Introduction to Next level XSS based Phishing Attacks to steal user credentials

Jasminder Pal Singh[1], **Sumeet Kaur**[2]

[12]*Yadavindra College of Engineering, Talwandi Sabo*

ABSTRACT

Being secure on the internet is one of the important issue these days. Companies are spending millions of dollars on making their web services more secure, Still, hundreds of vulnerabilities are discovered and exploited daily. In this paper a new method of phishing is proposed by exploiting one of the critical web vulnerability named Cross Site Scripting also known as XSS, That means attacker must be able to inject malicious javascript code into application to perform this attack. It is mostly undetectable by the major web browsers if the web application is vulnerable. This work will help to understand more deeply about this latest attack.

Keywords: *Cross-Site-Scripting(xss), Phishing, Web Security, Dom XSS, Reflected XSS, OWASP*

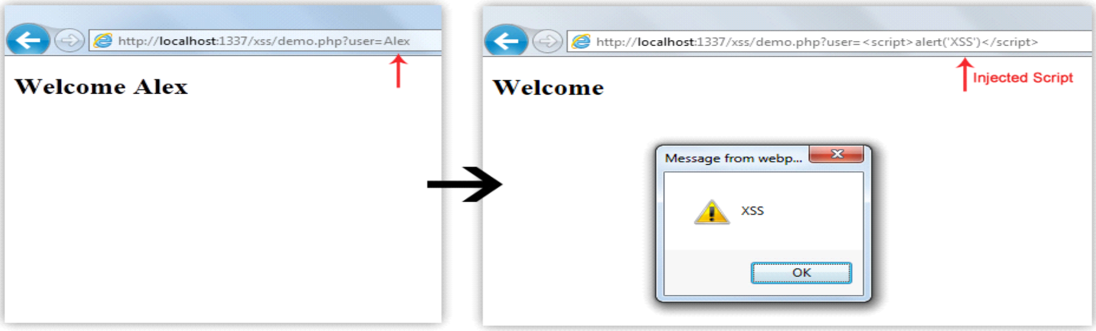
I. INTRODUCTION

Since **we** are talking about web applications, there are many types of security vulnerabilities which are discovered in the past years. These vulnerabilities targets stealing important information through various ways. After all information is a kind of wealth. As web applications are now widely spread over most of the sectors. Even in our daily life, we are dependent on websites to be updated with happenings in the world. Being aware about the web attacks is very important of to make our critical information safe online. Regarding this article we are only concerned with the vulnerability named Cross Site Scripting or XSS which is widely being spread over the web. Here we discussed some of the related terms.

Cross Site Scripting or XSS: Cross Site Scripting is a type of vulnerability by which attacker injects malicious scripts into the legit website via vulnerable part of the website generally in the form of browser side script. XSS is at 3rd position in the OWASP Top Ten Web Vulnerabilities of 2017 [3]. By exploiting the XSS vulnerability the attacker can execute scripts in the victim browser to hijack user sessions, stealing the confidential details, redirecting to some malicious website. XSS is categorized into following main types [2]:

- Stored XSS.
- Reflected XSS.
- DOM Based XSS

Reflected XSS vulnerability or Non Persistent XSS: Reflected XSS attacks are those where the scripts are injected mostly through URL or the parameters in the URL of the website. The attack is injected in the URL itself, when the victim visits the malicious URL the attack gets executed.



http://localhost:1337/xss/demo.php?user=Alex

Welcome Alex

http://localhost:1337/xss/demo.php?user=<script>alert('XSS')</script>

Welcome

Message from webp...

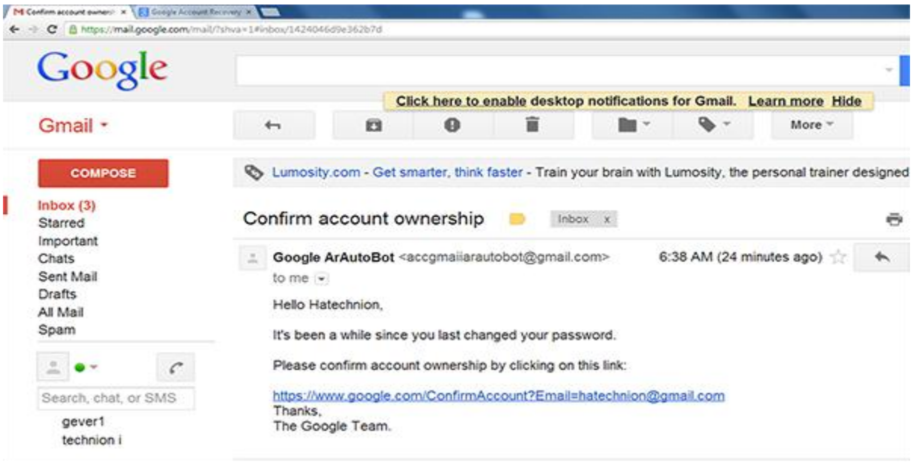
XSS

Figure 1: XSS Vulnerable Web Page before and after.

