Criteria for product security check

Version 2014.2

Content

Certificate management:
Ohjelmistoyrittäjät ry
toimisto@ohjelmistoyrittajat.fi
Phone +358 (0)50 448 5446
www.ohjelmistoyrittajat.fi

Auditing and certification:
Second Nature Security Oy (2NS)
info@2ns.fi
Phone +358 (0)10 322 9000
www.2ns.fi

Introduction

This document describes required criteria that shall be fulfilled to successfully pass the annual product security check in chosen security level.

The requirements for each security level are described in the table below:

Area	Criteria	Required?		
		Level 1	Level 2	Level 3
ISC-P-001 Input handling	Cross-Site Scripting vulnerabilities shall not be found	✔	✔	✔
	Injection vulnerabilities shall not be found	✔	✔	✔
	File inclusion vulnerabilities shall not be found	✔	✔	✔
	Command injection vulnerabilities shall not be found	✔	✔	✔
	HTTP Splitting vulnerabilities shall not be found	✔	✔	✔
	Open redirection vulnerabilities shall not be found	✔	✔	✔
	HTTP parameter pollution shall not be possible	✗	✗	✔
ISC-P-002 Configuration	Application platform configuration	✔	✔	✔
	Old, backup and unreferenced files shall not be available	✔	✔	✔
	There shall not be insecure cross-domain-policy	✔	✔	✔
	Unsecure HTTP methods shall not be used	✔	✔	✔
	SSL configuration shall be hardened	✗	✔	✔
	HTTP Strict Transport Security shall be used	✗	✗	✔
	Unneeded administrative interfaces shall not be available or shall be otherwise appropriately protected	✗	✗	✔
ISC-P-003 Session management	HttpOnly and Secure flags shall be set on cookies	✗	✔	✔
	Session variables shall be available only in cookies	✗	✔	✔
	Session fixation vulnerabilities shall not be found	✗	✔	✔

Area	Criteria	Required?		
		Level 1	Level 2	Level 3
	Session identifier shall be cryptographically secure random number token	✗	✗	✔
	Protection against Cross-Site Request Forgery attacks	✗	✗	✔
ISC-P-004 Authentication	Credentials shall be transferred over an encrypted channel	✗	✔	✔
	Protection against brute force attacks	✗	✔	✔
	Authentication schema cannot be bypassed	✗	✔	✔
	Remember me functionality shall be implemented securely	✗	✔	✔
	Password reset functionality shall be implemented securely	✗	✔	✔
	User shall be able to change the password	✗	✔	✔
	Password change shall require user's current password	✗	✔	✔
ISC-P-005 Authorization	Authorization schema cannot be bypassed	✗	✔	✔
	Privilege escalation vulnerabilities shall not be found	✗	✔	✔
	Insecure direct object references shall not be found	✗	✗	✔
ISC-P-006 Business logic	Business logic data validation shall be implemented	✗	✗	✔
	Requests cannot be forged	✗	✗	✔
	Confidential data shall be sent over an encrypted channel	✗	✗	✔
	Integrity checks shall be implemented	✗	✗	✔
	Works flows cannot be circumvented	✗	✗	✔
	Defenses against application misuses shall be implemented	✗	✗	✔
	File upload shall defend against malicious uploads	✗	✗	✔

Area	Criteria	Required?		
		Level 1	Level 2	Level 3
	Sensitive information shall not be stored in Cache	✗	✗	✔
	Sensitive information shall not be stored in forms	✗	✗	✔
ISC-P-007 Client-side testing	DOM based Cross-Site Scripting shall not be found	✗	✗	✔
	JavaScript execution vulnerabilities shall not be found	✗	✗	✔
	HTML injection vulnerabilities shall not be found	✗	✗	✔
	Client Side URL redirect vulnerabilities shall not be found	✗	✗	✔
	CSS injection vulnerabilities shall not be found	✗	✗	✔
	Client Side Resource Manipulation vulnerabilities shall not be found	✗	✗	✔
	Cross Site Flashing vulnerabilities shall not be found	✗	✗	✔
	Clickjacking vulnerabilities shall not be found	✗	✗	✔
	WebSockets shall be implemented securely	✗	✗	✔
	Web messaging related vulnerabilities shall not be found	✗	✗	✔
	Vulnerabilities related to Local Storage shall not be found	✗	✗	✔

ISC-P-001 Input Handling

ISC-P-001.1 Cross-Site Scripting vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	Yes	Automated testing tools, with manual verification
Level 2	Yes	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

Reflected or stored Cross-Site Scripting vulnerabilities shall not be found during the check. An attacker shall not be able to inject HTML or JavaScript code to the structure of the service. User input shall be sanitized and HTML special characters shall be replaced with HTML entities.

