Reduced Coupling with NIST Digital Identity Guidelines

The NIST Digital Identity Guidelines (SP 800-63) have long served as a reference for authentication and authorization controls. In version 4.x, certain chapters were closely aligned with NIST's structure and terminology.

While these guidelines remain an important reference, strict alignment introduced challenges, including less widely recognized terminology, duplication of similar requirements, and incomplete mappings. Version 5.0 moves away from this approach to improve clarity and relevance.

Moving Away from Common Weakness Enumeration (CWE)

The Common Weakness Enumeration (CWE) provides a useful taxonomy of software security weaknesses. However, challenges such as category-only CWEs, difficulties in mapping requirements to a single CWE, and the presence of imprecise mappings in version 4.x have led to the decision to discontinue direct CWE mappings in version 5.0.

Rethinking Level Definitions

Version 4.x described the levels as L1 ("Minimum"), L2 ("Standard"), and L3 ("Advanced"), with the implication that all applications handling sensitive data should meet at least L2.

Version 5.0 addresses several issues with this approach which are described in the following paragraphs.

As a practical matter, whereas version 4.x used tick marks for level indicators, 5.x uses a simple number on all formats of the standard including markdown, PDF, DOCX, CSV, JSON and XML. For backwards compatibility, legacy versions of the CSV, JSON and XML outputs which still use tick marks are also generated.

Easier Entry Level

Feedback indicated that the large number of Level 1 requirements (~120), combined with its designation as the "minimum"level that is not good enough for most applications, discouraged adoption. Version 5.0 aims to lower this barrier by defining Level 1 primarily around first-layer defense requirements, resulting in clearer and fewer requirements at that level. To demonstrate this numerically, in v4.0.3 there were 128 L1 requirements out of a total of 278 requirements, representing 46%. In 5.0.0 there are 70 L1 requirements out of a total of 345 requirements, representing 20%.

The Fallacy of Testability

A key factor in selecting controls for Level 1 in version 4.x was their suitability for assessment through "black box"external penetration testing. However, this approach was not fully aligned with the intent

of Level 1 as the minimum set of security controls. Some users argued that Level 1 was insufficient for securing applications, while others found it too difficult to test.

Relying on testability as a criterion is both relative and, at times, misleading. The fact that a requirement is testable does not guarantee that it can be tested in an automated or straightforward manner. Moreover, the most easily testable requirements are not always those with the greatest security impact or the simplest to implement.

As such, in version 5.0, the level decisions were made primarily based on risk reduction and also keeping in mind the effort to implement.

Not Just About Risk

The use of prescriptive, risk-based levels that mandate a specific level for certain applications has proven to be overly rigid. In practice, the prioritization and implementation of security controls depend on multiple factors, including both risk reduction and the effort required for implementation.

Therefore, organizations are encouraged to achieve the level that they feel like they should be achieving based on their maturity and the message they want to send to their users.

V1 Encoding and Sanitization

Control Objective

This chapter addresses the most common web application security weaknesses related to the unsafe processing of untrusted data. Such weaknesses can result in various technical vulnerabilities, where untrusted data is interpreted according to the syntax rules of the relevant interpreter.

For modern web applications, it is always best to use safer APIs, such as parameterized queries, auto-escaping, or templating frameworks. Otherwise, carefully performed output encoding, escaping, or sanitization becomes critical to the application's security.

Input validation serves as a defense-in-depth mechanism to protect against unexpected or dangerous content. However, since its primary purpose is to ensure that incoming content matches functional and business expectations, requirements related to this can be found in the "Validation and Business Logic"chapter.

V1.1 Encoding and Sanitization Architecture

In the sections below, syntax-specific or interpreter-specific requirements for safely processing unsafe content to avoid security vulnerabilities are provided. The requirements in this section cover the order in which this processing should occur and where it should take place. They also aim to

ensure that whenever data is stored, it remains in its original state and is not stored in an encoded or escaped form (e.g., HTML encoding), to prevent double encoding issues.

#	Description	Level
1.1.1	Verify that input is decoded or unescaped into a canonical form only once, it is only decoded when encoded data in that form is expected, and that this is done before processing the input further, for example it is not performed after input validation or sanitization.	2
1.1.2	Verify that the application performs output encoding and escaping either as a final step before being used by the interpreter for which it is intended or by the interpreter itself.	2

V1.2 Injection Prevention

Output encoding or escaping, performed close to or adjacent to a potentially dangerous context, is critical to the security of any application. Typically, output encoding and escaping are not persisted, but are instead used to render output safe for immediate use in the appropriate interpreter. Attempting to perform this too early may result in malformed content or render the encoding or escaping ineffective.

In many cases, software libraries include safe or safer functions that perform this automatically, although it is necessary to ensure that they are correct for the current context.

#	Description	Level
1.2.1	Verify that output encoding for an HTTP response, HTML document, or XML document is relevant for the context required, such as encoding the relevant characters for HTML elements, HTML attributes, HTML comments, CSS, or HTTP header fields, to avoid changing the message or document structure.	1
1.2.2	Verify that when dynamically building URLs, untrusted data is encoded according to its context (e.g., URL encoding or base64url encoding for query or path parameters). Ensure that only safe URL protocols are permitted (e.g., disallow javascript: or data:).	1
1.2.3	Verify that output encoding or escaping is used when dynamically building JavaScript content (including JSON), to avoid changing the message or document structure (to avoid JavaScript and JSON injection).	1

#	Description	Level
1.2.4	Verify that data selection or database queries (e.g., SQL, HQL, NoSQL, Cypher) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from SQL Injection and other database injection attacks. This is also relevant when writing stored procedures.	1
1.2.5	Verify that the application protects against OS command injection and that operating system calls use parameterized OS queries or use contextual command line output encoding.	1
1.2.6	Verify that the application protects against LDAP injection vulnerabilities, or that specific security controls to prevent LDAP injection have been implemented.	2
1.2.7	Verify that the application is protected against XPath injection attacks by using query parameterization or precompiled queries.	2
1.2.8	Verify that LaTeX processors are configured securely (such as not using the "–shell-escape"flag) and an allowlist of commands is used to prevent LaTeX injection attacks.	2
1.2.9	Verify that the application escapes special characters in regular expressions (typically using a backslash) to prevent them from being misinterpreted as metacharacters.	2
1.2.10	Verify that the application is protected against CSV and Formula Injection. The application must follow the escaping rules defined in RFC 4180 sections 2.6 and 2.7 when exporting CSV content. Additionally, when exporting to CSV or other spreadsheet formats (such as XLS, XLSX, or ODF), special characters (including '=', '+', '-', '@', '\t'(tab), and '\0'(null character)) must be escaped with a single quote if they appear as the first character in a field value.	3

Note: Using parameterized queries or escaping SQL is not always sufficient. Query parts such as table and column names (including "ORDER BY"column names) cannot be escaped. Including escaped user-supplied data in these fields results in failed queries or SQL injection.

V1.3 Sanitization

The ideal protection against using untrusted content in an unsafe context is to use context-specific encoding or escaping, which maintains the same semantic meaning of the unsafe content but renders it safe for use in that particular context, as discussed in more detail in the previous section.

Where this is not possible, sanitization becomes necessary, removing potentially dangerous characters or content. In some cases, this may change the semantic meaning of the input, but for security

reasons, there may be no alternative.

#	Description	Level
1.3.1	Verify that all untrusted HTML input from WYSIWYG editors or similar is sanitized using a well-known and secure HTML sanitization library or framework feature.	1
1.3.2	Verify that the application avoids the use of eval() or other dynamic code execution features such as Spring Expression Language (SpEL). Where there is no alternative, any user input being included must be sanitized before being executed.	1
1.3.3	Verify that data being passed to a potentially dangerous context is sanitized beforehand to enforce safety measures, such as only allowing characters which are safe for this context and trimming input which is too long.	2
1.3.4	Verify that user-supplied Scalable Vector Graphics (SVG) scriptable content is validated or sanitized to contain only tags and attributes (such as draw graphics) that are safe for the application, e.g., do not contain scripts and foreignObject.	2
1.3.5	Verify that the application sanitizes or disables user-supplied scriptable or expression template language content, such as Markdown, CSS or XSL stylesheets, BBCode, or similar.	2
1.3.6	Verify that the application protects against Server-side Request Forgery (SSRF) attacks, by validating untrusted data against an allowlist of protocols, domains, paths and ports and sanitizing potentially dangerous characters before using the data to call another service.	2
1.3.7	Verify that the application protects against template injection attacks by not allowing templates to be built based on untrusted input. Where there is no alternative, any untrusted input being included dynamically during template creation must be sanitized or strictly validated.	2
1.3.8	Verify that the application appropriately sanitizes untrusted input before use in Java Naming and Directory Interface (JNDI) queries and that JNDI is configured securely to prevent JNDI injection attacks.	2
1.3.9	Verify that the application sanitizes content before it is sent to memcache to prevent injection attacks.	2
1.3.10	Verify that format strings which might resolve in an unexpected or malicious way when used are sanitized before being processed.	2
1.3.11	Verify that the application sanitizes user input before passing to mail systems to protect against SMTP or IMAP injection.	2

#	Description	Level
1.3.12	Verify that regular expressions are free from elements causing exponential backtracking, and ensure untrusted input is sanitized to mitigate ReDoS or Runaway Regex attacks.	3

V1.4 Memory, String, and Unmanaged Code

The following requirements address risks associated with unsafe memory use, which generally apply when the application uses a systems language or unmanaged code.

In some cases, it may be possible to achieve this by setting compiler flags that enable buffer overflow protections and warnings, including stack randomization and data execution prevention, and that break the build if unsafe pointer, memory, format string, integer, or string operations are found.

#	Description	Level
1.4.1	Verify that the application uses memory-safe string, safer memory copy and pointer arithmetic to detect or prevent stack, buffer, or heap overflows.	2
1.4.2	Verify that sign, range, and input validation techniques are used to prevent integer overflows.	2
1.4.3	Verify that dynamically allocated memory and resources are released, and that references or pointers to freed memory are removed or set to null to prevent dangling pointers and use-after-free vulnerabilities.	2

V1.5 Safe Deserialization

The conversion of data from a stored or transmitted representation into actual application objects (deserialization) has historically been the cause of various code injection vulnerabilities. It is important to perform this process carefully and safely to avoid these types of issues.

In particular, certain methods of deserialization have been identified by programming language or framework documentation as insecure and cannot be made safe with untrusted data. For each mechanism in use, careful due diligence should be performed.

#	Description	Level
1.5.1	Verify that the application configures XML parsers to use a restrictive configuration and that unsafe features such as resolving external entities are disabled to prevent XML eXternal Entity (XXE) attacks.	1

#	Description	Level
1.5.2	Verify that deserialization of untrusted data enforces safe input handling, such as using an allowlist of object types or restricting client-defined object types, to prevent deserialization attacks. Deserialization mechanisms that are explicitly defined as insecure must not be used with untrusted input.	2
1.5.3	Verify that different parsers used in the application for the same data type (e.g., JSON parsers, XML parsers, URL parsers), perform parsing in a consistent way and use the same character encoding mechanism to avoid issues such as JSON Interoperability vulnerabilities or different URI or file parsing behavior being exploited in Remote File Inclusion (RFI) or Server-side Request Forgery (SSRF) attacks.	3

References

For more information, see also:

- OWASP LDAP Injection Prevention Cheat Sheet
- OWASP Cross Site Scripting Prevention Cheat Sheet
- OWASP DOM Based Cross Site Scripting Prevention Cheat Sheet
- OWASP XML External Entity Prevention Cheat Sheet
- OWASP Web Security Testing Guide: Client-Side Testing
- OWASP Java Encoding Project
- DOMPurify - Client-side HTML Sanitization Library
- RFC4180 - Common Format and MIME Type for Comma-Separated Values (CSV) Files

For more information, specifically on deserialization or parsing issues, please see:

- OWASP Deserialization Cheat Sheet
- An Exploration of JSON Interoperability Vulnerabilities
- Orange Tsai - A New Era of SSRF Exploiting URL Parser In Trending Programming Languages

V2 Validation and Business Logic

Control Objective

This chapter aims to ensure that a verified application meets the following high-level goals:

- Input received by the application matches business or functional expectations.
- The business logic flow is sequential, processed in order, and cannot be bypassed.

- Business logic includes limits and controls to detect and prevent automated attacks, such as continuous small funds transfers or adding a million friends one at a time.
- High-value business logic flows have considered abuse cases and malicious actors, and have protections against spoofing, tampering, information disclosure, and elevation of privilege attacks.

V2.1 Validation and Business Logic Documentation

Validation and business logic documentation should clearly define business logic limits, validation rules, and contextual consistency of combined data items, so it is clear what needs to be implemented in the application.

#	Description	Level
2.1.1	Verify that the application's documentation defines input validation rules for how to check the validity of data items against an expected structure. This could be common data formats such as credit card numbers, email addresses, telephone numbers, or it could be an internal data format.	1
2.1.2	Verify that the application's documentation defines how to validate the logical and contextual consistency of combined data items, such as checking that suburb and ZIP code match.	2
2.1.3	Verify that expectations for business logic limits and validations are documented, including both per-user and globally across the application.	2

V2.2 Input Validation

Effective input validation controls enforce business or functional expectations around the type of data the application expects to receive. This ensures good data quality and reduces the attack surface. However, it does not remove or replace the need to use correct encoding, parameterization, or sanitization when using the data in another component or for presenting it for output.

In this context, "input"could come from a wide variety of sources, including HTML form fields, REST requests, URL parameters, HTTP header fields, cookies, files on disk, databases, and external APIs.

A business logic control might check that a particular input is a number less than 100. A functional expectation might check that a number is below a certain threshold, as that number controls how many times a particular loop will take place, and a high number could lead to excessive processing and a potential denial of service condition.

While schema validation is not explicitly mandated, it may be the most effective mechanism for full validation coverage of HTTP APIs or other interfaces that use JSON or XML.

Please note the following points on Schema Validation:

- The “published version”of the JSON Schema validation specification is considered production-ready, but not strictly speaking “stable.”When using JSON Schema validation, ensure there are no gaps with the guidance in the requirements below.
- Any JSON Schema validation libraries in use should also be monitored and updated if necessary once the standard is formalized.
- DTD validation should not be used, and framework DTD evaluation should be disabled, to avoid issues with XXE attacks against DTDs.

