Checking the Security of a Website Using Phishing Website Detector

GRADUATE PROJECT TECHNICAL REPORT

Submitted to the Faculty of

The Department of Computing Sciences
Texas A&M University-Corpus Christi
Corpus Christi, TX

In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

By

Rakesh Sambhuni
Summer 2011

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. Longzhuang Li
Committee Member

Dr. John Fernandez
Committee Member
ABSTRACT

Phishing is a term that indicates the kind of identity or theft where deception is used to trick a user into disclosing or attaining confidential data with financial value. Phishing is an innovative format of attack, but it is identical to other attacks in action and outcome in serious privacy and security offenses. Phishing is an illegitimate act to find users’ personal information such as bank details, social security numbers and credit card account details, by showcasing itself as a truthful object, in the public network. When users provide confidential information, they are not aware of the fact that the websites they are using are phishing websites. So, by using skillful techniques, intruders can deceive users and gain profits. In order to eradicate these problems, a phishing website detector can be used. The aim of this project is to contribute towards the research on offering a secure phishing detection service to Internet users. This phishing website detector system will identify duplicate websites with the help of DNS and IP match, detection of cookies for secured website, DNS masking and Logo recognition and verification of digital certificates. This prototype system will provide immediate, automatic and inclusive system-level solutions to perform webpage authentication and webpage detection, adverse to phishing.
# TABLE OF CONTENTS

Abstract.................................................................................................................. ii

Table of Contents.................................................................................................. iii

List of Figures......................................................................................................... vi

List of Tables.......................................................................................................... ix

1. Background and Rationale....................................................................................... 1
   1.1 URL Manipulation ......................................................................................... 1
   1.2 Website Forgery .............................................................................................. 3
   1.3 Phone Phishing ............................................................................................... 3
   1.4 Man-in-the-middle Phishing .......................................................................... 3
   1.5 In-Session Phishing ......................................................................................... 4
   1.6 Key loggers ..................................................................................................... 4
   1.7 E-mail Spoofing ............................................................................................... 5

2. Literature Review.................................................................................................... 7
   2.1 Current Research ............................................................................................ 7
   2.2 Anti-Phishing Techniques.................................................................................. 7
      2.2.1 Checking for Encryption ......................................................................... 7
      2.2.2 One-time Passwords ................................................................................ 8
      2.2.3 Separate Login and Transaction Password ............................................. 8
      2.2.4 Stop Downloads ....................................................................................... 8
      2.2.5 Beware of Forgeries ................................................................................ 8
      2.2.6 Mail-Server Authentication ..................................................................... 9
      2.2.7 Digitally Signed E-mail with Desktop Verification ................................. 9
5.1 Source Code Testing ........................................................................................................23
5.2 Module Level Testing ....................................................................................................23
5.3 Integration Testing ........................................................................................................23
5.4 Tools Used ..................................................................................................................23
  5.4.1 SQLite .....................................................................................................................23
  5.4.2 Visual Studio 2010 .................................................................................................24
5.5 Test Cases ....................................................................................................................24
  5.5.1 Original Websites Detected ...................................................................................24
  5.5.2 Phishing Websites Detected ..................................................................................65
  5.5.3 Undetected Original Websites ..............................................................................73
5.6 Evaluation of Results .................................................................................................78
5.7 Performance Evaluation ............................................................................................83
6. Conclusion and Future Work .........................................................................................84
7. Bibliography ..................................................................................................................85
List of Figures

Figure 1: Flow Chart of E-mail Phishing ................................................................. 5
Figure 2: System Diagram .................................................................................. 14
Figure 3: WindowRegistered .............................................................................. 15
Figure 4: WindowRevoked ................................................................................. 16
Figure 5: Phishing Website Detector Interface .............................................. 18
Figure 6: Logo Manager Interface .................................................................. 19
Figure 7: Controlling the Logo of a Domain in the Database ............................ 20
Figure 8: Updating Domain Information ............................................................. 21
Figure 9: Test Case for Wells Fargo Website .................................................. 25
Figure 10: Test Case for Apple Website .............................................................. 26
Figure 11: Test Case for CapitalOne Website ................................................... 27
Figure 12: Test Case for Citgo Website .............................................................. 28
Figure 13: Test Case for Macys Website ............................................................ 29
Figure 14: Test case for Northern Trust website ............................................. 30
Figure 15: Test Case for Pay Pal website .......................................................... 31
Figure 16: Test Case for Pinlessworld Website ................................................. 32
Figure 17: Test Case for Prescription Solutions Website ................................. 33
Figure 18: Test Case for Sprint Website ............................................................. 34
Figure 19: Test Case for Stana card Website .................................................... 35
Figure 20: Test Case for Subway Website .......................................................... 36
Figure 21: Test case for Twitter Website ......................................................... 37
Figure 22: Test Case for Acer Website ............................................................... 38
Figure 23: Test Case for Amway Website .......................................................... 39
Figure 24: Test Case for Careers Abroad Website .......................................... 40
Figure 25: Test case for CCRTA Website .......................................................... 41
Figure 26: Test Case for Designer Advantage Website ..................................... 42
Figure 27: Test Case for Dominos Website ................................................................. 43
Figure 28: Test Case for EBay Website .................................................................... 44
Figure 29: Test Case for Euro Shipping Website ....................................................... 45
Figure 30: Test Case for Fast Web Development Website .......................................... 46
Figure 31: Test Case for Honda Website ..................................................................... 47
Figure 32: Test Case for Indeed Website ..................................................................... 48
Figure 33: Test Case for Peter Island Website ........................................................... 49
Figure 34: Test Case for Stanford Website ................................................................. 50
Figure 35: Test Case for Synergy Website ................................................................. 51
Figure 36: Test Case for TAMU Website ..................................................................... 52
Figure 37: Test Case for TAMUCC Website ............................................................... 53
Figure 38: Test Case for TAMUK Website ................................................................. 54
Figure 39: Test Case for Telugu Cinema Website ...................................................... 55
Figure 40: Test Case for the Hindu Website ............................................................... 56
Figure 41: Test Case for United Health Group Website .............................................. 57
Figure 42: Test Case for Valero Website ..................................................................... 58
Figure 43: Test Case for Versace Website ................................................................... 59
Figure 44: Test Case for Chase Website ..................................................................... 60
Figure 45: Test Case for Dell Website ........................................................................ 61
Figure 46: Test Case for Facebook Website ............................................................... 62
Figure 47: Test Case for Gmail Website ..................................................................... 63
Figure 48: Test Case for Career Builder Website ....................................................... 64
Figure 49: Test Case for Western Union Website ....................................................... 65
Figure 50: Test Case for Bancaja Savings Website ..................................................... 66
Figure 51: Test Case for Careers Abroad Fake Website ............................................. 67
Figure 52: Test Case for Design Advantage Fake Website ........................................... 68
Figure 53: Test Case for EnCana Fake Website ......................................................... 69
Figure 54: Test Case for Euro Shipping Fake Website........................................70
Figure 55: Test Case for Fast Web Development Fake Website.......................71
Figure 56: Test Case for Northern Trust Phishing Website.............................72
Figure 57: Test Case for Pay Pal Phishing Website.........................................73
Figure 58: Test Case for Yahoo Mail Website................................................74
Figure 59: Test Case for Yahoo Website........................................................75
Figure 60: Test Case for Orkut Website..........................................................76
Figure 61: Test Case for hi5 Website...............................................................77
Figure 62: Test Case for EnCana Website.......................................................78
List of Tables

