Getting Started Designing for a Level of Assurance

The following security requirements (or tailored variations thereof) would be appropriate to add to your Web application's requirements if you were for example targeting OWASP ASVS Level 1B:

Authentication Requirements

1. All pages and resources must require authentication except those specifically intended to be public.

   Note: You would use your ESAPI to meet this requirement.

2. All password fields must not echo the user's password when it is entered, and all password fields (or the forms that contain them) must have autocomplete disabled.

   Note: This requirement wouldn't be met using your ESAPI.

3. If a maximum number of authentication attempts is exceeded, the account must be locked for a period of time long enough to deter brute force attacks.

   Note: You would use your ESAPI to meet this requirement.

Session Management Requirements

4. The framework's default session management control implementation must be used by the application.

   Note: This requirement wouldn't be met using your ESAPI.

5. Sessions must be invalidated when the user logs out.

   Note: You may be able to use your ESAPI to meet this requirement.

6. Sessions must timeout after a specified period of inactivity.

   Note: You may be able to use your ESAPI to meet this requirement.

7. All pages that require authentication to access them must have logout links.

   Note: You would use your ESAPI to meet this requirement.

8. The session ID must never be disclosed other than in cookie headers; particularly in URLs, error messages, or logs; the application must not support URL rewriting of session cookies.

   Note: You may be able to use your ESAPI to meet this requirement.

Access Control Requirements

9. Users must only be able to access protected functions for which they possess specific authorization.

   Note: You would use your ESAPI to meet this requirement.

10. Users must only be able to access URLs for which they possess specific authorization.

    Note: You would use your ESAPI to meet this requirement.

11. Users must only be able to access data files for which they possess specific authorization.

    Note: You would use your ESAPI to meet this requirement.

12. Direct object references must be protected, such that only authorized objects are accessible to each user.

    Note: You would use your ESAPI to meet this requirement.

13. Directory browsing must be disabled unless deliberately desired.

    Note: You would use your ESAPI to meet this requirement.

Input Validation Requirements

14. The runtime environment must not be susceptible to buffer overflows, otherwise security controls prevent buffer overflows must be used.

    Note: You may be able to use your ESAPI to meet this requirement.

15. A positive validation pattern must be defined and applied to all input.

    Note: You would use your ESAPI to meet this requirement.

16. All input validation failures must result in input rejection or input sanitization.

    Note: You would use your ESAPI to meet this requirement.

Output Encoding/Escaping Requirements

17. All untrusted data that are output to HTML (including HTML elements, HTML attributes, javascript data values, CSS blocks, and URI attributes) must be properly escaped for the applicable context.

    Note: You would use your ESAPI to meet this requirement.

Error Handling and Logging Requirements

18. The application must not output error messages or stack traces containing sensitive data that could assist an attacker, including session ID and personal information.

    Note: You would use your ESAPI to meet this requirement.

Data Protection Requirements

19. All forms containing sensitive information must have disabled client side caching, including autocomplete features.

    Note: This requirement wouldn't be met using your ESAPI.

Communication Security Requirements

20. A path must be able to be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and each server certificate must be valid.

    Note: You may be able to use your ESAPI to meet this requirement.

HTTP Security Requirements

21. Redirects must not include unvalidated data.

Note: You would use your ESAPI to meet this requirement.

22. The application must only accept a defined set of HTTP request methods, such as GET and POST.

    Note: You may use your ESAPI to meet this requirement.

23. Every HTTP response must contain a content type header specifying a safe character set (e.g., UTF-8).

    Note: You may use your ESAPI to meet this requirement.