Whitepaper

SecurEyes
Infusing Security

# Phishing through Base-64 Encoded Reflective HTML Injection

# A Proof-of-Concept

Sabyasachi Samanta & Sudip Narayan Das

June 2010

# Phishing through Base-64 Encoded Reflective HTML Injection

TABLE OF CONTENTS

# Phishing through Base-64 Encoded Reflective HTML Injection


## Abstract

Through Phishing, an attacker steals critical information like user credentials, financial details, etc. from a victim. Phishing through a base-64 encoded reflective XSS vector is especially dangerous since the URL's domain is genuine and the vector is hidden in a genuine looking string, which is the icing on the cake.


## Introduction

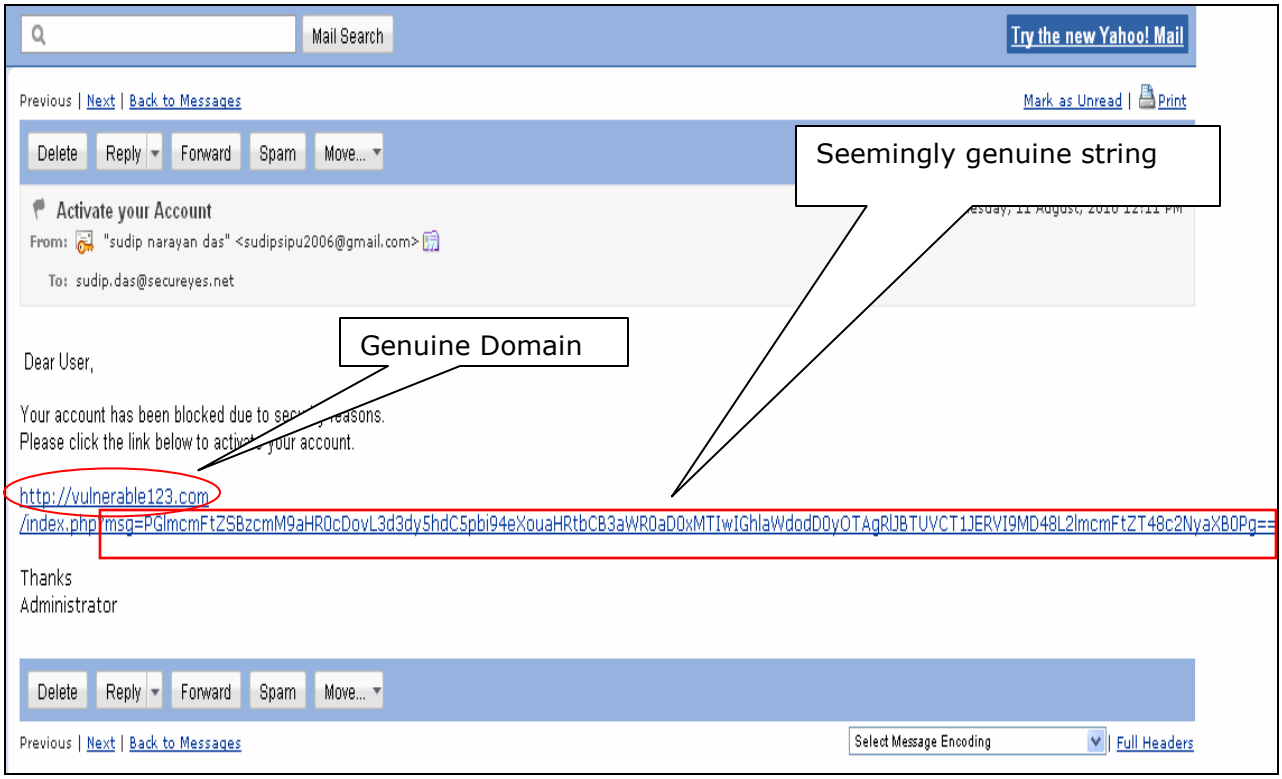
Phishing attacks using the domain name of the genuine site are especially deadly, since users cannot distinguish between the fake and the original. Such a phishing attack is possible when the application is prone to reflective XSS.

