**Module 1\_Assignment 2:**

**Title:Vulnerability Research Report on CVE-2025-48375**

**CVE ID:CVE-2025-48375**

**Description:**

Schule is open-source school management system software. Prior to version 1.0.1, the file forgot\_password.php (or equivalent endpoint responsible for email-based OTP generation) lacks proper rate limiting controls, allowing attackers to abuse the OTP request functionality. This vulnerability can be exploited to send an excessive number of OTP emails, leading to potential denial-of-service (DoS) conditions or facilitating user harassment through email flooding. Version 1.0.1 fixes the issue.

**Metrics:**

**CVSS Version 4.0**

**CVSS-BT:**[6.6 MEDIUM](https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator?name=CVE-2025-48375&vector=AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U&version=4.0&source=GitHub,%20Inc.)

**Vector:**

AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U

**Attack Vector (AV):** Network  
**Attack Complexity (AC):** Low  
**Attack Requirements (AT):** None  
**Privileges Required (PR):** None  
**User Interaction (UI):** None  
**Vulnerable System Confidentiality (VC):** None  
**Vulnerable System Integrity (VI):** None  
**Vulnerable System Availability (VA):** High  
**Subsequent System Confidentiality (SC):** None  
**Subsequent System Integrity (SI):** None

**Subsequent System Availability (SA):** None  
**Exploit Maturity (E):** Unreported

**Affected Code For CVE-2025-48375:**

else if(isset($\_POST['email'])){

$email = mysqli\_real\_escape\_string($conn, $\_POST['email']);

...

if(mysqli\_num\_rows($result) > 0){

...

$OTP = generateOTP();

$mail = getEmailObject($email, $OTP);

try {

$mail->send();

$\_SESSION['otp'] = $OTP . "";

} catch (Exception $e) {

...

}

}

}

**Weakness Enumeration:**

CWE-770: Allocation of Resources Without Limits or Throttling

**Description:**

The product allocates a reusable resource or group of resources on behalf of an actor without imposing any restrictions on the size or number of resources that can be allocated, in violation of the intended security policy for that actor.

**Extended Description:**

Code frequently has to work with limited resources, so programmers must be careful to ensure that resources are not consumed too quickly, or too easily. Without use of quotas, resource limits, or other protection mechanisms, it can be easy for an attacker to consume many resources by rapidly making many requests, or causing larger resources to be used than is needed. When too many resources are allocated, or if a single resource is too large, then it can prevent the code from working correctly, possibly leading to a denial of service.

**Denial of Service (DoS) Attack:**

A Denial of Service (DoS) attack is a cyberattack that aims to make a machine or network resource unavailable to its intended users. Attackers achieve this by disrupting the services of a host connected to a network, often by flooding it with traffic. This can result in a website, application, or other service becoming slow or inaccessible to legitimate users.

**Impacted Systems:**

The vulnerability identified as CVE-2025-48375 has been discovered in Schule, an open-source school management software. This system is typically used by educational institutions to handle daily administrative operations like student management, attendance tracking, communication via email, and more.

Due to the lack of rate-limiting mechanisms in its OTP email delivery feature, any version of Schule prior to v1.0.1 is considered vulnerable. Institutions that rely on older versions of this platform are at risk of resource exhaustion attacks, which may cause delays or downtime in critical functions such as account verification or login processes.

**Affected platforms may include:**

* Web servers hosting Schule versions older than 1.0.1.
* Email services integrated with Schule.
* Educational institutes using self-hosted or poorly maintained Schule instances.

**Remediation Approach :**

Upgrade to the Patched Version:

* Users should immediately upgrade Schule to version 1.0.1, where rate-limiting has been implemented in the OTP generation and delivery module.
* This version resolves the vulnerability by restricting the number of OTP requests per user within a specific time window.

Monitor OTP Request Logs:

* Continuously monitor system logs to detect unusual spikes in OTP requests, which could indicate a potential abuse or DoS attack in progress.

Use CAPTCHA Mechanisms:

* Incorporate CAPTCHA validation into the OTP request form to prevent automated abuse by bots or scripts.

**Reference:**

* <https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&search_type=all&isCpeNameSearch=false>
* <https://nvd.nist.gov/vuln/detail/CVE-2025-48375>
* <https://github.com/schule111/Schule/security/advisories/GHSA-h3f2-mc85-67gc>
* <https://cwe.mitre.org/data/definitions/770.html>