#	Description	Level
2.2.1	Verify that input is validated to enforce business or functional expectations for that input. This should either use positive validation against an allow list of values, patterns, and ranges, or be based on comparing the input to an expected structure and logical limits according to predefined rules. For L1, this can focus on input which is used to make specific business or security decisions. For L2 and up, this should apply to all input.	1
2.2.2	Verify that the application is designed to enforce input validation at a trusted service layer. While client-side validation improves usability and should be encouraged, it must not be relied upon as a security control.	1
2.2.3	Verify that the application ensures that combinations of related data items are reasonable according to the pre-defined rules.	2

V2.3 Business Logic Security

This section considers key requirements to ensure that the application enforces business logic processes in the correct way and is not vulnerable to attacks that exploit the logic and flow of the application.

#	Description	Level
2.3.1	Verify that the application will only process business logic flows for the same user in the expected sequential step order and without skipping steps.	1
2.3.2	Verify that business logic limits are implemented per the application’s documentation to avoid business logic flaws being exploited.	2
2.3.3	Verify that transactions are being used at the business logic level such that either a business logic operation succeeds in its entirety or it is rolled back to the previous correct state.	2

#	Description	Level
2.3.4	Verify that business logic level locking mechanisms are used to ensure that limited quantity resources (such as theater seats or delivery slots) cannot be double-booked by manipulating the application's logic.	2
2.3.5	Verify that high-value business logic flows require multi-user approval to prevent unauthorized or accidental actions. This could include but is not limited to large monetary transfers, contract approvals, access to classified information, or safety overrides in manufacturing.	3

V2.4 Anti-automation

This section includes anti-automation controls to ensure that human-like interactions are required and excessive automated requests are prevented.

#	Description	Level
2.4.1	Verify that anti-automation controls are in place to protect against excessive calls to application functions that could lead to data exfiltration, garbage-data creation, quota exhaustion, rate-limit breaches, denial-of-service, or overuse of costly resources.	2
2.4.2	Verify that business logic flows require realistic human timing, preventing excessively rapid transaction submissions.	3

References

For more information, see also:

- OWASP Web Security Testing Guide: Input Validation Testing
- OWASP Web Security Testing Guide: Business Logic Testing
- Anti-automation can be achieved in many ways, including the use of the OWASP Automated Threats to Web Applications
- OWASP Input Validation Cheat Sheet
- JSON Schema

V3 Web Frontend Security

Control Objective

This category focuses on requirements designed to protect against attacks executed via a web frontend. These requirements do not apply to machine-to-machine solutions.

V3.1 Web Frontend Security Documentation

This section outlines the browser security features that should be specified in the application's documentation.

#	Description	Level
3.1.1	Verify that application documentation states the expected security features that browsers using the application must support (such as HTTPS, HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), and other relevant HTTP security mechanisms). It must also define how the application must behave when some of these features are not available (such as warning the user or blocking access).	3

V3.2 Unintended Content Interpretation

Rendering content or functionality in an incorrect context can result in malicious content being executed or displayed.

#	Description	Level
3.2.1	Verify that security controls are in place to prevent browsers from rendering content or functionality in HTTP responses in an incorrect context (e.g., when an API, a user-uploaded file or other resource is requested directly). Possible controls could include: not serving the content unless HTTP request header fields (such as Sec-Fetch-*) indicate it is the correct context, using the sandbox directive of the Content-Security-Policy header field or using the attachment disposition type in the Content-Disposition header field.	1
3.2.2	Verify that content intended to be displayed as text, rather than rendered as HTML, is handled using safe rendering functions (such as createTextNode or textContent) to prevent unintended execution of content such as HTML or JavaScript.	1

#	Description	Level
3.2.3	Verify that the application avoids DOM clobbering when using client-side JavaScript by employing explicit variable declarations, performing strict type checking, avoiding storing global variables on the document object, and implementing namespace isolation.	3

V3.3 Cookie Setup

This section outlines requirements for securely configuring sensitive cookies to provide a higher level of assurance that they were created by the application itself and to prevent their contents from leaking or being inappropriately modified.

#	Description	Level
3.3.1	Verify that cookies have the 'Secure'attribute set, and if the '__Host-'prefix is not used for the cookie name, the '__Secure-'prefix must be used for the cookie name.	1
3.3.2	Verify that each cookie's 'SameSite'attribute value is set according to the purpose of the cookie, to limit exposure to user interface redress attacks and browser-based request forgery attacks, commonly known as cross-site request forgery (CSRF).	2
3.3.3	Verify that cookies have the '__Host-'prefix for the cookie name unless they are explicitly designed to be shared with other hosts.	2
3.3.4	Verify that if the value of a cookie is not meant to be accessible to client-side scripts (such as a session token), the cookie must have the 'HttpOnly' attribute set and the same value (e. g. session token) must only be transferred to the client via the 'Set-Cookie'header field.	2
3.3.5	Verify that when the application writes a cookie, the cookie name and value length combined are not over 4096 bytes. Overly large cookies will not be stored by the browser and therefore not sent with requests, preventing the user from using application functionality which relies on that cookie.	3

V3.4 Browser Security Mechanism Headers

This section describes which security headers should be set on HTTP responses to enable browser security features and restrictions when handling responses from the application.

#	Description	Level
3.4.1	Verify that a Strict-Transport-Security header field is included on all responses to enforce an HTTP Strict Transport Security (HSTS) policy. A maximum age of at least 1 year must be defined, and for L2 and up, the policy must apply to all subdomains as well.	1
3.4.2	Verify that the Cross-Origin Resource Sharing (CORS) Access-Control-Allow-Origin header field is a fixed value by the application, or if the Origin HTTP request header field value is used, it is validated against an allowlist of trusted origins. When 'Access-Control-Allow-Origin: *'needs to be used, verify that the response does not include any sensitive information.	1
3.4.3	Verify that HTTP responses include a Content-Security-Policy response header field which defines directives to ensure the browser only loads and executes trusted content or resources, in order to limit execution of malicious JavaScript. As a minimum, a global policy must be used which includes the directives object-src 'none'and base-uri 'none'and defines either an allowlist or uses nonces or hashes. For an L3 application, a per-response policy with nonces or hashes must be defined.	2
3.4.4	Verify that all HTTP responses contain an 'X-Content-Type-Options: nosniff' header field. This instructs browsers not to use content sniffing and MIME type guessing for the given response, and to require the response's Content-Type header field value to match the destination resource. For example, the response to a request for a style is only accepted if the response's Content-Type is 'text/css'. This also enables the use of the Cross-Origin Read Blocking (CORB) functionality by the browser.	2
3.4.5	Verify that the application sets a referrer policy to prevent leakage of technically sensitive data to third-party services via the 'Referer'HTTP request header field. This can be done using the Referrer-Policy HTTP response header field or via HTML element attributes. Sensitive data could include path and query data in the URL, and for internal non-public applications also the hostname.	2
3.4.6	Verify that the web application uses the frame-ancestors directive of the Content-Security-Policy header field for every HTTP response to ensure that it cannot be embedded by default and that embedding of specific resources is allowed only when necessary. Note that the X-Frame-Options header field, although supported by browsers, is obsolete and may not be relied upon.	2
3.4.7	Verify that the Content-Security-Policy header field specifies a location to report violations.	3

#	Description	Level
3.4.8	Verify that all HTTP responses that initiate a document rendering (such as responses with Content-Type text/html), include the Cross-Origin-Opener-Policy header field with the same-origin directive or the same-origin-allow-popups directive as required. This prevents attacks that abuse shared access to Window objects, such as tabnabbing and frame counting.	3

V3.5 Browser Origin Separation

When accepting a request to sensitive functionality on the server side, the application needs to ensure the request is initiated by the application itself or by a trusted party and has not been forged by an attacker.

Sensitive functionality in this context could include accepting form posts for authenticated and non-authenticated users (such as an authentication request), state-changing operations, or resource-demanding functionality (such as data export).

The key protections here are browser security policies like Same Origin Policy for JavaScript and also SameSite logic for cookies. Another common protection is the CORS preflight mechanism. This mechanism will be critical for endpoints designed to be called from a different origin, but it can also be a useful request forgery prevention mechanism for endpoints which are not designed to be called from a different origin.

#	Description	Level
3.5.1	Verify that, if the application does not rely on the CORS preflight mechanism to prevent disallowed cross-origin requests to use sensitive functionality, these requests are validated to ensure they originate from the application itself. This may be done by using and validating anti-forgery tokens or requiring extra HTTP header fields that are not CORS-safelisted request-header fields. This is to defend against browser-based request forgery attacks, commonly known as cross-site request forgery (CSRF).	1
3.5.2	Verify that, if the application relies on the CORS preflight mechanism to prevent disallowed cross-origin use of sensitive functionality, it is not possible to call the functionality with a request which does not trigger a CORS-preflight request. This may require checking the values of the 'Origin' and 'Content-Type'request header fields or using an extra header field that is not a CORS-safelisted header-field.	1

#	Description	Level
3.5.3	Verify that HTTP requests to sensitive functionality use appropriate HTTP methods such as POST, PUT, PATCH, or DELETE, and not methods defined by the HTTP specification as “safe”such as HEAD, OPTIONS, or GET. Alternatively, strict validation of the Sec-Fetch-* request header fields can be used to ensure that the request did not originate from an inappropriate cross-origin call, a navigation request, or a resource load (such as an image source) where this is not expected.	1
3.5.4	Verify that separate applications are hosted on different hostnames to leverage the restrictions provided by same-origin policy, including how documents or scripts loaded by one origin can interact with resources from another origin and hostname-based restrictions on cookies.	2
3.5.5	Verify that messages received by the postMessage interface are discarded if the origin of the message is not trusted, or if the syntax of the message is invalid.	2
3.5.6	Verify that JSONP functionality is not enabled anywhere across the application to avoid Cross-Site Script Inclusion (XSSI) attacks.	3
3.5.7	Verify that data requiring authorization is not included in script resource responses, like JavaScript files, to prevent Cross-Site Script Inclusion (XSSI) attacks.	3
3.5.8	Verify that authenticated resources (such as images, videos, scripts, and other documents) can be loaded or embedded on behalf of the user only when intended. This can be accomplished by strict validation of the Sec-Fetch-* HTTP request header fields to ensure that the request did not originate from an inappropriate cross-origin call, or by setting a restrictive Cross-Origin-Resource-Policy HTTP response header field to instruct the browser to block returned content.	3

V3.6 External Resource Integrity

This section provides guidance for the safe hosting of content on third-party sites.

#	Description	Level
3.6.1	Verify that client-side assets, such as JavaScript libraries, CSS, or web fonts, are only hosted externally (e.g., on a Content Delivery Network) if the resource is static and versioned and Subresource Integrity (SRI) is used to validate the integrity of the asset. If this is not possible, there should be a documented security decision to justify this for each resource.	3

V3.7 Other Browser Security Considerations

This section includes various other security controls and modern browser security features required for client-side browser security.

#	Description	Level
3.7.1	Verify that the application only uses client-side technologies which are still supported and considered secure. Examples of technologies which do not meet this requirement include NSAPI plugins, Flash, Shockwave, ActiveX, Silverlight, NACL, or client-side Java applets.	2
3.7.2	Verify that the application will only automatically redirect the user to a different hostname or domain (which is not controlled by the application) where the destination appears on an allowlist.	2
3.7.3	Verify that the application shows a notification when the user is being redirected to a URL outside of the application's control, with an option to cancel the navigation.	3
3.7.4	Verify that the application's top-level domain (e.g., site.tld) is added to the public preload list for HTTP Strict Transport Security (HSTS). This ensures that the use of TLS for the application is built directly into the main browsers, rather than relying only on the Strict-Transport-Security response header field.	3
3.7.5	Verify that the application behaves as documented (such as warning the user or blocking access) if the browser used to access the application does not support the expected security features.	3

References

For more information, see also:

- Set-Cookie __Host- prefix details

- OWASP Content Security Policy Cheat Sheet
- OWASP Secure Headers Project
- OWASP Cross-Site Request Forgery Prevention Cheat Sheet
- HSTS Browser Preload List submission form
- OWASP DOM Clobbering Prevention Cheat Sheet

V4 API and Web Service

Control Objective

Several considerations apply specifically to applications that expose APIs for use by web browsers or other consumers (commonly using JSON, XML, or GraphQL). This chapter covers the relevant security configurations and mechanisms that should be applied.

Note that authentication, session management, and input validation concerns from other chapters also apply to APIs, so this chapter cannot be taken out of context or tested in isolation.

V4.1 Generic Web Service Security

This section addresses general web service security considerations and, consequently, basic web service hygiene practices.

#	Description	Level
4.1.1	Verify that every HTTP response with a message body contains a Content-Type header field that matches the actual content of the response, including the charset parameter to specify safe character encoding (e.g., UTF-8, ISO-8859-1) according to IANA Media Types, such as “text/”, “/+xml” and “/xml”.	1
4.1.2	Verify that only user-facing endpoints (intended for manual web-browser access) automatically redirect from HTTP to HTTPS, while other services or endpoints do not implement transparent redirects. This is to avoid a situation where a client is erroneously sending unencrypted HTTP requests, but since the requests are being automatically redirected to HTTPS, the leakage of sensitive data goes undiscovered.	2
4.1.3	Verify that any HTTP header field used by the application and set by an intermediary layer, such as a load balancer, a web proxy, or a backend-for-frontend service, cannot be overridden by the end-user. Example headers might include X-Real-IP, X-Forwarded-*, or X-User-ID.	2

#	Description	Level
4.1.4	Verify that only HTTP methods that are explicitly supported by the application or its API (including OPTIONS during preflight requests) can be used and that unused methods are blocked.	3
4.1.5	Verify that per-message digital signatures are used to provide additional assurance on top of transport protections for requests or transactions which are highly sensitive or which traverse a number of systems.	3

V4.2 HTTP Message Structure Validation

This section explains how the structure and header fields of an HTTP message should be validated to prevent attacks such as request smuggling, response splitting, header injection, and denial of service via overly long HTTP messages.

These requirements are relevant for general HTTP message processing and generation, but are especially important when converting HTTP messages between different HTTP versions.

#	Description	Level
4.2.1	Verify that all application components (including load balancers, firewalls, and application servers) determine boundaries of incoming HTTP messages using the appropriate mechanism for the HTTP version to prevent HTTP request smuggling. In HTTP/1.x, if a Transfer-Encoding header field is present, the Content-Length header must be ignored per RFC 2616. When using HTTP/2 or HTTP/3, if a Content-Length header field is present, the receiver must ensure that it is consistent with the length of the DATA frames.	2
4.2.2	Verify that when generating HTTP messages, the Content-Length header field does not conflict with the length of the content as determined by the framing of the HTTP protocol, in order to prevent request smuggling attacks.	3
4.2.3	Verify that the application does not send nor accept HTTP/2 or HTTP/3 messages with connection-specific header fields such as Transfer-Encoding to prevent response splitting and header injection attacks.	3
4.2.4	Verify that the application only accepts HTTP/2 and HTTP/3 requests where the header fields and values do not contain any CR (`\r`), LF (`\n`), or CRLF (`\r\n`) sequences, to prevent header injection attacks.	3

#	Description	Level
4.2.5	Verify that, if the application (backend or frontend) builds and sends requests, it uses validation, sanitization, or other mechanisms to avoid creating URIs (such as for API calls) or HTTP request header fields (such as Authorization or Cookie), which are too long to be accepted by the receiving component. This could cause a denial of service, such as when sending an overly long request (e.g., a long cookie header field), which results in the server always responding with an error status.	3

V4.3 GraphQL

GraphQL is becoming more common as a way of creating data-rich clients that are not tightly coupled to a variety of backend services. This section covers security considerations for GraphQL.

