Chorizo major project

Bug Bounty

Old Session Does Not Expires After Password Change

Team Members:

E kuralamudhan

Peddireddy M Sai Lalith Aditya

Harsimar preet

Manne Esha Sai Priya

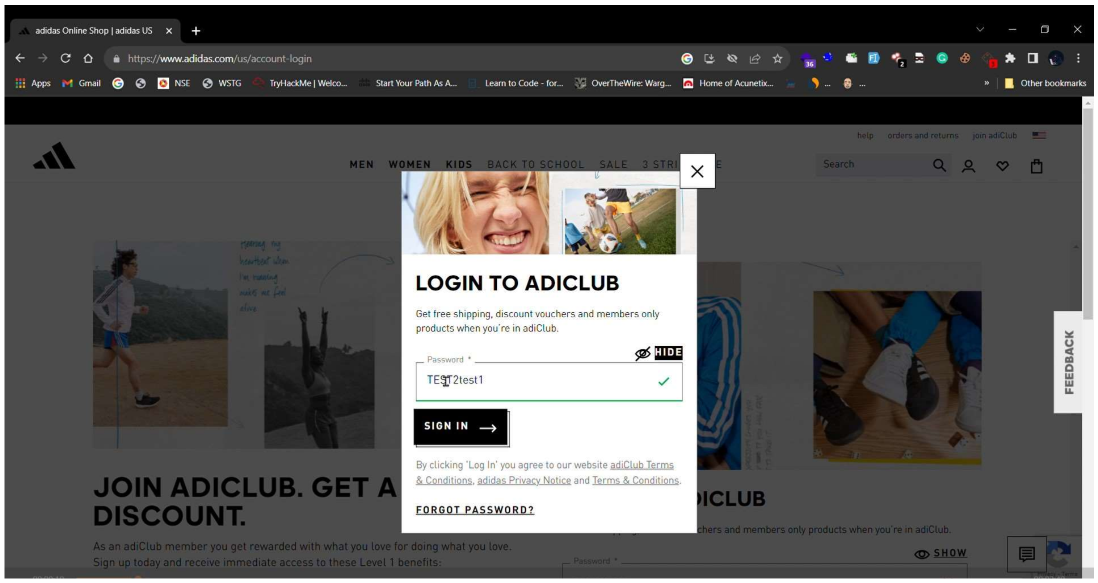
jagadish

Bug:

While conducting my research I discovered that the application failed to invalidate the session after the password change. In this scenario changing the password doesn't destroy the other sessions which are logged in with old passwords.

Steps to reproduce:

Login with the same account in Chrome and Firefox Simultaneously using the URL: https://www.adidas.com/us/men


adidas Online Shop | adidas US
https://www.adidas.com/us/account-login
MEN WOMEN KIDS BACK TO SCHOOL SALE
help orders and returns join adiClub
Search
FEEDBACK
HIDE
SIGN IN
SHOW

LOGIN TO ADICLUB

Get free shipping, discount vouchers and members only products when you're in adiClub.

Password *

TEST2test1

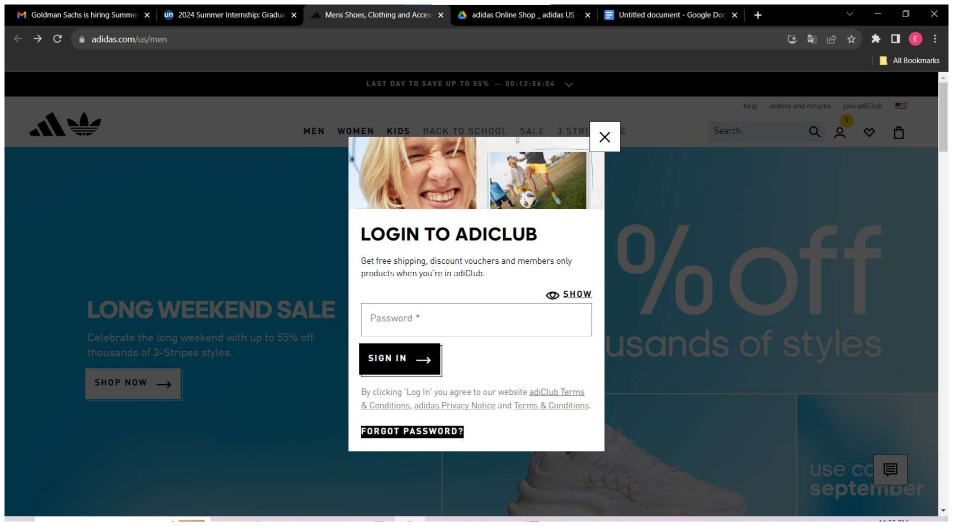
By clicking 'Log In' you agree to our website adiClub Terms & Conditions, adidas Privacy Notice and Terms & Conditions.

