



SpoofedMe: Social Login Attack

By,
Team 19
Dev Vishnu Dutta
Zhou Wu

Introduction

- Social Login Attack that could allow a hacker to impersonate someone by abusing the social login mechanism.
- Found by IBM X-Force's Application Security Research Team.
- This attack allowed an attacker to intrude into a Slashdot.org user account by using the "Sign In With LinkedIn" service. Once logged in, the attacker has complete access to the victim's account.

SpooferMe

- The attack requires the following combination of flaws:
 - A vulnerability that was found with some **social login identity providers**, including LinkedIn, Amazon and MYDIGIPASS.
 - A known design issue present in the affected **relying websites**, or those that rely on the identity providers to verify a user's identity.
- For the attack to work, the victim's email address must not already be used by an existing account at the vulnerable identity provider.

Continued...

- To perform the attack,
 - A cybercriminal registers a spoofed account within a vulnerable identity provider using the victim's email address.
 - Then, without having to actually confirm ownership of the email address, the attacker will log in to the relying website using social login with this fake account.
 - The relying website will check the user details asserted from the identity provider and log the attacker in to the victim's account based on the victim's email address value.

What is Social Login?

- Social login is an authentication mechanism that allows a user to use a single account within an identity provider (such as Facebook, Google+ or LinkedIn) for signing in to various third-party websites.

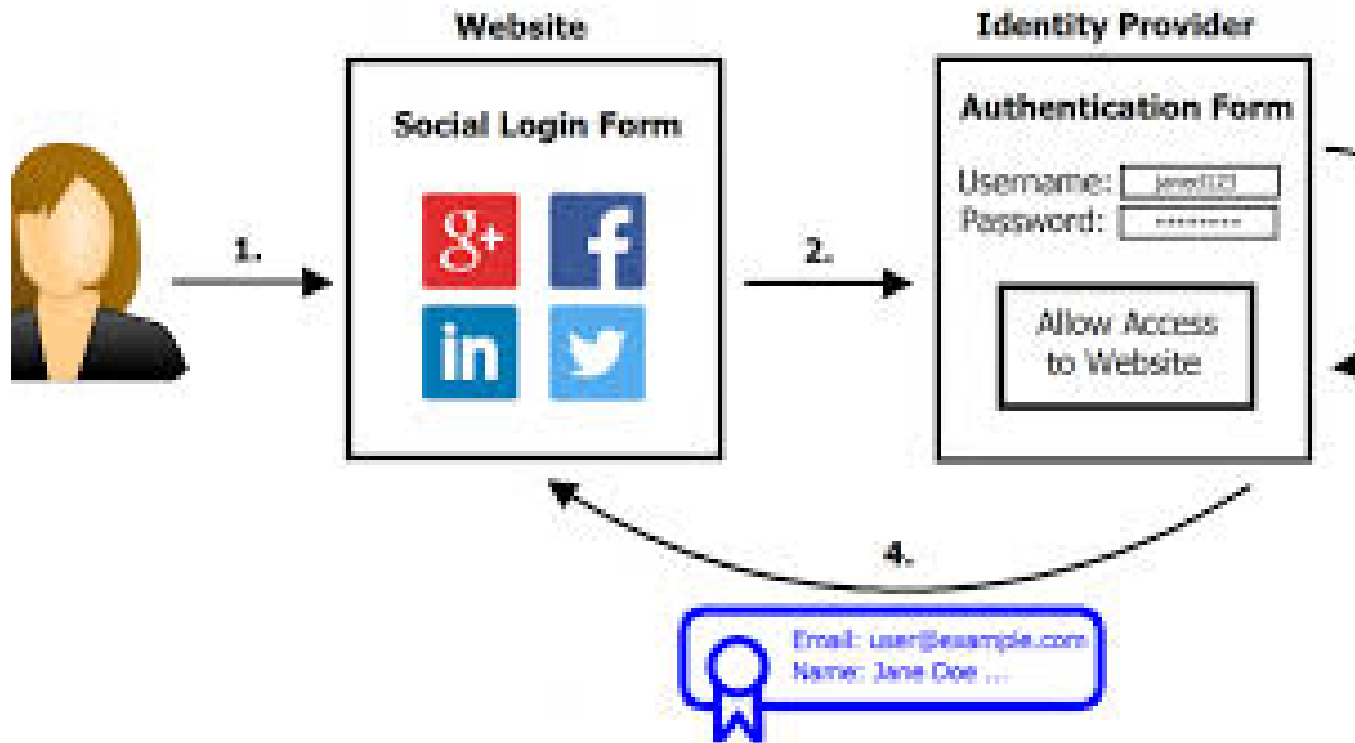
Explaining the Social Login Attack

- As the attacker, we would like to be able to intrude into an existing user's (the victim's) account within a website supporting a social login option.
- To achieve this, we will impersonate the victim with the help of the social login authentication process.