#	Description	Level
4.3.1	Verify that a query allowlist, depth limiting, amount limiting, or query cost analysis is used to prevent GraphQL or data layer expression Denial of Service (DoS) as a result of expensive, nested queries.	2
4.3.2	Verify that GraphQL introspection queries are disabled in the production environment unless the GraphQL API is meant to be used by other parties.	2

V4.4 WebSocket

WebSocket is a communications protocol that provides a simultaneous two-way communication channel over a single TCP connection. It was standardized by the IETF as RFC 6455 in 2011 and is distinct from HTTP, even though it is designed to work over HTTP ports 443 and 80.

This section provides key security requirements to prevent attacks related to communication security and session management that specifically exploit this real-time communication channel.

#	Description	Level
4.4.1	Verify that WebSocket over TLS (WSS) is used for all WebSocket connections.	1
4.4.2	Verify that, during the initial HTTP WebSocket handshake, the Origin header field is checked against a list of origins allowed for the application.	2

#	Description	Level
4.4.3	Verify that, if the application's standard session management cannot be used, dedicated tokens are being used for this, which comply with the relevant Session Management security requirements.	2
4.4.4	Verify that dedicated WebSocket session management tokens are initially obtained or validated through the previously authenticated HTTPS session when transitioning an existing HTTPS session to a WebSocket channel.	2

References

For more information, see also:

- OWASP REST Security Cheat Sheet
- Resources on GraphQL Authorization from graphql.org and Apollo.
- OWASP Web Security Testing Guide: GraphQL Testing
- OWASP Web Security Testing Guide: Testing WebSockets

V5 File Handling

Control Objective

The use of files can present a variety of risks to the application, including denial of service, unauthorized access, and storage exhaustion. This chapter includes requirements to address these risks.

V5.1 File Handling Documentation

This section includes a requirement to document the expected characteristics of files accepted by the application, as a necessary precondition for developing and verifying relevant security checks.

#	Description	Level
5.1.1	Verify that the documentation defines the permitted file types, expected file extensions, and maximum size (including unpacked size) for each upload feature. Additionally, ensure that the documentation specifies how files are made safe for end-users to download and process, such as how the application behaves when a malicious file is detected.	2

V5.2 File Upload and Content

File upload functionality is a primary source of untrusted files. This section outlines the requirements for ensuring that the presence, volume, or content of these files cannot harm the application.

#	Description	Level
5.2.1	Verify that the application will only accept files of a size which it can process without causing a loss of performance or a denial of service attack.	1
5.2.2	Verify that when the application accepts a file, either on its own or within an archive such as a zip file, it checks if the file extension matches an expected file extension and validates that the contents correspond to the type represented by the extension. This includes, but is not limited to, checking the initial 'magic bytes', performing image re-writing, and using specialized libraries for file content validation. For L1, this can focus just on files which are used to make specific business or security decisions. For L2 and up, this must apply to all files being accepted.	1
5.2.3	Verify that the application checks compressed files (e.g., zip, gz, docx, odt) against maximum allowed uncompressed size and against maximum number of files before uncompressing the file.	2
5.2.4	Verify that a file size quota and maximum number of files per user are enforced to ensure that a single user cannot fill up the storage with too many files, or excessively large files.	3
5.2.5	Verify that the application does not allow uploading compressed files containing symlinks unless this is specifically required (in which case it will be necessary to enforce an allowlist of the files that can be symlinked to).	3
5.2.6	Verify that the application rejects uploaded images with a pixel size larger than the maximum allowed, to prevent pixel flood attacks.	3

V5.3 File Storage

This section includes requirements to prevent files from being inappropriately executed after upload, to detect dangerous content, and to avoid untrusted data being used to control where files are being stored.

#	Description	Level
5.3.1	Verify that files uploaded or generated by untrusted input and stored in a public folder, are not executed as server-side program code when accessed directly with an HTTP request.	1
5.3.2	Verify that when the application creates file paths for file operations, instead of user-submitted filenames, it uses internally generated or trusted data, or if user-submitted filenames or file metadata must be used, strict validation and sanitization must be applied. This is to protect against path traversal, local or remote file inclusion (LFI, RFI), and server-side request forgery (SSRF) attacks.	1
5.3.3	Verify that server-side file processing, such as file decompression, ignores user-provided path information to prevent vulnerabilities such as zip slip.	3

V5.4 File Download

This section contains requirements to mitigate risks when serving files to be downloaded, including path traversal and injection attacks. This also includes making sure they don't contain dangerous content.

#	Description	Level
5.4.1	Verify that the application validates or ignores user-submitted filenames, including in a JSON, JSONP, or URL parameter and specifies a filename in the Content-Disposition header field in the response.	2
5.4.2	Verify that file names served (e.g., in HTTP response header fields or email attachments) are encoded or sanitized (e.g., following RFC 6266) to preserve document structure and prevent injection attacks.	2
5.4.3	Verify that files obtained from untrusted sources are scanned by antivirus scanners to prevent serving of known malicious content.	2

References

For more information, see also:

- OWASP File Upload Cheat Sheet
- Example of using symlinks for arbitrary file read
- Explanation of "Magic Bytes"from Wikipedia

V6 Authentication

Control Objective

Authentication is the process of establishing or confirming the authenticity of an individual or device. It involves verifying claims made by a person or about a device, ensuring resistance to impersonation, and preventing the recovery or interception of passwords.

NIST SP 800-63 is a modern, evidence-based standard that is valuable for organizations worldwide, but is particularly relevant to US agencies and those interacting with US agencies.

While many of the requirements in this chapter are based on the second section of the standard (known as NIST SP 800-63B “Digital Identity Guidelines - Authentication and Lifecycle Management”), the chapter focuses on common threats and frequently exploited authentication weaknesses. It does not attempt to comprehensively cover every point in the standard. For cases where full NIST SP 800-63 compliance is necessary, please refer to NIST SP 800-63.

Additionally, NIST SP 800-63 terminology may sometimes differ, and this chapter often uses more commonly understood terminology to improve clarity.

A common feature of more advanced applications is the ability to adapt authentication stages required based on various risk factors. This feature is covered in the “Authorization”chapter, since these mechanisms also need to be considered for authorization decisions.

V6.1 Authentication Documentation

This section contains requirements detailing the authentication documentation that should be maintained for an application. This is crucial for implementing and assessing how the relevant authentication controls should be configured.

#	Description	Level
6.1.1	Verify that application documentation defines how controls such as rate limiting, anti-automation, and adaptive response, are used to defend against attacks such as credential stuffing and password brute force. The documentation must make clear how these controls are configured and prevent malicious account lockout.	1
6.1.2	Verify that a list of context-specific words is documented in order to prevent their use in passwords. The list could include permutations of organization names, product names, system identifiers, project codenames, department or role names, and similar.	2

#	Description	Level
6.1.3	Verify that, if the application includes multiple authentication pathways, these are all documented together with the security controls and authentication strength which must be consistently enforced across them.	2

V6.2 Password Security

Passwords, called “Memorized Secrets”by NIST SP 800-63, include passwords, passphrases, PINs, unlock patterns, and picking the correct kitten or another image element. They are generally considered “something you know”and are often used as a single-factor authentication mechanism.

As such, this section contains requirements for making sure that passwords are created and handled securely. Most of the requirements are L1 as they are most important at that level. From L2 onwards, multi-factor authentication mechanisms are required, where passwords may be one of those factors.

The requirements in this section mostly relate to § 5.1.1.2 of NIST’s Guidance.

#	Description	Level
6.2.1	Verify that user set passwords are at least 8 characters in length although a minimum of 15 characters is strongly recommended.	1
6.2.2	Verify that users can change their password.	1
6.2.3	Verify that password change functionality requires the user’s current and new password.	1
6.2.4	Verify that passwords submitted during account registration or password change are checked against an available set of, at least, the top 3000 passwords which match the application’s password policy, e.g. minimum length.	1
6.2.5	Verify that passwords of any composition can be used, without rules limiting the type of characters permitted. There must be no requirement for a minimum number of upper or lower case characters, numbers, or special characters.	1
6.2.6	Verify that password input fields use type=password to mask the entry. Applications may allow the user to temporarily view the entire masked password, or the last typed character of the password.	1
6.2.7	Verify that “paste”functionality, browser password helpers, and external password managers are permitted.	1

#	Description	Level
6.2.8	Verify that the application verifies the user's password exactly as received from the user, without any modifications such as truncation or case transformation.	1
6.2.9	Verify that passwords of at least 64 characters are permitted.	2
6.2.10	Verify that a user's password stays valid until it is discovered to be compromised or the user rotates it. The application must not require periodic credential rotation.	2
6.2.11	Verify that the documented list of context specific words is used to prevent easy to guess passwords being created.	2
6.2.12	Verify that passwords submitted during account registration or password changes are checked against a set of breached passwords.	2

V6.3 General Authentication Security

This section contains general requirements for the security of authentication mechanisms as well as setting out the different expectations for levels. L2 applications must force the use of multi-factor authentication (MFA). L3 applications must use hardware-based authentication, performed in an attested and trusted execution environment (TEE). This could include device-bound passkeys, eIDAS Level of Assurance (LoA) High enforced authenticators, authenticators with NIST Authenticator Assurance Level 3 (AAL3) assurance, or an equivalent mechanism.

While this is a relatively aggressive stance on MFA, it is critical to raise the bar around this to protect users, and any attempt to relax these requirements should be accompanied by a clear plan on how the risks around authentication will be mitigated, taking into account NIST's guidance and research on the topic.

Note that at the time of release, NIST SP 800-63 considers email as not acceptable as an authentication mechanism (archived copy).

The requirements in this section relate to a variety of sections of NIST's Guidance, including: § 4.2.1, § 4.3.1, § 5.2.2, and § 6.1.2.

#	Description	Level
6.3.1	Verify that controls to prevent attacks such as credential stuffing and password brute force are implemented according to the application's security documentation.	1
6.3.2	Verify that default user accounts (e.g., "root", "admin", or "sa") are not present in the application or are disabled.	1

#	Description	Level
6.3.3	Verify that either a multi-factor authentication mechanism or a combination of single-factor authentication mechanisms, must be used in order to access the application. For L3, one of the factors must be a hardware-based authentication mechanism which provides compromise and impersonation resistance against phishing attacks while verifying the intent to authenticate by requiring a user-initiated action (such as a button press on a FIDO hardware key or a mobile phone). Relaxing any of the considerations in this requirement requires a fully documented rationale and a comprehensive set of mitigating controls.	2
6.3.4	Verify that, if the application includes multiple authentication pathways, there are no undocumented pathways and that security controls and authentication strength are enforced consistently.	2
6.3.5	Verify that users are notified of suspicious authentication attempts (successful or unsuccessful). This may include authentication attempts from an unusual location or client, partially successful authentication (only one of multiple factors), an authentication attempt after a long period of inactivity or a successful authentication after several unsuccessful attempts.	3
6.3.6	Verify that email is not used as either a single-factor or multi-factor authentication mechanism.	3
6.3.7	Verify that users are notified after updates to authentication details, such as credential resets or modification of the username or email address.	3
6.3.8	Verify that valid users cannot be deduced from failed authentication challenges, such as by basing on error messages, HTTP response codes, or different response times. Registration and forgot password functionality must also have this protection.	3

V6.4 Authentication Factor Lifecycle and Recovery

Authentication factors may include passwords, soft tokens, hardware tokens, and biometric devices. Securely handling the lifecycle of these mechanisms is critical to the security of an application, and this section includes requirements related to this.

The requirements in this section mostly relate to § 5.1.1.2 or § 6.1.2.3 of NIST's Guidance.

#	Description	Level
6.4.1	Verify that system generated initial passwords or activation codes are securely randomly generated, follow the existing password policy, and expire after a short period of time or after they are initially used. These initial secrets must not be permitted to become the long term password.	1
6.4.2	Verify that password hints or knowledge-based authentication (so-called "secret questions") are not present.	1
6.4.3	Verify that a secure process for resetting a forgotten password is implemented, that does not bypass any enabled multi-factor authentication mechanisms.	2
6.4.4	Verify that if a multi-factor authentication factor is lost, evidence of identity proofing is performed at the same level as during enrollment.	2
6.4.5	Verify that renewal instructions for authentication mechanisms which expire are sent with enough time to be carried out before the old authentication mechanism expires, configuring automated reminders if necessary.	3
6.4.6	Verify that administrative users can initiate the password reset process for the user, but that this does not allow them to change or choose the user's password. This prevents a situation where they know the user's password.	3

V6.5 General Multi-factor authentication requirements

This section provides general guidance that will be relevant to various different multi-factor authentication methods.

The mechanisms include:

- Lookup Secrets
- Time based One-time Passwords (TOTPs)
- Out-of-Band mechanisms

Lookup secrets are pre-generated lists of secret codes, similar to Transaction Authorization Numbers (TAN), social media recovery codes, or a grid containing a set of random values. This type of authentication mechanism is considered "something you have"because the codes are deliberately not memorable so will need to be stored somewhere.

Time based One-time Passwords (TOTPs) are physical or soft tokens that display a continually changing pseudo-random one-time challenge. This type of authentication mechanism is considered "something you have". Multi-factor TOTPs are similar to single-factor TOTPs, but require a valid PIN code, biometric unlocking, USB insertion or NFC pairing, or some additional value (such as transaction signing calculators) to be entered to create the final One-time Password (OTP).

Details on out-of-band mechanisms will be provided in the next section.

The requirements in these sections mostly relate to § 5.1.2, § 5.1.3, § 5.1.4.2, § 5.1.5.2, § 5.2.1, and § 5.2.3 of NIST's Guidance.