Table 1: Test Cases and their Results using Phishing Website Detector.............79

Table 2: Results of Phishing websites Using Phishing Website Detector...........81

Table 3: Results of Undetected Original Websites...........................................82

Table 4: Performance of Phishing Website Detector...........................................83
1. BACKGROUND AND RATIONALE

Phishing is a type of practice done on the Internet where personal details are obtained by unlawful methods. It is an online kind of pretexting (rewriting or changing the original information) where fraud can take place by an attacker who appears to be someone else to get the most sensitive details from users. It is also called "Brand Spoofing". The people who do phishing are called phishing artists. Phishing is done through e-mail or instant messaging, which asks the users to give their significant information on a fake website. Although these websites looks like they are legally registered and display themselves as the original entity, they are not safe [3].

The chief objective of hackers is to follow and observe transactions, then block or change the online payment services. Sometimes in the banking sector, the user is enrolled in a certain plan, but if the details are leaked, the plan might get corrupt and changed into a different plan. Such types of attacks are quite common in phishing and it happens through e-mail services. These phishing artists send millions of e-mails randomly across lists from trustworthy sources like banks or credit card companies, targeting the people who lack knowledge of computer fraud. These days, phishing is mainly concentrated on the download websites where the user cannot upload a file without an account. So, details like social security numbers, addresses, e-mails and contact numbers have to be provided to get access to these types of accounts. In such cases, the intruder can hack the username and password and get the confidential details [4].

1.1 URL Manipulation

The aim of phishing artists is to attack using fraudulent e-mails. In order to get sensitive information, one of the key methods of implementing phishing is through URL manipulation or link manipulation. With the help of e-mails, phishing artists send
millions of e-mails appearing as original organizations, but the URL which is mentioned in e-mail is false. To deceive users, hackers use a spoofed URL; on clicking it, users are taken to a fake website. Phishers try to trick users by misspelling the URL or by adding a special character to the existing URL [9]. For example, phishers may provide http:www.gotomycard.com instead of a secure https:www.gotomycard.com. As the former URL is false and unsecured, the URL leads to a different web server which is the server of hackers. Alternatively, phishers use anchor text in order to falsify the URL as a legal one. Once the users click on the URL, the information is stored in a hacker’s server. To deal with such URL problems, almost all the web browsers have started to take security steps. A few websites do not work in browsers like Internet explorer [5]. Whereas, browsers like Mozilla Firefox and Opera, pop up a warning message and ask the user to proceed or cancel the page [9].

URL manipulation also has a new dimension in the form of “IDN spoofing”. IDN spoofing stands for internationalized domain name homograph spoofing attack. In this spoofing, the phisher also exploits the concept of using similar characters in the URL. Sometimes users get e-mails from seemingly trusted sources to update or validate their accounts [7]. All these URL’s are possibly phishing URL’s. The user gets the fraudulent e-mails very frequently asking them to click the URL and update the account status. If the user does not reply, then the phishers starts threatening the users by sending e-mails, stating their accounts could be terminated. Such type of e-mails may panic the victims and provoke them to enter the confidential information [9].
1.2 Website Forgery

Website forgery is the most widely used method in phishing. In general, an intruder is capable of exploiting existing errors in the most trusted webpages. An intruder makes a similar website and utilizes the vulnerabilities of the original website for the purpose of phishing. Phishing can also take place by modifying the logo of the website. Logos in the phishing websites are designed to look identical to the original ones. This website forgery can also be done in the address bar; where instead of placing the exact URL, the address of the website can be misspelt. The website is modified in such a way that it is difficult to find whether the website is the original or not. Spams and phishing are almost similar. Spams like “Your bid has won” and “congratulations! You won” are also phishing messages generated by using the website forgery method [1].

1.3 Phone Phishing

Phishing can also take place through phone. Personal information like phone numbers can be extracted through phishing. The phisher could pretend to be a banker of a reputed bank and may ask the account details for the confirmation of the account and sometimes the user will be asked to enter the account details using the keypad of the phone. Alternatively, the phishing artists will attack with text messages. Phishers will text the users until the users reply to their messages. These kinds of attacks make the security systems so vulnerable and easy to deceive [10]. The detection and avoidance of phone phishing is a tedious task. Phone phishing is the most common phishing technique these days, as it is hard to detect.

1.4 Man-in-the-middle Phishing

These types of phishing attacks are the toughest to detect because the attackers place themselves in between the victim and the legal website. For
example, if a user is planning to buy a product online, he/she has to enter their details. These details are retrieved in the middle of the transaction and stored in the phisher’s database and that particular transaction will not be effected [11]. Hackers have the details then and they can use them whenever they need. Generally this man-in-the-middle attack takes place when a normal conversation is held through Internet. If the user talks or chats with the customer care service and exchanges his/her information, the chances of phishing are high.