It is clear from the Fig 1: the injected script or code in the user parameter of the URL is successfully executed which means the website is vulnerable to Reflected XSS. That means attacker can steal confidential cookies, hijack session of user since any kind of JavaScript code can be in injected into the URL.

DOM Based XSS: DOM stands for Document Object Model. Basically it’s an API used by Javascript(JS) to access contents of a webpage. It allows JS to easily modify contents and dynamically update webpage contents. DOM Based XSS is attack in which the attacker code is executed as a result of modifying contents of DOM elements. DOM Based XSS is another type of Cross Site Scripting which is very difficult to detect. One must have good knowledge of JavaScript to detect it. DOM Based XSS can be Reflected means in the URL etc. or can be residing in DOM elements itself [5].

Phishing: Phishing is a method of attempting to steal confidential details like username/password, credit card numbers etc by posing a customized web page as a legit entity. When the victim fills in the details on the customized web page then filled details will be sent to the attacker’s server. Phishing attacks can be performed in several ways. [1]



https://mail.google.com/mail/?shva=1#inbox/1424046d9e362b7d

Click here to enable desktop notifications for Gmail. Learn more Hide

Lumosity.com - Get smarter, think faster - Train your brain with Lumosity, the personal trainer designed

Confirm account ownership

Google ArAutoBot <accgmaiiarautobot@gmail.com> 6:38 AM (24 minutes ago)

to me

Hello Hatechnion,

It's been a while since you last changed your password.

Please confirm account ownership by clicking on this link:

https://www.google.com/ConfirmAccount?Email=hatechnion@gmail.com
Thanks,
The Google Team.

Figure 2: Phishing Email Example

Normal Phishing: In normal phishing attack, a well customized email is sent to random emails. As shown in FIG 2: the email looks so genuine that a less aware user can be trapped easily.