#	Description	Level
6.5.1	Verify that lookup secrets, out-of-band authentication requests or codes, and time-based one-time passwords (TOTPs) are only successfully usable once.	2
6.5.2	Verify that, when being stored in the application's backend, lookup secrets with less than 112 bits of entropy (19 random alphanumeric characters or 34 random digits) are hashed with an approved password storage hashing algorithm that incorporates a 32-bit random salt. A standard hash function can be used if the secret has 112 bits of entropy or more.	2
6.5.3	Verify that lookup secrets, out-of-band authentication code, and time-based one-time password seeds, are generated using a Cryptographically Secure Pseudorandom Number Generator (CSPRNG) to avoid predictable values.	2
6.5.4	Verify that lookup secrets and out-of-band authentication codes have a minimum of 20 bits of entropy (typically 4 random alphanumeric characters or 6 random digits is sufficient).	2
6.5.5	Verify that out-of-band authentication requests, codes, or tokens, as well as time-based one-time passwords (TOTPs) have a defined lifetime. Out of band requests must have a maximum lifetime of 10 minutes and for TOTP a maximum lifetime of 30 seconds.	2
6.5.6	Verify that any authentication factor (including physical devices) can be revoked in case of theft or other loss.	3
6.5.7	Verify that biometric authentication mechanisms are only used as secondary factors together with either something you have or something you know.	3
6.5.8	Verify that time-based one-time passwords (TOTPs) are checked based on a time source from a trusted service and not from an untrusted or client provided time.	3

V6.6 Out-of-Band authentication mechanisms

This usually involves the authentication server communicating with a physical device over a secure secondary channel. For example, sending push notifications to mobile devices. This type of authentication mechanism is considered "something you have".

Unsafe out-of-band authentication mechanisms such as e-mail and VOIP are not permitted. PSTN and SMS authentication are currently considered to be "restricted"authentication mechanisms by

NIST and should be deprecated in favor of Time based One-time Passwords (TOTPs), a cryptographic mechanism, or similar. NIST SP 800-63B § 5.1.3.3 recommends addressing the risks of device swap, SIM change, number porting, or other abnormal behavior, if telephone or SMS out-of-band authentication absolutely has to be supported. While this ASVS section does not mandate this as a requirement, not taking these precautions for a sensitive L2 app or an L3 app should be seen as a significant red flag.

Note that NIST has also recently provided guidance which discourages the use of push notifications. While this ASVS section does not do so, it is important to be aware of the risks of "push bombing".

#	Description	Level
6.6.1	Verify that authentication mechanisms using the Public Switched Telephone Network (PSTN) to deliver One-time Passwords (OTPs) via phone or SMS are offered only when the phone number has previously been validated, alternate stronger methods (such as Time based One-time Passwords) are also offered, and the service provides information on their security risks to users. For L3 applications, phone and SMS must not be available as options.	2
6.6.2	Verify that out-of-band authentication requests, codes, or tokens are bound to the original authentication request for which they were generated and are not usable for a previous or subsequent one.	2
6.6.3	Verify that a code based out-of-band authentication mechanism is protected against brute force attacks by using rate limiting. Consider also using a code with at least 64 bits of entropy.	2
6.6.4	Verify that, where push notifications are used for multi-factor authentication, rate limiting is used to prevent push bombing attacks. Number matching may also mitigate this risk.	3

V6.7 Cryptographic authentication mechanism

Cryptographic authentication mechanisms include smart cards or FIDO keys, where the user has to plug in or pair the cryptographic device to the computer to complete authentication. The authentication server will send a challenge nonce to the cryptographic device or software, and the device or software calculates a response based upon a securely stored cryptographic key. The requirements in this section provide implementation-specific guidance for these mechanisms, with guidance on cryptographic algorithms being covered in the "Cryptography"chapter.

Where shared or secret keys are used for cryptographic authentication, these should be stored using the same mechanisms as other system secrets, as documented in the "Secret Management"section in the "Configuration"chapter.

The requirements in this section mostly relate to § 5.1.7.2 of NIST's Guidance.

#	Description	Level
6.7.1	Verify that the certificates used to verify cryptographic authentication assertions are stored in a way protects them from modification.	3
6.7.2	Verify that the challenge nonce is at least 64 bits in length, and statistically unique or unique over the lifetime of the cryptographic device.	3

V6.8 Authentication with an Identity Provider

Identity Providers (IdPs) provide federated identity for users. Users will often have more than one identity with multiple IdPs, such as an enterprise identity using Azure AD, Okta, Ping Identity, or Google, or consumer identity using Facebook, Twitter, Google, or WeChat, to name just a few common alternatives. This list is not an endorsement of these companies or services, but simply an encouragement for developers to consider the reality that many users have many established identities. Organizations should consider integrating with existing user identities, as per the risk profile of the IdP's strength of identity proofing. For example, it is unlikely a government organization would accept a social media identity as a login for sensitive systems, as it is easy to create fake or throw-away identities, whereas a mobile game company may well need to integrate with major social media platforms to grow their active player base.

Secure use of external identity providers requires careful configuration and verification to prevent identity spoofing or forged assertions. This section provides requirements to address these risks.

#	Description	Level
6.8.1	Verify that, if the application supports multiple identity providers (IdPs), the user's identity cannot be spoofed via another supported identity provider (eg. by using the same user identifier). The standard mitigation would be for the application to register and identify the user using a combination of the IdP ID (serving as a namespace) and the user's ID in the IdP.	2
6.8.2	Verify that the presence and integrity of digital signatures on authentication assertions (for example on JWTs or SAML assertions) are always validated, rejecting any assertions that are unsigned or have invalid signatures.	2
6.8.3	Verify that SAML assertions are uniquely processed and used only once within the validity period to prevent replay attacks.	2

#	Description	Level
6.8.4	Verify that, if an application uses a separate Identity Provider (IdP) and expects specific authentication strength, methods, or recentness for specific functions, the application verifies this using the information returned by the IdP. For example, if OIDC is used, this might be achieved by validating ID Token claims such as 'acr', 'amr', and 'auth_time'(if present). If the IdP does not provide this information, the application must have a documented fallback approach that assumes that the minimum strength authentication mechanism was used (for example, single-factor authentication using username and password).	2

References

For more information, see also:

- NIST SP 800-63 - Digital Identity Guidelines
- NIST SP 800-63B - Authentication and Lifecycle Management
- NIST SP 800-63 FAQ
- OWASP Web Security Testing Guide: Testing for Authentication
- OWASP Password Storage Cheat Sheet
- OWASP Forgot Password Cheat Sheet
- OWASP Choosing and Using Security Questions Cheat Sheet
- CISA Guidance on "Number Matching"
- Details on the FIDO Alliance

V7 Session Management

Control Objective

Session management mechanisms allow applications to correlate user and device interactions over time, even when using stateless communication protocols (such as HTTP). Modern applications may use multiple session tokens with distinct characteristics and purposes. A secure session management system is one that prevents attackers from obtaining, utilizing, or otherwise abusing a victim's session. Applications maintaining sessions must ensure that the following high-level session management requirements are met:

- Sessions are unique to each individual and cannot be guessed or shared.
- Sessions are invalidated when no longer required and are timed out during periods of inactivity.

Many of the requirements in this chapter relate to selected NIST SP 800-63 Digital Identity Guidelines controls, focusing on common threats and commonly exploited authentication weaknesses.

Note that requirements for specific implementation details of certain session management mechanisms can be found elsewhere:

- HTTP Cookies are a common mechanism for securing session tokens. Specific security requirements for cookies can be found in the “Web Frontend Security”chapter.
- Self-contained tokens are frequently used as a way of maintaining sessions. Specific security requirements can be found in the “Self-contained Tokens”chapter.

V7.1 Session Management Documentation

There is no single pattern that suits all applications. Therefore, it is not feasible to define universal boundaries and limits that suit all cases. A risk analysis with documented security decisions related to session handling must be conducted as a prerequisite to implementation and testing. This ensures that the session management system is tailored to the specific requirements of the application.

Regardless of whether a stateful or “stateless”session mechanism is chosen, the analysis must be complete and documented to demonstrate that the selected solution is capable of satisfying all relevant security requirements. Interaction with any Single Sign-on (SSO) mechanisms in use should also be considered.

#	Description	Level
7.1.1	Verify that the user’s session inactivity timeout and absolute maximum session lifetime are documented, are appropriate in combination with other controls, and that the documentation includes justification for any deviations from NIST SP 800-63B re-authentication requirements.	2
7.1.2	Verify that the documentation defines how many concurrent (parallel) sessions are allowed for one account as well as the intended behaviors and actions to be taken when the maximum number of active sessions is reached.	2
7.1.3	Verify that all systems that create and manage user sessions as part of a federated identity management ecosystem (such as SSO systems) are documented along with controls to coordinate session lifetimes, termination, and any other conditions that require re-authentication.	2

V7.2 Fundamental Session Management Security

This section satisfies the essential requirements of secure sessions by verifying that session tokens are securely generated and validated.

#	Description	Level
7.2.1	Verify that the application performs all session token verification using a trusted, backend service.	1
7.2.2	Verify that the application uses either self-contained or reference tokens that are dynamically generated for session management, i.e. not using static API secrets and keys.	1
7.2.3	Verify that if reference tokens are used to represent user sessions, they are unique and generated using a cryptographically secure pseudo-random number generator (CSPRNG) and possess at least 128 bits of entropy.	1
7.2.4	Verify that the application generates a new session token on user authentication, including re-authentication, and terminates the current session token.	1

V7.3 Session Timeout

Session timeout mechanisms serve to minimize the window of opportunity for session hijacking and other forms of session abuse. Timeouts must satisfy documented security decisions.

#	Description	Level
7.3.1	Verify that there is an inactivity timeout such that re-authentication is enforced according to risk analysis and documented security decisions.	2
7.3.2	Verify that there is an absolute maximum session lifetime such that re-authentication is enforced according to risk analysis and documented security decisions.	2

V7.4 Session Termination

Session termination may be handled either by the application itself or by the SSO provider if the SSO provider is handling session management instead of the application. It may be necessary to decide whether the SSO provider is in scope when considering the requirements in this section as some may be controlled by the provider.

Session termination should result in requiring re-authentication and be effective across the application, federated login (if present), and any relying parties.

For stateful session mechanisms, termination typically involves invalidating the session on the backend. In the case of self-contained tokens, additional measures are required to revoke or block these tokens, as they may otherwise remain valid until expiration.

#	Description	Level
7.4.1	Verify that when session termination is triggered (such as logout or expiration), the application disallows any further use of the session. For reference tokens or stateful sessions, this means invalidating the session data at the application backend. Applications using self-contained tokens will need a solution such as maintaining a list of terminated tokens, disallowing tokens produced before a per-user date and time or rotating a per-user signing key.	1
7.4.2	Verify that the application terminates all active sessions when a user account is disabled or deleted (such as an employee leaving the company).	1
7.4.3	Verify that the application gives the option to terminate all other active sessions after a successful change or removal of any authentication factor (including password change via reset or recovery and, if present, an MFA settings update).	2
7.4.4	Verify that all pages that require authentication have easy and visible access to logout functionality.	2
7.4.5	Verify that application administrators are able to terminate active sessions for an individual user or for all users.	2

V7.5 Defenses Against Session Abuse

This section provides requirements to mitigate the risk posed by active sessions that are either hijacked or abused through vectors that rely on the existence and capabilities of active user sessions. For example, using malicious content execution to force an authenticated victim browser to perform an action using the victim's session.

Note that the level-specific guidance in the "Authentication"chapter should be taken into account when considering requirements in this section.

#	Description	Level
7.5.1	Verify that the application requires full re-authentication before allowing modifications to sensitive account attributes which may affect authentication such as email address, phone number, MFA configuration, or other information used in account recovery.	2
7.5.2	Verify that users are able to view and (having authenticated again with at least one factor) terminate any or all currently active sessions.	2

#	Description	Level
7.5.3	Verify that the application requires further authentication with at least one factor or secondary verification before performing highly sensitive transactions or operations.	3

V7.6 Federated Re-authentication

This section relates to those writing Relying Party (RP) or Identity Provider (IdP) code. These requirements are derived from the NIST SP 800-63C for Federation & Assertions.

#	Description	Level
7.6.1	Verify that session lifetime and termination between Relying Parties (RPs) and Identity Providers (IdPs) behave as documented, requiring re-authentication as necessary such as when the maximum time between IdP authentication events is reached.	2
7.6.2	Verify that creation of a session requires either the user's consent or an explicit action, preventing the creation of new application sessions without user interaction.	2

References

For more information, see also:

- OWASP Web Security Testing Guide: Session Management Testing
- OWASP Session Management Cheat Sheet

V8 Authorization

Control Objective

Authorization ensures that access is granted only to permitted consumers (users, servers, and other clients). To enforce the Principle of Least Privilege (POLP), verified applications must meet the following high-level requirements:

- Document authorization rules, including decision-making factors and environmental contexts.
- Consumers should have access only to resources permitted by their defined entitlements.

V8.1 Authorization Documentation

Comprehensive authorization documentation is essential to ensure that security decisions are consistently applied, auditable, and aligned with organizational policies. This reduces the risk of unauthorized access by making security requirements clear and actionable for developers, administrators, and testers.

#	Description	Level
8.1.1	Verify that authorization documentation defines rules for restricting function-level and data-specific access based on consumer permissions and resource attributes.	1
8.1.2	Verify that authorization documentation defines rules for field-level access restrictions (both read and write) based on consumer permissions and resource attributes. Note that these rules might depend on other attribute values of the relevant data object, such as state or status.	2
8.1.3	Verify that the application's documentation defines the environmental and contextual attributes (including but not limited to, time of day, user location, IP address, or device) that are used in the application to make security decisions, including those pertaining to authentication and authorization.	3
8.1.4	Verify that authentication and authorization documentation defines how environmental and contextual factors are used in decision-making, in addition to function-level, data-specific, and field-level authorization. This should include the attributes evaluated, thresholds for risk, and actions taken (e.g., allow, challenge, deny, step-up authentication).	3

V8.2 General Authorization Design

Implementing granular authorization controls at the function, data, and field levels ensures that consumers can access only what has been explicitly granted to them.

#	Description	Level
8.2.1	Verify that the application ensures that function-level access is restricted to consumers with explicit permissions.	1
8.2.2	Verify that the application ensures that data-specific access is restricted to consumers with explicit permissions to specific data items to mitigate insecure direct object reference (IDOR) and broken object level authorization (BOLA).	1

#	Description	Level
8.2.3	Verify that the application ensures that field-level access is restricted to consumers with explicit permissions to specific fields to mitigate broken object property level authorization (BOPLA).	2
8.2.4	Verify that adaptive security controls based on a consumer's environmental and contextual attributes (such as time of day, location, IP address, or device) are implemented for authentication and authorization decisions, as defined in the application's documentation. These controls must be applied when the consumer tries to start a new session and also during an existing session.	3

V8.3 Operation Level Authorization

The immediate application of authorization changes in the appropriate tier of an application's architecture is crucial to preventing unauthorized actions, especially in dynamic environments.