1.5 In-Session Phishing

This type of phishing is based on the activities of users in a web browsing session. The activities of the victims are continuously monitored until they log into a phished account. Such types of accounts are called target accounts. If the user enters into the target account and submits all the details, the hacker gets the details and will stop monitoring that particular user and start implementing it on others [1]. Since the hackers have the credentials; they can start exploiting the user’s details. If the user has logged on to an online banking account and the user does not use it for a while after logging in, then a pop up message appears which says “this session has expired”. In the meantime, phishing can take place. Users must be aware of the online phishing problem which implies high chances of risk [1]. Users should not allow the web browser to remember the username and password details of any kind of account, since web hackers are capable to pull the information from that sort of condition too.

1.6 Key Loggers

Key loggers are the most unexpected way of phishing. A user might get an electronic mail which asks the user to click on the URL. When the user clicks the provided URL, there might be a chance that the software called keyboard logger or
key logger will be installed. With this software, whatever the users type on their computer can be traced out by the phishers [2]. In this case, confidential data typed in the computer can be accessed easily. With the help of key loggers, hackers can peep into the users’ web browsers and get the required information to change or corrupt computer files [8].

### 1.7 E-mail Spoofing

E-mail spoofing is an activity in which the header of the e-mail and the address of the sender are changed to look as if the e-mail is created by a trusted source. It is frequently used in multiple forms for malicious and fraudulent purposes. For example, the user get e-mails from a system administrator asking the user to alter his respective password and warns him if he is not willing to change [8].

**Flow Chart for E-mail Phishing**
Figure 1 represents the flow chart for e-mail phishing. The e-mail received by a user could also be a possible chance of a phishing attack. There is a good chance that an e-mail is sent by phishers, if that e-mail contains any executable attachment or URLs asking for personal information [13]. The users are vulnerable to such e-mails. The users should be aware of the sender and the host from which they received the e-mail. If it is none of the above situations then it could be a safe e-mail.
2. Literature Review

2.1 Current Research

An excellent phishing website fools most of the users. Existing anti-phishing techniques are outdated, as new phishing techniques are emerging to deceive the users thoroughly [3]. Most of the phishing websites look identical to their original counterparts but in reality, they run on different servers. These phishing attacks take place because of the lack of computer knowledge on users' part. The users are responsible to check the website legitimacy. The website legitimacy can be checked by the following strategies:

2.2 Anti-Phishing Techniques

2.2.1 Checking for Encryption

The users should check the padlock symbol in their address bar (after the page loads) to determine the website’s security. Most of the users do not even know whether an address bar contains a domain name or an IP address. The users should be able to recognize the content of the website to determine the websites legitimacy [1]. If the users are familiar with the URL, most of the phishing attacks can be detected. In order to check whether the website is encrypted, the user has to look for the padlock symbol in the address bar to confirm that the particular website is encrypted. The user should check the certificate expiration date, in order to be secure.
2.2.2 One-time Passwords

In order to protect users from phishing, the concept of one-time password is introduced. One-time passwords will expire after using them once. One-time passwords are used to login to user’s accounts. With the introduction of one-time passwords, the personal information of the users can be protected. Phishers always try to get users’ passwords and get the sensitive information. By using one-time passwords, the password entered into the account is expired after using it once and new password has to be given to login again [1].

2.2.3 Separate Login and Transaction Password

Another preventive measure that can be taken is to have two different passwords for a transaction. Especially, this can be used for securing the financial transactions. If the phisher takes control of the usernames and passwords, there is still a chance to prevent the transaction from happening. The user needs to have a different transactional password. A one-time transactional password can be generated and sent to the user via SMS [3].

2.2.4 Stop Downloads

In any e-mail, if there is a link that asks the users to download anything, the users must not download such e-mails since it can directly get the financial information from the bank accounts [15].

2.2.5 Beware of Forgeries

Phishers can simply change the “from” domain name in e-mails. The easiest way for the user to detect a website or an e-mail is by checking the URL and the e-
mail layout. If an e-mail says it comes from a reputed company, it does not mean that it is always true [15].

2.2.6 Mail-Server Authentication

The phishers can take over the users’ ids and passwords by sending them annoying e-mails which would force them to click on the URL that is directed to a phishing site. These e-mails can be spam or junk e-mails which look exactly like the original e-mails from an authenticated user. To prevent these kinds of unauthorized e-mails, the user can be validated in such a way that he/she gets e-mails that are server authenticated [14]. The message or an e-mail that is received by the user via the Internet is checked at the mail server for any relation with the phishing sites. The sender and receiver both need to be authorized users. An incoming e-mail is verified for any kind of vulnerability and it is transmitted to receivers after being authenticated by the server.

2.2.7 Digitally Signed E-mail with Desktop Verification

The phishers can always misguide the user by pretending to be a repudiated and trustworthy person or website the user is looking for. Phishers send e-mails with attachments which can potentially lead the user into a misconception and being deceived. The phisher uses the reputation that the user has on a particular website. So, to prevent users from losing the trust in those website, developers are using digital signatures to ensure the user that their e-mails are not fraudulent [1] [3]. But the verification of these digital signatures turned out to be a problem as it is an expensive process and not all the users have an ability to handle them. As the user receives an e-mail with a digital signature that is verified by the feature incorporated on his/her business desktop machine. So, each time the e-mail is opened on the
desktop with this feature, the signature is verified else the access to the attachment is denied.

