Audit report for league/oauth2-server - December 2016

Introduction

"league/oauth2-server is a standards compliant implementation of an OAuth 2.0 authorization server written in PHP which makes working with OAuth 2.0 trivial. You can easily configure an OAuth 2.0 server to protect your API with access tokens, or allow clients to request new access tokens and refresh them." From https://github.com/thephpleague/oauth2-server

Scope

For this audit, I used the master branch of the code located at https://github.com/thephpleague/oauth2-server and I concentrated on locating the following types of flaws over the course of 2 weeks in December 2016:

1. Unvalidated Parameters
2. Cross-Site Scripting
3. Buffer Overflows
4. Command Injection
5. Error Handling Problems
6. Session and Cookie Hijacking

Findings

Insufficient validation of RSA public/private keys @ src/CryptKey.php:16

```
const RSA_KEY_PATTERN =
      '/^(-----BEGIN (RSA )?(PUBLIC|PRIVATE) KEY-----\n)(.|\n)+(-----END (RSA )?(PUBLIC|PRIVATE) KEY-----)$/';
```

> Fortunately, this issue is mitigated by the fact that Alex Bilbie has commented that he will be removing this from future releases.

The validation in use here currently relies on just checking that the key starts with `-----BEGIN PRIVATE KEY-----` and end with `-----END PRIVATE KEY-----`. It is the opinion of this auditor that there should a better attempt to validate the existence if a private/public key than just relying on the header or footer.

Conclusion

This audit yielded one unvalidated parameter flaw which I deem to be a non-issue as the project's developer has commented towards removing this code in future releases. My audit was unable to identify vectors relating to xss, buffer overflows, command injection, error handling or session/cookie hijacking.