Document Title:
===========
PayPal Inc Bug Bounty #115 - Identity Check Restriction Bypass Vulnerability

References (Source):
===============
http://www.vulnerability-lab.com/get_content.php?id=1486

Video: http://www.vulnerability-lab.com/get_content.php?id=1485

Release Date:
==========
2015-05-02

Vulnerability Laboratory ID (VL-ID):
===========================
1486

Common Vulnerability Scoring System:
===========================
6.1

Abstract Advisory Information:
=====================
The Vulnerability Laboratory Core Research Team discovered a restriction filter bypass in the official PayPal Inc Mobile API for Apple iOS.

Vulnerability Disclosure Timeline:
========================
2015-04-30: Researcher Notification & Coordination (Milan A Solanki - Safehacking4mas)
2015-05-02: Vendor Notification (PayPal Inc - Security & Bug Bounty Team)
2015-00-00: Vendor Response/Feedback (PayPal Inc - Security & Bug Bounty Team)
2015-00-00: Vendor Fix/Patch (PayPal Inc - Developer Team)
2015-00-00: Public Disclosure (Vulnerability Laboratory)

Discovery Status:
=============
Unpublished

Affected Product(s):
===============
PayPal Inc
Product: Mobile Web Application (API) 2015 Q2

Exploitation Technique:
=================
Remote

Severity Level:
===========
High

Technical Details & Description:
========================

By processing multiple login we saw a bug in the mobile app api next to the identity check. Normally an user account logs in and if the account is restricted by several requests a stable form popup to call paypal or write a ticket mail. By processing to request the form multiple times with an existing account (x01445@gmail.com:chaos666) we was able to bypass the auth verification check to approve the account owner with compromised cookies.

The api loads the website context and the user is able to include inside of the identity check with a browser engine the own user account. Even if the account is restricted the user can access via mobile api with the exisiting cookies.

The security identity check to approve has been included to verify that no user logs in to unauthorized- or restricted accounts. In that case we demonstrate in the video how we bypass the validation and how it should look normally with a final request.

Proof of Concept (PoC):
==================

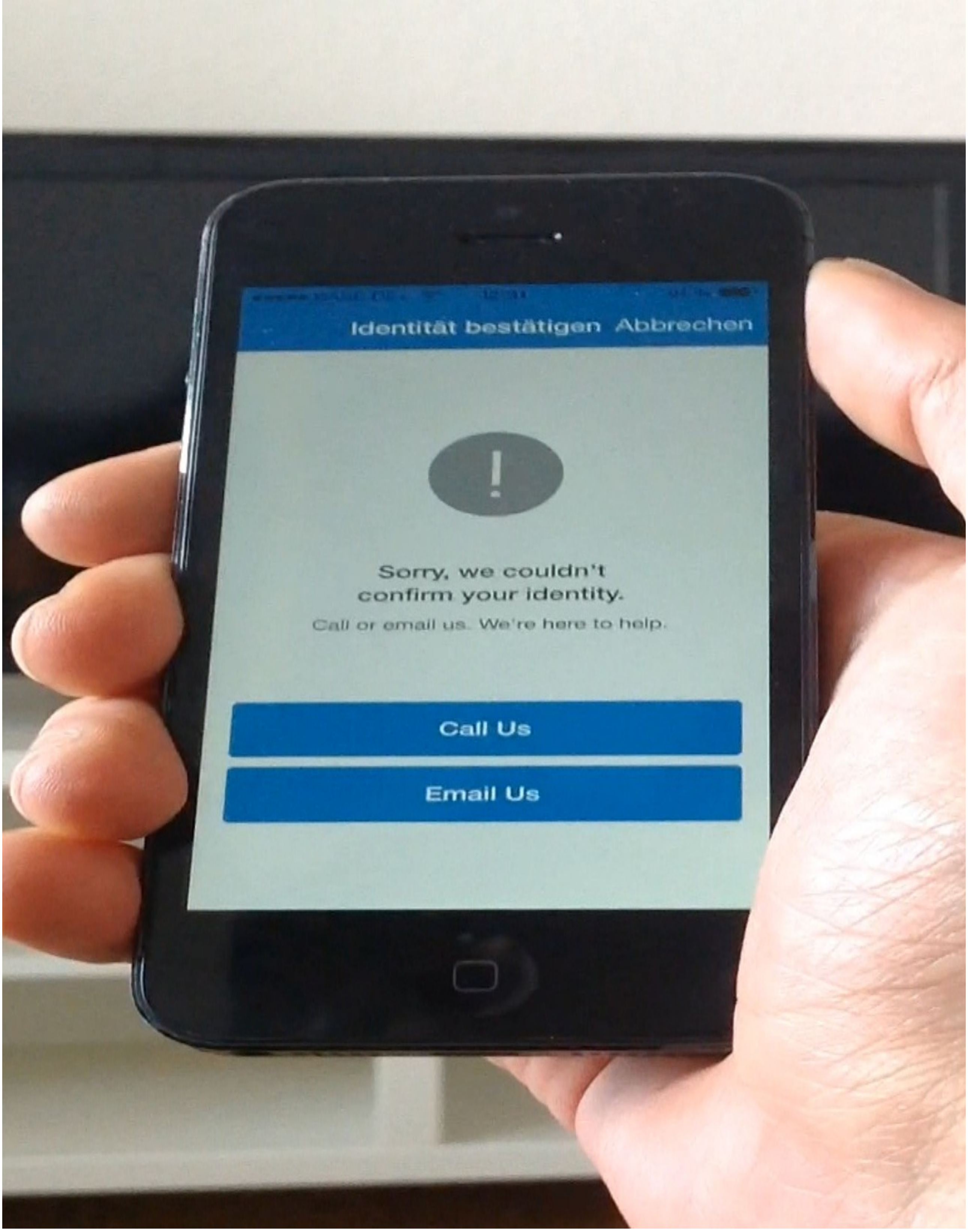
The security vulnerability can be exploited by remote attackers with low privileged application user account and without user interaction. For security demonstration or to reproduce the security vulnerability follow the provided information and steps below to continue.