2.2.8 Digitally Signed E-mail with Gateway Verification

As it is not possible for all the users to have a business machine, an alternative option has to be provided to the users. The e-mail from the sender to the receiver needs to pass through a gateway that was included in the mail server. Any e-mail sent via the Internet is verified at the server. It needs to be authenticated by the server. So, the e-mails with any sort of a digital signature are verified at the time of authentication. The e-mail needs to pass through digital signature verification gateway at the server [3]. The e-mails which can get through this procedure are only transmitted to the receiver or the end user. This ensures security for all the users and builds trust between the sender and receiver.
3. NARRATIVE

3.1 Scope

Phishing frequently impacts users’ privacy and safety. Internet Service Providers (ISPs) are facing a huge problem in the Internet community from phishers and hackers [2]. The scope of this project revolves around the identification, reduction and elimination of phishing activities and protection of users from phishing artists. In order to protect and maintain websites or to secure the information of users, the field of information security recommends four different stages in a phishing website detection system. They are described in the sections below:

3.1.1 Detection

The proposed phishing website detection system will detect threats and indicate that e-mails, websites or the URL’s are not secured and help the user avoid the hacker’s trap. Such a type of detection builds confidence in both the users and the Internet community. The phishing website detection system will guide users by providing knowledge of Internet threats. In phishing detection, there are two types of techniques: the white list technique and the heuristic based mechanism. These two techniques act as filters in detecting phishing websites. In white list technique, a few anti-phishing websites are listed. If the user accessed websites are not in the white list, then these will be concluded as phishing websites. The heuristic based mechanism works with various aspects like visual similarities, keywords and domain name to decide whether the website is a phishing website or not [6].
3.1.2 Protection

A phishing website detector will contribute helpful information to protect the user automatically from phishing websites. This prototype will be built in such a way that it will protect the user from security violations and intrusions.

3.1.3 Reaction

In the reaction phase, after the phishing website is detected, the phishing website detector will eliminate the phishing website from future attacks. All phishing websites detected by this prototype system will be recorded.

3.1.4 Recovery

In the recovery phase, the personal information of the user will be recovered. The data stolen from the user is hosted on a remote phishing website, which is away from the phisher. So, it is important to recover the data before the phisher reconciles the stolen data from the remote website.
4. SYSTEM DESIGN

The goal of this project is to build a system that can identify phishing attacks and defend users’ personal and confidential details from intruders. This prototype system is intended to provide instant, quick, automatic and robust results for webpage authentication and webpage detection against phishing.

The system design is explained in four parts. In the first part, a GUI was developed which acts as a client server system that interacts with a database server. The database used in this project is SQL Server 2005. The system was developed in C# and ASP.net framework. The database will store the mapping of DNS names along with the IP addresses. Authorized logos of different websites and their URL’s are also stored in the database. The database structure consists of the image of logo database, the phishing DNS database and the secure DNS database. In the second part, the actions performed by the user on his/her browser are recorded. The prevention and detection of the phishing activities are performed by authenticating the DNS name and the IP address. The activities of the browser are monitored, and vulnerable activities are recorded with the help of browser’s history. Details like the DNS name, browser name, the existence of any attachments are displayed as a message to the user. From these details, the phishing sites can be easily monitored.

In the third part, the original website logos are saved along with the URL. The logos are recognized with the help of a specifically designed control. These controls will check the logo and verify its originality. The conformity of the logo match is given by the control with a message. In the fourth part, the information of the cookies is obtained, if the website is authorized. In this part, the cookies are detected and deleted.
4.1 System Diagram

This is the system diagram of the phishing website detector application

Fig 2: System Diagram of Phishing Website detector Application

Figure 2 represents the system diagram of the phishing website detector application. This system contains a web browser (Internet Explorer) which is contacted by the three Windows Shell APIs (WindowRegistered, WindowRevoked and NavigationComplete2). The details from the browser are obtained by the phishing website detector application through the three APIs to check the websites’ security. The obtained details can also be stored into a database.
4.2 Identifying Running Instance of the Internet Explorer

To identify the running instance of the Internet Explorer, Windows Shell API (Application Programming Interface) was used. Windows Shell APIs were used for quickly integrating the Internet and the Internet related content easily into the applications. In this system three Windows Shell APIs were used. They are explained in the below sections:

4.2.1 WindowRegistered

WindowRegistered API was used to find the IE window and the domain name in the IE window that is registered in phishing website detector application.

![WindowRegistered API](image)

Fig 3: WindowRegistered API

4.2.2 WindowRevoked

Since, the domain name was already registered in the application; the WindowRevoked API was used to revoke the details of DNS, cookies, logos and certificates. These details were used to generate a report when any domain name was entered in the Internet Explorer.
4.2.3 NavigationComplete2

NavigationComplete2 API was used when any tab has to be opened. In such cases, the navigation of the previous tab gets completed and the navigation of the new tab gets started.

4.3 Phishing Website Detector

Phishing website detector is used to identify phishing websites. It is also used to prove the security of the website using DNS check, Cookie Check, Logo Matching and Digital Certification Verification.

4.3.1 DNS Check

DNS check can be done by extracting the URL from the address bar. When the domain name is entered in the Internet Explorer, the phishing website detector application requests the DNS records from the Internet service Provider (ISP) and it compares the details with the authoritative name server records of the domain. If IP
address of the Internet Service Provider is matched with the IP address of the authoritative name server, then the DNS check is successful and the IP address is valid. Otherwise, the DNS check is failed and the IP address is invalid.

4.3.2 Logo Matching

Logo Matching is checked using White-List technique. In White-List technique, few websites and their logos are already stored in the database. In the same way, the logo of the domain is pre-saved in the phishing website detector application. Logo Matching can be done by extracting the logo URL from the website. Once the URL is extracted, click on the Logo Manager button to add a logo image. Then click on the new button to add new logo URL. Enter the URL and the domain into their respective text fields and then click on the Add button to add the logo image to the database. This image is given as the input to the MD5 (Message Digest 5) and SHA512 (Secure Hash Algorithm) and these algorithms generate a 32 digit hash value as the output which is unique for every image. Since, these algorithms are one way hash functions, if the hash value is generated once, it cannot be changed. After adding the logo of the domain, the domain name is displayed in the domain list box. The image of the domain can be updated using the Update button. If the logo hash value is matched with the authorized logo of the website, then the logo of the domain is successful.

