**Recommendations for Enhanced Security**

During our penetration testing engagement, we identified several vulnerabilities that could potentially impact both users and servers. Here is a detailed overview of the issues we discovered:

1. **Phone number verification:** We observed that the current system allows multiple users to register with the same phone number, lacking server-side verification. This can lead to identity confusion and potential security breaches.
2. **Rate limit requests:** We noticed that the server lacks proper rate-limiting mechanisms. This makes the system vulnerable to denial-of-service (DoS) attacks, where an attacker can flood the server with requests, causing it to become unresponsive and impacting legitimate users' access.
3. **Information Disclosure:** We have identified a potential information disclosure vulnerability within the system. Specifically, JavaScript (JS) and PHP files that contain critical web application functionality can be easily accessed by users through direct URL access. This presents a serious concern as it could expose sensitive implementation details and potentially offer attackers insights into the operation of the web application. (See js.txt/php.txt in attachments).

Addressing these vulnerabilities promptly is crucial to maintain the security and reliability of your application. We recommend the following actions:

* **Phone Number Verification:** Implement robust server-side verification procedures for phone number registration to prevent identity confusion and unauthorized access.
* **Rate Limiting:** Establish proper rate-limiting mechanisms to mitigate the risk of DoS attacks. This will help maintain the server's responsiveness and ensure equitable access for legitimate users.
* **Information Disclosure:** To prevent unauthorized access to sensitive source code, implement appropriate access controls and security measures for the JS and PHP files. Restrict direct URL access and ensure that only authorized users have access to these files.

We are committed to supporting your organization's security improvement efforts beyond the scope of this report. If you have any questions or require further clarification regarding the recommendations provided in this report, please do not hesitate to reach out. We understand that implementing security measures can sometimes be intricate, and we are here to assist you in any way we can.

Feel free to contact us through the provided communication channels, and we will promptly address your inquiries. Your organization's security is of utmost importance to us, and we are here to support your journey towards a more robust and resilient security environment.

-----------------------------------------------------------------------------------------------------------------------------------------

**BY Amine SAJID & Hakim ECHAROUDI**