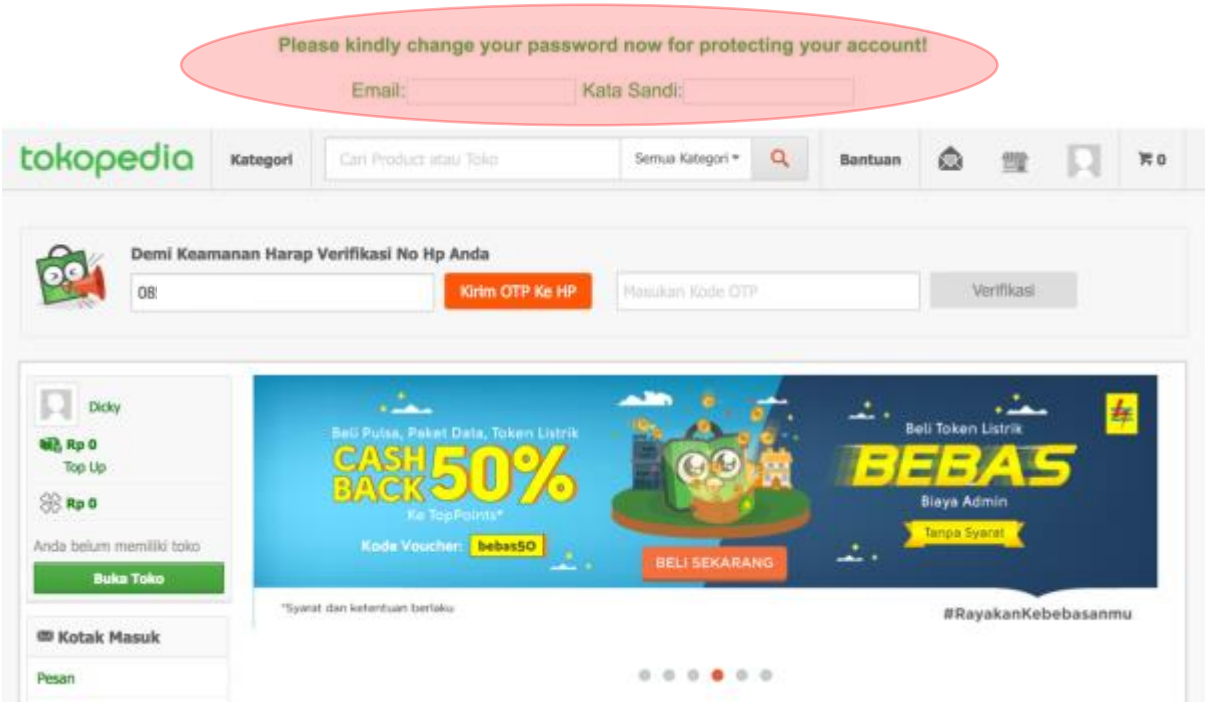
Open URL Redirection that could Result Fraud Issue

- (Unvalidated Redirects and Forwards) -



August 17th, 2016

@YoKoAcc (yk@firstsight.me)

[Indonesian Version]

Revision Detail

Version	Detail
0.1	-

Table of Contents

Table of Figures

I. ABSTRACT

Auto Redirection (pengalihan otomatis) merupakan suatu fitur yang lumrah dibuat oleh pengembang aplikasi untuk memudahkan para penggunanya mengunjungi suatu halaman tanpa perlu mengetiknya secara manual. Dalam hal yang lebih umum, pengalihan ini sering "diberikan" oleh pengembang ketika terdapat seorang pengunjung ingin mengakses ke suatu halaman yang biasanya hanya dapat diakses oleh pengunjung yang sudah login (member).

Sebagai contoh spesifik untuk hal di dalam situs Tokopedia, ketika seorang pengunjung hendak mengelola toko online nya melalui fitur "**User Management**" yang terdapat pada halaman https://www.tokopedia.com/user-management.pl, maka pengunjung hanya cukup mengunjungi portal https://admin.tokopedia.com yang dilanjutkan dengan mengklik menu "**Ayo, Coba Fitur Ini!**" yang terdapat di halaman paling bawah.