4.3.3 Cookie Check

According to the HTTP standards, only a domain name can set a cookie for itself. To find the Cookie Check, compare the domain name of the cookie with the URL. If the domain name of the cookie does not match with the domain name of the URL, then Cookie Check is failed. A cookie contains the information of the domain, the domain ID, the start date, the expiration date and the pages which the user
visited in that particular domain. Cookies can be deleted with the help of **Cookie Clean** button in the phishing website detector application.

### 4.3.4 Digital Certification Verification

Digital certificates are nothing but SSL certificates which are present in the address bar. With the help of these digital certificates, the security of the website can be proved. This application checks whether the domain is using a secured HTTP protocol (HTTPS). It also checks whether the website contains a padlock symbol with a certificate. If the domain does not contain an SSL certificate, then the certification fails for that domain. If a domain uses the secured protocol and contains a padlock symbol with a certificate, then the certificate is successful for that domain.

### 4.4 Phishing Website Detector Interface

The phishing website detector interface consists of a log termed **IE Protect**. This log contains a **Logo Manager** button and **Cookies Clean** button with a report column.

![Phishing Website Detector Interface](image.png)

*Fig 5: Phishing Website Detector Interface*
The interface shown in the Figure 5 opens when any website is accessed in Internet Explorer. The report column displays the information of cookies, DNS check, logos and certificates. The Logo Manager button is used to add and delete the domain names. The Cookies Clean button is used to delete the cookies of a specific domain.

The report is displayed using the following symbols:

- This symbol is displayed when the report is in the null state.
- This symbol is displayed if the report is successful.
- This symbol is displayed when the report has failed.
- This symbol is displayed if the certificate has successful.

4.5 Logo Manager

The Logo manager interface contains the buttons New, Add, Delete and Cancel.

Fig 6: Logo Manager Interface
The **Logo Manager** button is used to save and delete the logo of a domain in a database. Figure 6 shows the phishing website detector interface and the logo manager interface. The logo manager interface displays buttons and text fields. The URL of the logo should be entered into the URL text field. The website address should be given to the domain text field. When the **Add** button is clicked, the application automatically generates the Md5 and sha512 hash values of a logo.

### 4.6 Controlling the Logo of a Domain in the Database

Logo Manager is used to perform basic addition and deletion operations on the logos of a domain in the database.

Fig 7: Controlling the Logo of a Domain in the Database
The buttons in the above interface are used to control the logo of a domain in the database. The **New** button is used to add the logo of a new domain into the database which is displayed in list box. **Delete** button is used to delete the existing logo of a domain from the database.

### 4.7 Updating Domain Information

Several domains can be saved and added to the database. The list of the domains is visible in the list box. The **Update** button is used to update the logo of the domain.

![Fig 8: Updating Domain Information](image)

The above interface shows how to update the domain information in the database. For example, the URL (obtained by the Wells Fargo logo) and domain name of the Wells Fargo (www.wellsfargo.com) website are provided to the
application. Once the details are provided, domain is added and updated to the database.
5. TESTING AND EVALUATION

Testing and evaluation of this prototype was carried out by following standard testing strategies.

5.1 Source Code Testing

The code of this prototype was developed in modules and therefore the source code of every module was tested. For example, logo matching module was tested by checking whether the logo of the website was correctly captured and stored. Similarly, DNS and IP matching module was tested to ensure that it correctly recorded and matched the DNS name and IP address of the given website.

5.2 Module Level Testing

Since phishing website detector has many modules, every module was individually tested. For example, cookies detection module was tested by checking whether the extracted cookies belonged to the authorized websites.

5.3 Integration Testing

After testing all the modules individually, the modules were integrated and developed into a system. The developed system was then tested to check the performance of the system. Based on the test results, performance of the phishing website detector was evaluated.

5.4 Tools Used

5.4.1 SQLite

The tool used for testing this project is SQLite. SQLite is a self-contained database engine. SQLite source code is in the public domain and it almost implements the SQL standard. SQLite comes with a standalone command-line
interface (CLI) that can be used to administer SQLite Databases. SQLite reduces the latency. SQLite stores the entire database as a single cross platform file [12].

5.4.2 Visual Studio 2010

It is used for Console and graphical user interface applications. The integrated debugger of Visual Studio 2010 works as a source-level debugger and a machine-level debugger. Visual Studio 2010 is compatible for both C# and .Net Framework.

5.5 Test Cases

This phishing website detector was tested with different websites and the results were obtained in the form of cookie check, DNS check, logo match and certificates. The certificates of every website were checked. The IP address of every website was obtained and checked whether the IP address was valid or in-valid.

5.5.1 Original Websites Detected

Test Cases 1-41 are the examples of websites that are detected by phishing website detector

Test Case 1

Testing the phishing website detector functionality on the URL: https://www.wellsfargo.com
Figure 9 represents the test case for Wells Fargo Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Wells Fargo servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

Test Case 2

Testing the phishing website detector functionality on the URL: http://www.apple.com
Figure 10 represents the test case for Apple Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Apple servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

**Test Case 3**

Testing the phishing website detector functionality on the URL: https://www.capitalone.com
Figure 11 represents the test case for CapitalOne Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by CapitalOne servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

**Test Case 4**

Testing the phishing website detector functionality on the URL: http://www.citgo.com
Figure 12 represents the test case for Citgo Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Citgo servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

Test Case 5

Testing the phishing website detector functionality on the URL: http://www.macys.com
Figure 13 represents the test case for Macys Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by macys servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

**Test Case 6**

Testing the phishing website detector functionality on the URL: http://www.northerntrust.com
Figure 14 represents the test case for Northern Trust Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Northern Trust servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

Test case 7

Testing the phishing website detector functionality on the URL: https://www.paypal.com
Figure 15 represents the test case for PayPal Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by PayPal servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

Test Case 8

Testing the phishing website detector functionality on the URL: https://www.pinlessworld.com
Figure 16 represents the test case for Pinlessworld Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Pinlessworld servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

**Test Case 9**

Testing the phishing website detector functionality on the URL: https://www.prescriptionsolutions.com
Figure 17 represents the test case for Prescription Solutions Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Prescription Solutions servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

**Test Case 10**

Testing the phishing website detector functionality on the URL: http://www.sprint.com
Figure 18 represents the test case for Sprint Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Sprint servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

Test Case 11

Testing the phishing website detector functionality on the URL: http://www.stanacard.com
Figure 19 represents the test case for Stana Card Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Stana Card servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

**Test Case 12**

Testing whether the phishing website detector functionality on the URL: http://www.subway.com
Figure 20 represents the test case for Subway Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Subway servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

Test Case 13

Testing the phishing website detector functionality on the URL: http://www.twitter.com
Figure 21 represents the test case for Twitter Website. This domain is successful in all the cases. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Twitter servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate was checked and it was successful for this domain.