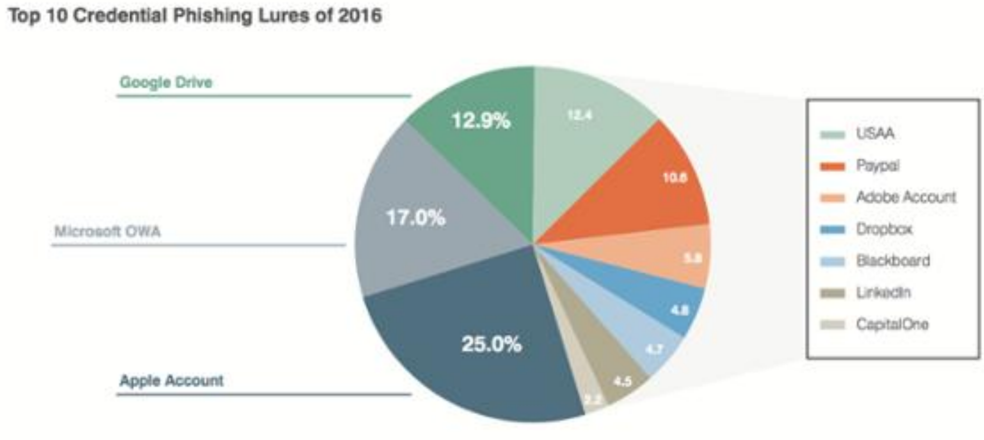


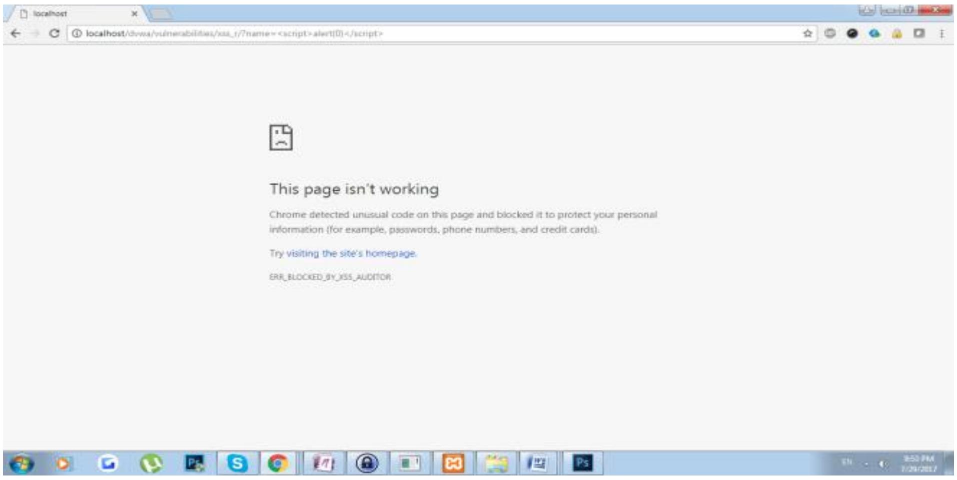
Figure 7: Top 10 credential phishing lures, with percent share

Figure 3: Most targeted websites via phishing in 2016 [6]

As the FIG 3: shows, In the year 2016, the top most lures include Google Drive, Apple ID, PayPal Accounts etc [6].

Spear Phishing : In spear phishing attacker first gathers information about the target and then use the information to create a more legit email to lure the victim. The success rate of spear phishing is way more than the normal phishing technique because the email looks genuine in all aspects. [1] .

Web Browser Web Application Firewall and XSS: Recently browsers like Mozilla and Chrome came up with XSS


localhost
localhost/dvwa/vulnerabilities/xss_r/?name=<script>alert(0)</script>

This page isn't working

Chrome detected unusual code on this page and blocked it to protect your personal information (for example, passwords, phone numbers, and credit cards).

Try visiting the site's homepage.

ERR_BLOCKED_BY_XSS_AUDITOR

Figure 4: XSS Attack protection by Google Chrome XSS Auditor

Auditors which looks for pattern in the URL for malicious code and deny loading contents of the webpage. As shown in FIG 4, XSS attack detected by Google Chrome and stopped loading contents of webpage.