The video demonstrates a flaw inside of the mobile app api that redirects an user account with restricted credentials inside of the app to the original website source. The cookies authorize the account to login even if the regular portal denies it because of the identity approval. The issue is not connected to the 6 month ago reported restriction bypass and reveals a signifanct risk to user accounts because of fraud and account theft.

The video deomstrates a security bug in the official paypal mobile ios api. The bug allows to bypas the account restriction by usage of a validation flaw inside of the service. The identity check approves restricted user accounts. In the first released issue we demonstrated how to bypass the auth. In case of the new issue the researcher demonstrates how to bypass the identity check that approves the paypal account. The attacker bypass the validation by multiple requests and dumps the real website for login inside the app with cookies and co.

Note: We have already verified that the issue is exploitable in the mobile android app of paypal inc.

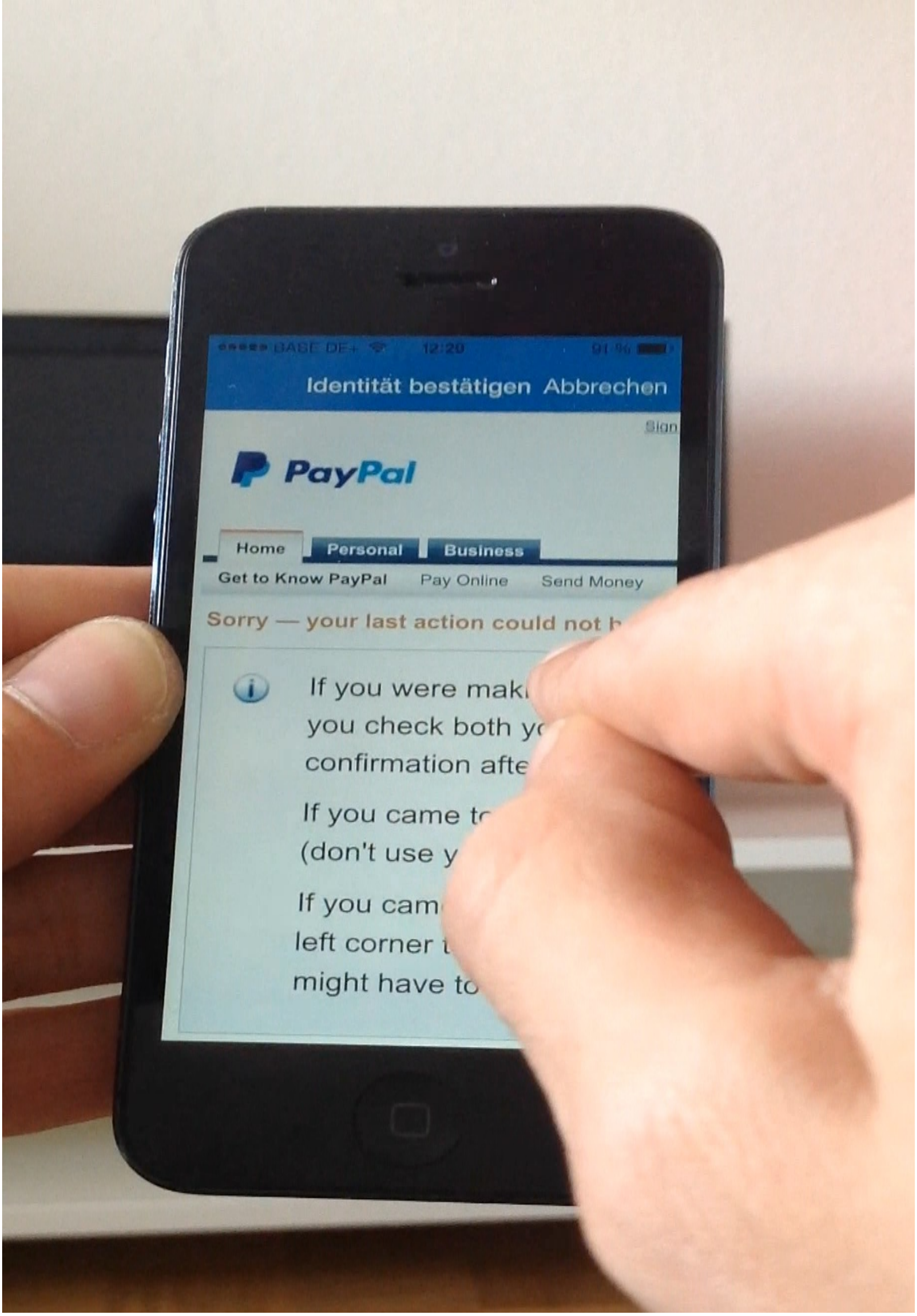
Pictures Description: PoC
The first image shows how it looks like when the account is being blocked. The user is not anymore able to do anything then to call or write a email to solve the problem. The first image shows how it looks like when the account is being blocked. The user is not anymore able to do anything then to call or write a email to solve the problem.