Test Case 14

Testing the phishing website detector functionality on the URL: www.acer.com
Figure 22 represents the test case of Acer website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Acer server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 15**

Testing the phishing website detector functionality on the URL: http://www.amway.com
Fig 23: Test Case for Amway Website

Figure 23 represents the test case of Amway website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Amway server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

Test Case 16

Testing the phishing website detector functionality on the URL: http://www.careersabroad.co.uk
Figure 24 represents the test case of Careers Abroad website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Careers Abroad server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 17**

Testing the phishing website detector functionality on the URL: http://www.ccrta.org
Figure 25 represents the test case of CCRTA website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of CCRTA server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 18**

Testing the phishing website detector functionality on the URL: http://www.designeradvantage.com
Figure 26 represents the test case of Designer Advantage website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Designer Advantage server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 19**

Testing the phishing website detector functionality on the URL: http://www.dominos.com
Figure 27 represents the test case of Dominos website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Dominos server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 20**

Testing the phishing website detector functionality on the URL: http://www.ebay.com
Figure 28 represents the test case of EBay website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of EBay server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

Test Case 21

Testing the phishing website detector functionality on the URL: http://www.euroshipping-voyages.com
Fig 29: Test Case for Euro Shipping-voyages Website

Figure 29 represents the test case of Euro Shipping-voyages website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Euro Shipping-voyages server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 22**

Testing the phishing website detector functionality on the URL: http://www.fastwebdevelopmentllc.com
Figure 30 represents the test case of Fast Web Development LLC website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Fast Web Development LLC server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 23**

Testing the phishing website detector functionality on the URL:
http://www.honda.com
Figure 31 represents the test case of Honda website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Honda server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

Test Case 24

Testing the phishing website detector functionality on the URL: http://www.indeed.com
Fig 32: Test Case for Indeed Website

Figure 32 represents the test case of Indeed website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Indeed server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

Test Case 25

Testing the phishing website detector functionality on the URL: http://www.peterisland.com
Figure 33 represents the test case of Peter Island website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Peter Island server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 26**

Testing the phishing website detector website functionality on the URL: http://www.stanford.edu
Figure 34 represents the test case of Stanford website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Stanford server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 27**

Testing the phishing website detector functionality on the URL: http://www.synergy.com
Figure 35 represents the test case of Synergy website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Synergy server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

Test Case 28

Testing the phishing website detector functionality on the URL: http://www.tamu.edu
Figure 36 represents the test case of Texas A&M University website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Texas A&M University server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

Test Case 29

Testing the phishing website detector website functionality on the URL: http://www.tamucc.edu
Figure 37 represents the test case of TAMUCC (Texas A&M University-Corpus Christi) website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of TAMUCC server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 30**

Testing the phishing website detector functionality on the URL: http://www.tamuk.edu
Figure 38 represents the test case of TAMUK (Texas A&M University-Kingsville) website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of TAMUK server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 31**

Testing the phishing website detector functionality on the URL: http://www.telugucinema.com
Figure 39 represents the test case of Telugucinema website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Telugucinema server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 32**

Testing the phishing website detector functionality on the URL: http://www.thehindu.com
Figure 40 represents the test case of The Hindu website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of The Hindu server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 33**

Testing the phishing website detector functionality on the URL: http://www.unitedhealthgroup.com
Figure 41 represents the test case of United Health Group website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of United Health Group server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 34**

Testing the phishing website detector functionality on the URL: http://www.valero.com
Figure 42 represents the test case of Valero website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Valero server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 35**

Testing the phishing website detector functionality on the URL: http://www.versace.com
Figure 43 represents the test case of Versace website. This domain has a valid IP address and the DNS was checked with the IP address of the ISP and authoritative records of Versace server. Therefore, DNS check was shown successful. Since logo of this domain was already saved, logo match was also successful. Cookie check of this domain was valid, therefore cookie check was successful. The certificate of this website was checked and it was not secured; it failed.

**Test Case 36**

Testing the phishing website detector functionality on the URL: http://www.chase.com
Fig 44: Test Case for Chase Website

Figure 44 represents the test case for Chase Website. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Chase servers. The IP address of ISP and authoritative records were checked and were unmatched. Hence, DNS check failed for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate check was successful as the domain provides a valid certificate.

Test Case 37

Testing the phishing website detector functionality on the URL: http://www.dell.com
Figure 45 represents the test case for Dell Website. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Dell servers. The IP address of ISP and authoritative records were checked and were unmatched. Hence, DNS check failed for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate check was successful as the domain provides a valid certificate.

**Test Case 38**

Testing the phishing website detector functionality on the URL: https://www.facebook.com
Figure 46 represents the test case for Facebook Website. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Facebook servers. The IP address of ISP and authoritative records were checked and were unmatched. Hence, DNS check failed. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate check was successful as the domain provides a valid certificate.

**Test Case 39**

Testing the phishing website detector functionality on the URL: https://www.gmail.com
Figure 47 represents the test case for Gmail Website. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Gmail servers. The IP address of ISP and authoritative records were checked and were unmatched. Hence, DNS check failed for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate check was successful as the domain provides a valid certificate.

Test Case 40

Testing the phishing website detector functionality on the URL: http://www.careerbuilder.com
Figure 48 represents the test case for Career Builder Website. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Chase servers. The IP address of ISP and authoritative records were checked and were unmatched. Hence, DNS check failed. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate of this website was checked and it was not secured; it failed.

