Security baseline

Security by design

The platform is security designed in accordance with OWASP version 4:

- Level 2: Compliant
- Level 3: +90% supported

In addition the platform supports a wide range of security schemes and logging features, needed for support of ISO27001, ISAE3000 etc.

The platform is subject to periodic penetration testing. Last customer testing was july 2021.

Default security

By default the Tempus Serva is verifiably secure to all common threat vectors, such as

- SQL injection
- Cross-Site Scripting
- Session highjacking
- Login replays
- etc

Protective measure includes common hardening efforts, such as

- Data sanitization
- Request throtling
- CSRF tokens
- etc

In addition to this baseline additional features can be activated per installation.

- Built-in: Features in the product itself
- External: Measures controlled in application server or operating system

---

Revision #1
Created 3 April 2025 13:20:23 by Theis Villumsen
Updated 7 April 2025 14:21:22 by Theis Villumsen