from a well-known provider and the service is available and functioning properly.

Mitigation of the security vulnerability

SST identified the vulnerability arising from a java code imbedded inside a JSP file which is used to generate the HTML page that lets the new employees to create official accounts for them. Below is a screen shot of the insecure code:

```
88  public static void main (String [] args) {
89      □
90      Scanner input = new Scanner(System.in);
91      System.out.println("Please enter an email address to create your official employee account: ");
92
93      String account = input.next();
94
95      input.close();
96
97      createAccount employeeAccount = new createAccount(account);  // create employee account
98
99      System.out.println("Your official company account was successfully created!");
```

As it can be seen in the picture above, an employee account is created without any type of verification of email accounts. Line 97 in the code, takes whatever email address the user has inputted (as string) and uses it to create an employee account based on *createAccount* class. The email address is not checked against any database of known data breaches. Following is a screen shot of output the user gets when they enter an email address when prompted by the insecure code:

```
Please enter an email address to create your official employee account:
jack.ryan@gmail.com
Your official company account was successfully created!
```

To fix this vulnerability, SST decided to introduce a code that would call the *REST api* (provided by the IT security firm) to check the email address entered by the user, against the database of known breached accounts. We wrote the following java code which is embedded inside the IT security firm's code and allows us to pass the email addresses to their database for a possible match, while implementing the rules set by the policy No. OP35-92 discussed earlier. Below is a screen shot of the revised code mitigating the security risk:

```
88  public static void main (String [] args) {
89
90      // create a client for checking the email addresses to be passed to the third party IT security firm
91      HaveIBeenPwnedApiClient client = new HaveIBeenPwnedApiClient("abcd1234efgh5678ijklm1234567tuvwxyz");
92
93      Scanner input = new Scanner(System.in);
94      System.out.println("Your are about to create your official company account: \n " +
95      "\nPer company policy OP35-92, email addresses that are used to set up official company accounts,  " +
96      "\nshould not have been compromised in more than 3 data beaches. " +
97      "\nPlease enter an email address based on which you wish to create your company account:");
98
99      String account = input.next();
100     // create a list of breaches involving the entered email address
101     List<Breach> breachesByAccount = client.getBreachesForAccount(account);
102     int timesPwned = breachesByAccount.size();  // get the number of times the entered email address was compromised
103
104     int count = 1;
105     // do not allow the use of email addresses that appear in more than 3 breaches (per policy No. OP35-92 )
106     while (timesPwned > 3 ) {
107         System.out.println("\nThe email address that you have entered have been compromised in " + timesPwned +
108         " data breaches. Please enter a different email address: ");
109         account = input.next();
110         breachesByAccount = client.getBreachesForAccount(account);
111         timesPwned = breachesByAccount.size();
112         count ++;
113
114         // make the user wait for 30 minutes if they enter more than 3 insecure email addresses
115         if (count > 2 && timesPwned > 3) {
116             System.out.println("The email address that you have entered have been compromised in " + timesPwned +
117             " data breaches. \nYou have now entered three insecure email addresses." +
118             "\nPlease wait 30 minutes before trying again");
119             System.exit(0);
120         }
121     }
122     createAcccunt employeeAccount = new createAccount(account);  // create employee account
123     System.out.println("Congratulations! Your official company account was successfully created." +
124     "\nYour email address has been compromised " + timesPwned + " times which is within allowable limit.");
125     input.close();
```

As it can be seen in the illustration above, a line has been added in the code (line 101) that creates a list for getting breaches, if any, in which the entered email address has been compromised.
List<Breach> breachesByAccount = client.getBreachesForAccount(account);
Here *account* parameter indicates the email address that has been passed into the method for the *client* object. The variable *timesPwed* (line 102) which is an integer variable, gives the number of breaches in which the given email address has been involved.

Since per company policy No. OP35-92 no email accounts that have been compromised in more than 3 breaches can be used to create employee accounts, the code should be able to disqualify such email addresses from employee account creation process. This has been achieved by introduction of a *while*

loop (line 106). The condition for the *while loop* ensures that if an email account has appeared in more than 3 breaches, it cannot be used to create an employee account. Meanwhile, in case such an email address is entered, a prompt is given to the user to enter another email address. When the user enters another email address, it is passed to the *client.getBreachesForAccount(account)* as a parameter. The newly entered email address is then passed to *REST api* and checked against the database of known breaches and the process repeats. If the email address fails to be certified for creation of account a second time, the user will be given a final chance enter another email address. If in the third attempt, the email address fails to be certified, the session would be terminated. This is achieved by using *if (count > 2 && timesPwned > 3)* an if statement that terminates the session if at the third try, the user enters an insecure email address (line 115). The second parameter here *timesPwned > 3* ensures that if in the third try the user enters an email address that is certified, the condition of the *if statement* would become false, thus preventing the *if statement* from shutting down the session. The program would jump out of the *if statement* and continue to the next line which would create the employee account using the *createAccount* class (line 122).

It was decided that in case an email address was entered that matched those in the database of breached accounts, the information about the number of breaches should be displayed to the employee. This would help them decided whether they wished to use such email address for setting up any future accounts. It was decided that this would also keep the employees more informed about the threats of security breaches. That information would help them develop a better security mindset. Below is a screen shot of how the program behaves when 3 insecure email addresses are entered for the purpose of employee account creation:

```
Your are about to create your official company account:

Per company policy OP35-92, email addresses that are used to set up official company accounts,
should not have been compromised in more than 3 data breaches.
Please enter an email address based on which you wish to create your company account:
jack.ryan@gmail.com

The email address that you have entered have been compromised in 16 data breaches. Please enter a different email address:
john.payne@gmail.com

The email address that you have entered have been compromised in 7 data breaches. Please enter a different email address:
smith.jones@gmail.com

The email address that you have entered have been compromised in 10 data breaches.
You have now entered three insecure email addresses.
Please wait 30 minutes before trying again
```

As it can be seen, after 3 unsuccessful attempts, the user is locked out for 30 minutes. The following screen shot shows the behavior of the program if two uncertified email addresses are entered, followed by a certified email address:

```
Your are about to create your official company account:

Per company policy OP35-92, email addresses that are used to set up official company accounts,
should not have been compromised in more than 3 data breaches.
Please enter an email address based on which you wish to create your company account:
jack.ryan@gmail.com

The email address that you have entered have been compromised in 16 data breaches. Please enter a different email address:
smith.jones@gmail.com

The email address that you have entered have been compromised in 10 data breaches. Please enter a different email address:
andrew.hillthorne12@gmail.com
Congratulations! Your official company account was successfully created.
Your email address has been compromised 0 times which is within allowable limit.
```

As it can be seen, the program creates the account if the third email address succeeds to certify. Finally, the following screen shot displays the behavior of the program if an email address is certified before the third attempt. As it can be seen, entering an email address that succeeds to certify, results in creation of the employee account based on that email address.

```
Your are about to create your official company account:

Per company policy OP35-92, email addresses that are used to set up official company accounts,
should not have been compromised in more than 3 data breaches.
Please enter an email address based on which you wish to create your company account:
lisa.mason@gmail.com

The email address that you have entered have been compromised in 15 data breaches. Please enter a different email address:
liza.aryan12@gmail.com
Congratulations! Your official company account was successfully created.
Your email address has been compromised 3 times which is within allowable limit.
```

With active contribution of SST, the security fix has been applied to the vulnerable code by the DEV team and tested in the Test environment. The result was determined to be satisfactory. Therefore, this feature was deployed in PROD environment on the relevant webpage of InstaNeTV's website on October 25 and is functioning as expected.

Conclusion

Broken Authentication is number two on the most recent list of OWASP to 10 security threats. This means that every year millions of accounts are compromised by hackers using this method. A robust and well-developed system for verification of user credentials can greatly reduce the risk of exploits by this method. Some approaches to mitigate this threat include: use of multiple tokens to verify the credentials, refraining the use of accounts credentials that have appeared in several data breaches in other accounts, time out or shut down of active sessions after a set number of unsuccessful login attempts, and a few other approaches. Per policy No. OP35-92 which regulates the use of personal email addresses for the creation of employee accounts, InstaNeTV only allows the use of email accounts that have not been compromised in more than 3 breaches in the past. Furthermore, a session time-out feature has also been added to prevent or greatly reduce the effectiveness of brute force attacks that may be carried for credential stuffing. It is hoped that these measures, along with our policy of defense in depth, would make the websites and services of InstaNeTV increasingly secure. It should be noted that development of a security mindset for our employees is as important as any other efforts at software security. Therefore, every effort should be made to strengthen this mindset. It is only then that we can be confident about the security of our assets and quality of our services.