Test Case 41

Testing the phishing website detector functionality on the URL: http://www.westernunion.com
Fig 49: Test Case for Western Union Website

Figure 49 represents the test case for Western Union Website. The Logo Match (LM) is successful with the pre-saved logo in database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Western Union servers. The IP address of ISP and authoritative records were checked and were unmatched. Hence, DNS check failed for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate of this website was checked and it was not secured; it failed.

5.5.2 Phishing Websites Detected

Test Cases 42- 49 are the examples of the phishing websites that are detected by Phishing Website Detector.
Test Case 42

Testing the phishing website detector functionality on the URL: http://www.bancajabsaving.org

Fig 50: Test Case for Bancaja Savings Fake Website

Fig 50 represents the test case for Bancaja Saving’s fake website. Since it is a fake website, all the reports for this domain were failed. The IP address of IPS and the authoritative records of the Bancaja Saving’s server were not matched. Hence, it failed. The Logo of the Bancaja Saving’s fake website and the Bancaja Saving’s original website did not matched; hence the logo matching was failed. The certificate of this website was checked and it was unsecured. The Cookies of this domain were also in-valid and unsecured.

Test Case 43

Testing the phishing website detector functionality on the URL: http://www.e-londonjobs.com (careers abroad fake website)
Fig 51: Test Case for Careers Abroad Fake Website (e-London jobs)

Fig 51 represents the test case for Careers Abroad fake website. This website redirects to www.e-londonjobs.com. Since it is a fake website, all the reports for this domain were failed. The IP address of IPS and the authoritative records of the Careers Abroad server were not matched. Hence, it failed. The Logo of the Careers Abroad fake website and the Careers Abroad original website did not matched; hence the logo matching was failed. The certificate of this website was checked and it was unsecured. The Cookies of this domain were also in-valid and unsecured.

**Test Case 44**

Testing the phishing website detector functionality on the URL: http://www.designadvantage-inc.com
Fig 52: Test case for Design Advantage Fake Website

Fig 52 represents the test case for Design Advantage fake website. Since it is a fake website, all the reports for this domain were failed. The IP address of IPS and the authoritative records of the Design Advantage server were not matched. Hence, it failed. The Logo of the Design Advantage fake website and the Design Advantage original website did not matched; hence the logo matching was failed. The certificate of this website was checked and it was unsecured. The Cookies of this domain were also in-valid and unsecured.

Test Case 45

Testing the phishing website detector functionality on the URL: http://www.encan.com (fake for EnCana Website)
Fig 53: Test Case for EnCana Fake Website

Fig 53 represents the test case for EnCana fake website. Since it is a fake website, all the reports for this domain were failed. The IP address of IPS and the authoritative records of the EnCana server were not matched. Hence, it failed. The Logo of the EnCana fake website and the EnCana original website did not matched; hence the logo matching was failed. The certificate of this website was checked and it was unsecured. The Cookies of this domain were also in-valid and unsecured.

Test Case 46

Testing the phishing website detector functionality on the URL: http://www.lnx.euroshippingltd.com (fake website of Euro Shipping)
Fig 54: Test Case for Euro Shipping Fake Website

Fig 54 represents the test case for Euro Shipping fake website. Since it is a fake website, all the reports for this domain were failed. The IP address of IPS and the authoritative records of the Euro Shipping server were not matched. Hence, it failed. The Logo of the Euro Shipping website and the Euro Shipping original website did not matched; hence the logo matching was failed. The certificate of this website was checked and it was unsecured. The Cookies of this domain were also in-valid and unsecured.

Test Case 47

Testing the phishing website detector functionality on the URL: http://www.fastwdmail.com (fake website of Fast Web Development)
Fig 55 represents the test case for Fast Web Development fake website. Since it is a fake website, all the reports for this domain were failed. The IP address of IPS and the authoritative records of the Fast Web Development server were not matched. Hence, it failed. The Logo of the Fast Web Development and the Fast Web Development original website did not matched; hence the logo matching was failed. The certificate of this website was checked and it was unsecured. The Cookies of this domain were also invalid and unsecured.

**Test Case 48**

Testing the phishing website detector functionality on the URL: http://www.northtrust.com (fake website of Northern Trust)
Fig 56: Test Case for Northern Trust Phishing Website

Fig 56 represents the test case for Northern Trust fake website. This website redirects to the http://www.northtrust.com. Since it is a fake website, all the reports for this domain were failed. The IP address of IPS and the authoritative records of the Northern Trust server were not matched. Hence, it failed. The Logo of the Northern Trust fake website and the Northern Trust original website were compared and found unmatched; hence the logo matching was failed. The certificate of this website was checked and it was unsecured. The Cookies of this domain were also in-valid and unsecured.

Test Case 49

Testing the phishing website detector functionality on the URL: http://www.happy999.p40.net (fake website of PayPal)
Fig 57: Test Case for PayPal Fake Website

Fig 57 represents the test case for PayPal fake website. Since it is a fake website, all the reports for this domain were failed. The IP address of IPS and the authoritative records of the PayPal server were not matched. Hence, it failed. The Logo of the PayPal fake website and the PayPal original website did not matched; hence the logo matching was failed. The certificate of this website was checked and it was unsecured. The Cookies of this domain were also in-valid and unsecured.

5.5.3 Undetected Original Websites

Test Cases 50-54 are the examples of the undetected original websites by phishing website detector

Test Case 50

Testing the Logo Matching on the URL: https://www.login.yahoo.com (Yahoo mail)
Figure 58 represents the test case for Yahoo mail Website. The Logo Match (LM) was failed, even when the logo was pre-saved in the database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Yahoo servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate of this domain was checked and it was successful.

Test Case 51

Testing the Logo Matching on the URL: http://www.yahoo.com (Undetected)
Figure 59 represents the test case for Yahoo Website. The Logo Match (LM) was failed, even when the logo was pre-saved in the database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Yahoo servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate of this domain was check and it was failed.