FORGOT PASSWORD?

JOIN ADICLUB. GET A DISCOUNT.

As an adiClub member you get rewarded with what you love for doing what you love. Sign up today and receive immediate access to these Level 1 benefits:

Change the pass in Chrome Browser by clicking on the forget password using the URL: https://www.adidas.com/us/men


Goldman Sachs is hiring Summer
2024 Summer Internship: Gradu
Mens Shoes, Clothing and Acces
adidas Online Shop _ adidas US
Untitled document - Google Doc
adidas.com/us/men
All Bookmarks
LAST DAY TO SAVE UP TO 55% — 00:12:56:54
help
orders and returns
join adiClub
MEN
WOMEN
KIDS
BACK TO SCHOOL
SALE
Search
LONG WEEKEND SALE
Celebrate the long weekend with up to 55% off thousands of 3-Stripes styles.
SHOP NOW
% off
usands of styles

LOGIN TO ADICLUB

Get free shipping, discount vouchers and members only products when you're in adiClub.

SHOW

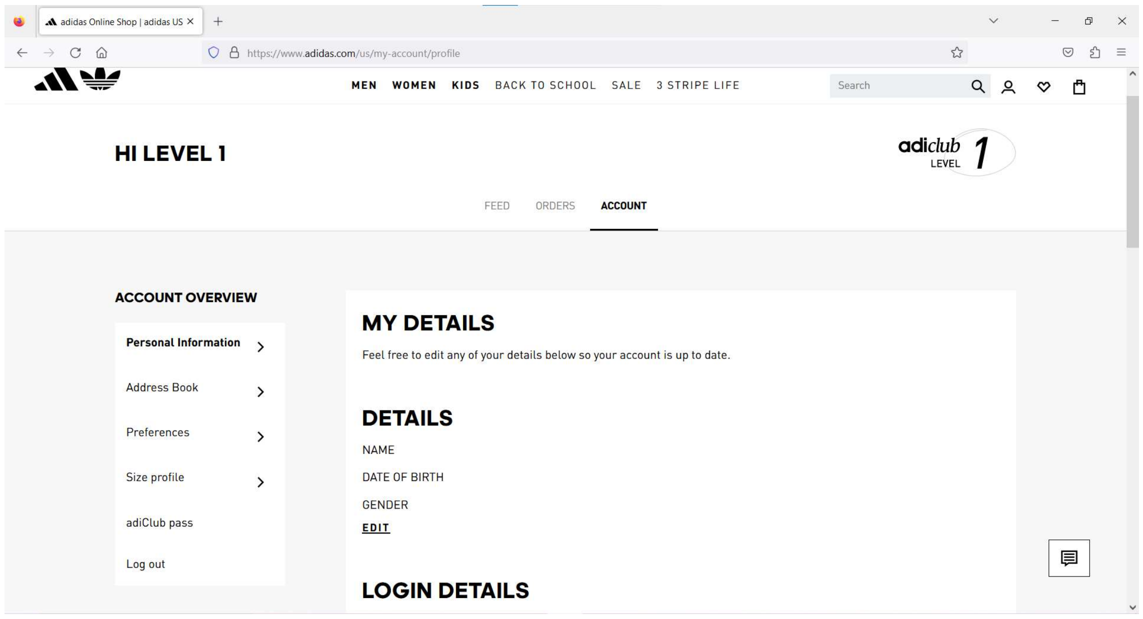
Password *

SIGN IN

By clicking 'Log In' you agree to our website adiClub Terms & Conditions, adidas Privacy Notice and Terms & Conditions.

