New issue

projectworlds Online Time Table Generator Portal-Source code /admin/add_student.php Unrestricted Upload to Getshell #11

Open

ydnd opened 3 weeks ago

projectworlds Online Time Table Generator Portal-Source code /admin/add_student.php Unrestricted Upload to Getshell

NAME OF AFFECTED PRODUCT(S)

- projectworlds Online Time Table Generator Portal-Source code

Vendor Homepage

- https://projectworlds.in/online-time-table-generator-php-mysql/

AFFECTED AND/OR FIXED VERSION(S)

- Affected Version: Current release (as of 2025-03-14)
- Fixed Version: Not patched as of vulnerability disclosure

Submitter

- IEeee

Vulnerable File

- /admin/add_student.php

Software Link

- https://projectworlds.in/wp-content/uploads/2023/04/timetable.zip

PROBLEM TYPE

- CWE-434: Unrestricted Upload of File with Dangerous Type

Vulnerability Type

- Remote Code Execution via Unrestricted File Upload

Root Cause

- The file upload functionality in "/admin/add_student.php" lacks proper validation of user-supplied files. Attackers can upload malicious scripts (php) due to missing file type checks and extension filtering. The server executes these files in the web-accessible upload directory, leading to full system compromise.

Impact

- Malware Distribution
- Remote Code Execution (RCE)
- Data Breach
- Denial of Service (DoS)
- Web Shell Installation
- Bypassing Security Controls
- Reputation Damage

DESCRIPTION

- The portal's file upload module fails to validate file types and extensions. By crafting a malicious file (e.g., "shell.php") and submitting it via the upload form, attackers can bypass security controls. Add a new student information with an email address of jack@gmail.com and submit the 1.php file with the following contents: . The server stores the file in "student/image/jack@gmail.com" without sanitization, allowing remote code execution via HTTP requests to the uploaded file.

- parameter '$eid' -> email

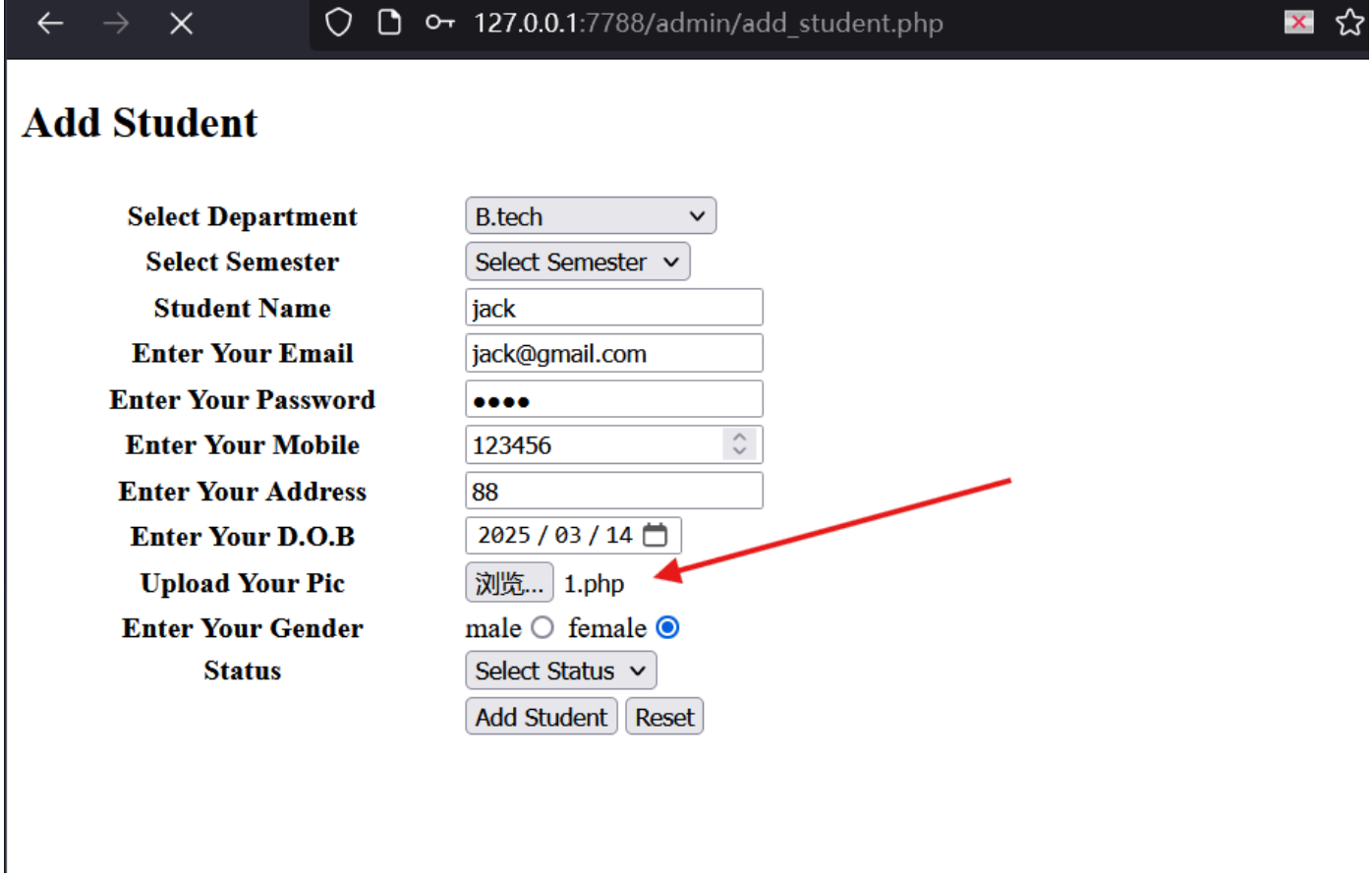
```
mkdir("../student/image/$eid");
     move_uploaded_file($_FILES['pic']['tmp_name'],"../student/image/$eid/".$_FILES['pic']
['name']);
```