Sorry, we couldn't confirm your identity.

Call or email us. We're here to help.

After usage of a valid cookie that is not expired by storing in the device we was able to include it twice. So the results was that inside the identity check the website was loaded by a redirect.



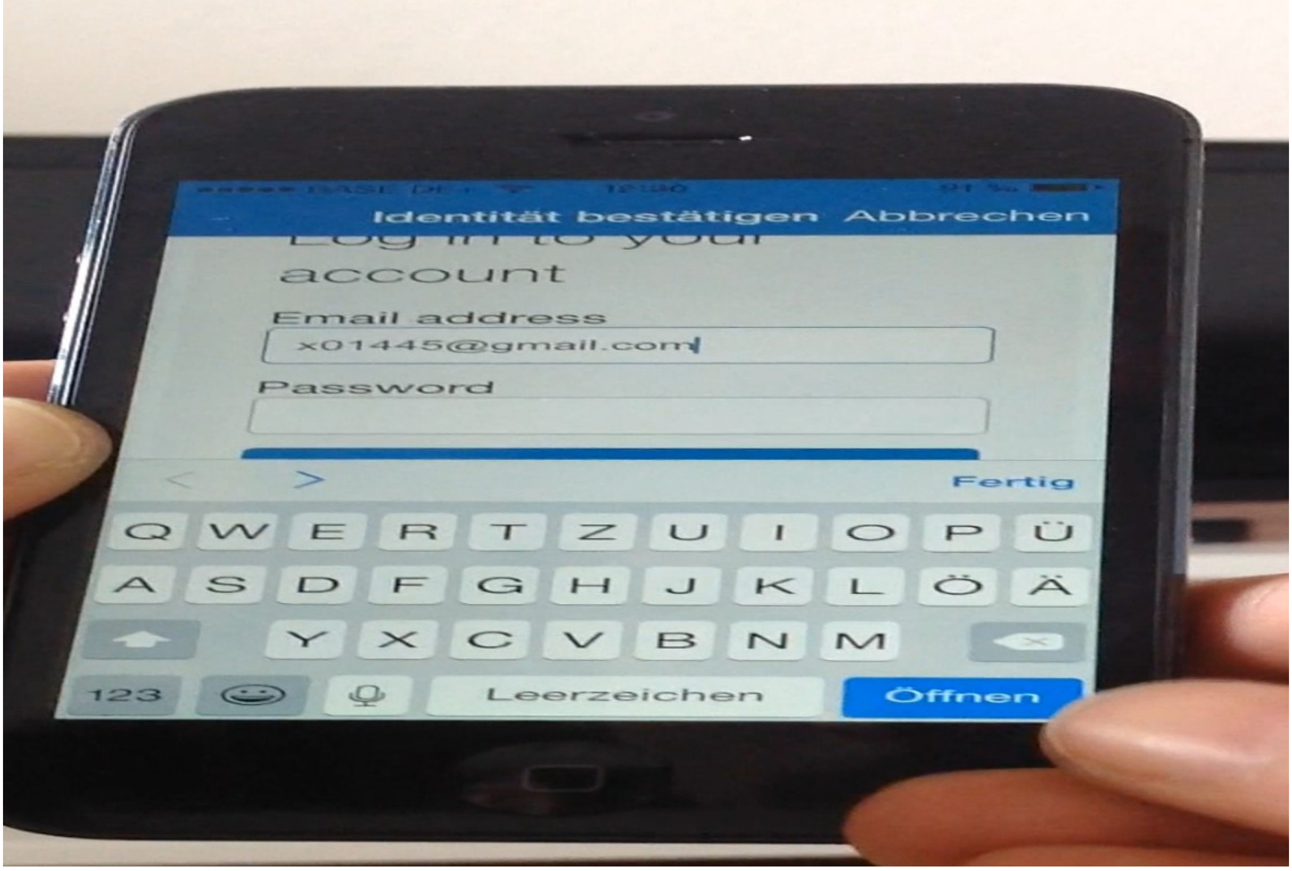
Sorry — your last action could not h

If you were mak
you check both y
confirmation afte

If you came t