FORGOT PASSWORD?

Go to firefox and Update any information, the information will be updated.



HI LEVEL 1

ACCOUNT OVERVIEW

- Personal Information
- Address Book
- Preferences
- Size profile
- adiClub pass
- Log out

MY DETAILS

Feel free to edit any of your details below so your account is up to date.

DETAILS

NAME

DATE OF BIRTH

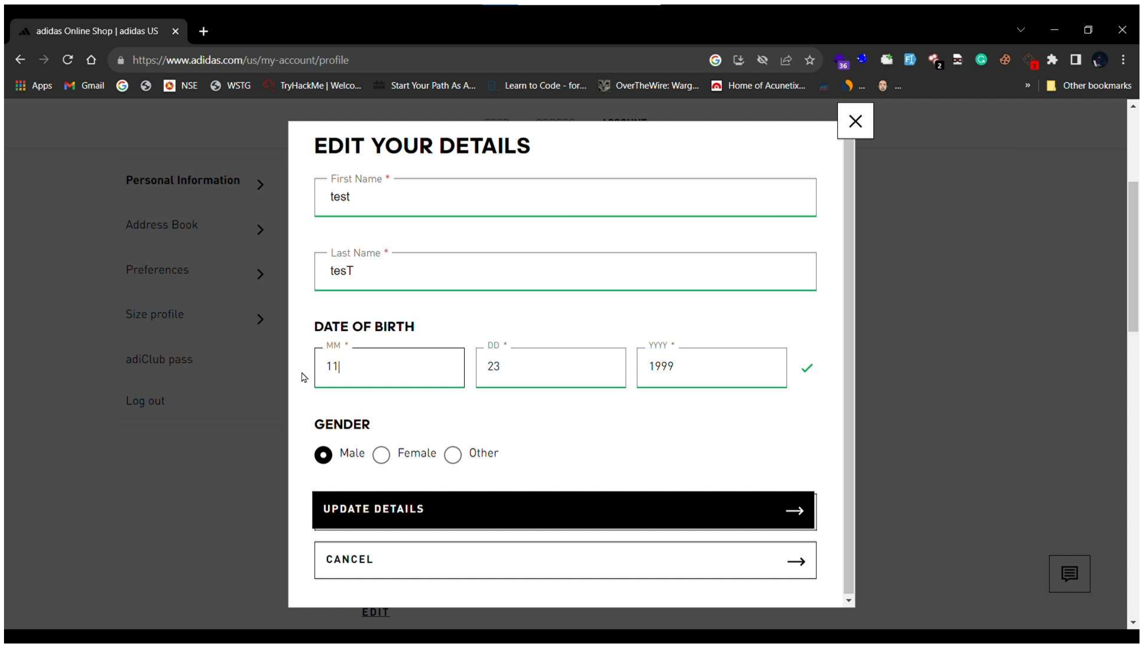
GENDER

EDIT

LOGIN DETAILS

Impact

The attacker can reuse the same cookies to login again without the user credentials.