Vulnerability Details and POC

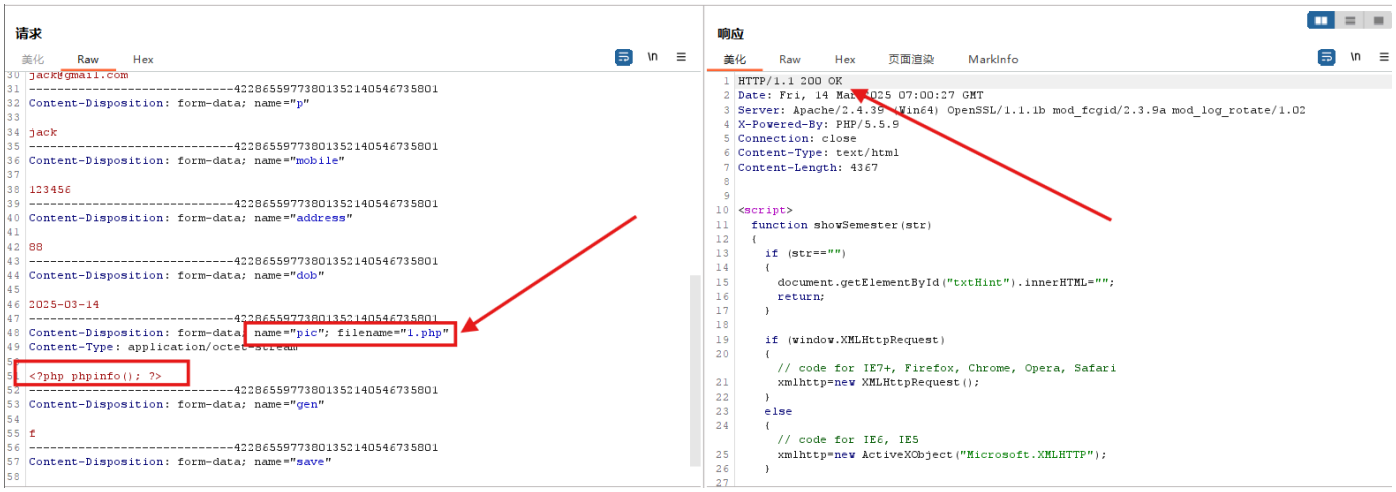
Vulnerable Parameter:

- File upload field: "$_FILES['pic']['name']" (POST request)

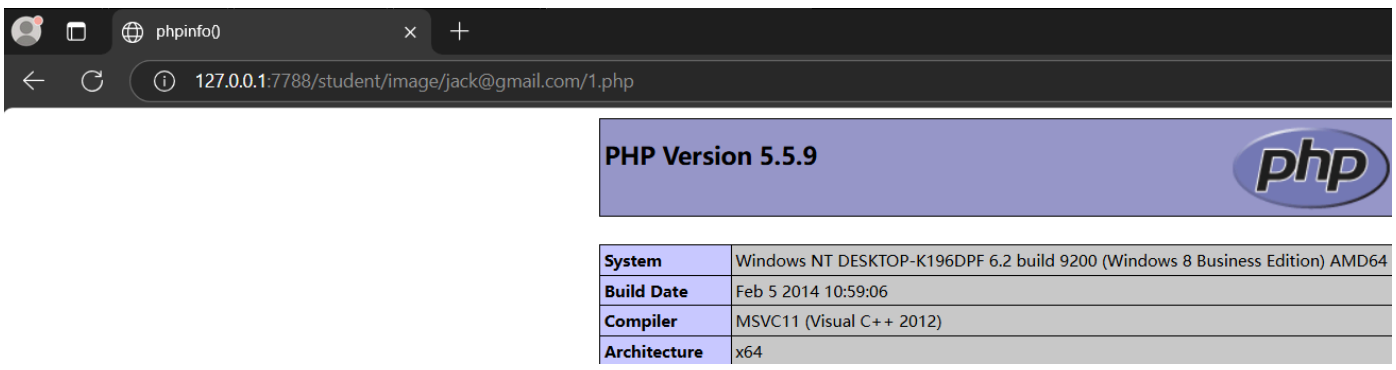
The following are the steps I reproduced.

