Unauthenticated Resume Exposure in CodeAstro Online Job Portal (PHP MySQL)

Details

- **Vendor:** CodeAstro
- **Product:** Online Job Portal Project in PHP MySQL
- **Version:** 1.0
- **Vulnerability Type:** Improper Access Control / Information Disclosure
- **CWE:** CWE-284, CWE-200, CWE-548
- **Affected Endpoint:** /users/user-cvs/
- **Impact:** Unauthenticated access to all user resumes

Description

The application stores user resumes in a publicly accessible directory (`/users/user-cvs/`) without enforcing authentication or authorization checks.

An unauthenticated attacker can directly access and download any user's resume by requesting the file URL.

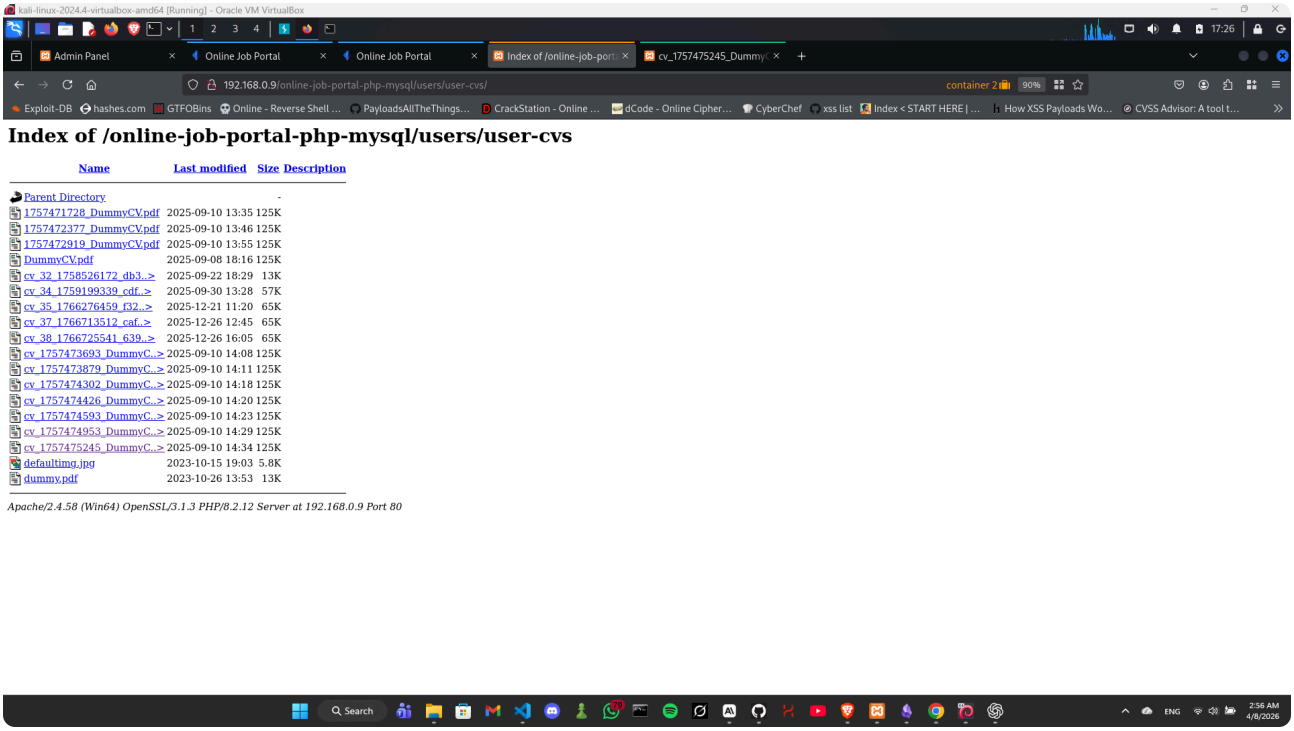
Additionally, directory listing is enabled on this directory, allowing attackers to enumerate all uploaded resumes without needing to guess filenames.

Proof of Concept

Step 1: Access Directory Listing

GET /online-job-portal-php-mysql/users/user-cvs/ HTTP/1.1 Host: target

Result:
A list of all uploaded resume files is displayed.



Step 2: Download a Resume Without Authentication

GET /online-job-portal-php-mysql/users/user-cvs/cv_1757475245_DummyCV.pdf HTTP/1.1 Host: target

---

Step 3: No Authentication Required

- Request works without login
- No session cookies required

- Any user or attacker can access files directly

Impact

An attacker can access and download all user resumes, which may contain sensitive personal information such as:

- Full names
- Email addresses
- Phone numbers
- Work experience

This can lead to privacy violations, data harvesting, and potential identity theft.

Vulnerable Code (Conceptual)

The application directly exposes files from a public directory without validating user permissions before access.

Recommendation

- Restrict access to the `/users/user-cvs/` directory
- Disable directory listing on the server
- Implement proper authentication and authorization checks before serving files
- Store sensitive files outside the web root and serve them via controlled endpoints

---

Author

- Imad Alvi

References

https://codeastro.com/online-job-portal-project-in-php-mysql-with-source-code/

Releases

No releases published

Packages

No packages published

Contributors 1

Xmyronn imad alvi