By implementing Base-64 encoding to pass URL parameter values, site owners mistakenly believe that they have secured their site against reflective XSS. Encoded value can be easily decoded, changed in any way the attacker wants, and then encoded again. Base-64 encoding of parameter values provide no protection against reflective XSS and HTML injection attacks; rather, it ends up increasing the success rate such attacks as will be demonstrated in this paper.

# Phishing through Base-64 Encoded Reflective HTML Injection

## A Likely Scenario

An attacker sends the following maliciously crafted URL to the E-Mail account of an application user.



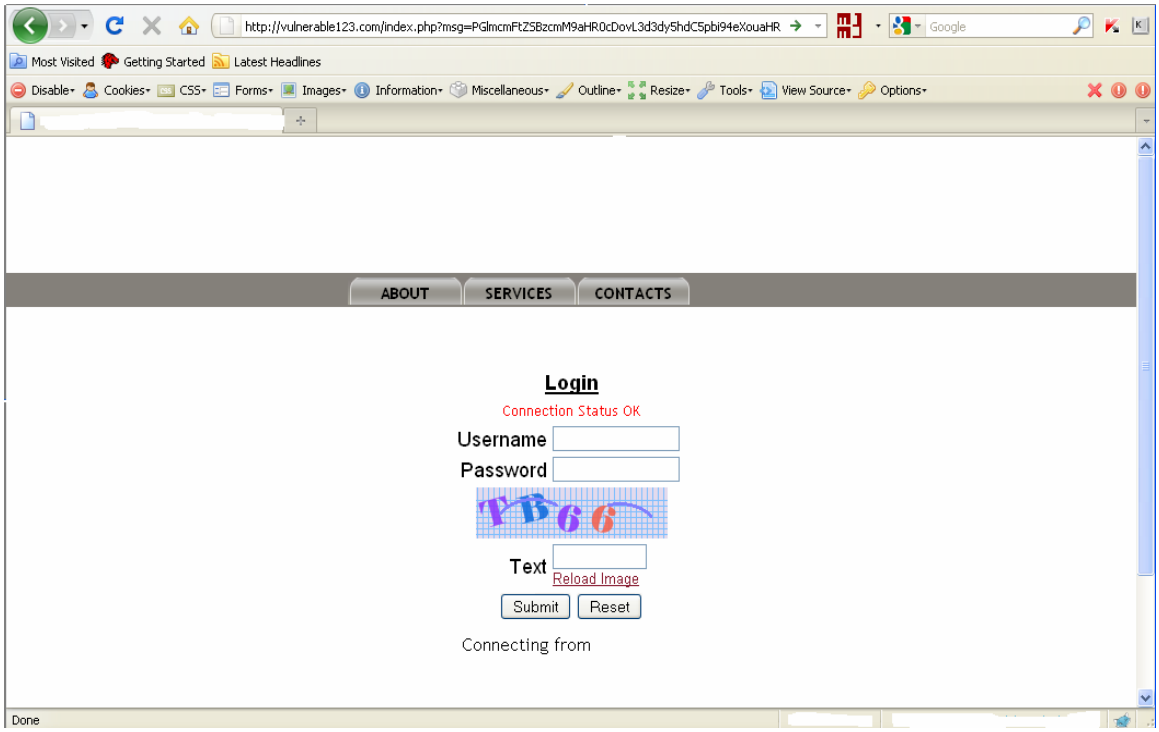

http://vulnerable123.com/index.php?msg=PGlmcmFtZSBzcmM9aHR0cDovL3d3dy5hdC5pbi94eXouaHRtbCB3aWR0aD0xMTIwIGhlaWdodD0yOTAgRlJBTUVCT1JERVI9MD48L2lmcmFtZT48c2NyaXB0Pg==

The victim user thinks the URL is genuine by seeing the domain name and is also familiar with the Base-64 encoded string in the URL.