Continued...

- The following three players are involved in a social login authentication process:
 - User
 - Identity Provider
 - Relying website

Simplified Social Login Authentication Process



Continued...

- The social login attack depends on a combination of two things:
 - the identity provider vulnerability
 - one of the relying website design problems

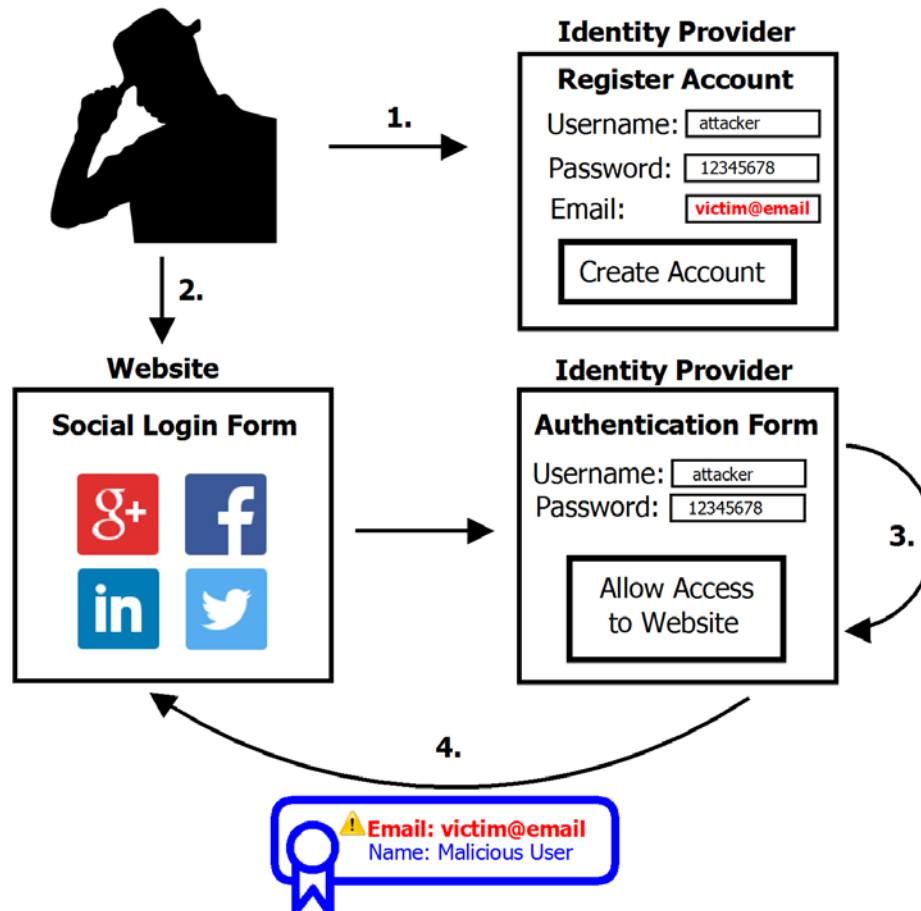
The Identity Provider Vulnerability

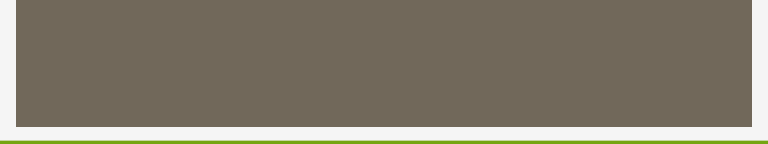
- The identity provider transfers the user's identity fields to the relying website. The vulnerability we identified is that some identity providers agree to supply the account's email addresses without positively verified

Known Relying Website Design Problems

- 1. Using an Email Address as a Unique Identifier
- 2. Account Linking

Attack Stages





Demo: Below is a video of the attack (taken before LinkedIn patched its vulnerability), on a Slashdot.org website account, using LinkedIn as the vulnerable identity provider.

- <https://youtu.be/kC0s3S00Dmk>

Reference:

- <http://securityintelligence.com/spoofed-microsoft-social-login-attack-discovered-by-ibm-x-force-researchers/#.VSR5ghPF-0x>