ISC-P-001.2 Injection vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	Yes	Automated testing tools, with manual verification
Level 2	Yes	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

Injection vulnerabilities shall not be found during the check. Injection vulnerabilities are weaknesses where an attacker is able to affect to the structure of query made to background system. These include, but not limited to, following vulnerabilities:

- SQL injections
- LDAP injections
- XML injections

User input shall be sanitized so that user input cannot affect to the structure of the background queries.

ISC-P-001.3 File inclusion vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	Yes	Automated testing tools, with manual verification
Level 2	Yes	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

File inclusion vulnerabilities shall not be found during the check. File inclusion vulnerabilities are weaknesses that allow an attacker to read files from the server's file system or from any other location readable by the target server. User input shall not be used to determine location of the files in the server's file system.

ISC-P-001.4 Command injection vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	Yes	Automated testing tools, with manual verification
Level 2	Yes	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

Command injection vulnerabilities shall not be found during the check. Command injection vulnerabilities are weaknesses that allow an attacker to execute operating system level commands on the server. User input shall be sanitized and it cannot be used directly in input that goes to operating system commands.

ISC-P-001.5 HTTP Splitting vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	Yes	Automated testing tools, with manual verification
Level 2	Yes	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

HTTP Splitting vulnerabilities shall not be found during the check. HTTP Splitting vulnerabilities are weaknesses that allow an attacker to inject custom headers to HTTP responses or generate new responses. User input shall be sanitized and new line and carriage return characters shall be URL encoded if the user input is used in HTTP headers.

ISC-P-001.6 Open redirection vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	Automated testing tools, with manual verification
Level 2	No	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

Open redirection vulnerabilities shall not be found during the check. These are vulnerabilities that allow victim's browser to be redirected to 3rd party website via the vulnerable target site.

ISC-P-001.7 HTTP parameter pollution shall not be possible

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

HTTP parameter pollution vulnerabilities shall not be found during the check. These are vulnerabilities where an attacker is able to exploit behavior of the application, when same parameters are given twice in same request. When the same parameter is given twice in same request, an application must be able to handle situation safely without possibility for malicious actions.

ISC-P-002 Configuration

ISC-P-002.1 Application platform configuration

Criteria Level	Required	Methodology
Level 1	Yes	Automated testing tools, with manual verification
Level 2	Yes	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

Application platform configuration vulnerabilities shall not be found. These are vulnerabilities that are not related directly to the application itself, but the platform it is using (OS, web server, application server, libraries, etc.). These vulnerabilities can be caused by weak configurations or unpatched software. Application platform configuration shall be hardened and patched to pass the criterion.

ISC-P-002.2 Old, backup and unreferenced files shall not be available

Criteria Level	Required	Methodology
Level 1	Yes	Automated testing tools, with manual verification
Level 2	Yes	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

Old, backup and unreferenced files shall not be found from the service. These are files that are left for backup reasons and might allow an attacker access to possibly dangerous features or allows an attacker to view source code of backed up files. It must be made sure that there is no unneeded files left to the service and content of those files cannot be retrieved.

ISC-P-002.3 There shall not be insecure cross-domain policy

Criteria Level	Required	Methodology
Level 1	Yes	Automated testing tools, with manual verification
Level 2	Yes	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

Cross-domain policies set to the service shall not be insecure. Cross-domain communications shall not be allowed unless needed by certain features. In those cases, cross-domain communication shall be allowed only for those features and only from domains that are needed feature to work. When cross-domain policies are utilized and communications between domains is allowed, that cannot reveal confidential information to untrusted stakeholders.

ISC-P-002.4 Unsecure HTTP methods shall not be used

Criteria Level	Required	Methodology
Level 1	Yes	Automated testing tools, with manual verification
Level 2	Yes	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

Unsecure HTTP methods shall not be used and the server cannot support those. Following methods cannot be used in the service:

- TRACE
- CONNECT
- PUT (if used, the service shall utilize it in secure manner – e.g. RESTful URLs)
- DELETE (if used, the service shall utilize it in secure manner – e.g. RESTful URLs)

Web server shall be configured not to support methods mentioned above. In case of PUT and DELETE methods, application itself shall make sure that those methods are used in safe manner.