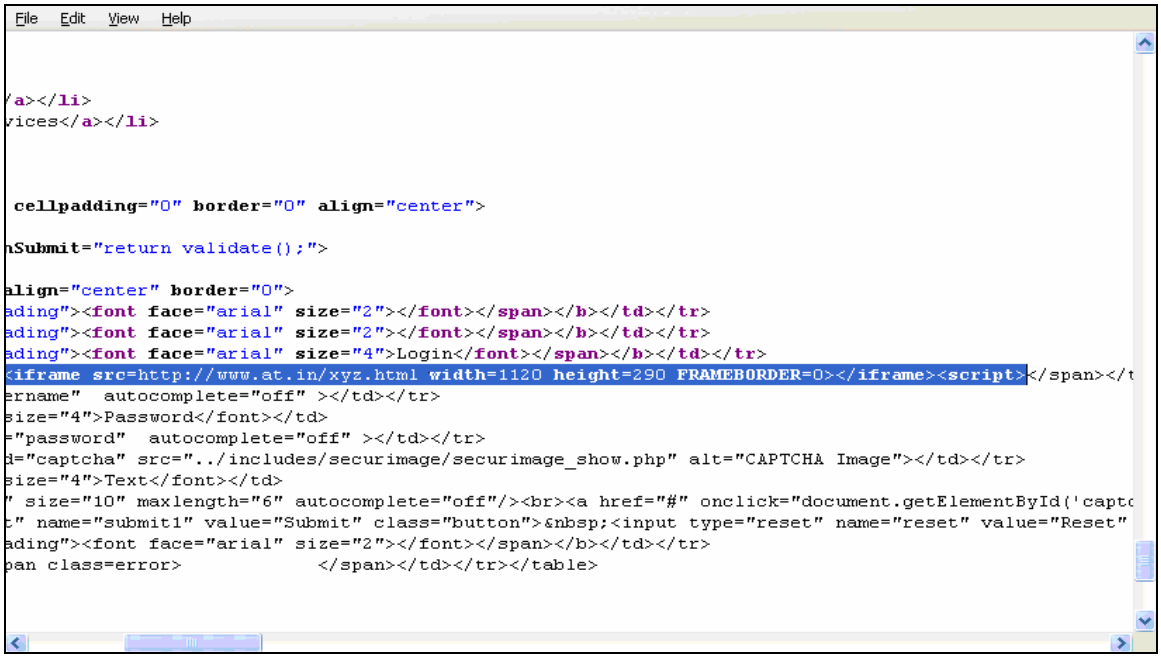
# Phishing through Base-64 Encoded Reflective HTML Injection

## The Exploit

The attacker clicks on the URL and is shown the following page:



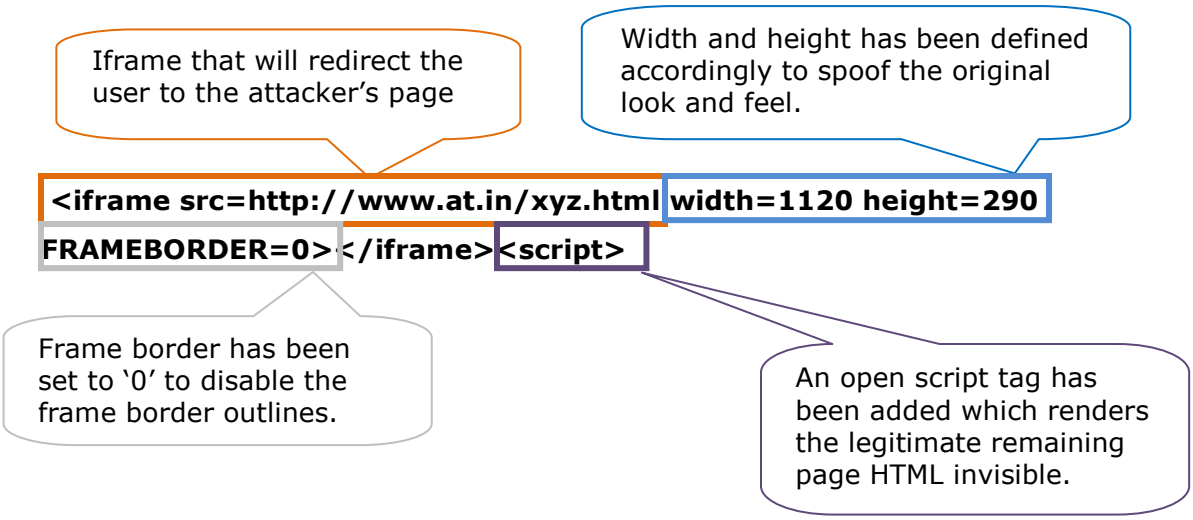

The above page appears to be a legitimate one which is actually not the case. The screenshot of the HTML source code of the above page shows a malicious Iframe has also been inserted in the main frame.



