Application security

Security testing

XPOBAY's infrastructure is subject to security benchmarking and monitoring so that we maintain or exceed industry security standards. We also use a combination of regular scheduled scans of our application, as well as bug bounty programs, to ensure that every area of our application has undergone rigorous security testing. We also leverage the services of an external third party to perform a yearly penetration testing exercise against our platform to make sure we've got every angle covered.

Security controls

We protect XPOBAY using a number of security controls including a Web Application Firewall (WAF). We never give, rent, or sell access to your data to anyone else, nor do we make use of it ourselves for any purpose other than to provide our services. See our full privacy policy for more information. We store each account's data within a unique identifier, which is used to retrieve data via the application or the API. Each request is authenticated and logged.

Secure code development

We follow industry best practices and standards such as OWASP and SANS. We have separate environments and databases for different stages of the application development. We do not use production data in our test and development environments.

User access

Passwords storage and verification are based on a one-way encryption method, meaning passwords are stored using a strong salted hash. Email addresses are validated against a strong salted hash, stored along with the email.

The databases are further protected by access restrictions, and key information (including your password) is encrypted when stored.

Logging and cookie management

We use cookies for user authentication. We use session IDs to identify user connections. Those session IDs are contained in HTTPS-only cookies not available to JavaScript.

All key actions on the application are centrally logged, audited and monitored.