#	Description	Level
8.3.1	Verify that the application enforces authorization rules at a trusted service layer and doesn't rely on controls that an untrusted consumer could manipulate, such as client-side JavaScript.	1
8.3.2	Verify that changes to values on which authorization decisions are made are applied immediately. Where changes cannot be applied immediately, (such as when relying on data in self-contained tokens), there must be mitigating controls to alert when a consumer performs an action when they are no longer authorized to do so and revert the change. Note that this alternative would not mitigate information leakage.	3
8.3.3	Verify that access to an object is based on the originating subject's (e.g. consumer's) permissions, not on the permissions of any intermediary or service acting on their behalf. For example, if a consumer calls a web service using a self-contained token for authentication, and the service then requests data from a different service, the second service will use the consumer's token, rather than a machine-to-machine token from the first service, to make permission decisions.	3

V8.4 Other Authorization Considerations

Additional considerations for authorization, particularly for administrative interfaces and multi-tenant environments, help prevent unauthorized access.

#	Description	Level
8.4.1	Verify that multi-tenant applications use cross-tenant controls to ensure consumer operations will never affect tenants with which they do not have permissions to interact.	2
8.4.2	Verify that access to administrative interfaces incorporates multiple layers of security, including continuous consumer identity verification, device security posture assessment, and contextual risk analysis, ensuring that network location or trusted endpoints are not the sole factors for authorization even though they may reduce the likelihood of unauthorized access.	3

References

For more information, see also:

- OWASP Web Security Testing Guide: Authorization
- OWASP Authorization Cheat Sheet

V9 Self-contained Tokens

Control Objective

The concept of a self-contained token is mentioned in the original RFC 6749 OAuth 2.0 from 2012. It refers to a token containing data or claims on which a receiving service will rely to make security decisions. This should be differentiated from a simple token containing only an identifier, which a receiving service uses to look up data locally. The most common examples of self-contained tokens are JSON Web Tokens (JWTs) and SAML assertions.

The use of self-contained tokens has become very widespread, even outside of OAuth and OIDC. At the same time, the security of this mechanism relies on the ability to validate the integrity of the token and to ensure that the token is valid for a particular context. There are many pitfalls with this process, and this chapter provides specific details of the mechanisms that applications should have in place to prevent them.

V9.1 Token source and integrity

This section includes requirements to ensure that the token has been produced by a trusted party and has not been tampered with.

#	Description	Level
9.1.1	Verify that self-contained tokens are validated using their digital signature or MAC to protect against tampering before accepting the token's contents.	1
9.1.2	Verify that only algorithms on an allowlist can be used to create and verify self-contained tokens, for a given context. The allowlist must include the permitted algorithms, ideally only either symmetric or asymmetric algorithms, and must not include the 'None'algorithm. If both symmetric and asymmetric must be supported, additional controls will be needed to prevent key confusion.	1
9.1.3	Verify that key material that is used to validate self-contained tokens is from trusted pre-configured sources for the token issuer, preventing attackers from specifying untrusted sources and keys. For JWTs and other JWS structures, headers such as 'jku', 'x5u', and 'jwk'must be validated against an allowlist of trusted sources.	1

V9.2 Token content

Before making security decisions based on the content of a self-contained token, it is necessary to validate that the token has been presented within its validity period and that it is intended for use by the receiving service and for the purpose for which it was presented. This helps avoid insecure cross-usage between different services or with different token types from the same issuer.

Specific requirements for OAuth and OIDC are covered in the dedicated chapter.

#	Description	Level
9.2.1	Verify that, if a validity time span is present in the token data, the token and its content are accepted only if the verification time is within this validity time span. For example, for JWTs, the claims 'nbf'and 'exp'must be verified.	1
9.2.2	Verify that the service receiving a token validates the token to be the correct type and is meant for the intended purpose before accepting the token's contents. For example, only access tokens can be accepted for authorization decisions and only ID Tokens can be used for proving user authentication.	2
9.2.3	Verify that the service only accepts tokens which are intended for use with that service (audience). For JWTs, this can be achieved by validating the 'aud' claim against an allowlist defined in the service.	2

#	Description	Level
9.2.4	Verify that, if a token issuer uses the same private key for issuing tokens to different audiences, the issued tokens contain an audience restriction that uniquely identifies the intended audiences. This will prevent a token from being reused with an unintended audience. If the audience identifier is dynamically provisioned, the token issuer must validate these audiences in order to make sure that they do not result in audience impersonation.	2

References

For more information, see also:

- OWASP JSON Web Token Cheat Sheet for Java Cheat Sheet (but has useful general guidance)

V10 OAuth and OIDC

Control Objective

OAuth2 (referred to as OAuth in this chapter) is an industry-standard framework for delegated authorization. For example, using OAuth, a client application can obtain access to APIs (server resources) on a user's behalf, provided the user has authorized the client application to do so.

By itself, OAuth is not designed for user authentication. The OpenID Connect (OIDC) framework extends OAuth by adding a user identity layer on top of OAuth. OIDC provides support for features including standardized user information, Single Sign-On (SSO), and session management. As OIDC is an extension of OAuth, the OAuth requirements in this chapter also apply to OIDC.

The following roles are defined in OAuth:

- The OAuth client is the application that attempts to obtain access to server resources (e.g., by calling an API using the issued access token). The OAuth client is often a server-side application.
  - A confidential client is a client capable of maintaining the confidentiality of the credentials it uses to authenticate itself with the authorization server.
  - A public client is not capable of maintaining the confidentiality of credentials for authenticating with the authorization server. Therefore, instead of authenticating itself (e.g., using 'client_id'and 'client_secret'parameters), it only identifies itself (using a 'client_id' parameter).
- The OAuth resource server (RS) is the server API exposing resources to OAuth clients.
- The OAuth authorization server (AS) is a server application that issues access tokens to OAuth clients. These access tokens allow OAuth clients to access RS resources, either on behalf of an

end-user or on the OAuth client's own behalf. The AS is often a separate application, but (if appropriate) it may be integrated into a suitable RS.
- The resource owner (RO) is the end-user who authorizes OAuth clients to obtain limited access to resources hosted on the resource server on their behalf. The resource owner consents to this delegated authorization by interacting with the authorization server.

The following roles are defined in OIDC:

- The relying party (RP) is the client application requesting end-user authentication through the OpenID Provider. It assumes the role of an OAuth client.
- The OpenID Provider (OP) is an OAuth AS that is capable of authenticating the end-user and provides OIDC claims to an RP. The OP may be the identity provider (IdP), but in federated scenarios, the OP and the identity provider (where the end-user authenticates) may be different server applications.

OAuth and OIDC were initially designed for third-party applications. Today, they are often used by first-party applications as well. However, when used in first-party scenarios, such as authentication and session management, the protocol adds some complexity, which may introduce new security challenges.

OAuth and OIDC can be used for many types of applications, but the focus for ASVS and the requirements in this chapter is on web applications and APIs.

Since OAuth and OIDC can be considered logic on top of web technologies, general requirements from other chapters always apply, and this chapter cannot be taken out of context.

This chapter addresses best current practices for OAuth2 and OIDC aligned with specifications found at https://oauth.net/2/ and https://openid.net/developers/specs/. Even if RFCs are considered mature, they are updated frequently. Thus, it is important to align with the latest versions when applying the requirements in this chapter. See the references section for more details.

Given the complexity of the area, it is vitally important for a secure OAuth or OIDC solution to use well-known industry-standard authorization servers and apply the recommended security configuration.

Terminology used in this chapter aligns with OAuth RFCs and OIDC specifications, but note that OIDC terminology is only used for OIDC-specific requirements; otherwise, OAuth terminology is used.

In the context of OAuth and OIDC, the term "token"in this chapter refers to:

- Access tokens, which shall only be consumed by the RS and can either be reference tokens that are validated using introspection or self-contained tokens that are validated using some key material.
- Refresh tokens, which shall only be consumed by the authorization server that issued the token.
- OIDC ID Tokens, which shall only be consumed by the client that triggered the authorization flow.

The risk levels for some of the requirements in this chapter depend on whether the client is a confidential client or regarded as a public client. Since using strong client authentication mitigates many attack vectors, a few requirements might be relaxed when using a confidential client for L1 applications.

V10.1 Generic OAuth and OIDC Security

This section covers generic architectural requirements that apply to all applications using OAuth or OIDC.

#	Description	Level
10.1.1	Verify that tokens are only sent to components that strictly need them. For example, when using a backend-for-frontend pattern for browser-based JavaScript applications, access and refresh tokens shall only be accessible for the backend.	2
10.1.2	Verify that the client only accepts values from the authorization server (such as the authorization code or ID Token) if these values result from an authorization flow that was initiated by the same user agent session and transaction. This requires that client-generated secrets, such as the proof key for code exchange (PKCE) 'code_verifier', 'state'or OIDC 'nonce', are not guessable, are specific to the transaction, and are securely bound to both the client and the user agent session in which the transaction was started.	2

V10.2 OAuth Client

These requirements detail the responsibilities for OAuth client applications. The client can be, for example, a web server backend (often acting as a Backend For Frontend, BFF), a backend service integration, or a frontend Single Page Application (SPA, aka browser-based application).

In general, backend clients are regarded as confidential clients and frontend clients are regarded as public clients. However, native applications running on the end-user device can be regarded as confidential when using OAuth dynamic client registration.

#	Description	Level
10.2.1	Verify that, if the code flow is used, the OAuth client has protection against browser-based request forgery attacks, commonly known as cross-site request forgery (CSRF), which trigger token requests, either by using proof key for code exchange (PKCE) functionality or checking the 'state'parameter that was sent in the authorization request.	2

#	Description	Level
10.2.2	Verify that, if the OAuth client can interact with more than one authorization server, it has a defense against mix-up attacks. For example, it could require that the authorization server return the 'iss'parameter value and validate it in the authorization response and the token response.	2
10.2.3	Verify that the OAuth client only requests the required scopes (or other authorization parameters) in requests to the authorization server.	3

V10.3 OAuth Resource Server

In the context of ASVS and this chapter, the resource server is an API. To provide secure access, the resource server must:

- Validate the access token, according to the token format and relevant protocol specifications, e.g., JWT-validation or OAuth token introspection.
- If valid, enforce authorization decisions based on the information from the access token and permissions which have been granted. For example, the resource server needs to verify that the client (acting on behalf of RO) is authorized to access the requested resource.

Therefore, the requirements listed here are OAuth or OIDC specific and should be performed after token validation and before performing authorization based on information from the token.

#	Description	Level
10.3.1	Verify that the resource server only accepts access tokens that are intended for use with that service (audience). The audience may be included in a structured access token (such as the 'aud'claim in JWT), or it can be checked using the token introspection endpoint.	2
10.3.2	Verify that the resource server enforces authorization decisions based on claims from the access token that define delegated authorization. If claims such as 'sub', 'scope', and 'authorization_details'are present, they must be part of the decision.	2
10.3.3	Verify that if an access control decision requires identifying a unique user from an access token (JWT or related token introspection response), the resource server identifies the user from claims that cannot be reassigned to other users. Typically, it means using a combination of 'iss'and 'sub'claims.	2

#	Description	Level
10.3.4	Verify that, if the resource server requires specific authentication strength, methods, or recentness, it verifies that the presented access token satisfies these constraints. For example, if present, using the OIDC ‘acr’, ‘amr’and ‘auth_time’claims respectively.	2
10.3.5	Verify that the resource server prevents the use of stolen access tokens or replay of access tokens (from unauthorized parties) by requiring sender-constrained access tokens, either Mutual TLS for OAuth 2 or OAuth 2 Demonstration of Proof of Possession (DPoP).	3

V10.4 OAuth Authorization Server

These requirements detail the responsibilities for OAuth authorization servers, including OpenID Providers.

For client authentication, the ‘self_signed_tls_client_auth’method is allowed with the prerequisites required by section 2.2 of RFC 8705.

#	Description	Level
10.4.1	Verify that the authorization server validates redirect URIs based on a client-specific allowlist of pre-registered URIs using exact string comparison.	1
10.4.2	Verify that, if the authorization server returns the authorization code in the authorization response, it can be used only once for a token request. For the second valid request with an authorization code that has already been used to issue an access token, the authorization server must reject a token request and revoke any issued tokens related to the authorization code.	1
10.4.3	Verify that the authorization code is short-lived. The maximum lifetime can be up to 10 minutes for L1 and L2 applications and up to 1 minute for L3 applications.	1
10.4.4	Verify that for a given client, the authorization server only allows the usage of grants that this client needs to use. Note that the grants ‘token’(Implicit flow) and ‘password’(Resource Owner Password Credentials flow) must no longer be used.	1

#	Description	Level
10.4.5	Verify that the authorization server mitigates refresh token replay attacks for public clients, preferably using sender-constrained refresh tokens, i.e., Demonstrating Proof of Possession (DPoP) or Certificate-Bound Access Tokens using mutual TLS (mTLS). For L1 and L2 applications, refresh token rotation may be used. If refresh token rotation is used, the authorization server must invalidate the refresh token after usage, and revoke all refresh tokens for that authorization if an already used and invalidated refresh token is provided.	1
10.4.6	Verify that, if the code grant is used, the authorization server mitigates authorization code interception attacks by requiring proof key for code exchange (PKCE). For authorization requests, the authorization server must require a valid 'code_challenge'value and must not accept a 'code_challenge_method'value of 'plain'. For a token request, it must require validation of the 'code_verifier'parameter.	2
10.4.7	Verify that if the authorization server supports unauthenticated dynamic client registration, it mitigates the risk of malicious client applications. It must validate client metadata such as any registered URIs, ensure the user's consent, and warn the user before processing an authorization request with an untrusted client application.	2
10.4.8	Verify that refresh tokens have an absolute expiration, including if sliding refresh token expiration is applied.	2
10.4.9	Verify that refresh tokens and reference access tokens can be revoked by an authorized user using the authorization server user interface, to mitigate the risk of malicious clients or stolen tokens.	2
10.4.10	Verify that confidential client is authenticated for client-to-authorized server backchannel requests such as token requests, pushed authorization requests (PAR), and token revocation requests.	2
10.4.11	Verify that the authorization server configuration only assigns the required scopes to the OAuth client.	2
10.4.12	Verify that for a given client, the authorization server only allows the 'response_mode'value that this client needs to use. For example, by having the authorization server validate this value against the expected values or by using pushed authorization request (PAR) or JWT-secured Authorization Request (JAR).	3
10.4.13	Verify that grant type 'code'is always used together with pushed authorization requests (PAR).	3

#	Description	Level
10.4.14	Verify that the authorization server issues only sender-constrained (Proof-of-Possession) access tokens, either with certificate-bound access tokens using mutual TLS (mTLS) or DPoP-bound access tokens (Demonstration of Proof of Possession).	3
10.4.15	Verify that, for a server-side client (which is not executed on the end-user device), the authorization server ensures that the 'authorization_details' parameter value is from the client backend and that the user has not tampered with it. For example, by requiring the usage of pushed authorization request (PAR) or JWT-secured Authorization Request (JAR).	3
10.4.16	Verify that the client is confidential and the authorization server requires the use of strong client authentication methods (based on public-key cryptography and resistant to replay attacks), such as mutual TLS ('tls_client_auth', 'self_signed_tls_client_auth') or private key JWT ('private_key_jwt').	3

V10.5 OIDC Client

As the OIDC relying party acts as an OAuth client, the requirements from the section "OAuth Client" apply as well.