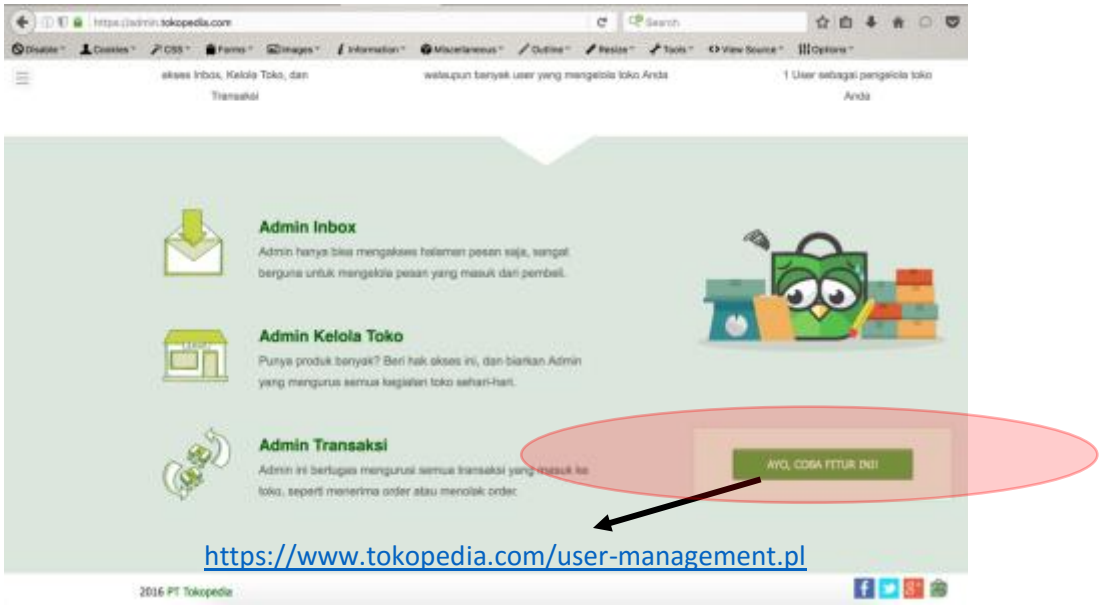


Figure 1 "User Management" Page via Admin.Tokopedia.Com

Bila melihat dari konteks bisnis, hal ini pun tentu lebih baik dikarenakan pengguna tidak akan komplain mengenai sukarnya pengalaman mengunjungi fitur "User Management" secara manual.

Mengingat bahwa fitur "User Management" ini hanya dapat digunakan oleh para member, maka ketika seorang member mencoba mengakses fitur ini dalam keadaan belum login, maka member itu akan dihadapkan pada halaman login yang juga akan di-redirect otomatis ke fitur ini setelah member terkait melakukan aktivitas login.

Di dalam hal ini, permasalahan muncul ketika halaman redirect dari halaman login menuju fitur "User Management" belum di-validasi dengan baik sehingga seorang Attacker akan dapat "membelokan" korbannya untuk mengunjungi suatu halaman palsu yang telah dipersiapkan.

II. INTRODUCTION

2.1. **Open URL Redirection**

Open URL Redirection merupakan suatu kerentanan yang memanfaatkan kelemahan pada suatu aplikasi dalam melakukan validasi URL terhadap input baik di dalam suatu parameter yang dikhususkan untuk URL maupun tidak. Dengan memanfaatkan kerentanan ini, maka seorang Attacker akan dapat membawa korban menuju ke suatu halaman palsu yang tentunya dapat mengakibatkan suatu fraud. Pada OWASP Top 10 2013, kerentanan ini telah "ditempatkan" pada peringkat 10 yang masuk ke dalam point A10 terkait "Unvalidated Redirects and Forwards".

2.2. **Base64 Encoding**

Mengutip sedikit penjelasan pada pelaporan Reflected XSS yang telah disampaikan pada 11 Agustus 2016 mengenai Base64 Encoding, banyak developer berpikir bahwa Base64 merupakan suatu hal yang dapat digunakan untuk melindungi nilai teks asli yang dikirimkan, diproses, maupun disimpan. Namun secara kenyataan, Base64 tidak memiliki sifat confidential di dalamnya sehingga tidak menjadi standar untuk mengamankan suatu nilai teks asli.