EDIT YOUR DETAILS

First Name *	test
Last Name *	tesT

DATE OF BIRTH

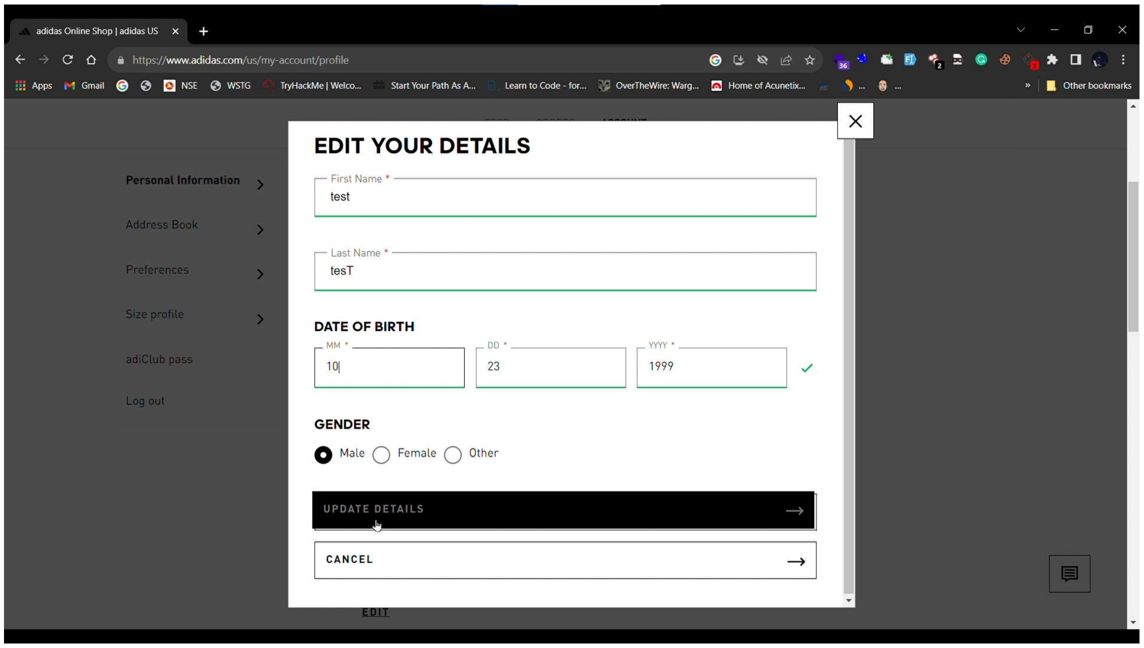
MM *	DD *	YYYY *
11	23	1999

GENDER

[✓ Male] Female Other

UPDATE DETAILS

CANCEL



EDIT YOUR DETAILS

First Name *	test
Last Name *	tesT

DATE OF BIRTH

MM *	DD *	YYYY *
10	23	1999

GENDER

[✓ Male] Female Other

UPDATE DETAILS

CANCEL

Mitigation:

Session Expiration Policies:

Implement Session Expiration: Configure your application to automatically log users out after a certain period of inactivity. This should be a relatively short timeframe, such as 15-30 minutes of inactivity.

Logout on Password Change: Whenever a user changes their password, log them out of all active sessions immediately.

Token Rotation:

Use Session Tokens: If your application relies on session tokens, make sure that these tokens are rotated regularly. When a password change occurs, invalidate all existing tokens associated with the user and issue new ones.

Implement Short-lived Tokens: Session tokens should have a short lifespan, typically limited to the duration of a single session or a few minutes. Avoid using long-lived tokens that could persist for an extended period.

Clear User Sessions:

On Password Change: When a user changes their password, invalidate all their existing sessions immediately. This can be done by revoking the session tokens or cookies associated with the user.

Session Management:

Unique Session Identifiers: Ensure that each session has a unique identifier tied to the user's account. This identifier should be changed whenever the user changes their password.

Centralized Session Management: Use a centralized session management system to keep track of active sessions and allow for easy revocation when needed.

Security Testing:

Regular Security Audits: Periodically audit your application's security, including session management. Look for vulnerabilities and test whether old sessions persist after a password change.

User Education:

User Notifications: Inform users about the session expiration and password change policies in place. Clearly communicate that a password change will log them out of all active sessions.

Logging and Monitoring:

Session Activity Logging: Keep detailed logs of session activity, including login, logouts, and password changes. Monitor these logs for any unusual or unauthorized activity.

Two-Factor Authentication (2FA):

Encourage or Require 2FA: Implementing 2FA adds an extra layer of security, making it more difficult for unauthorized users to access accounts even if old sessions persist.

Regular Updates:

Keep Software Up to Date: Ensure that your application's software, libraries, and frameworks are regularly updated to address security vulnerabilities.