ISC-P-002.5 SSL Configuration shall be hardened

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools, with manual verification
Level 3	Yes	Automated testing tools and manual testing

SSL implementation on the server shall be hardened properly. Following requirements shall be fulfilled to pass this criterion:

- Certificate shall be granted to the domain name in question
- Certificate shall be valid and it cannot be expired
- The certificate cannot be self-signed
- Certificate shall be signed by trusted 3rd party CA
- Certificate shall be signed with at least SHA256 hash algorithm
- RSA key length and Diffie-Hellman parameter strength shall be at least 2048 bits
- SSL/TLS implementation shall support TLSv1.2
- SSLv2.0 shall not be supported
- SSLv3.0 should not be supported[1]
- SSL/TLS implementation shall prioritize cipher suites that provide perfect forward secrecy (Diffie-Hellman key exchange)
- Anonymous key exchange cipher suites shall not be supported
- Cipher strength shall be at least 128 bits[2]

[1] This requirement is not yet enforced due to possible compatibility issues. It's highly recommended to disable SSLv3, if possible. SSLv3 support will not fail the criterion, but existence of POODLE vulnerability will be commented on the report.
[2] 3DES has cipher strength of 112 bits, but it is allowed as a last resort option to support Internet Explorer in Windows XP installations

ISC-P-002.6 HTTP Strict Transport Security shall be used

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

HTTP Strict Transport Security shall be used to force users to use encrypted HTTPS connection. HSTS header guides browsers only to use encrypted HTTPS connection. Only allowed exception is, if clear-text HTTP interface provides completely different application and there is no confidential information sent over HTTP connection.

ISC-P-002.7 Unneeded administrative interfaces shall not be available or shall be otherwise appropriately protected

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

Administrative interfaces shall not be available to public Internet. If those are found during the check, product owner shall provide following information:

- Is there any protection against brute-force attacks – if yes, explain implemented controls
- Why access to administrative interfaces should be allowed from public Internet

There shall be adequate controls to prevent brute force attacks:

- There shall be continuous process to follow usage of administrative interface
- There shall be lockout feature that will slow down possible brute force attacks
- Users shall be forces to use strong passwords (used passwords must have at least 2^{64} possible combinations – e.g. 12 characters long, special characters, numbers and capitals required OR 5 random words from Finnish language)

Also plausible reason why administrative interface should be available from the public Internet shall be given.

ISC-P-003 Session Management

ISC-P-003.1 HttpOnly and Secure flags shall be set on cookies

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

Cookies that identify users and sessions or transfer other confidential data shall have HttpOnly and Secure flags set. These options have following effect:

- Cookies cannot be read by client-side code (cookies are only sent in HTTP requests)
- Cookies are sent only by using encrypted HTTPS protocol

ISC-P-003.2 Session variables shall be available only in cookies

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

Session variables cannot be transferred anywhere else than in cookies. For example, if session variables are stored in server response content, this criterion will not be met:

ISC-P-003.3 Session fixation vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

Session fixation vulnerabilities cannot be found during the check. These are vulnerabilities that allow an attacker to force victim to use pre-known session identifier (e.g. attacker's own session identifier). These will allow an attacker to act on the service with victim's privileges.

Also session identifier shall be regenerated, whenever the authorization level changes (e.g. user logs in to the service). Session shall be destroyed if the user logs out from the service.

ISC-P-003.4 Session identifier shall be cryptographically secure random number token

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

Session identifier that is used by the service shall be cryptographically secure. That means that the token has to have at least 100 bits of entropy.

ISC-P-003.5 Protection against Cross-Site Request Forgery Attacks

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

There shall be protection implemented against Cross-Site Request Forgery attacks. An attacker shall not be able to commit actions from the 3rd party website to the target service by utilizing victim's browser. Please note that checking the Referer HTTP header is not adequate control.

ISC-P-004 Authentication

ISC-P-004.1 Credentials shall be transferred over an encrypted channel

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

Service shall pass credentials over encrypted channel. Also session identifiers shall be transferred over an encrypted channel.

ISC-P-004.2 Protection against brute force attacks

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

The service shall implement protection against brute force attacks, if there is a publicly available login interface on the service (this does not include administrative interfaces – see ISC-P-002.7). Blocking IP addresses in case of too many failed logins will fulfill the criterion.

ISC-P-004.3 Authentication schema cannot be bypassed

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

An attacker shall not be able to bypass the implemented authentication schema. The criterion includes, but not limited to, following scenarios:

- SQL injections in login interface
- Weak session identifiers
- Session fixation
- Knowing or guessing paths for resources that require authentication
- Easily guessable information in requests (e.g. username in cookies)

ISC-P-004.4 Remember me functionality shall be implemented securely

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

If the service implements remember me functionality, it shall be implemented in secure manner. User shall be identified by the cryptographically secure token. The token shall be renewed every time that the user uses token to log in to the service and the previous token shall expire. Also the token shall expire if the user has not visited in the service for 365 days.

The feature shall not authenticate users based on information that is easy to guess. Also the information that is used to authenticate users shall not be stored in browsers (e.g. passwords in cookies).

ISC-P-004.5 Password reset functionality shall be implemented securely

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

If the service has authentication and it includes password reset functionality, it shall be implemented securely. The reset functionality shall not:

- Return user's original passwords (passwords cannot be stored in format that can be reverted to clear-text)
- Send new password in email without forcing the password change in first login

Recommended way to implement the reset functionality is to send unique link to user's email that includes cryptographically strong random number token (entropy shall be at least 100 bits). By visiting the link, user is able to change the password without knowing the previous one. Link shall be unique and it can be used only once. After usage, the link shall expire and it cannot be used again.

ISC-P-004.6 User shall be able to change the password

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

If the service uses local passwords (users are authenticated against local password database), users shall be able to change their own password whenever needed.

ISC-P-004.7 Password change shall require user's current password

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

If the service includes password change feature, it shall be implemented in secure manner. The password change feature shall require user's current password to authorize password change.

ISC-P-005 Authorization

ISC-P-005.1 Authorization schema cannot be bypassed

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

During the check, vulnerabilities that allow bypassing the authorization schema cannot be found. For example vulnerabilities are, but not limited to:

- Ability to access resources that user has no privileges
- Ability to access administrative features without required permissions

ISC-P-005.2 Privilege escalation vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	Yes	Automated testing tools with partial manual testing
Level 3	Yes	Automated testing tools and manual testing

During the check, vulnerabilities that allow an attacker to escalate his privileges shall not be found. This includes vulnerabilities, where an attacker is able to elevate his privileges (e.g. from normal user → administrator).

ISC-P-005.3 Insecure direct object references shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

There shall be no direct object reference vulnerabilities found during the check. These are vulnerabilities, where an attacker is able to access resources he has no privileges by changing object reference in request. These references are for example, but not limited to:

- Database identifiers
- Files in server's file system

ISC-P-006 Business logic

ISC-P-006.1 Business logic data validation shall be implemented

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

Data validation for business logic shall be implemented. This means that the service shall validate that the data conforms validity requirements set by business logic. For example, when SSN is given as an input it shall be validated that the input is valid SSN.

ISC-P-006.2 Requests cannot be forged

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

There shall not be vulnerabilities that allow forging of requests found during the check. This means situations, where an attacker is able to circumvent the GUI application and send direct requests to the backend. These situations might be example:

- Activation of debugging features by knowing “secret” URL parameter
- Ability to use discount code multiple times by flagging it as unused

ISC-P-006.3 Confidential data shall be sent over an encrypted channel

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

Application shall not send confidential data over an unencrypted channel. This includes, but not limited to, following data:

- Personally identifiable information
- Credit card numbers
- Other data that is confidential from organization or user's point of view.

ISC-P-006.4 Integrity checks shall be implemented

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

Service shall implement checks that can verify integrity of business logic data. Service shall make sure that an attacker is not able to forge information that is stored on the service. For example, but not limited to, this includes following cases:

- An attacker is able to forge logs
- An attacker is able to modify price of an order
- An attacker is able to change his username in the system, even it should not be possible

ISC-P-006.5 Workflows cannot be circumvented

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

The system shall verify that an attacker is not able to circumvent any workflows required by the system. For example, an attacker should not able to circumvent the order workflow to bypass the payment step in ecommerce service. Other case could be for example, a situation where an attacker is able to bypass his superior's acceptance when asking for pay rise.