III. SUMMARY OF ISSUE

Seperti yang telah disampaikan pada point sebelumnya, permasalahan keamanan pada laporan ini berkaitan dengan kerentanan yang "mengizinkan" seorang Attacker untuk dapat membelokan korbannya menuju suatu halaman palsu pada salah satu URL di situs Tokopedia yang belum melakukan validasi terhadap setiap URL yang di-input-kan secara langsung maupun tidak langsung.

IV. INFORMATION AND SITUATION OF THIS POC

Untuk dapat memahami dengan baik akan permasalahan yang ada, pada bagian ini akan disampaikan kembali secara spesifik mengenai beberapa informasi yang berkaitan dengan proses yang berjalan secara umum dari aplikasi maupun akar dari permasalahan yang ada.

Saat seorang member yang belum login mencoba mengunjungi fitur "User Management", maka seorang member akan dihadapkan pada halaman login dengan URL lengkap sebagai berikut:

https://accounts.tokopedia.com/authorize?response_type=code&client_id=1001&state=eyJsZCI6Imh0dHBzOi8vd3d3LnRva29wZWRpYS5jb20vdXNlci1tYW5hZ2VtZW50LnBsIiwicmVmIjoiaHR0cHM6Ly9h

ZG1pbi50b2tvcGVkaWEuY29tLyIsInV1aWQiOiJlYWQzMjM0Yi0zN2M5LTRjMGQtYWY4Mi02Y2NlMjMyYWIwZDYiLCJ0aGVtZSI6ImRlZmF1bHQifQ&redirect_uri=https%3A%2F%2Faccounts.tokopedia.com%2Fappauth%2Fcode&p=https://www.tokopedia.com&contactus=&theme=default

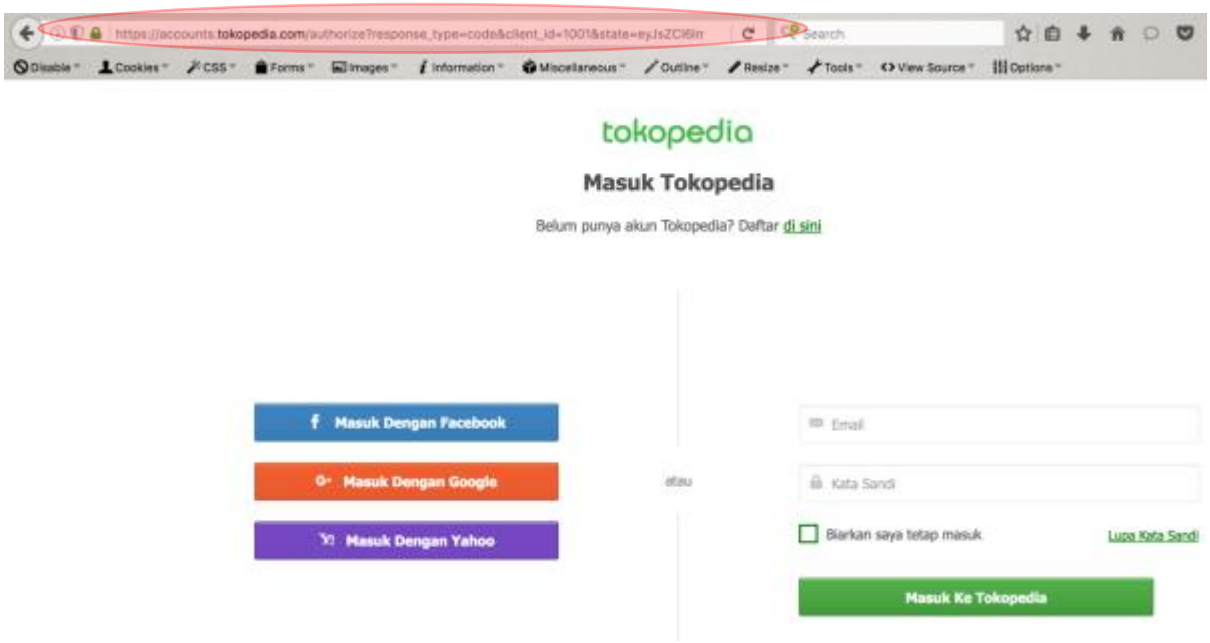


Figure 2 Redirect to Login Page with "Provided URL"