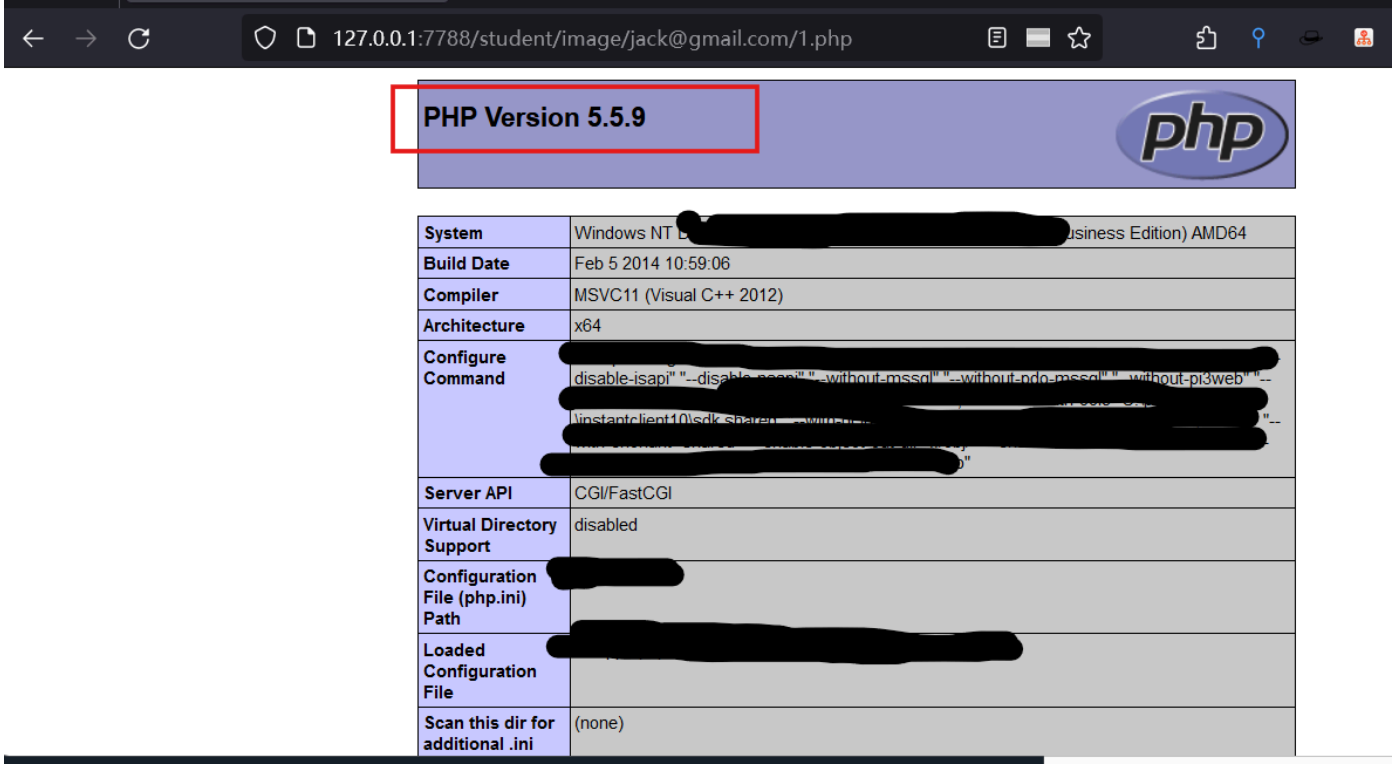


No protection, any file can upload



Access path, phpinfo() executed successfully.





Suggested repair

- **Input Validation & Filtering**: Ensure parameter allows only expected characters (e.g., digits or letters) to prevent path traversal attacks.
- **Filename Sanitization**: Strictly validate uploaded filenames. Avoid using user-provided original names and restrict allowed file extensions.
- **Randomized Storage Names**: Generate randomized filenames to prevent attackers from directly accessing malicious files.
- **File Type Verification**: Validate both file extensions and MIME types to detect spoofed formats.
- **Storage Directory Permissions**: Store uploaded files in a non-web-accessible directory or configure the server to disable script execution.
- **Server Configuration**: For Apache/Nginx, restrict execution permissions in upload directories (e.g., `php_flag engine off`).
- **Error Handling**: Avoid exposing internal path details by using custom error pages.

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants