Phishing Automation-ICANHACK

ICANHACK- Android Application

Asst. Prof. Feon Jaison
Mohit Bagaria
Master of Computer Application
In
Information Security Management Systems
Jain (Deemed-to-be University) Bangalore, India

ABSTRACT: Phishing is the top-rated attack which attackers use to steal sensitive information of target users like: Credentials, Credit Card Number, SSN, etc. Phishing Automation will help attackers to hack the confidential data. it provides all websites phishing pages which attacker can use to get the target users personal information. This application can be used to steal target user's sensitive information. It saves the creating process of phishing pages and setting up the designs and algorithms.

I. INTRODUCTION

Phishing attack is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, message or link. The recipient is then tricked into clicking a malicious link. Which can lead to the installation of malware, fake websites, freezing of the system and revealing of sensitive information. This application provides a fake page of top-rated sites including different sites like-social, banking, many more. Attacker just have to copy the link of fake page and send it to the target user and when user enters his/her credentials or sensitive information and the information will be sent to the attacker.

ICANHACK gives the predefined phishing pages of different websites. Attacker just have to send that particular page link to the target user by using any kind of social media, along with this attacker can mask that link into legitimate link. Now, when user enters their credentials., it goes to the attacker account as a notification.

II. ICANHACK MODULES

1: Account Sign Up: End users have to create an account with this application to access the services/features of this ICANHACK. For creating an account user have to enter his Email Id or User Name and Password, which will be stored in Firebase database for validation check.

2: Account Sign In: End user can login into this application by using their credentials, which they have used at the time of account creation.

3: Website Category: Now, End user has to select the website category like: Social, Banking, Shopping, etc. one of them. The Category has been created based on the website nature.

Example: Facebook makes the connection between different users at global level. So, it comes under the social category. Same as well other website also been categorized. These are the different categories available in ICANHACK: - Social, Banking, Entertainment, Shopping, Other. All the category has minimum 4-5 top websites phishing page.

4: Phishing Link: Now End user has to select a particular website which he/she will be using as target website. After, click on the Copy Link button. It will copy the Phishing page link into your clipboard. The page will be stored on Firebase database with the minimal changes which requires to harvest the credentials.

5: Link Sharing: End user will; share the copied link with target user. He/she can use any kind of social media to share the link based on the intelligence of end user. ICANHACK gives some of the samples in Option called "How to mask the Link". This will help end user to hide the link behind text. So, it gives the genuine look to the target users.

5.1 Credentials Harvesting: Now the target user will trigger the phishing link and believe that it is genuine page or official mail from the authorized party. Further, target user will enter personal/sensitive information on the phishing page and on button click event. The information will be sent to the End user on ICANHACK application.

III. DATABASE

1: End User Credentials: Firebase database stores all the application user's information to verify the authorized user only can access the application.

2: Phishing Pages: Firebase Storage keep all the malicious pages. These all pages modified by the developer So, the End user can harvest the target user's sensitive information.

3: Link Connectivity: The malicious pages link will be connected to the application on particular websites options.

IV. FLOW DIAGRAM

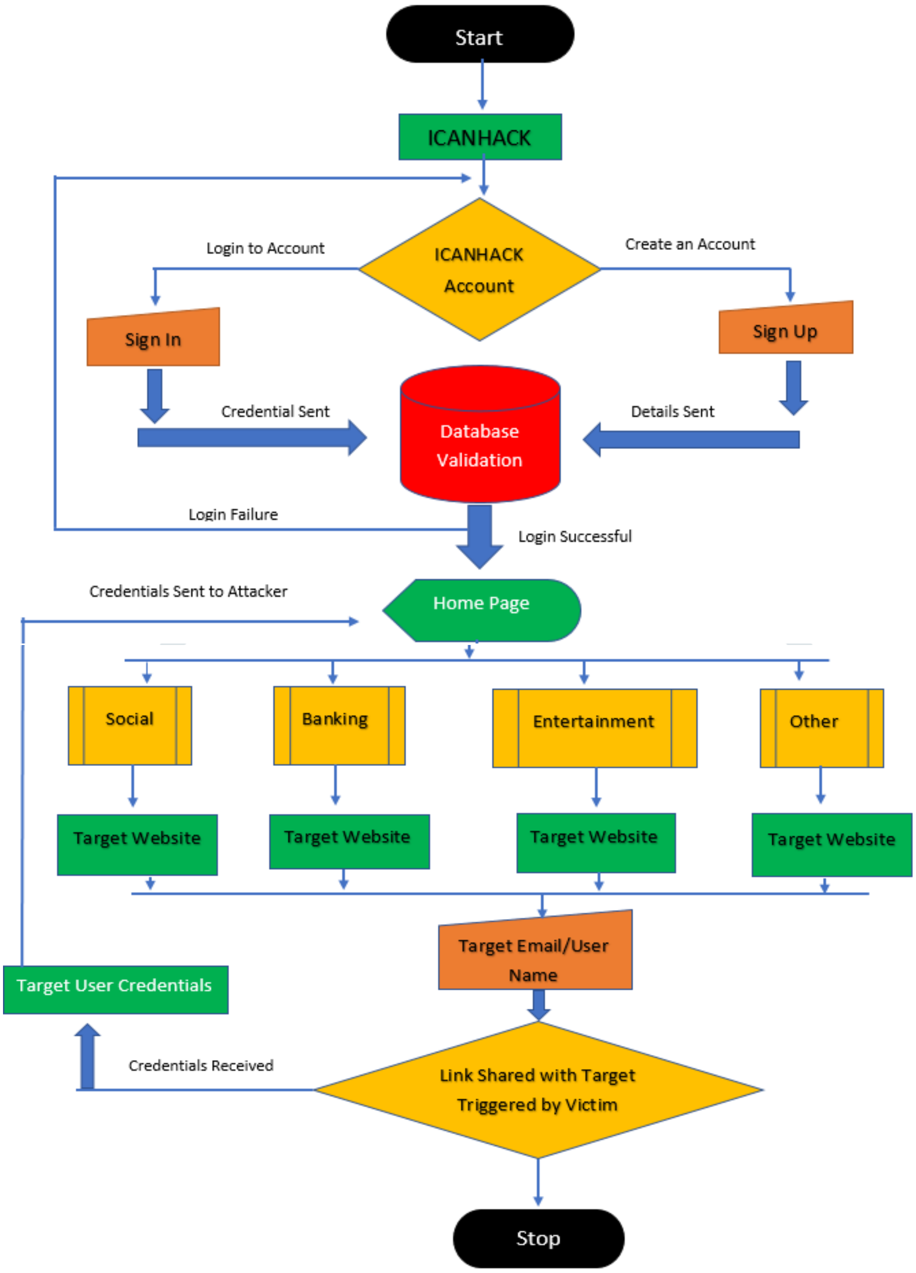


Figure 4.1

Figure 4.1 shows the working flow of ICANHACK application from account creation to credentials receiving. It gives better clarity to understand all the different modules of this application. Like: Account Signup, Login, Website Category and many more.

In above figure we can see the first user have to create an account with ICANHACK by entering his/her personal information Like: Email and password. After that user can Login to the application by entering the same credentials. If it goes successful then Home page will appear on the screen or else it shows error message based on the error Like: Wrong Credentials, etc. Now After successful login end user have to select one of the website categories among Social, Banking, Shopping, Entertainment, Others. This selection will depend on the end user that which website credentials he/she wants from the particular target person. Now end user will choose the particular website like: Facebook, Gmail, Netflix, etc. and click on Copy the Link Button to get the phishing page link.

Further steps can be different from person to person. Now, end user will share the copied phishing page link with target user by using different kind of social sites or connection mechanism. Now, target user will enter his/her credentials or sensitive information, after button click event the information will be sent to the End user account on ICANHACK application.

In this Phishing automation "ICANHACK" we have certain dependencies, these can stop our motive of the application. Let's discuss about different dependencies in next module.

V. DEPENDENCIES

1: Multi-Factor Authentication: Now a days all the websites/E-Commerce are giving M-Factor Authentication service by default. So, if people were enabled this service on their account. This application won't be helpful to bypass this security mechanism.

2: Password Keep Changes: Educational campaigns and awareness program helps users to know about this kind of attacks. End users are more sensitive now a days and they keep monitoring their accounts activity, logs and keep changes their passwords.

3: Detect Phishing Links: There are multiple ways to detect a link before opening or clicking or that. Like: Https, and drag the mouse on link, open link in JPG format before proceeding in real time, etc.

4: Educational Campaigns: Government and security agencies are more active to prevent the users and nation security from Cyber Warfare and Cyber-attacks. They organize different campaigns in schools/universities to share the trending attack methods and preventive mechanism.

VI. EXPERIMENTAL EVALUATION

1: Authentication: Authentication is the most important pillar of information security. ICANHACK using Google Firebase database to store the user's account login id and password. It has a feature to check the validity of user and make sure only the authorize person can login to the particular account.

2: Encryption: Google Firebase Database using SHA 512 Encryption key to make sure the user's credentials cannot be visible without proper authentication and authorization. So, it's very difficult to break the SHA code into plain text. The database keeps deleting the target user id and password in each 15 days, that adds more security.

3: Links Integrity: Before sending the phishing link we should verify the link and redirections. So, when the target user clicks on that, it looks like genuine page and he/she enter their credentials on phishing page. We can use different methods to check like: URL to PNG conversation, URL Query. These website gives the screenshot of the website and redirections details.

VII. RESULTS

Let's check the ICANHACK GUI and working mechanism. Below you can find few screenshots, which gives more clarity that how this application can be designed. The screenshot shows how different websites can be added into single point and what are the change you need to do on phishing page to harvest the sensitive information.