(don't use y

If you cam
left corner t
might have to

After the load to the website in the inner app context we tried to login to the paypal online-service.



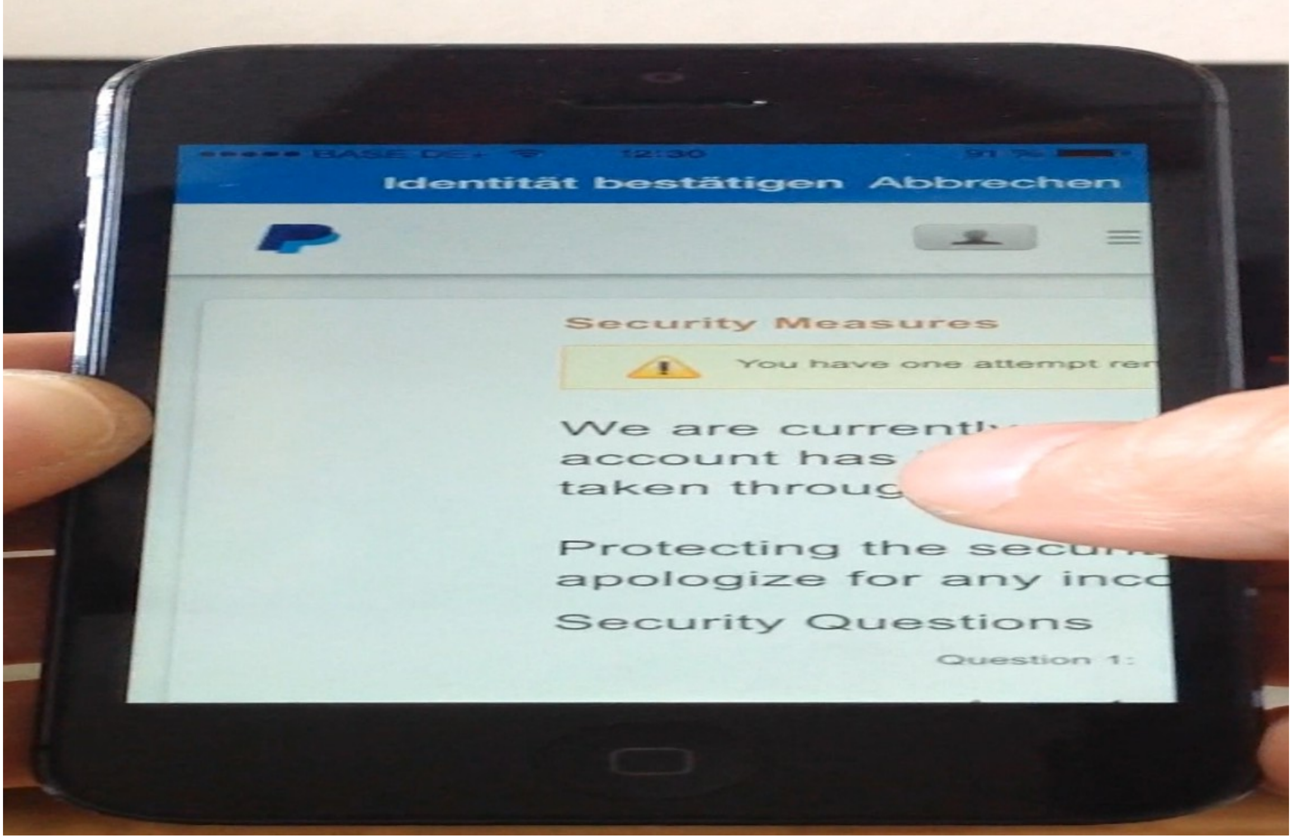
Log in to your account

Email address

x01445@gmail.com

Password

With the cookies in the app and the inner context load of the website we was able to successful login to the paypal website with the blocked credentials.