Test Case 52

Testing the Logo Matching on the URL: http://www.orkut.com (Undetected)
Figure 60 represents the test case for Orkut Website. The Logo Match (LM) was failed, even when the logo was pre-saved in the database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by Orkut servers. The IP address of ISP and authoritative records were unmatched. Hence, DNS check was failed. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate of this domain was check and it was successful.

**Test Case 53**

Testing the Logo matching on the URL: http://www.hi5.com (Undetected)
Figure 61 represents the test case for hi5 Website. The Logo Match (LM) was failed, even when the logo was pre-saved in the database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by hi5 servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate of this domain was check and it was failed.

**Test Case 54**

Testing the Logo Matching on the URL: http://www.encana-ca.com (Undetected)
Figure 62 represents the test case for EnCana Website. The Logo Match (LM) was failed, even when the logo was pre-saved in the database. The results for the DNS check were requested from the Internet Service Provider and compared with the authoritative records provided by EnCana servers. The IP address of ISP and authoritative records were matched. Hence, DNS check was successful for this domain. Cookie check for this domain was valid, as cookies are set in this domain and matched with the domain of the URL. The certificate of this domain was check and it was failed.

5.6 Evaluation of Results

Table 1 shows the different test cases considered and results obtained with the phishing website detector. The below table gives the output for randomly picked domains and the output is displayed in the log of phishing website detector. Every test input (Domain Name) has four different output parameters (Logo Matching, DNS Check, Cookie Check and Certificate) and all the test cases are carried out in
The performance of the phishing website detector is estimated by checking the security of these websites.

Table 1: Results of Detected Websites using Phishing Website Detector

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Cookie Check</th>
<th>DNS Check</th>
<th>Logo Matching</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.wellsfargo.com">www.wellsfargo.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.apple.com">www.apple.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.capitalone.com">www.capitalone.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.citgo.com">www.citgo.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.macys.com">www.macys.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.northerntrust.com">www.northerntrust.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.paypal.com">www.paypal.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.pinlessworld.com">www.pinlessworld.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.prescriptionsolutions.com">www.prescriptionsolutions.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.sprint.com">www.sprint.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.stanacard.com">www.stanacard.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.subway.com">www.subway.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.twitter.com">www.twitter.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
</tr>
<tr>
<td>Website</td>
<td>1st Attempt</td>
<td>2nd Attempt</td>
<td>3rd Attempt</td>
<td>Result</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
<td>-------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td><a href="http://www.acer.com">www.acer.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.amway.com">www.amway.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.careersabroad.com">www.careersabroad.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.ccrta.org">www.ccrta.org</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.designeradvantage.com">www.designeradvantage.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.dominos.com">www.dominos.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.ebay.com">www.ebay.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.euroshipping-voyages.com">www.euroshipping-voyages.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.fastwebdevelopment.com">www.fastwebdevelopment.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.honda.com">www.honda.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.indeed.com">www.indeed.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.peterisland.com">www.peterisland.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.stanford.edu">www.stanford.edu</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.synergy.com">www.synergy.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.tamu.edu">www.tamu.edu</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.tamucc.edu">www.tamucc.edu</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.tamuk.edu">www.tamuk.edu</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Cookie Check</td>
<td>DNS Check</td>
<td>Logo Matching</td>
<td>Certificate</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------</td>
<td>-----------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td><a href="http://www.bancajabsaving.org">www.bancajabsaving.org</a></td>
<td>Failed</td>
<td>Failed</td>
<td>Failed</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.e-londonjobs.com">www.e-londonjobs.com</a></td>
<td>Failed</td>
<td>Failed</td>
<td>Failed</td>
<td>Failed</td>
</tr>
</tbody>
</table>

### Table 2: Results of Detected Phishing websites Using Phishing Website Detector
Table 3: Results of Undetected Websites Using Phishing Website Detector

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Cookie Check</th>
<th>DNS Check</th>
<th>Logo Matching</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.login.yahoo.com">www.login.yahoo.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.yahoo.com">www.yahoo.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
<td>Successful</td>
</tr>
<tr>
<td><a href="http://www.orkut.com">www.orkut.com</a></td>
<td>Successful</td>
<td>Failed</td>
<td>Failed</td>
<td>Successful</td>
</tr>
<tr>
<td>www hi5.com</td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
<td>Failed</td>
</tr>
<tr>
<td><a href="http://www.encana-ca.com">www.encana-ca.com</a></td>
<td>Successful</td>
<td>Successful</td>
<td>Failed</td>
<td>Failed</td>
</tr>
</tbody>
</table>
5.7 Performance Evaluation

The Phishing Website Detector application was tested with 54 websites. Out of 54 websites, 46 websites were genuine and 8 websites were phishing websites. The Phishing Website Detector detected 41 out of 46 genuine websites. 5 out of 46 genuine websites were not detected by the detector. All 8 phishing websites were identified by the application. The success rate of the application is tabulated in Table

Table 4: Performance of Phishing Website Detector

<table>
<thead>
<tr>
<th>Success Rate of Genuine Websites</th>
<th>Success Rate of Phishing Websites</th>
<th>Overall Success Rate of Phishing Website Detector</th>
</tr>
</thead>
<tbody>
<tr>
<td>41/46 = 89.13%</td>
<td>8/8 = 100%</td>
<td>49/54=90.74%</td>
</tr>
</tbody>
</table>
6. Conclusion and Future Work

This project is a small contribution towards the research on offering a secure phishing detection service to Internet users while they are accessing the Internet. It protects users from loss of sensitive information. This prototype system will provide immediate, automatic and inclusive system-level solutions to perform webpage authentication and webpage detection, adverse to phishing. This application was tested with 54 websites. 46 of 54 websites are genuine of which 41 were detected by the phishing website detector application. The rest 8 websites were Phishing websites which were detected.

Future work of this project could include implementing and checking the compatibility with other web browsers like Mozilla Firefox, Google Chrome, Safari, etc. Additional work can be performed to improve the success rate of the Phishing Website Detector.
7. BIBLIOGRAPHY