# Phishing through Base-64 Encoded Reflective HTML Injection

## Behind the Scenes

The attacker exploits the Base-64 encoding for value of the 'msg' URL parameter. He frames the following malicious vector:



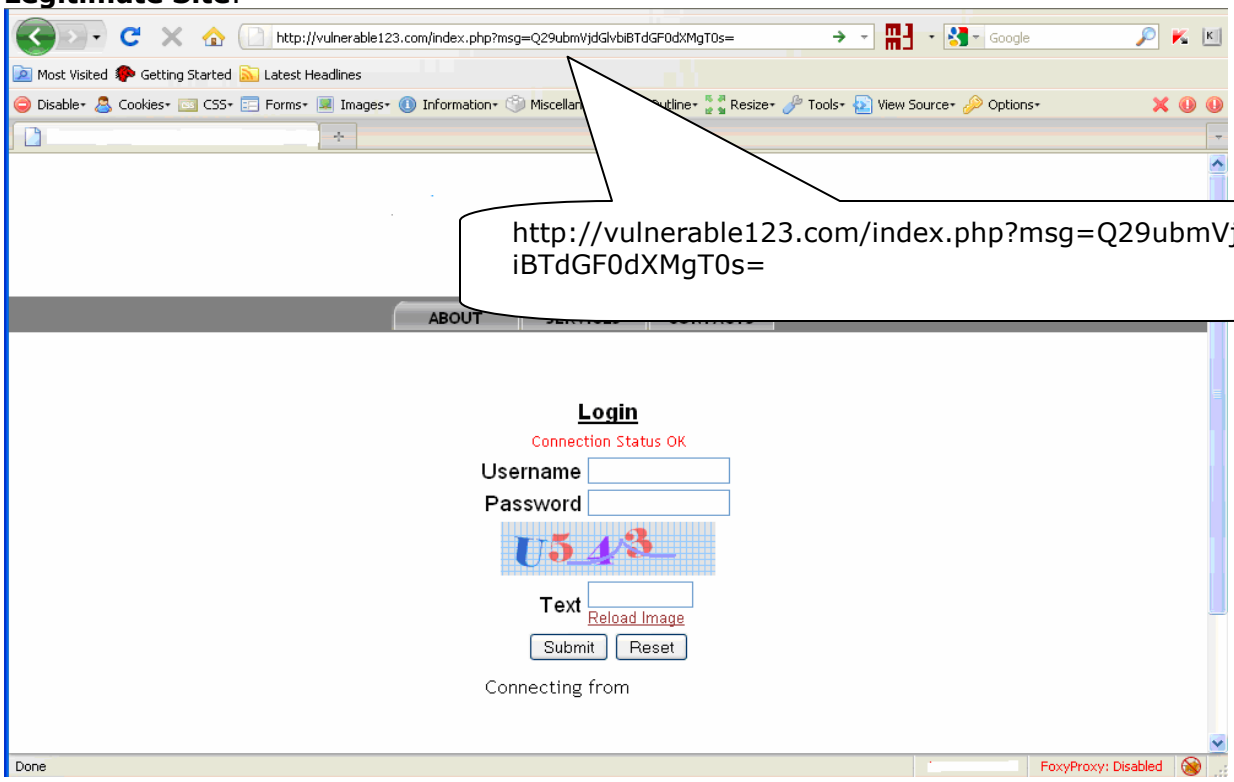

The above iframe is encoded into the following Base-64 encoded string:

**PGlmcmFtZSBzcmM9aHR0cDovL3d3dy5hdC5pbi94eXouaHRtbCB3aWR0aD0x**
**MTIwIGhlaWdodD0yOTAgRlJBTUVCT1JERVI9MD48L2lmcmFtZT48c2NyaXB0**
**Pg==**

