



# **Information Disclosure of Sensitive Information on Verification Login Page**

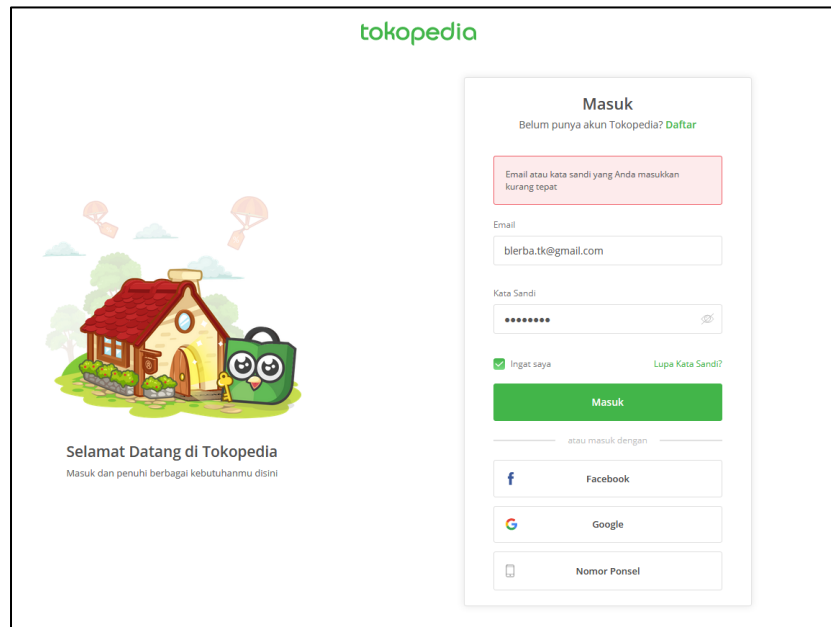
**on 13 February 2019**

**by Muhammad Thomas Fadhila Yahya**

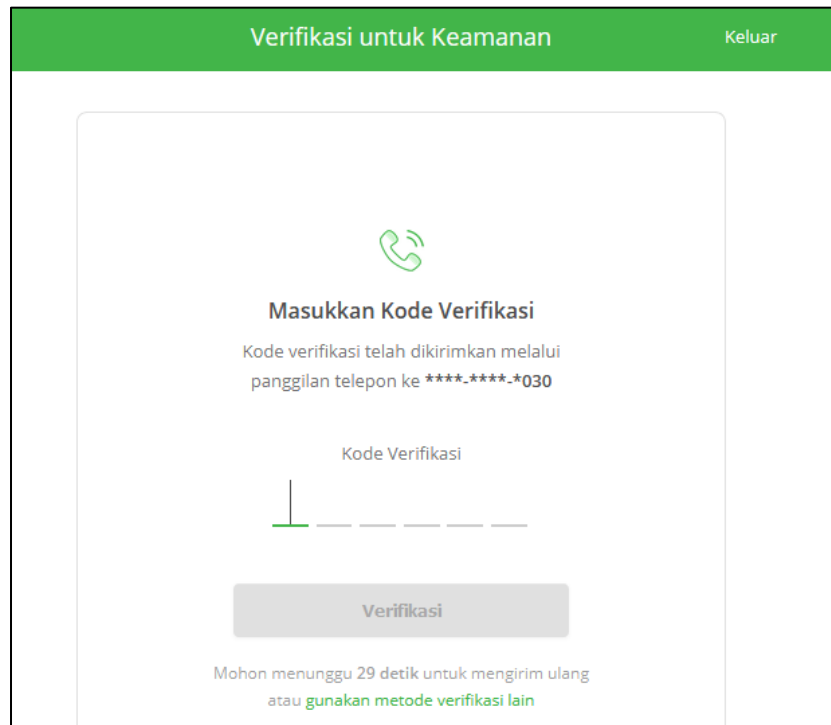
<b>Description</b>	<p><b>Information disclosure</b> is when an application fails to properly protect sensitive information from parties that are not supposed to have access to such information in normal circumstances.</p> <p>These type of issues are not exploitable in most cases, but are considered as 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.</p>
<b>Affected Endpoint</b>	<p><a href="https://accounts.tokopedia.com/otp/c/page?d=Wed%2C+13+Feb+2019+11%3A11%3A19+%2B0700&amp;h=h4YnAMzDb4zAVjThQXtGbx2C7Hv80Fk4TAUXe%2BvGqk%3D&amp;ld=https%3A%2F%2Faccounts.tokopedia.com%2Fotp%2Finterrupt%2Fsl&amp;otp_type=13">https://accounts.tokopedia.com/otp/c/page?d=Wed%2C+13+Feb+2019+11%3A11%3A19+%2B0700&amp;h=h4YnAMzDb4zAVjThQXtGbx2C7Hv80Fk4TAUXe%2BvGqk%3D&amp;ld=https%3A%2F%2Faccounts.tokopedia.com%2Fotp%2Finterrupt%2Fsl&amp;otp_type=13</a></p>
<b>Impact</b>	<ol style="list-style-type: none"> <li>1. Steal user's sensitive information like name, phone number, email, registration date and birthday.</li> <li>2. Using sensitive information to do phishing to steal verification code.</li> </ol>
<b>Steps to Reproduce</b>	<ol style="list-style-type: none"> <li>1. Login to Tokopedia account. <b>(Pict 1.1)</b></li> <li>2. Tokopedia will redirect to Verification Page and there will two options such SMS Verification and Call Verification.</li> <li>3. Select one of verifications, try to intercept the connection. <b>(Pict 1.2)</b></li> <li>4. In connection body parameter email and phone number are cover-up but there's interesting information in cookie connection <b>(Pict 1.3) (Pict 1.4)</b></li> <li>5. Try to URL decode those information. <b>(Pict 1.5)</b></li> <li>6. Evidently those information are user's sensitive information such as: name, phone number, email, registration date, and birthday. <b>(Pict 1.5)</b></li> </ol>

POC

List of screenshot



Pict 1.1 Login Page



Pict 1.2 Verification Page

## Bug Bounty Report Tokopedia | 4

	<div data-bbox="594 203 1424 550"> </div> <p><b>Pict 1.3 Connection Intercept</b></p> <div data-bbox="594 659 1424 982"> </div> <p><b>Pict 1.4 Information in Cookie</b></p> <div data-bbox="594 1089 1424 1285"> </div> <p><b>Pict 1.5 Session Information Disclosure</b></p> <div data-bbox="207 1371 529 1495"> <p><b>Remediation</b></p> </div> <div data-bbox="529 1371 1429 1495"> <ol style="list-style-type: none"> <li>1. Whenever sensitive data is stored, ensure that it is properly protected using strong encryption.</li> </ol> </div> <div data-bbox="207 1495 529 1608"> <p><b>References</b></p> </div> <div data-bbox="529 1495 1429 1608"> <ol style="list-style-type: none"> <li>1. <a href="#">CWE-200: Information Exposure</a> [cwe.mitre.org]</li> <li>2. <a href="#">Information Leakage</a> [projects.webappsec.org]</li> </ol> </div>
--	---