Sample description of a vulnerability

Remark: Do not list this sample in your report!

Identification of the vulnerability

Protection Mechanism Failure: Content Security Policy (CSP) script-src unsafe-inline

Description and motivation

The Content Security Policy (CSP) defends against XSS and framing attacks. Due to misconfigured CSP it is possible that malicious JavaScript code or other sources can be loaded and executed within the web browser.

Countermeasures

Adopt the web application that no inline JavaScript and eval is necessary. Remove inline style sources and adopt the CSP by removing *unsafe-inline* and *unsafe-eval* on *style-src* and *script-src* . If inline scripts and style sources are needed protect them with a hash or a nonce.

Documentation

- The CSP can be found in the HTTP-Response header after calling the root URL / of the application.
- CSP keys & values: *Content-Security-Policy: default-src 'self'; style-src 'self' **‘unsafe-inline’**; script-src 'self' **'unsafe-eval' 'unsafe-inline'**; frame-ancestors 'none'; form-action 'self'*