II. RELATED WORK

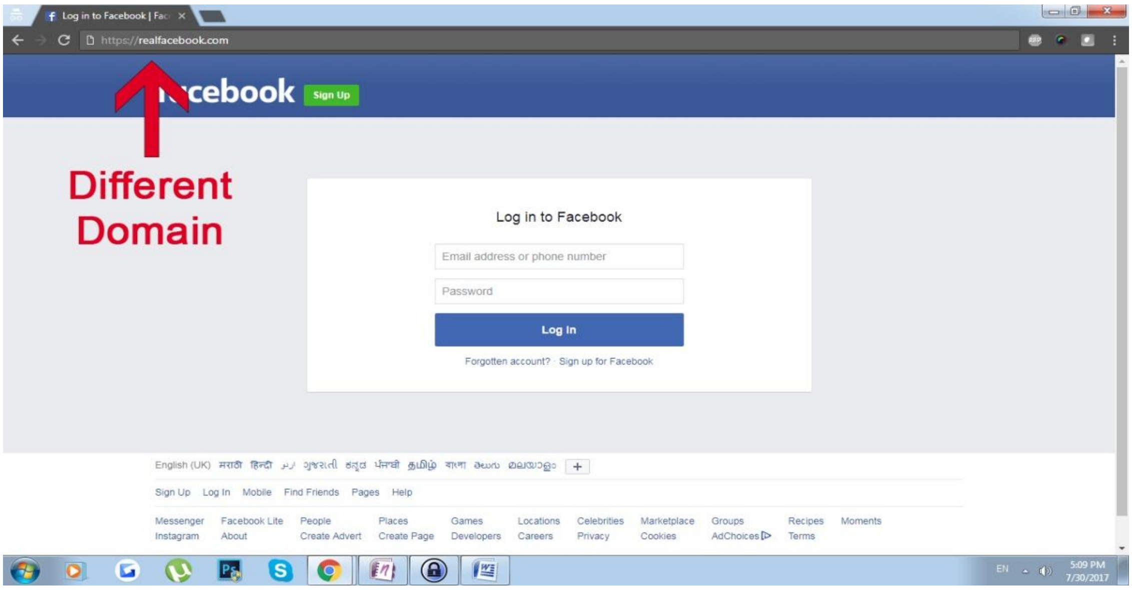

Log in to Facebook | Fac
https://realfacebook.com
facebook
Sign Up
Different Domain
Log in to Facebook
Email address or phone number
Password
Log In
Forgotten account? · Sign up for Facebook
English (UK) मराठी हिन्दी اردو ગુજરાતી ಕನ್ನಡ ਪੰਜਾਬੀ தமிழ் বাংলা తెలుగు മലയാളം +
Sign Up Log In Mobile Find Friends Pages Help
Messenger Facebook Lite People Places Games Locations Celebrities Marketplace Groups Recipes Moments
Instagram About Create Advert Create Page Developers Careers Privacy Cookies AdChoices Terms
EN 5:09 PM 7/30/2017

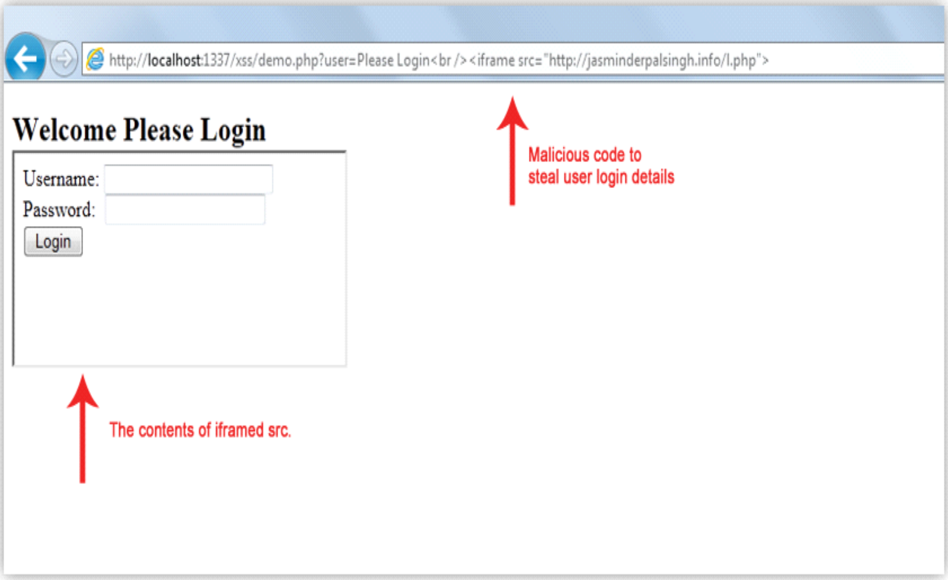
Figure 5: A facebook phishing page

As shown in FIG 5, in phishing a duplicate web page is designed which looks exactly same as the original web page. This duplicate web page is then customized to steal the filled details, after customizing, it is uploaded to some website whose domain name is different from the original website. Since the domain name of the customized pages is always different, it is an easy way to detect those websites by checking the domain name before clicking any link and this type of phishing is now detected automatically by major browsers .

III. PROPOSED WORK AND IMPLEMENTATION

Traditional XSS attacks can be detected automatically by major web browsers . XSS based phishing attacks cannot be detected by most of the browsers if the application is vulnerable to XSS and domain name is same as original website.

Working of next phising level: Proposed method for phishing attack is achieved by exploiting the XSS(Reflected or DOM Based) vulnerability and by using the Iframe object of HTML mostly. As shown in FIG 6, In the url there is a GET parameter named “user” in which we injected iframe code which caused the injected frame contents to load into the parent webpage.



http://localhost:1337/xss/demo.php?user=Please Login<br /><iframe src="http://jasminderpalsingh.info/l.php">

Welcome Please Login

Username:

Password:

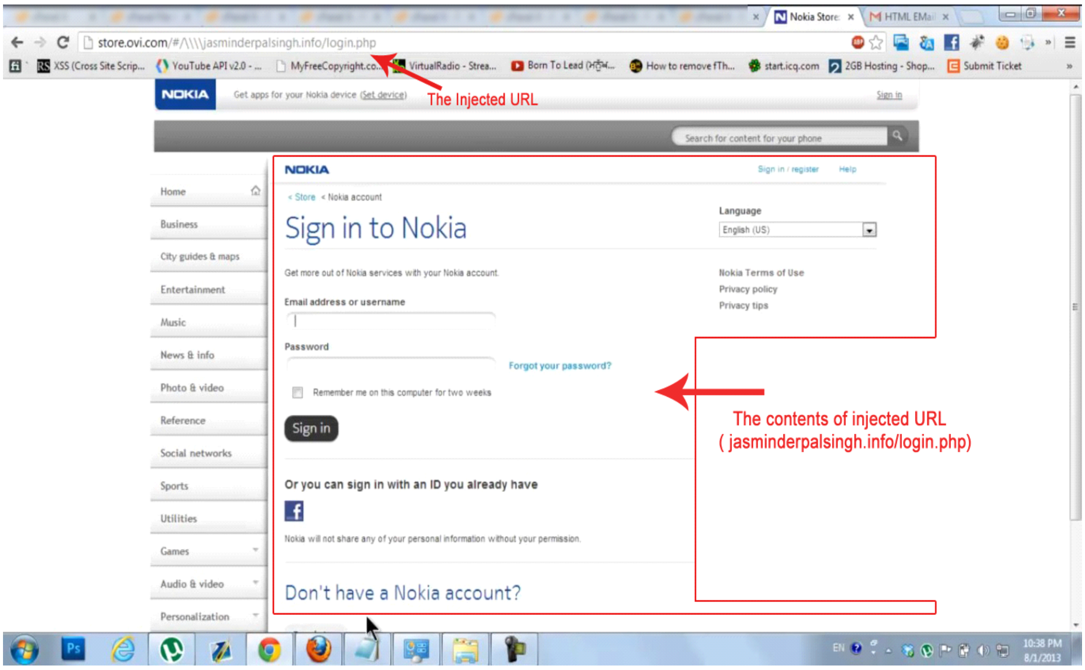
Malicious code to steal user login details

The contents of iframed src.

Figure 6: Injecting iframe via XSS

If someone fills the username and password in the input boxes, it will be sent information to the attacker . As shown in FIG 6: the page is looking very realistic and the domain name is same , that’s the reason the victim can be easily trapped and their login details can be stolen easily.

DOM Based XSS Phishing attack example on Nokia OVI Store



store.ovi.com/#/\\\jasminderpalsingh.info/login.php

The Injected URL

Sign in to Nokia

Get more out of Nokia services with your Nokia account.

Email address or username

Password

Forgot your password?

□ Remember me on this computer for two weeks

Or you can sign in with an ID you already have

Nokia will not share any of your personal information without your permission.

Don't have a Nokia account?

The contents of injected URL (jasminderpalsingh.info/login.php)

Figure 7: DOM Based XSS vulnerability with phishing exploit

As shown in FIG 7: The vulnerable code allows even external URL(jasminderpalsingh.info/login.php in FIG) content to be loaded in the parent page DOM via CORS (Cross Origin Resource Sharing). Due to lack of CORS protection, application allowed to inject malicious content into main domain DOM . As you can see the page is looking totally legit but if someone will fill in their details in the login area their details will be sent to my specified email address instantly. This vulnerability is totally undetectable by automatic XSS web browser auditors.

IV.CONCLUSION

With the wide growth of web applications, the parallel web attacks are increasing at fast rate. To be secure on the internet these days is a challenging , but if you are aware of what is happening in the world of web application security then its easy to be safe. Daily tens of vulnerabilities are being discovered and exploited . I tried to include every aspect regarding this new phishing technique , but its not enough to be secure. Read more about the other top 10 web vulnerabilities of 2017 collected by OWASP

REFERENCES

[1.] Dr. M. Nazreen Banu,S. Munawara Banu(2013) A Comprehensive Study of Phishing Attacks , (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) , 2013, 783-786

[2.] Ankit Shrivastava, Santosh Choudhary, Ashish Kumar(2016), XSS vulnerability assessment and prevention in web application, Paper presented at the 2nd International Conference on Next Generation Computing Technologies (NGCT-2016)

[3.] Top 10 2017-Top 10 - OWASP, https://www.owasp.org/index.php/Top_10_2017-Top_10

[4.] Cross-site Scripting (XSS) – OWASP, https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

[5.] Cross-site Scripting (XSS) – OWASP, https://www.owasp.org/index.php/DOM_Based_XSS

[6.] Must-Know Phishing Statistics 2017, https://blog.barkly.com/phishing-statistics-2017

[7.] Google Account Recovery Vulnerability, http://www.orenh.com/2013/11/