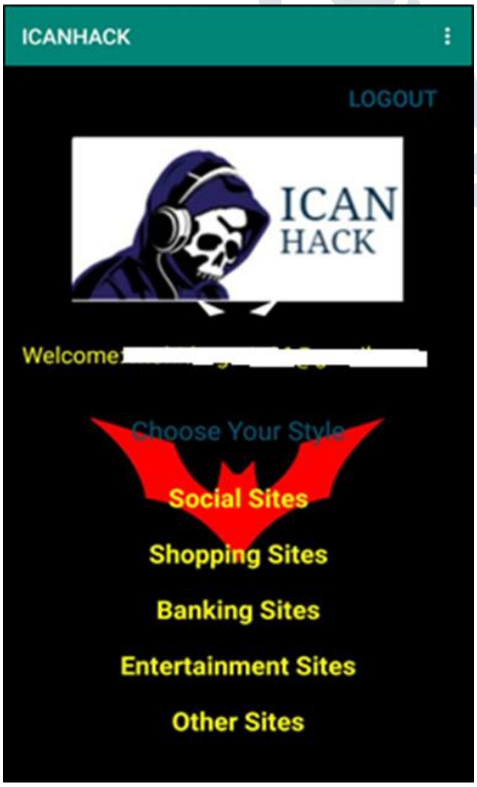


Figure 7.1

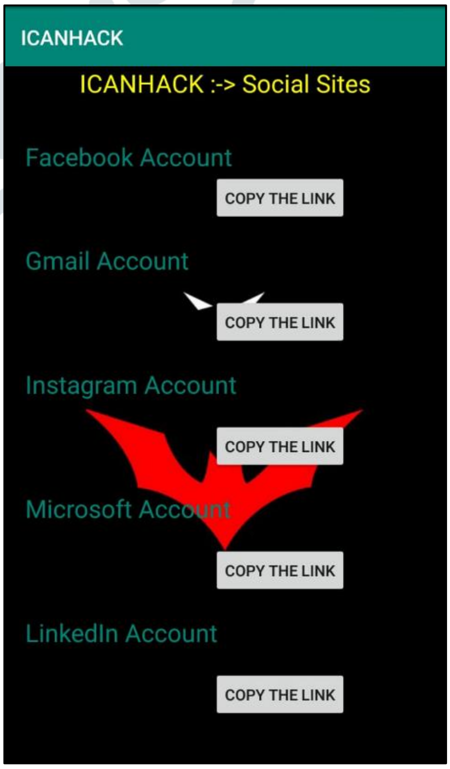
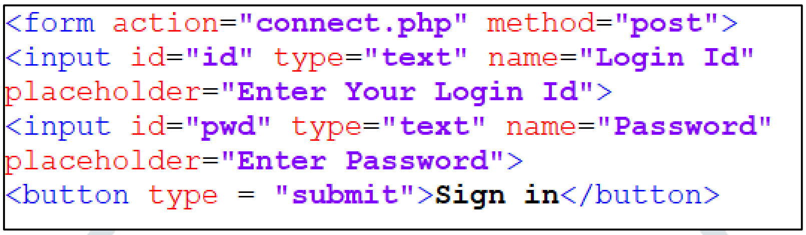


Figure 7.2

Figure 7.1 shows different websites categories, which public mostly uses and most sensitive information will be stored in this kind of websites only. Now, the End user has to select one category on which he is going to choose the website. This whole process depends on end users mind and what kind of information and which accounts credentials he/she wants from the targeted user. Let's choose Social sites, after clicking on Social Sites button. Now End user has to select which websites he/she is going to user for further attack.

Figure 7.2 contains the Top-Rated social sites name and their phishing pages links. As in previous Figure 7.1 we have chosen Social Sites option to understand the procedure in better way. Let's move further- Here end user has to select any websites depends on the information requirement. Let's take Facebook Account and after that just click on Copy the Link button. Now the phishing page link will be copied in your clipboard. Now end user just have to send this link to the target user and wait for his/her response/information. Now after entering the credentials by targeted user on Facebook phishing page. The end user will receive an notification that stated the information which target user has entered to login his/her account.



```
<form action="connect.php" method="post">
<input id="id" type="text" name="Login Id"
placeholder="Enter Your Login Id">
<input id="pwd" type="text" name="Password"
placeholder="Enter Password">
<button type = "submit">Sign in</button>
```

Figure 7.3 Phishing Code Sample

Figure 7.3 shows the main code which needs to be change in a way that it transforms the Official page and Phishing page. In the figure you can see the URL and HTTP method that end user has to keep same to receive the target user information on your database/application

VIII. CONCLUSION

Phishing is a highly profitable activity for cybercriminals. It's a major threat to E-Commerce an E-Banking applications. Phishing and its specific forms such as spear phishing reveal that internet users may be vulnerable. If they are not properly trained and do not know the immense dangers. The scammers are making huge losses by stealing financial data from the users. No single technology will completely stop phishing. Good organizations and practices, awareness training and improvements in security technology has the potential to drastically reduce the prevalence of phishing.

BIOGRAPHY

Asst. Prof. Feon Jaison
Faculty & Guide Department of Computer Science & IT-MCA
Jain (Deemed-to-be University) Bangalore, India

Mohit Bagaria
Master of Computer Application in Information Security Management Systems
Jain (Deemed-to-be University) Bangalore, India