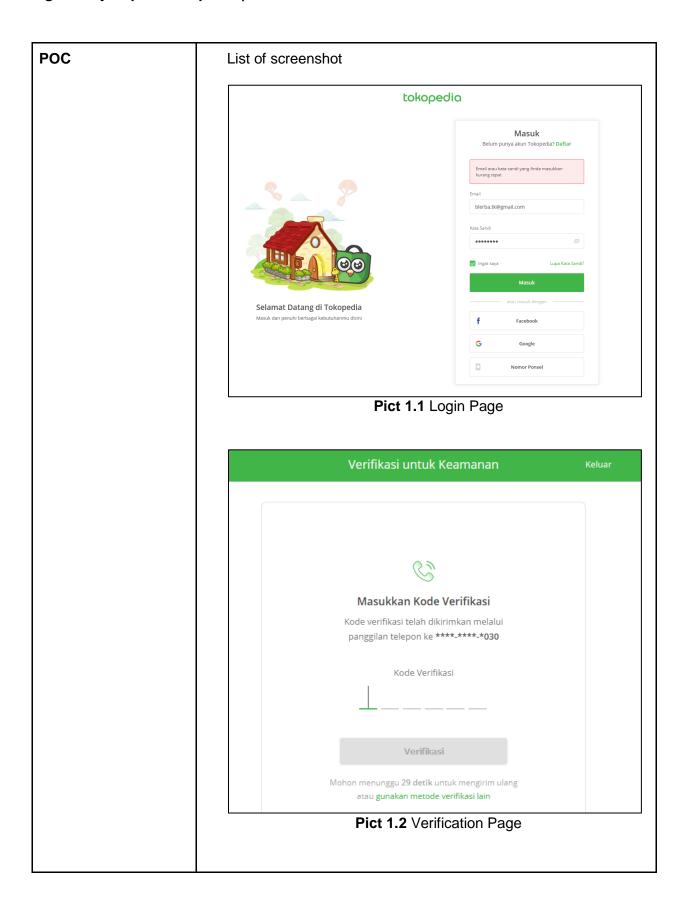


Information Disclosure of Sensitive Information on Verification Login Page

on 13 February 2019 by Muhammad Thomas Fadhila Yahya

Description	Information disclosure is when an application fails to properly protect sensitive information from parties that are not supposed to have access to such information in normal circumstances. These type of issues are not exploitable in most cases, but are considered as web application security issues because they allows attackers to gather information which can be used later in the attack lifecycle, in order to achieve more than they could if they didn't get
	access to such information.
Affected Endpoint	https://accounts.tokopedia.com/otp/c/page?d=Wed%2C+13+Feb+2019+11%3A11%3A19+%2B0700&h=h4YnAMzDb4zAVjThQXtGbxa2C7Hv80Fk4TAUXe%2BvGqk%3D&ld=https%3A%2F%2Faccounts.tokopedia.com%2Fotp%2Finterrupt%2Fsl&otp_type=13
Impact	 Steal user's sensitive information like name, phone number, email, registration date and birthday. Using sensitive information to do phishing to steal verification code.
Steps to Reproduce	 Login to Tokopedia account. (Pict 1.1) Tokopedia will redirect to Verification Page and there will two options such SMS Verification and Call Verification. Select one of verifications, try to intercept the connection. (Pict 1.2) In connection body parameter email and phone number are cover-up but there's interesting information in cookie connection (Pict 1.3) (Pict 1.4) Try to URL decode those information. (Pict 1.5) Evidently those information are user's sensitive information such as: name, phone number, email, registration date, and birthday. (Pict 1.5)



```
Host: accounts.tokopedial.com
User-Agent: Mozilla/S.0 (Windows NT 6.1; WOW64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en:q=0.5
                                                                                                                                                                                            Accept-Encoding; gzip, deflate
Referer: https://accounts.tokopedia.com/otp/c/page?d=Wed%2C+13+Feb+2019+11%3A26%3A12+%2B07004h=17EKdH1%2Bd0e5F0b9aH0RX
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
                                                                                                                                                                                            Content-Length: 113
                                                                                                                                                                                          Content-Length: 113
Connection: close
Connection: close
Connection: close
Contection: close
Contection
                                                                                                                                                                                               k=557766ca6101ac46b0113f8b0080e513&otp_type=13&msisdn=****-****-*030&email=b********$40g****.com&original_param=
                                                                                                                                                                                                                                                                                                                Pict 1.3 Connection Intercept
                                                                                                                                                                                                T

**prof/page7d=Tux12<-11-9-mb-2019-2013455/3413+12807004h=MaPGCNS7LMSV28co5VM02U74287mEqx1141sHx38amCfcv3544d=https%1342fv2faccounts.toRopedia.com/2fctp%2f

**tetruspxtFs1cotp_typ=*13 MTTf/.1

**tetruspxtFs1cotp_typ=*13 MTf/.1

**tetruspxt
                                                                                                                                                                                                                                                                                                   Pict 1.4 Information In Cookie
                                                                                                                                                                                             gender verified":"Male","name":"Johny Ago","first name":"Johny"
                                                                                                                                                                                            "Johny","email":"blerba.tk@gmail.com","mobile":"085380502030",
                                                                                                                                                                                            Pict 1.5 Sensitive Information Disclosure
Remediation
                                                                                                                                                                                          Whenever sensitive data is stored, ensure that it is properly
                                                                                                                                                                                          protected using strong encryption.
References
                                                                                                                                                                                          CWE-200: Information Exposure [cwe.mitre.org]
                                                                                                                                                                1.
                                                                                                                                                                                          Information Leakage [projects.webappsec.org]
```