

Password Crypt security review

The Alexandra Institute has performed a security review of the Password Crypt system for secure storing and sharing of passwords.

The review has been carried out by examining source code and performing a penetration test of a test setup provided by Password Crypt. The focus of the review has been on the backend system, as a robust backend should be secure against malicious clients and if a single client is compromised, only data residing at that client is compromised. The review has been a limited review, focused on the most common vulnerabilities described in the OWASP top 10 as well as some additional common vulnerabilities.

The review was performed in two phases: An initial phase where vulnerabilities were discovered and a followup phase where the implemented mitigative actions were verified.

After the second phase, the system only contains some minor security issues, ranging from low risk to informational.

Based on the review, we have given the overall security rating **very high** on a scale from very high (no high or medium risks, and few low risks), high (no high risks, only few medium risks, and some low risks), medium (few high and some medium risks) to low (many high risk findings).

The remaining issues are somewhat hard to reduce further and rely primarily on the policies and procedures related to the further development and deployment of Password Crypt.