Bila dilihat dengan baik pada URL yang telah diberikan, maka kita pun dapat memecahnya menjadi beberapa parameter:

- response_type
- client_id
- state
- redirect_url
- p
- contactus
- theme

Seperti yang terlihat pada URL berikut parameter yang ada, kita dapat melihat satu bagian yang unik pada parameter "state" yang setelah ditelaah ternyata parameter ini menggunakan Base64. Adapun setelah kita decode value dari

"eyJsZCI6Imh0dHBzOi8vd3d3LnRva29wZWRpYS5jb20vdXNlci1tYW5hZ2VtZW50LnBsIiwicmVmIjoiaHR0cHM6Ly9hZG1pbi50b2tvcGVkaWEuY29tLyIsInV1aWQiOiJlYWQzMjM0Yi0zN2M5LTRjMGQtYWY4Mi02Y2NlMjMyYWIwZDYiLCJ0aGVtZSI6ImRlZmF1bHQifQ"

memiliki nilai asli:

{"ld":"https://www.tokopedia.com/user-management.pl","ref":"https://admin.tokopedia.com/","uuid":"ead3234b-37c9-4c0d-af82-6cce232ab0d6","theme":"default"}

Dalam hal ini, kita pun dapat melihat lebih jelas bahwa terdapat beberapa parameter kembali yang sebenarnya dikirimkan oleh aplikasi menuju server, yaitu:

- **id**: digunakan untuk mendaratkan pengunjung ke halaman yang tertuang di dalamnya;
- **Ref**: digunakan sebagai informasi akan Reference URL;
- **Uuid**: belum diketahui dengan pasti. Kemungkinan hal ini adalah session id karena nilainya selalu berubah dalam periode tertentu;
- **Theme**: tema tampilan yang digunakan oleh aplikasi.

V. STEP TO REPRODUCE

5.1. Persiapkan fake URL yang ingin diubah ke Base64 untuk kemudian disisipkan ke URL yang akan dikirimkan kepada korban. Dalam hal ini, fake URL yang "dituju" dapat digunakan untuk menampilkan halaman palsu, mengunduh suatu malware, ataupun mengeksploitasi kerentanan berbasiskan browser / "lingkungan" browser.

5.1.1. Untuk skenario halaman palsu: Dalam hal ini http://firstsight.me/a/b/c.php merupakan URL yang dipersiapkan dengan menggunakan tag iframe untuk menarik halaman Tokopedia. URL ini pun telah "dilengkapi" dengan informasi palsu berupa penggantian kata sandi.