Security Measures

You have one attempt re

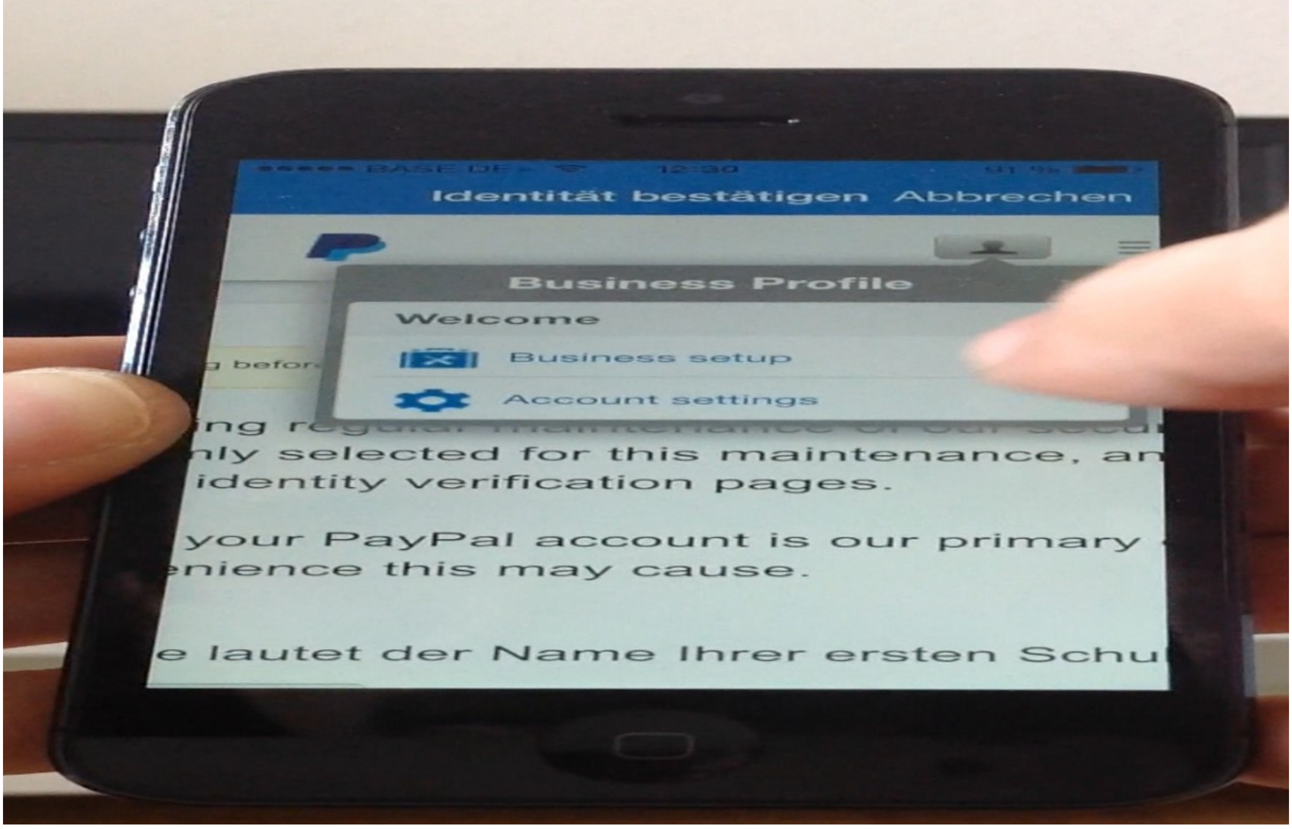
We are currentl
account has
taken throug

Protecting the secu
apologize for any inco

Security Questions

Question 1:

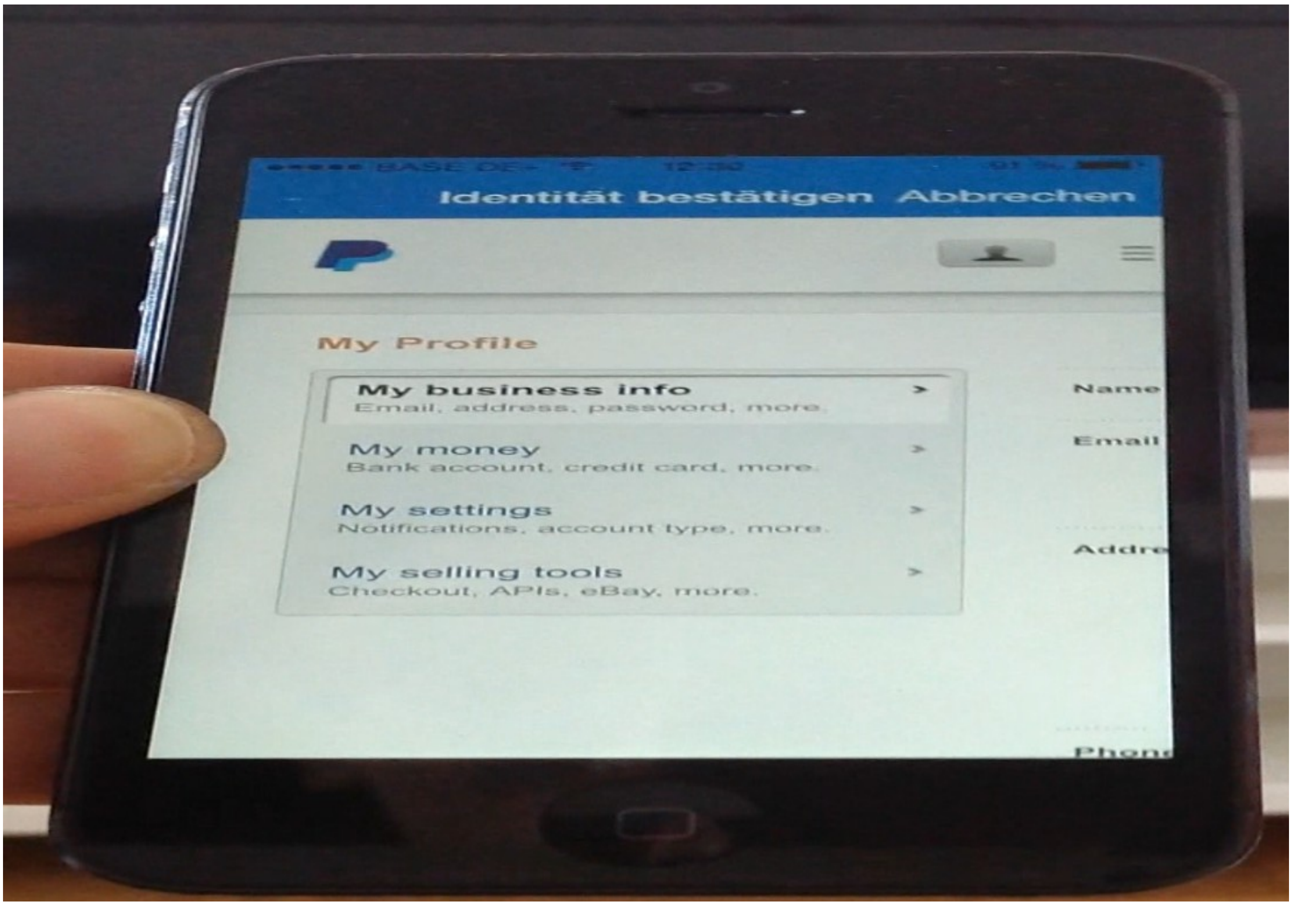
We approved what functions are available and can be changed in that status and decided to use the currency. We changed the currency of € in candian dollar and saved it with the compromised cookie via mobile app api.