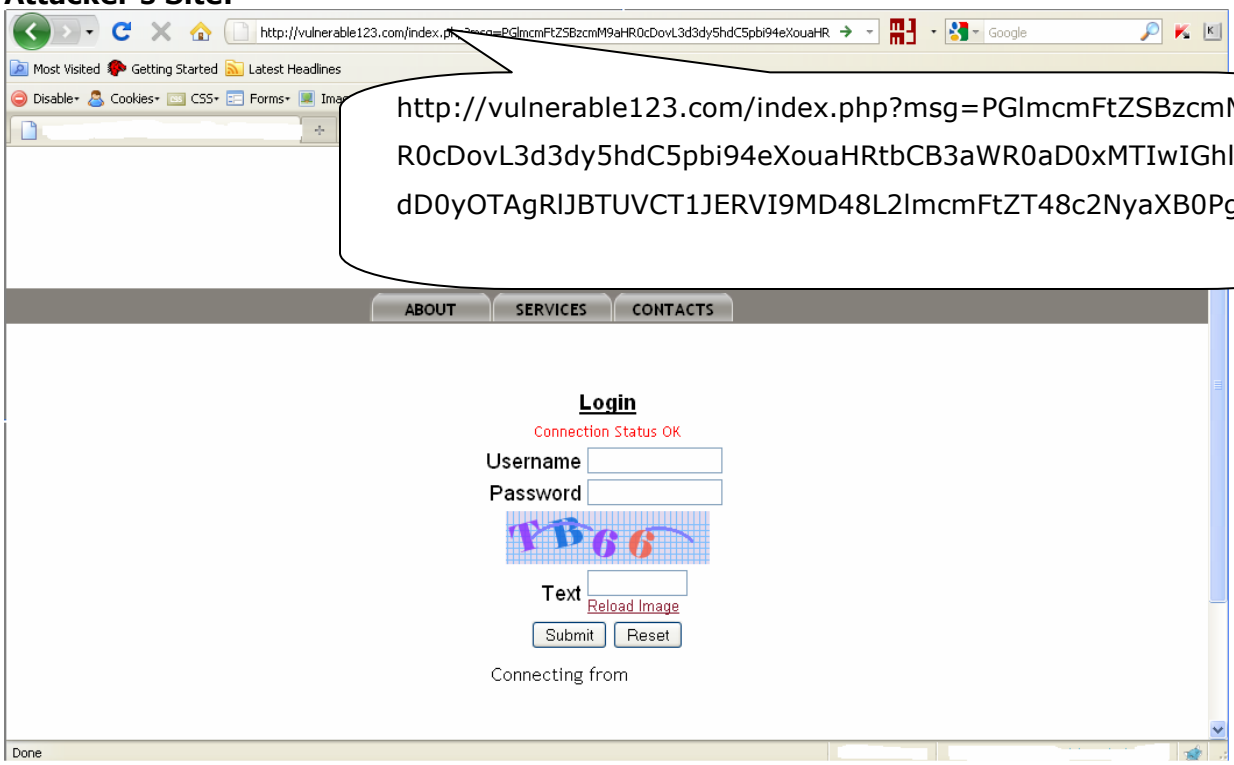
The '*xyz.html*' page of the attacker's site is just the replica of the original Login page of the application as demonstrated below.

# Phishing through Base-64 Encoded Reflective HTML Injection

**Legitimate Site**:




**Attacker's Site:**



# Phishing through Base-64 Encoded Reflective HTML Injection

The html source of the attacker's site is:


## The Impact

Hiding the attack vectors in base-64 encoding can be devastating to a site's reputation. It can lead to phishing attacks, reflective XSS attacks, as well as defacements.

## Recommended Resolutions

'Security through Obscurity' measures should be avoided. Further, strict 'white list' based server side validation should be performed against user entered strings.

In the event where reflection of user entered strings is required, proper output encoding should be performed to prevent malicious codes from being executed.

# Phishing through Base-64 Encoded Reflective HTML Injection

---

## About The Author

Sabyasachi Samanta and Sudip Narayan Das are senior IT Security Consultants at SecurEyes, and between them, they have secured over 300 web applications. They can be reached at sabyasachi.samanta@secureyes.net and sudip.das@secureyes.net respectively.

## About SecurEyes

SecurEyes is a Bangalore based firm specializing in IT security. SecurEyes offers a wide range of security services and products to its clients. For more information, please visit our website: http://www.secureyes.net/.