Note that the "Authentication with an Identity Provider"section in the "Authentication"chapter also contains relevant general requirements.

#	Description	Level
10.5.1	Verify that the client (as the relying party) mitigates ID Token replay attacks. For example, by ensuring that the 'nonce'claim in the ID Token matches the 'nonce'value sent in the authentication request to the OpenID Provider (in OAuth2 refereed to as the authorization request sent to the authorization server).	2
10.5.2	Verify that the client uniquely identifies the user from ID Token claims, usually the 'sub'claim, which cannot be reassigned to other users (for the scope of an identity provider).	2
10.5.3	Verify that the client rejects attempts by a malicious authorization server to impersonate another authorization server through authorization server metadata. The client must reject authorization server metadata if the issuer URL in the authorization server metadata does not exactly match the pre-configured issuer URL expected by the client.	2

#	Description	Level
10.5.4	Verify that the client validates that the ID Token is intended to be used for that client (audience) by checking that the ‘aud’claim from the token is equal to the ‘client_id’value for the client.	2
10.5.5	Verify that, when using OIDC back-channel logout, the relying party mitigates denial of service through forced logout and cross-JWT confusion in the logout flow. The client must verify that the logout token is correctly typed with a value of ‘logout+jwt’, contains the ‘event’claim with the correct member name, and does not contain a ‘nonce’claim. Note that it is also recommended to have a short expiration (e.g., 2 minutes).	2

V10.6 OpenID Provider

As OpenID Providers act as OAuth authorization servers, the requirements from the section “OAuth Authorization Server”apply as well.

Note that if using the ID Token flow (not the code flow), no access tokens are issued, and many of the requirements for OAuth AS are not applicable.

#	Description	Level
10.6.1	Verify that the OpenID Provider only allows values ‘code’, ‘ciba’, ‘id_token’, or ‘id_token code’for response mode. Note that ‘code’is preferred over ‘id_token code’(the OIDC Hybrid flow), and ‘token’(any Implicit flow) must not be used.	2
10.6.2	Verify that the OpenID Provider mitigates denial of service through forced logout. By obtaining explicit confirmation from the end-user or, if present, validating parameters in the logout request (initiated by the relying party), such as the ‘id_token_hint’.	2

V10.7 Consent Management

These requirements cover the verification of the user’s consent by the authorization server. Without proper user consent verification, a malicious actor may obtain permissions on the user’s behalf through spoofing or social-engineering.

#	Description	Level
10.7.1	Verify that the authorization server ensures that the user consents to each authorization request. If the identity of the client cannot be assured, the authorization server must always explicitly prompt the user for consent.	2
10.7.2	Verify that when the authorization server prompts for user consent, it presents sufficient and clear information about what is being consented to. When applicable, this should include the nature of the requested authorizations (typically based on scope, resource server, Rich Authorization Requests (RAR) authorization details), the identity of the authorized application, and the lifetime of these authorizations.	2
10.7.3	Verify that the user can review, modify, and revoke consents which the user has granted through the authorization server.	2

References

For more information on OAuth, please see:

- oauth.net
- OWASP OAuth 2.0 Protocol Cheat Sheet

For OAuth-related requirements in ASVS following published and in draft status RFC-s are used:

- RFC6749 The OAuth 2.0 Authorization Framework
- RFC6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage
- RFC6819 OAuth 2.0 Threat Model and Security Considerations
- RFC7636 Proof Key for Code Exchange by OAuth Public Clients
- RFC7591 OAuth 2.0 Dynamic Client Registration Protocol
- RFC8628 OAuth 2.0 Device Authorization Grant
- RFC8707 Resource Indicators for OAuth 2.0
- RFC9068 JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens
- RFC9126 OAuth 2.0 Pushed Authorization Requests
- RFC9207 OAuth 2.0 Authorization Server Issuer Identification
- RFC9396 OAuth 2.0 Rich Authorization Requests
- RFC9449 OAuth 2.0 Demonstrating Proof of Possession (DPoP)
- RFC9700 Best Current Practice for OAuth 2.0 Security
- draft OAuth 2.0 for Browser-Based Applications
- draft The OAuth 2.1 Authorization Framework

For more information on OpenID Connect, please see:

- OpenID Connect Core 1.0

- FAPI 2.0 Security Profile

V11 Cryptography

Control Objective

The objective of this chapter is to define best practices for the general use of cryptography, as well as to instill a fundamental understanding of cryptographic principles and inspire a shift toward more resilient and modern approaches. It encourages the following:

- Implementing robust cryptographic systems that fail securely, adapt to evolving threats, and are future-proof.
- Utilizing cryptographic mechanisms that are both secure and aligned with industry best practices.
- Maintaining a secure cryptographic key management system with appropriate access controls and auditing.
- Regularly evaluating the cryptographic landscape to assess new risks and adapt algorithms accordingly.
- Discovering and managing cryptographic use cases throughout the application's lifecycle to ensure that all cryptographic assets are accounted for and secured.

In addition to outlining general principles and best practices, this document also provides more in-depth technical information about the requirements in Appendix C - Cryptography Standards. This includes algorithms and modes that are considered "approved"for the purposes of the requirements in this chapter.

Requirements that use cryptography to solve a separate problem, such as secrets management or communications security, will be in different parts of the standard.

V11.1 Cryptographic Inventory and Documentation

Applications need to be designed with strong cryptographic architecture to protect data assets according to their classification. Encrypting everything is wasteful; not encrypting anything is legally negligent. A balance must be struck, usually during architectural or high-level design, design sprints, or architectural spikes. Designing cryptography "on the fly"or retrofitting it will inevitably cost much more to implement securely than simply building it in from the start.

It is important to ensure that all cryptographic assets are regularly discovered, inventoried, and assessed. Please see the appendix for more information on how this can be done.

The need to future-proof cryptographic systems against the eventual rise of quantum computing is also critical. Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to

remain secure against attacks by quantum computers, which are expected to break widely used algorithms such as RSA and elliptic curve cryptography (ECC).

Please see the appendix for current guidance on vetted PQC primitives and standards.

#	Description	Level
11.1.1	Verify that there is a documented policy for management of cryptographic keys and a cryptographic key lifecycle that follows a key management standard such as NIST SP 800-57. This should include ensuring that keys are not overshared (for example, with more than two entities for shared secrets and more than one entity for private keys).	2
11.1.2	Verify that a cryptographic inventory is performed, maintained, regularly updated, and includes all cryptographic keys, algorithms, and certificates used by the application. It must also document where keys can and cannot be used in the system, and the types of data that can and cannot be protected using the keys.	2
11.1.3	Verify that cryptographic discovery mechanisms are employed to identify all instances of cryptography in the system, including encryption, hashing, and signing operations.	3
11.1.4	Verify that a cryptographic inventory is maintained. This must include a documented plan that outlines the migration path to new cryptographic standards, such as post-quantum cryptography, in order to react to future threats.	3

V11.2 Secure Cryptography Implementation

This section defines the requirements for the selection, implementation, and ongoing management of core cryptographic algorithms for an application. The objective is to ensure that only robust, industry-accepted cryptographic primitives are deployed, in alignment with current standards (e.g., NIST, ISO/IEC) and best practices. Organizations must ensure that each cryptographic component is selected based on peer-reviewed evidence and practical security testing.

#	Description	Level
11.2.1	Verify that industry-validated implementations (including libraries and hardware-accelerated implementations) are used for cryptographic operations.	2

#	Description	Level
11.2.2	Verify that the application is designed with crypto agility such that random number, authenticated encryption, MAC, or hashing algorithms, key lengths, rounds, ciphers and modes can be reconfigured, upgraded, or swapped at any time, to protect against cryptographic breaks. Similarly, it must also be possible to replace keys and passwords and re-encrypt data. This will allow for seamless upgrades to post-quantum cryptography (PQC), once high-assurance implementations of approved PQC schemes or standards are widely available.	2
11.2.3	Verify that all cryptographic primitives utilize a minimum of 128-bits of security based on the algorithm, key size, and configuration. For example, a 256-bit ECC key provides roughly 128 bits of security where RSA requires a 3072-bit key to achieve 128 bits of security.	2
11.2.4	Verify that all cryptographic operations are constant-time, with no ‘short-circuit’operations in comparisons, calculations, or returns, to avoid leaking information.	3
11.2.5	Verify that all cryptographic modules fail securely, and errors are handled in a way that does not enable vulnerabilities, such as Padding Oracle attacks.	3

V11.3 Encryption Algorithms

Authenticated encryption algorithms built on AES and CHACHA20 form the backbone of modern cryptographic practice.

#	Description	Level
11.3.1	Verify that insecure block modes (e.g., ECB) and weak padding schemes (e.g., PKCS#1 v1.5) are not used.	1
11.3.2	Verify that only approved ciphers and modes such as AES with GCM are used.	1
11.3.3	Verify that encrypted data is protected against unauthorized modification preferably by using an approved authenticated encryption method or by combining an approved encryption method with an approved MAC algorithm.	2
11.3.4	Verify that nonces, initialization vectors, and other single-use numbers are not used for more than one encryption key and data-element pair. The method of generation must be appropriate for the algorithm being used.	3

#	Description	Level
11.3.5	Verify that any combination of an encryption algorithm and a MAC algorithm is operating in encrypt-then-MAC mode.	3

V11.4 Hashing and Hash-based Functions

Cryptographic hashes are used in a wide variety of cryptographic protocols, such as digital signatures, HMAC, key derivation functions (KDF), random bit generation, and password storage. The security of the cryptographic system is only as strong as the underlying hash functions used. This section outlines the requirements for using secure hash functions in cryptographic operations.

For password storage, as well as the cryptography appendix, the OWASP Password Storage Cheat Sheet will also provide useful context and guidance.

#	Description	Level
11.4.1	Verify that only approved hash functions are used for general cryptographic use cases, including digital signatures, HMAC, KDF, and random bit generation. Disallowed hash functions, such as MD5, must not be used for any cryptographic purpose.	1
11.4.2	Verify that passwords are stored using an approved, computationally intensive, key derivation function (also known as a “password hashing function”), with parameter settings configured based on current guidance. The settings should balance security and performance to make brute-force attacks sufficiently challenging for the required level of security.	2
11.4.3	Verify that hash functions used in digital signatures, as part of data authentication or data integrity are collision resistant and have appropriate bit-lengths. If collision resistance is required, the output length must be at least 256 bits. If only resistance to second pre-image attacks is required, the output length must be at least 128 bits.	2
11.4.4	Verify that the application uses approved key derivation functions with key stretching parameters when deriving secret keys from passwords. The parameters in use must balance security and performance to prevent brute-force attacks from compromising the resulting cryptographic key.	2

V11.5 Random Values

Cryptographically secure Pseudo-random Number Generation (CSPRNG) is incredibly difficult to get right. Generally, good sources of entropy within a system will be quickly depleted if over-used, but

sources with less randomness can lead to predictable keys and secrets.

#	Description	Level
11.5.1	Verify that all random numbers and strings which are intended to be non-guessable must be generated using a cryptographically secure pseudo-random number generator (CSPRNG) and have at least 128 bits of entropy. Note that UUIDs do not respect this condition.	2
11.5.2	Verify that the random number generation mechanism in use is designed to work securely, even under heavy demand.	3

V11.6 Public Key Cryptography

Public Key Cryptography will be used where it is not possible or not desirable to share a secret key between multiple parties.

As part of this, there exists a need for approved key exchange mechanisms, such as Diffie-Hellman and Elliptic Curve Diffie-Hellman (ECDH) to ensure that the cryptosystem remains secure against modern threats. The “Secure Communication”chapter provides requirements for TLS so the requirements in this section are intended for situations where Public Key Cryptography is being used in use cases other than TLS.

#	Description	Level
11.6.1	Verify that only approved cryptographic algorithms and modes of operation are used for key generation and seeding, and digital signature generation and verification. Key generation algorithms must not generate insecure keys vulnerable to known attacks, for example, RSA keys which are vulnerable to Fermat factorization.	2
11.6.2	Verify that approved cryptographic algorithms are used for key exchange (such as Diffie-Hellman) with a focus on ensuring that key exchange mechanisms use secure parameters. This will prevent attacks on the key establishment process which could lead to adversary-in-the-middle attacks or cryptographic breaks.	3

V11.7 In-Use Data Cryptography

Protecting data while it is being processed is paramount. Techniques such as full memory encryption, encryption of data in transit, and ensuring data is encrypted as quickly as possible after use is recommended.

#	Description	Level
11.7.1	Verify that full memory encryption is in use that protects sensitive data while it is in use, preventing access by unauthorized users or processes.	3
11.7.2	Verify that data minimization ensures the minimal amount of data is exposed during processing, and ensure that data is encrypted immediately after use or as soon as feasible.	3

References

For more information, see also:

- OWASP Web Security Testing Guide: Testing for Weak Cryptography
- OWASP Cryptographic Storage Cheat Sheet
- FIPS 140-3
- NIST SP 800-57

V12 Secure Communication

Control Objective

This chapter includes requirements related to the specific mechanisms that should be in place to protect data in transit, both between an end-user client and a backend service, as well as between internal and backend services.

The general concepts promoted by this chapter include:

- Ensuring that communications are encrypted externally, and ideally internally as well.
- Configuring encryption mechanisms using the latest guidance, including preferred algorithms and ciphers.
- Ensuring that communications are not being intercepted by unauthorized parties through the use of signed certificates.

In addition to outlining general principles and best practices, the ASVS also provides more in-depth technical information about cryptographic strength in Appendix C - Cryptography Standards.

V12.1 General TLS Security Guidance

This section provides initial guidance on how to secure TLS communications. Up-to-date tools should be used to review TLS configuration on an ongoing basis.

While the use of wildcard TLS certificates is not inherently insecure, a compromise of a certificate that is deployed across all owned environments (e.g., production, staging, development, and test) may lead to a compromise of the security posture of the applications using it. Proper protection, management, and the use of separate TLS certificates in different environments should be employed if possible.

#	Description	Level
12.1.1	Verify that only the latest recommended versions of the TLS protocol are enabled, such as TLS 1.2 and TLS 1.3. The latest version of the TLS protocol must be the preferred option.	1
12.1.2	Verify that only recommended cipher suites are enabled, with the strongest cipher suites set as preferred. L3 applications must only support cipher suites which provide forward secrecy.	2
12.1.3	Verify that the application validates that mTLS client certificates are trusted before using the certificate identity for authentication or authorization.	2
12.1.4	Verify that proper certification revocation, such as Online Certificate Status Protocol (OCSP) Stapling, is enabled and configured.	3
12.1.5	Verify that Encrypted Client Hello (ECH) is enabled in the application's TLS settings to prevent exposure of sensitive metadata, such as the Server Name Indication (SNI), during TLS handshake processes.	3

V12.2 HTTPS Communication with External Facing Services

Ensure all HTTP traffic to external-facing services which the application exposes is sent encrypted, with publicly trusted certificates.

#	Description	Level
12.2.1	Verify that TLS is used for all connectivity between a client and external facing, HTTP-based services, and does not fall back to insecure or unencrypted communications.	1
12.2.2	Verify that external facing services use publicly trusted TLS certificates.	1

V12.3 General Service to Service Communication Security

Server communications (both internal and external) involve more than just HTTP. Connections to and from other systems must also be secure, ideally using TLS.

#	Description	Level
12.3.1	Verify that an encrypted protocol such as TLS is used for all inbound and outbound connections to and from the application, including monitoring systems, management tools, remote access and SSH, middleware, databases, mainframes, partner systems, or external APIs. The server must not fall back to insecure or unencrypted protocols.	2
12.3.2	Verify that TLS clients validate certificates received before communicating with a TLS server.	2
12.3.3	Verify that TLS or another appropriate transport encryption mechanism used for all connectivity between internal, HTTP-based services within the application, and does not fall back to insecure or unencrypted communications.	2
12.3.4	Verify that TLS connections between internal services use trusted certificates. Where internally generated or self-signed certificates are used, the consuming service must be configured to only trust specific internal CAs and specific self-signed certificates.	2
12.3.5	Verify that services communicating internally within a system (intra-service communications) use strong authentication to ensure that each endpoint is verified. Strong authentication methods, such as TLS client authentication, must be employed to ensure identity, using public-key infrastructure and mechanisms that are resistant to replay attacks. For microservice architectures, consider using a service mesh to simplify certificate management and enhance security.	3

References

For more information, see also:

- OWASP - Transport Layer Security Cheat Sheet
- Mozilla's Server Side TLS configuration guide
- Mozilla's tool to generate known good TLS configurations.
- O-Saft - OWASP Project to validate TLS configuration

V13 Configuration

Control Objective

The application's default configuration must be secure for use on the Internet.

This chapter provides guidance on the various configurations necessary to achieve this, including those applied during development, build, and deployment.

Topics covered include preventing data leakage, securely managing communication between components, and protecting secrets.

V13.1 Configuration Documentation

This section outlines documentation requirements for how the application communicates with internal and external services, as well as techniques to prevent loss of availability due to service inaccessibility. It also addresses documentation related to secrets.

#	Description	Level
13.1.1	Verify that all communication needs for the application are documented. This must include external services which the application relies upon and cases where an end user might be able to provide an external location to which the application will then connect.	2
13.1.2	Verify that for each service the application uses, the documentation defines the maximum number of concurrent connections (e.g., connection pool limits) and how the application behaves when that limit is reached, including any fallback or recovery mechanisms, to prevent denial of service conditions.	3
13.1.3	Verify that the application documentation defines resource-management strategies for every external system or service it uses (e.g., databases, file handles, threads, HTTP connections). This should include resource-release procedures, timeout settings, failure handling, and where retry logic is implemented, specifying retry limits, delays, and back-off algorithms. For synchronous HTTP request–response operations it should mandate short timeouts and either disable retries or strictly limit retries to prevent cascading delays and resource exhaustion.	3
13.1.4	Verify that the application's documentation defines the secrets that are critical for the security of the application and a schedule for rotating them, based on the organization's threat model and business requirements.	3

V13.2 Backend Communication Configuration

Applications interact with multiple services, including APIs, databases, or other components. These may be considered internal to the application but not included in the application's standard access control mechanisms, or they may be entirely external. In either case, it is necessary to configure the application to interact securely with these components and, if required, protect that configuration.

Note: The “Secure Communication”chapter provides guidance for encryption in transit.

#	Description	Level
13.2.1	Verify that communications between backend application components that don’t support the application’s standard user session mechanism, including APIs, middleware, and data layers, are authenticated. Authentication must use individual service accounts, short-term tokens, or certificate-based authentication and not unchanging credentials such as passwords, API keys, or shared accounts with privileged access.	2
13.2.2	Verify that communications between backend application components, including local or operating system services, APIs, middleware, and data layers, are performed with accounts assigned the least necessary privileges.	2
13.2.3	Verify that if a credential has to be used for service authentication, the credential being used by the consumer is not a default credential (e.g., root/root or admin/admin).	2
13.2.4	Verify that an allowlist is used to define the external resources or systems with which the application is permitted to communicate (e.g., for outbound requests, data loads, or file access). This allowlist can be implemented at the application layer, web server, firewall, or a combination of different layers.	2
13.2.5	Verify that the web or application server is configured with an allowlist of resources or systems to which the server can send requests or load data or files from.	2
13.2.6	Verify that where the application connects to separate services, it follows the documented configuration for each connection, such as maximum parallel connections, behavior when maximum allowed connections is reached, connection timeouts, and retry strategies.	3

V13.3 Secret Management

Secret management is an essential configuration task to ensure the protection of data used in the application. Specific requirements for cryptography can be found in the “Cryptography”chapter, but this section focuses on the management and handling aspects of secrets.

#	Description	Level
13.3.1	Verify that a secrets management solution, such as a key vault, is used to securely create, store, control access to, and destroy backend secrets. These could include passwords, key material, integrations with databases and third-party systems, keys and seeds for time-based tokens, other internal secrets, and API keys. Secrets must not be included in application source code or included in build artifacts. For an L3 application, this must involve a hardware-backed solution such as an HSM.	2
13.3.2	Verify that access to secret assets adheres to the principle of least privilege.	2
13.3.3	Verify that all cryptographic operations are performed using an isolated security module (such as a vault or hardware security module) to securely manage and protect key material from exposure outside of the security module.	3
13.3.4	Verify that secrets are configured to expire and be rotated based on the application's documentation.	3

V13.4 Unintended Information Leakage

Production configurations should be hardened to avoid disclosing unnecessary data. Many of these issues are rarely rated as significant risks but are often chained with other vulnerabilities. If these issues are not present by default, it raises the bar for attacking an application.

For example, hiding the version of server-side components does not eliminate the need to patch all components, and disabling folder listing does not remove the need to use authorization controls or keep files away from the public folder, but it raises the bar.

#	Description	Level
13.4.1	Verify that the application is deployed either without any source control metadata, including the .git or .svn folders, or in a way that these folders are inaccessible both externally and to the application itself.	1
13.4.2	Verify that debug modes are disabled for all components in production environments to prevent exposure of debugging features and information leakage.	2
13.4.3	Verify that web servers do not expose directory listings to clients unless explicitly intended.	2
13.4.4	Verify that using the HTTP TRACE method is not supported in production environments, to avoid potential information leakage.	2

#	Description	Level
13.4.5	Verify that documentation (such as for internal APIs) and monitoring endpoints are not exposed unless explicitly intended.	2
13.4.6	Verify that the application does not expose detailed version information of backend components.	3
13.4.7	Verify that the web tier is configured to only serve files with specific file extensions to prevent unintentional information, configuration, and source code leakage.	3

References

For more information, see also:

- OWASP Web Security Testing Guide: Configuration and Deployment Management Testing

V14 Data Protection

Control Objective

Applications cannot account for all usage patterns and user behaviors, and should therefore implement controls to limit unauthorized access to sensitive data on client devices.

This chapter includes requirements related to defining what data needs to be protected, how it should be protected, and specific mechanisms to implement or pitfalls to avoid.

Another consideration for data protection is bulk extraction, modification, or excessive usage. Each system's requirements are likely to be very different, so determining what is "abnormal"must consider the threat model and business risk. From an ASVS perspective, detecting these issues is handled in the "Security Logging and Error Handling"chapter, and setting limits is handled in the "Validation and Business Logic"chapter.

V14.1 Data Protection Documentation

A key prerequisite for being able to protect data is to categorize what data should be considered sensitive. There are likely to be several different levels of sensitivity, and for each level, the controls required to protect data at that level will be different.

There are various privacy regulations and laws that affect how applications must approach the storage, use, and transmission of sensitive personal information. This section no longer tries to duplicate

these types of data protection or privacy legislation, but rather focuses on key technical considerations for protecting sensitive data. Please consult local laws and regulations, and consult a qualified privacy specialist or lawyer as required.

#	Description	Level
14.1.1	Verify that all sensitive data created and processed by the application has been identified and classified into protection levels. This includes data that is only encoded and therefore easily decoded, such as Base64 strings or the plaintext payload inside a JWT. Protection levels need to take into account any data protection and privacy regulations and standards which the application is required to comply with.	2
14.1.2	Verify that all sensitive data protection levels have a documented set of protection requirements. This must include (but not be limited to) requirements related to general encryption, integrity verification, retention, how the data is to be logged, access controls around sensitive data in logs, database-level encryption, privacy and privacy-enhancing technologies to be used, and other confidentiality requirements.	2

V14.2 General Data Protection

This section contains various practical requirements related to the protection of data. Most are specific to particular issues such as unintended data leakage, but there is also a general requirement to implement protection controls based on the protection level required for each data item.

#	Description	Level
14.2.1	Verify that sensitive data is only sent to the server in the HTTP message body or header fields, and that the URL and query string do not contain sensitive information, such as an API key or session token.	1
14.2.2	Verify that the application prevents sensitive data from being cached in server components, such as load balancers and application caches, or ensures that the data is securely purged after use.	2
14.2.3	Verify that defined sensitive data is not sent to untrusted parties (e.g., user trackers) to prevent unwanted collection of data outside of the application's control.	2

#	Description	Level
14.2.4	Verify that controls around sensitive data related to encryption, integrity verification, retention, how the data is to be logged, access controls around sensitive data in logs, privacy and privacy-enhancing technologies, are implemented as defined in the documentation for the specific data's protection level.	2
14.2.5	Verify that caching mechanisms are configured to only cache responses which have the expected content type for that resource and do not contain sensitive, dynamic content. The web server should return a 404 or 302 response when a non-existent file is accessed rather than returning a different, valid file. This should prevent Web Cache Deception attacks.	3
14.2.6	Verify that the application only returns the minimum required sensitive data for the application's functionality. For example, only returning some of the digits of a credit card number and not the full number. If the complete data is required, it should be masked in the user interface unless the user specifically views it.	3
14.2.7	Verify that sensitive information is subject to data retention classification, ensuring that outdated or unnecessary data is deleted automatically, on a defined schedule, or as the situation requires.	3
14.2.8	Verify that sensitive information is removed from the metadata of user-submitted files unless storage is consented to by the user.	3

V14.3 Client-side Data Protection

This section contains requirements preventing data from leaking in specific ways at the client or user agent side of an application.

#	Description	Level
14.3.1	Verify that authenticated data is cleared from client storage, such as the browser DOM, after the client or session is terminated. The 'Clear-Site-Data' HTTP response header field may be able to help with this but the client-side should also be able to clear up if the server connection is not available when the session is terminated.	1
14.3.2	Verify that the application sets sufficient anti-caching HTTP response header fields (i.e., Cache-Control: no-store) so that sensitive data is not cached in browsers.	2

#	Description	Level
14.3.3	Verify that data stored in browser storage (such as localStorage, sessionStorage, IndexedDB, or cookies) does not contain sensitive data, with the exception of session tokens.	2

References

For more information, see also:

- Consider using the Security Headers website to check security and anti-caching header fields
- Documentation about anti-caching headers by Mozilla
- OWASP Secure Headers project
- OWASP Privacy Risks Project
- OWASP User Privacy Protection Cheat Sheet
- Australian Privacy Principle 11 - Security of personal information
- European Union General Data Protection Regulation (GDPR) overview
- European Union Data Protection Supervisor - Internet Privacy Engineering Network
- Information on the “Clear-Site-Data”header
- White paper on Web Cache Deception

V15 Secure Coding and Architecture

Control Objective

Many ASVS requirements either relate to a particular area of security, such as authentication or authorization, or pertain to a particular type of application functionality, such as logging or file handling.

This chapter provides general security requirements to consider when designing and developing applications. These requirements focus not only on clean architecture and code quality but also on specific architecture and coding practices necessary for application security.

V15.1 Secure Coding and Architecture Documentation

Many requirements for establishing a secure and defensible architecture depend on clear documentation of decisions made regarding the implementation of specific security controls and the components used within the application.

This section outlines the documentation requirements, including identifying components considered to contain “dangerous functionality”or to be “risky components.”

A component with “dangerous functionality”may be an internally developed or third-party component that performs operations such as deserialization of untrusted data, raw file or binary data parsing, dynamic code execution, or direct memory manipulation. Vulnerabilities in these types of operations pose a high risk of compromising the application and potentially exposing its underlying infrastructure.

A “risky component”is a 3rd party library (i.e., not internally developed) with missing or poorly implemented security controls around its development processes or functionality. Examples include components that are poorly maintained, unsupported, at the end-of-life stage, or have a history of significant vulnerabilities.

This section also emphasizes the importance of defining appropriate timeframes for addressing vulnerabilities in third-party components.

#	Description	Level
15.1.1	Verify that application documentation defines risk based remediation time frames for 3rd party component versions with vulnerabilities and for updating libraries in general, to minimize the risk from these components.	1
15.1.2	Verify that an inventory catalog, such as software bill of materials (SBOM), is maintained of all third-party libraries in use, including verifying that components come from pre-defined, trusted, and continually maintained repositories.	2
15.1.3	Verify that the application documentation identifies functionality which is time-consuming or resource-demanding. This must include how to prevent a loss of availability due to overusing this functionality and how to avoid a situation where building a response takes longer than the consumer’s timeout. Potential defenses may include asynchronous processing, using queues, and limiting parallel processes per user and per application.	2
15.1.4	Verify that application documentation highlights third-party libraries which are considered to be “risky components”.	3
15.1.5	Verify that application documentation highlights parts of the application where “dangerous functionality”is being used.	3

V15.2 Security Architecture and Dependencies

This section includes requirements for handling risky, outdated, or insecure dependencies and components through dependency management.

It also includes using architectural-level techniques such as sandboxing, encapsulation, containerization, and network isolation to reduce the impact of using “dangerous operations”or “risky compo-

nents"(as defined in the previous section) and prevent loss of availability due to overusing resource-demanding functionality.

#	Description	Level
15.2.1	Verify that the application only contains components which have not breached the documented update and remediation time frames.	1
15.2.2	Verify that the application has implemented defenses against loss of availability due to functionality which is time-consuming or resource-demanding, based on the documented security decisions and strategies for this.	2
15.2.3	Verify that the production environment only includes functionality that is required for the application to function, and does not expose extraneous functionality such as test code, sample snippets, and development functionality.	2
15.2.4	Verify that third-party components and all of their transitive dependencies are included from the expected repository, whether internally owned or an external source, and that there is no risk of a dependency confusion attack.	3
15.2.5	Verify that the application implements additional protections around parts of the application which are documented as containing "dangerous functionality"or using third-party libraries considered to be "risky components". This could include techniques such as sandboxing, encapsulation, containerization or network level isolation to delay and deter attackers who compromise one part of an application from pivoting elsewhere in the application.	3

V15.3 Defensive Coding

This section covers vulnerability types, including type juggling, prototype pollution, and others, which result from using insecure coding patterns in a particular language. Some may not be relevant to all languages, whereas others will have language-specific fixes or may relate to how a particular language or framework handles a feature such as HTTP parameters. It also considers the risk of not cryptographically validating application updates.

It also considers the risks associated with using objects to represent data items and accepting and returning these via external APIs. In this case, the application must ensure that data fields that should not be writable are not modified by user input (mass assignment) and that the API is selective about what data fields get returned. Where field access depends on a user's permissions, this should be considered in the context of the field-level access control requirement in the Authorization chapter.

#	Description	Level
15.3.1	Verify that the application only returns the required subset of fields from a data object. For example, it should not return an entire data object, as some individual fields should not be accessible to users.	1
15.3.2	Verify that where the application backend makes calls to external URLs, it is configured to not follow redirects unless it is intended functionality.	2
15.3.3	Verify that the application has countermeasures to protect against mass assignment attacks by limiting allowed fields per controller and action, e.g., it is not possible to insert or update a field value when it was not intended to be part of that action.	2
15.3.4	Verify that all proxying and middleware components transfer the user's original IP address correctly using trusted data fields that cannot be manipulated by the end user, and the application and web server use this correct value for logging and security decisions such as rate limiting, taking into account that even the original IP address may not be reliable due to dynamic IPs, VPNs, or corporate firewalls.	2
15.3.5	Verify that the application explicitly ensures that variables are of the correct type and performs strict equality and comparator operations. This is to avoid type juggling or type confusion vulnerabilities caused by the application code making an assumption about a variable type.	2
15.3.6	Verify that JavaScript code is written in a way that prevents prototype pollution, for example, by using Set() or Map() instead of object literals.	2
15.3.7	Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (query string, body parameters, cookies, or header fields).	2

V15.4 Safe Concurrency

Concurrency issues such as race conditions, time-of-check to time-of-use (TOCTOU) vulnerabilities, deadlocks, livelocks, thread starvation, and improper synchronization can lead to unpredictable behavior and security risks. This section includes various techniques and strategies to help mitigate these risks.

#	Description	Level
15.4.1	Verify that shared objects in multi-threaded code (such as caches, files, or in-memory objects accessed by multiple threads) are accessed safely by using thread-safe types and synchronization mechanisms like locks or semaphores to avoid race conditions and data corruption.	3
15.4.2	Verify that checks on a resource's state, such as its existence or permissions, and the actions that depend on them are performed as a single atomic operation to prevent time-of-check to time-of-use (TOCTOU) race conditions. For example, checking if a file exists before opening it, or verifying a user's access before granting it.	3
15.4.3	Verify that locks are used consistently to avoid threads getting stuck, whether by waiting on each other or retrying endlessly, and that locking logic stays within the code responsible for managing the resource to ensure locks cannot be inadvertently or maliciously modified by external classes or code.	3
15.4.4	Verify that resource allocation policies prevent thread starvation by ensuring fair access to resources, such as by leveraging thread pools, allowing lower-priority threads to proceed within a reasonable timeframe.	3

References

For more information, see also:

- OWASP Prototype Pollution Prevention Cheat Sheet
- OWASP Mass Assignment Prevention Cheat Sheet
- OWASP CycloneDX Bill of Materials Specification
- OWASP Web Security Testing Guide: Testing for HTTP Parameter Pollution

V16 Security Logging and Error Handling

Control Objective

Security logs are distinct from error or performance logs and are used to record security-relevant events such as authentication decisions, access control decisions, and attempts to bypass security controls, such as input validation or business logic validation. Their purpose is to support detection, response, and investigation by providing high-signal, structured data for analysis tools like SIEMs.

Logs should not include sensitive personal data unless legally required, and any logged data must be protected as a high-value asset. Logging must not compromise privacy or system security. Applications must also fail securely, avoiding unnecessary disclosure or disruption.

For detailed implementation guidance, refer to the OWASP Cheat Sheets in the references section.

V16.1 Security Logging Documentation

This section ensures a clear and complete inventory of logging across the application stack. This is essential for effective security monitoring, incident response, and compliance.

#	Description	Level
16.1.1	Verify that an inventory exists documenting the logging performed at each layer of the application's technology stack, what events are being logged, log formats, where that logging is stored, how it is used, how access to it is controlled, and for how long logs are kept.	2

V16.2 General Logging

This section provides requirements to ensure that security logs are consistently structured and contain the expected metadata. The goal is to make logs machine-readable and analyzable across distributed systems and tools.

Naturally, security events often involve sensitive data. If such data is logged without consideration, the logs themselves become classified and therefore subject to encryption requirements, stricter retention policies, and potential disclosure during audits.

Therefore, it is critical to log only what is necessary and to treat log data with the same care as other sensitive assets.

The requirements below establish foundational requirements for logging metadata, synchronization, format, and control.

#	Description	Level
16.2.1	Verify that each log entry includes necessary metadata (such as when, where, who, what) that would allow for a detailed investigation of the timeline when an event happens.	2
16.2.2	Verify that time sources for all logging components are synchronized, and that timestamps in security event metadata use UTC or include an explicit time zone offset. UTC is recommended to ensure consistency across distributed systems and to prevent confusion during daylight saving time transitions.	2
16.2.3	Verify that the application only stores or broadcasts logs to the files and services that are documented in the log inventory.	2

#	Description	Level
16.2.4	Verify that logs can be read and correlated by the log processor that is in use, preferably by using a common logging format.	2
16.2.5	Verify that when logging sensitive data, the application enforces logging based on the data's protection level. For example, it may not be allowed to log certain data, such as credentials or payment details. Other data, such as session tokens, may only be logged by being hashed or masked, either in full or partially.	2

V16.3 Security Events

This section defines requirements for logging security-relevant events within the application. Capturing these events is critical for detecting suspicious behavior, supporting investigations, and fulfilling compliance obligations.

This section outlines the types of events that should be logged but does not attempt to provide exhaustive detail. Each application has unique risk factors and operational context.

Note that while ASVS includes logging of security events in scope, alerting and correlation (e.g., SIEM rules or monitoring infrastructure) are considered out of scope and are handled by operational and monitoring systems.

#	Description	Level
16.3.1	Verify that all authentication operations are logged, including successful and unsuccessful attempts. Additional metadata, such as the type of authentication or factors used, should also be collected.	2
16.3.2	Verify that failed authorization attempts are logged. For L3, this must include logging all authorization decisions, including logging when sensitive data is accessed (without logging the sensitive data itself).	2
16.3.3	Verify that the application logs the security events that are defined in the documentation and also logs attempts to bypass the security controls, such as input validation, business logic, and anti-automation.	2
16.3.4	Verify that the application logs unexpected errors and security control failures such as backend TLS failures.	2

V16.4 Log Protection

Logs are valuable forensic artifacts and must be protected. If logs can be easily modified or deleted, they lose their integrity and become unreliable for incident investigations or legal proceedings. Logs may expose internal application behavior or sensitive metadata, making them an attractive target for attackers.

This section defines requirements to ensure that logs are protected from unauthorized access, tampering, and disclosure, and that they are safely transmitted and stored in secure, isolated systems.

#	Description	Level
16.4.1	Verify that all logging components appropriately encode data to prevent log injection.	2
16.4.2	Verify that logs are protected from unauthorized access and cannot be modified.	2
16.4.3	Verify that logs are securely transmitted to a logically separate system for analysis, detection, alerting, and escalation. The aim is to ensure that if the application is breached, the logs are not compromised.	2

V16.5 Error Handling

This section defines requirements to ensure that applications fail gracefully and securely without disclosing sensitive internal details.

#	Description	Level
16.5.1	Verify that a generic message is returned to the consumer when an unexpected or security-sensitive error occurs, ensuring no exposure of sensitive internal system data such as stack traces, queries, secret keys, and tokens.	2
16.5.2	Verify that the application continues to operate securely when external resource access fails, for example, by using patterns such as circuit breakers or graceful degradation.	2
16.5.3	Verify that the application fails gracefully and securely, including when an exception occurs, preventing fail-open conditions such as processing a transaction despite errors resulting from validation logic.	2

#	Description	Level
16.5.4	Verify that a "last resort"error handler is defined which will catch all unhandled exceptions. This is both to avoid losing error details that must go to log files and to ensure that an error does not take down the entire application process, leading to a loss of availability.	3

Note: Certain languages, (including Swift, Go, and through common design practice, many functional languages,) do not support exceptions or last-resort event handlers. In this case, architects and developers should use a pattern, language, or framework-friendly way to ensure that applications can securely handle exceptional, unexpected, or security-related events.

References

For more information, see also:

- OWASP Web Security Testing Guide: Testing for Error Handling
- OWASP Authentication Cheat Sheet section about error messages
- OWASP Logging Cheat Sheet
- OWASP Application Logging Vocabulary Cheat Sheet

V17 WebRTC

Control Objective

Web Real-Time Communication (WebRTC) enables real-time voice, video, and data exchange in modern applications. As adoption increases, securing WebRTC infrastructure becomes critical. This section provides security requirements for stakeholders who develop, host, or integrate WebRTC systems.

The WebRTC market can be broadly categorized into three segments:

1. Product Developers: Proprietary and open-source vendors that create and supply WebRTC products and solutions. Their focus is on developing robust and secure WebRTC technologies that can be used by others.
2. Communication Platforms as a Service (CPaaS): Providers that offer APIs, SDKs, and the necessary infrastructure or platforms to enable WebRTC functionalities. CPaaS providers may use products from the first category or develop their own WebRTC software to offer these services.
3. Service Providers: Organizations that leverage products from product developers or CPaaS providers, or develop their own WebRTC solutions. They create and implement applications

for online conferencing, healthcare, e-learning, and other domains where real-time communication is crucial.

The security requirements outlined here are primarily focused on Product Developers, CPaaS, and Service Providers who:

- Utilize open-source solutions to build their WebRTC applications.
- Use commercial WebRTC products as part of their infrastructure.
- Use internally developed WebRTC solutions or integrate various components into a cohesive service offering.

It is important to note that these security requirements do not apply to developers who exclusively use SDKs and APIs provided by CPaaS vendors. For such developers, the CPaaS providers are typically responsible for most of the underlying security concerns within their platforms, and a generic security standard like ASVS may not fully address their needs.

V17.1 TURN Server

This section defines security requirements for systems that operate their own TURN (Traversal Using Relays around NAT) servers. TURN servers assist in relaying media in restrictive network environments but can pose risks if misconfigured. These controls focus on secure address filtering and protection against resource exhaustion.

#	Description	Level
17.1.1	Verify that the Traversal Using Relays around NAT (TURN) service only allows access to IP addresses that are not reserved for special purposes (e.g., internal networks, broadcast, loopback). Note that this applies to both IPv4 and IPv6 addresses.	2
17.1.2	Verify that the Traversal Using Relays around NAT (TURN) service is not susceptible to resource exhaustion when legitimate users attempt to open a large number of ports on the TURN server.	3

V17.2 Media

These requirements only apply to systems that host their own WebRTC media servers, such as Selective Forwarding Units (SFUs), Multipoint Control Units (MCUs), recording servers, or gateway servers. Media servers handle and distribute media streams, making their security critical to protect communication between peers. Safeguarding media streams is paramount in WebRTC applications to prevent eavesdropping, tampering, and denial-of-service attacks that could compromise user privacy and communication quality.

In particular, it is necessary to implement protections against flood attacks such as rate limiting, validating timestamps, using synchronized clocks to match real-time intervals, and managing buffers to prevent overflow and maintain proper timing. If packets for a particular media session arrive too quickly, excess packets should be dropped. It is also important to protect the system from malformed packets by implementing input validation, safely handling integer overflows, preventing buffer overflows, and employing other robust error-handling techniques.

Systems that rely solely on peer-to-peer media communication between web browsers, without the involvement of intermediate media servers, are excluded from these specific media-related security requirements.

This section refers to the use of Datagram Transport Layer Security (DTLS) in the context of WebRTC. A requirement related to having a documented policy for the management of cryptographic keys can be found in the “Cryptography”chapter. Information on approved cryptographic methods can be found either in the Cryptography Appendix of the ASVS or in documents such as NIST SP 800-52 Rev. 2 or BSI TR-02102-2 (Version 2025-01).

#	Description	Level
17.2.1	Verify that the key for the Datagram Transport Layer Security (DTLS) certificate is managed and protected based on the documented policy for management of cryptographic keys.	2
17.2.2	Verify that the media server is configured to use and support approved Datagram Transport Layer Security (DTLS) cipher suites and a secure protection profile for the DTLS Extension for establishing keys for the Secure Real-time Transport Protocol (DTLS-SRTP).	2
17.2.3	Verify that Secure Real-time Transport Protocol (SRTP) authentication is checked at the media server to prevent Real-time Transport Protocol (RTP) injection attacks from leading to either a Denial of Service condition or audio or video media insertion into media streams.	2
17.2.4	Verify that the media server is able to continue processing incoming media traffic when encountering malformed Secure Real-time Transport Protocol (SRTP) packets.	2
17.2.5	Verify that the media server is able to continue processing incoming media traffic during a flood of Secure Real-time Transport Protocol (SRTP) packets from legitimate users.	3
17.2.6	Verify that the media server is not susceptible to the “ClientHello”Race Condition vulnerability in Datagram Transport Layer Security (DTLS) by checking if the media server is publicly known to be vulnerable or by performing the race condition test.	3