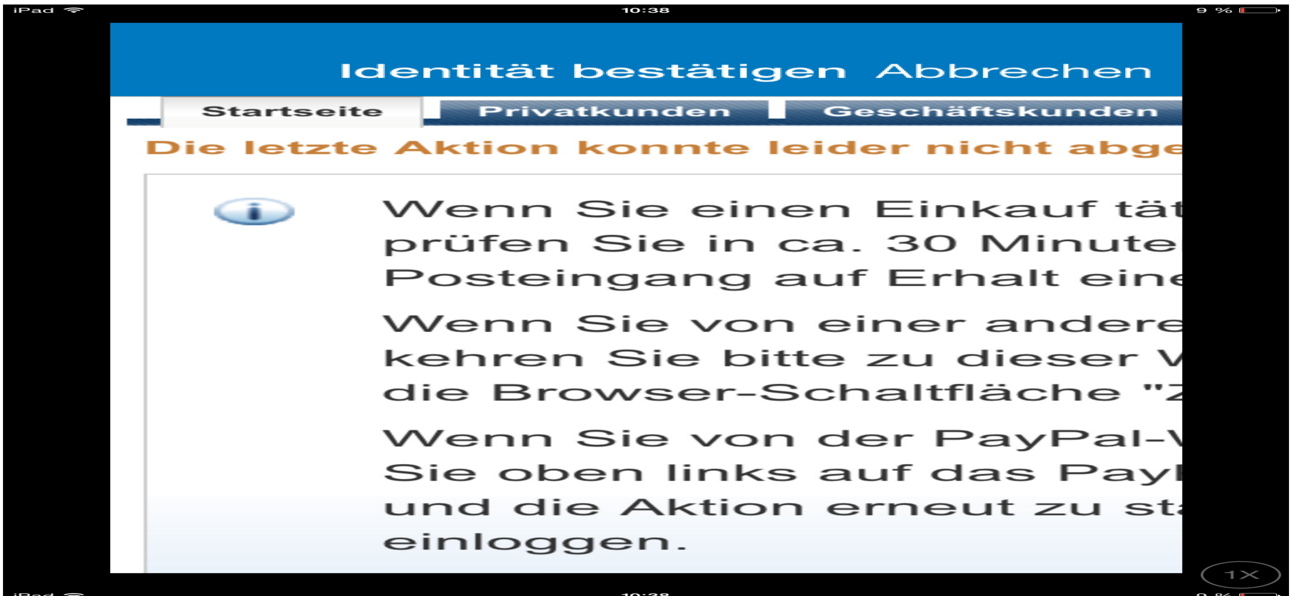
ing r
nly selected for this maintenance, an
identity verification pages.

your PayPal account is our primary
nience this may cause.

e lautet der Name Ihrer ersten Schu


BASE DE 12:30 91 %
Identität bestätigen Abbrechen
My Profile
My business info
Email, address, password, more.
My money
Bank account, credit card, more.
My settings
Notifications, account type, more.
My selling tools
Checkout, APIs, eBay, more.
Name
Email
Addre
Phon

This is how it looks like to login with stored cookies through the ipad mobile paypal app.

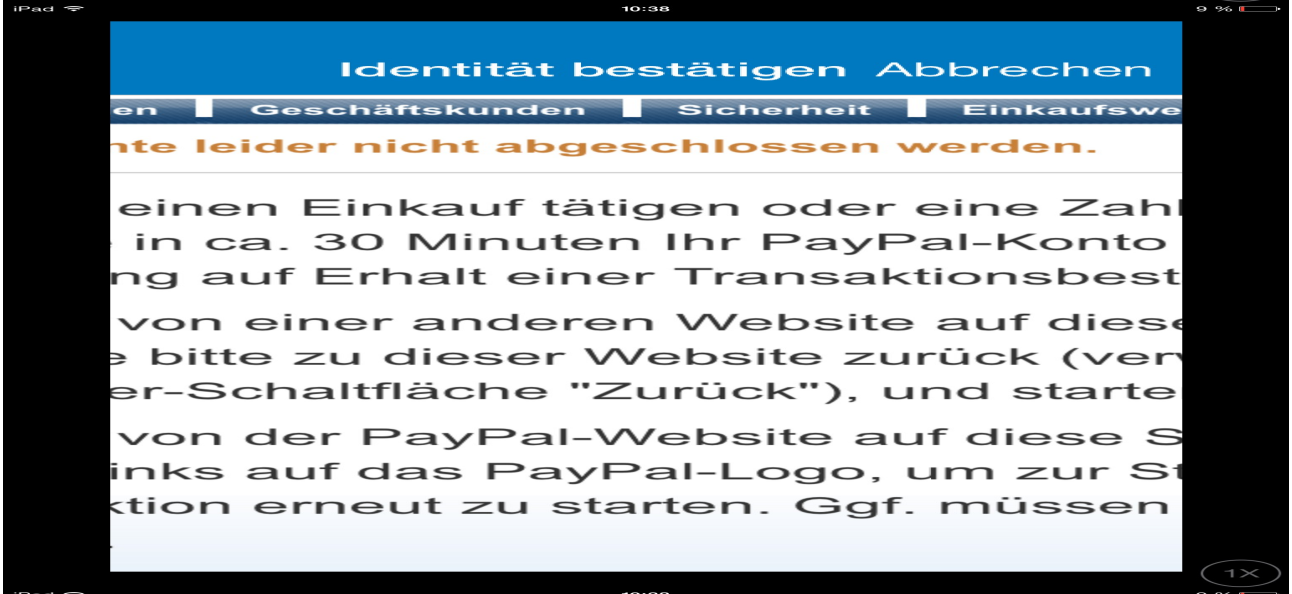


Die letzte Aktion konnte leider nicht abge

Wenn Sie einen Einkauf tät
prüfen Sie in ca. 30 Minute
Posteingang auf Erhalt eine

Wenn Sie von einer andere
kehren Sie bitte zu dieser V
die Browser-Schaltfläche "Z

Wenn Sie von der PayPal-V
Sie oben links auf das Payl
und die Aktion erneut zu sta
einloggen.