ISC-P-006.6 Defenses against application misuses shall be implemented

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

Defenses against application misuse shall be implemented. If the service includes functionalities that an attacker is able to use for malicious purposes, defenses against these malicious actions shall be implemented. This includes, but not limited to, following issues:

- An attacker is able to exploit feedback form to send spam
- An attacker is able to make unlimited amount of queries that generate costs to the service (i.e. the service makes own queries to another service and the pricing is based on amount of queries made)

ISC-P-006.7 File upload shall defend against malicious uploads

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

Unsecure file upload features cannot be found during the check. When users are allowed to upload files, allowed file types shall be specified and contents of the files shall be checked against the specified types.

For example, but not limited to, following issues will be reported:

- Upload of dangerous file types
- Code execution via file upload
- Upload of wrong type of files

ISC-P-006.8 Sensitive information shall not be stored in cache

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

Checked service shall guide browsers not to store sensitive information to browser cache. Confidential and sensitive information shall be recognized and pages that contain that kind of information shall not be stored in cache.

ISC-P-006.9 Sensitive information shall not be stored in forms

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

Checked service shall guide browsers not to use form auto fill features in form fields that contain sensitive information. Only exception is the password field in login feature – in this case it is recommended to add option to disable autocomplete feature if user is using the service from a public workstation.

ISC-P-007 Client-side testing

ISC-P-007.1 DOM based Cross-Site Scripting vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

During the check, there shall not be DOM based Cross-Site Scripting vulnerabilities. These are Cross-Site Scripting vulnerabilities, where the vulnerability is in client-side technologies (i.e. JavaScript).

ISC-P-007.2 JavaScript execution vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

There shall not be not vulnerabilities found during the security check that enables users to execute JavaScript on the service. These include, but not limited to, for example unsecure use of eval-functions.

ISC-P-007.3 HTML injection vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

There shall not be no vulnerabilities on the client-side technologies that makes possible to inject HTML code to the page structure. If the HTML injection is possible there is high risk of Cross-Site Scripting vulnerabilities.

ISC-P-007.4 Client Side URL redirect vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

There shall not be any vulnerabilities on client-side technologies that allow an attacker to redirect victim to a 3rd party site. Every feature that uses user input to redirect client to 3rd party site is susceptible to the vulnerability.

ISC-P-007.5 CSS injection vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

There shall not be no vulnerabilities that allow an attacker to inject own CSS code to the context of the website. In worst-case scenarios these vulnerabilities might lead to Cross-Site Scripting attacks.

ISC-P-007.6 Client Side Resource Manipulation vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

There shall not be client side resource vulnerabilities. These are vulnerabilities that allow an attacker to modify references to other resources due to weaknesses in client side implementations. For example, an attacker might be able to give source attribute for a script tag via URL.

ISC-P-007.7 Cross Site Flashing vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

There shall not be cross-site flashing vulnerabilities found during the security check. If the service includes Flash animations, these vulnerabilities can be exploited to configure Flash implementations via URL parameters. For example, an attacker might be able to configure source of the contents showed in the Flash animation.

ISC-P-007.8 Clickjacking vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

There shall not be Clickjacking vulnerabilities found from the service during the check. Clickjacking vulnerabilities are weaknesses that can be exploited if the target service allows loading itself to the frames. This feature can be exploited to commit actions on the service as a victim. To fulfill the criterion, service shall disallow loading itself to frames.

If the service is used in frames, SAMEORIGIN header shall be used to specify sources where the service can be loaded to frames. If this is not possible, plausible explanation shall be given to testers.

ISC-P-007.9 WebSockets shall be implemented securely

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

If the service uses WebSockets, these shall be implemented in secure manner. In these implementations, there shall not be for example, but not limited to, following vulnerabilities:

- Authentication and authorization issues
- Input sanitization issues

ISC-P-007.10 WebMessaging related vulnerabilities shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

If the service utilizes WebMessaging to communicate between frames and/or windows, these shall be implemented in secure manner. If the service is implemented to receive these events, origin of the events shall be checked. Messages should be accepted only from trusted sources.

ISC-P-007.11 Vulnerabilities related to Local Storage shall not be found

Criteria Level	Required	Methodology
Level 1	No	N/A
Level 2	No	N/A
Level 3	Yes	Automated testing tools and manual testing

Vulnerabilities that allow exploitation of local storage features shall not be found during the security check.

Appendix A

Open Source Security Testing Methodology Manual – http://www.osstmm.org

The Open Web Application Security Project – http://owasp.org

Common Vulnerability Scoring System – http://www.first.org/cvss/cvss-guide

OWASP Testing Guide – https://www.owasp.org/index.php/OWASP_Testing_Project