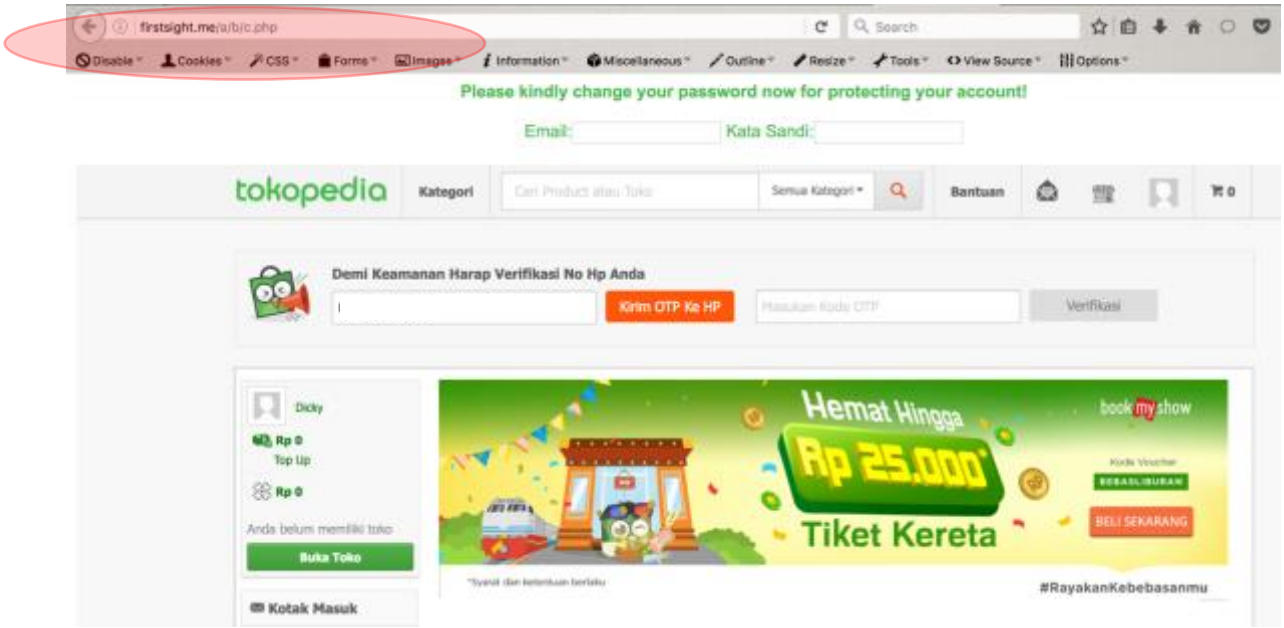


Figure 3 Halaman Palsu dengan Informasi Palsu pada http://firstsight.me/a/b/c.php

Setelah halaman palsu dipersiapkan, maka langkah berikutnya adalah mengubahnya menjadi base64 dengan parameter lengkap seperti yang telah diutarakan pada sub bab IV.

{"ld":"**http://firstsight.me/a/b/c.php**","ref":"https://tokopedia.com/","uuid":"ead3234b-37c9-4c0d-af82-6cce232ab0d6","theme":"default"}

Mengingat bahwa uuid tidak berpengaruh sedikitpun, maka Attacker cukup mengubah parameter "**id**" saja seperti yang tertuang dalam tulisan berwarna merah di atas.

Berikut ini merupakan value setelah diubah ke base64:

"eyJsZCI6Imh0dHA6Ly9maXJzdHNpZ2h0Lm1lL2EvYi9jLnBocCIsInJlZiI6Imh0dHBzOi8vdG9rb3BlZGlhLmNvbS8iLCJ1dWlkIjoiZWFkMzIzNGItMzdjOS00YzBkLWFmODItNmNjZTIzMmFiMGQ2IiwidGhlbWUiOiJkZWZhdWx0In0" → **Tanpa tanda kutip** dan **tanpa sama dengan.**

Adapun hasil akhirnya yaitu menjadi seperti ini:

https://accounts.tokopedia.com/authorize?response_type=code&client_id=1001&state=eyJsZCI6Imh0dHA6Ly9maXJzdHNpZ2h0Lm1lL2EvYi9jLnBocCIsInJlZiI6Imh0dHBzOi8vdG9rb3BlZGlhLmNvbS8iLCJ1dWlkIjoiZWFkMzIzNGItMzdjOS00YzBkLWFmODItNmNjZTIzMmFiMGQ2IiwidGhlbWUiOiJkZWZhdWx0In0&redirect_uri=https%3A%2F%2Faccounts.tokopedia.com%2Fappauth%2Fcode&p=https://www.tokopedia.com&contactus=&theme=default

5.1.2. Untuk skenario memaksa pengguna mengunduh suatu malware (contoh menggunakan aplikasi 7zip – bukan malware), maka URL di parameter id hanya tinggal diganti menuju ke halaman unduhan dari suatu program (sebagai contoh ke halaman http://www.7-zip.org/a/7z1602.exe).

Adapun hasil akhirnya yaitu menjadi seperti ini:

https://accounts.tokopedia.com/authorize?response_type=code&client_id=1001&state=eyJsZCI6Imh0dHA6Ly93d3cuNy16aXAub3JnL2EvN3oxNjAyLmV4ZSIsInJlZiI6Imh0dHBzOi8vdG9rb3BlZGlhLmNvbS8iLCJ1dWlkIjoiZWFkMzIzNGItMzdjOS00YzBkLWFmODItNmNjZTIzMmFiMGQ2IiwidGhlbWUiOiJkZWZhdWx0In0&redirect_uri=https%3A%2F%2Faccounts.tokopedia.com%2Fappauth%2Fcode&p=https://www.tokopedia.com&contactus=&theme=default

5.1.3. Untuk skenario browser / browser environment based exploitation, seorang pengguna hanya perlu dihadapkan pada suatu URL yang telah disisipkan suatu shellcode yang dapat digunakan untuk mengeksploitasi kerentanan pada browser ataupun "lingkungan" browser milik pengguna. Tentunya hal ini akan memerlukan tambahan informasi berupa versi browser yang digunakan oleh pengguna ataupun third party application seperti adobe flash player / jre.

5.2. Langkah kedua, setelah URL yang telah disisipkan dengan fake URL telah selesai, maka seorang Attacker hanya perlu mengirimkannya kepada korban yang dituju baik secara langsung maupun tidak langsung.

VI. ADDITIONAL INFORMATION

Untuk dapat memaksimalkan informasi yang disampaikan pada laporan ini, berikut ini terlampir beberapa kondisi tambahan yang perlu diperhatikan:

6.1. Mengingat bahwa kerentanan ini terkait Open URL Redirection, maka efeknya pun tidak berpengaruh terhadap versi browser yang digunakan. Akan tetapi bila diperlukan, pengujian ini dilakukan dengan browser Safari, Firefox, dan Chrome versi terbaru. Adapun versi yang digunakan adalah Version 9.1.1 (10601.6.17) untuk Safari, Version 52.0.2743.116 (64-bit) untuk Chrome, dan 48.0 untuk Firefox;

6.2. Berbeda pada report sebelumnya yang mengharuskan pengguna untuk tidak login terlebih dahulu, pada kasus ini, URL justru hanya berlaku untuk **pengguna yang sudah** melakukan login ke dalam aplikasi. Dalam hal ini, pengguna yang belum login ke dalam aplikasi tidak akan pernah dapat tereksekusi ke halaman yang dituju oleh Attacker. Hal ini tidak lain dikarenakan fitur redirect dari halaman login belum berjalan otomatis sehingga pengunjung diharuskan untuk kembali ke halaman admin.tokopedia.com untuk dapat menggunakan fitur "User Management";

6.3. Attacker harus memastikan bahwa value yang diubah ke base64 tidak memiliki karakter lain selain huruf dan angka. Dalam hal ini, parameter **id** yang rentan hanya dapat "menerima" karakter huruf dan angka saja. Bila ternyata ditambahkan karakter lain seperti tanda plus (+), maka aplikasi tidak akan membuat pengguna untuk berkunjung ke fake URL yang disisipkan;

6.4. PoC Video (Unlisted at Youtube): https://youtu.be/Vdt5a7ppnOc

6.5. Untuk keperluan PoC, maka Fake URL dari firstsight.me/a/b/c.php tidak dihapus terlebih dahulu.

VII. RECOMMENDATION

Dalam hal ini, tentunya terdapat beberapa rekomendasi yang dapat dipertimbangkan untuk menutupi kerentanan yang ada:

7.1. Memberikan penyaringan terhadap setiap URL yang di-input-kan baik secara tidak langsung maupun tidak langsung sehingga hanya dapat lari ke wilayah Tokopedia saja.

7.2. Melindungi value dengan enkripsi (bukan dengan encoding) sehingga seorang Attacker tidak akan dapat dengan mudah menebak konten yang ditampilkan oleh aplikasi (dalam hal ini, konten yang disajikan pada value "**state**" yang tertuang pada sub bab IV).

VIII. REFERENCES

8.1. https://www.owasp.org/index.php/Top_10_2013-A10-Unvalidated_Redirects_and_Forwards;

8.2. http://ezine.echo.or.id/issue30/008.txt