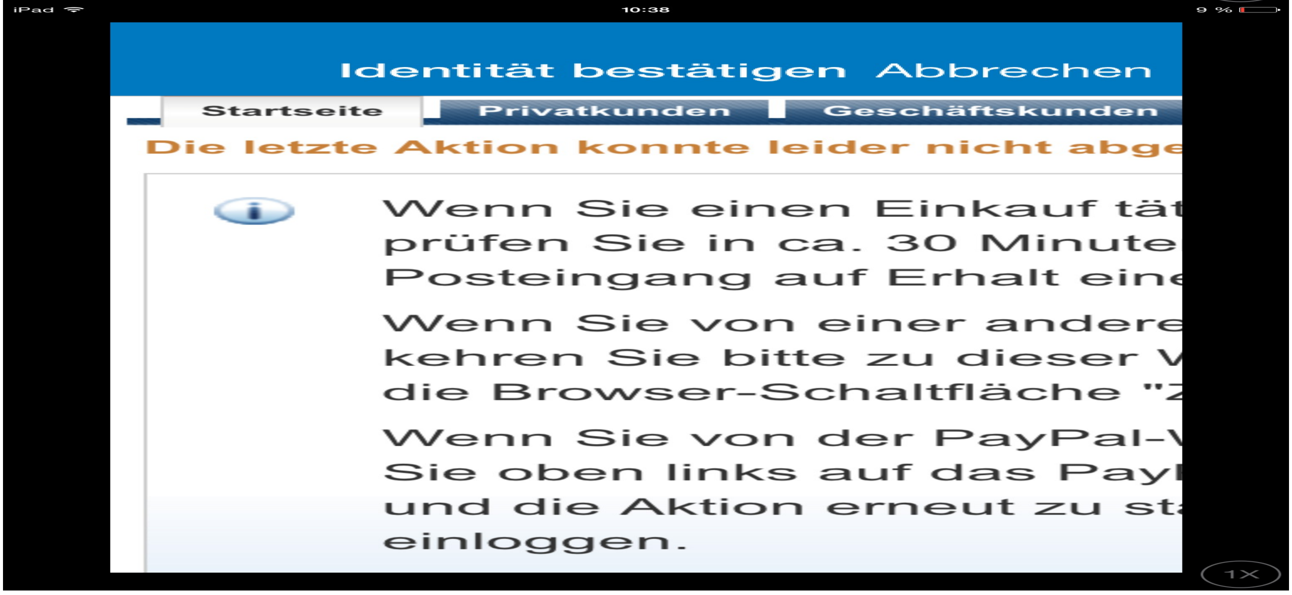


nte leider nicht abgeschlossen werden.

einen Einkauf tätigen oder eine Zahl
in ca. 30 Minuten Ihr PayPal-Konto
ng auf Erhalt einer Transaktionsbest

von einer anderen Website auf diese
bitte zu dieser Website zurück (ver
er-Schaltfläche "Zurück"), und starte

von der PayPal-Website auf diese S
inks auf das PayPal-Logo, um zur St
ktion erneut zu starten. Ggf. müssen



Die letzte Aktion konnte leider nicht abge

Wenn Sie einen Einkauf tät
prüfen Sie in ca. 30 Minute
Posteingang auf Erhalt eine

Wenn Sie von einer andere
kehren Sie bitte zu dieser V
die Browser-Schaltfläche "Z

Wenn Sie von der PayPal-V
Sie oben links auf das Payl
und die Aktion erneut zu sta
einloggen.

Solution - Fix & Patch:

=================

The vulnerability can be patched by a secure redirect of a multi requesting source to the main mobile api. Disallow to load the website context with the app cookies after a successful login through a restricted account to prevent. Disallow the usage of stored cookies for the approval or auth to prevent session restriction and account access auth bypass exploitation.

Security Risk:

==========

The security risk of the remote mobile api identity approval check bypass is estimated as high. (CVSS 6.1)

Credits & Authors:

==============

Vulnerability Laboratory [Research Team] - Benjamin Kunz Mejri (admin@vulnerability-lab.com or admin@evolution-sec.com)