Central HRIS for MoHFW

Application Security Checklist For API integration

House 1, Avenue 1, Block D, Section 11, Mirpur.. Dhaka 1216
e-mail: info@activationltd.com website: activationltd.com

Table of content

House 1, Avenue 1, Block D, Section 11, Mirpur.. Dhaka 1216
e-mail: info@activationltd.com website: activationltd.com

Web application security summary

This checklist can be used as a standard when performing a remote security test on a web application.

Security testers should use this checklist when performing a remote security test of a web application. A risk analysis for the web application should be performed before starting with the checklist. Every test on the checklist should be completed or explicitly marked as being not applicable. Once a test is completed the checklist should be updated with the appropriate result icon and a document cross-reference. The completed checklist should never be delivered standalone but should be incorporated in a report detailing the risk analysis and checklist results and the scope and context of the
performed remote security test.

Certified Secure Web Application Security Test Checklist	Result	Comment
1.0 Deployment		
1.1 Test for missing security updates	NA	
1.2 Test for unsupported or end-of-life software versions	NA	
1.3 Test for HTTP TRACK and TRACE methods	P	
1.4 Test for extraneous functionality	P	
1.5 Test the server using the Server Security Test Checklist	NA	Server is managed by a separate vendor assigned by client
2.0 Information Disclosure		
2.1 Test for extraneous files in the document root	P	
2.2 Test for extraneous directory listings	P	
2.3 Test for accessible debug functionality	P	

House 1, Avenue 1, Block D, Section 11, Mirpur.. Dhaka 1216
e-mail: info@activationltd.com website: activationltd.com

2.4 Test for sensitive information in log and error messages	P	
2.5 Test for sensitive information in robots.txt	P	
2.6 Test for sensitive information in source code	P	
2.7 Test for disclosure of internal addresses	P	Except for public assets all assets are retrieved dynamically through asset name resolution
3.0 Privacy and Confidentiality		
3.1 Test for sensitive information stored in URLs	P	
3.2 Test for unencrypted sensitive information stored at the client-side	P	
3.3 Test for sensitive information stored in (externally) archived pages	P	
3.4 Test for content included from untrusted sources	P	
3.5 Test for caching of pages with sensitive information	P	
3.6 Test for insecure transmission of sensitive information	P	
3.7 Test for non SSL/TLS pages on sites processing sensitive information	P	
3.8 Test for SSL/TLS pages served with mixed content	P	
3.9 Test for missing HSTS header on full SSL sites	P	
3.10 Test for known vulnerabilities in SSL/TLS	NA	
3.11 Test for weak, untrusted or expired SSL certificates	NA	
3.12 Test for the usage of unproven cryptographic primitives	NA	
3.13 Test for the incorrect usage of cryptographic primitives	NA	
4.0 State Management		
4.1 Test for client-side state management	P	
4.2 Test for invalid state transitions	P	
5.0 Authentication and Authorization		
5.1 Test for missing authentication or authorization	P	
5.2 Test for client-side authentication	P	
5.3 Test for predictable and default credentials	NA	Client prefers not to have it due to a user groups limitation of handling password

House 1, Avenue 1, Block D, Section 11, Mirpur.. Dhaka 1216
e-mail: info@activationltd.com website: activationltd.com

5.4 Test for predictable authentication or authorization tokens	P	
5.5 Test for authentication or authorization based on obscurity	P	
5.6 Test for identifier-based authorization	NA	
5.7 Test for acceptance of weak passwords	NA	
5.8 Test for plaintext retrieval of passwords	P	
5.9 Test for missing rate limiting on authentication functionality	P	
5.10 Test for missing re-authentication when changing credentials	NA	
5.11 Test for missing logout functionality	P	
6.0 User Input		
6.1 Test for SQL injection	P	
6.2 Test for path traversal and filename injection	P	
6.3 Test for cross-site scripting	P	
6.4 Test for system command injection	P	
6.5 Test for XML injection	P	
6.6 Test for XPath injection	P	
6.7 Test for XSL(T) injection	P	
6.8 Test for SSI injection	P	
6.9 Test for HTTP header injection	P	
6.10 Test for HTTP parameter injection	P	
6.11 Test for LDAP injection	NA	
6.12 Test for dynamic scripting injection	NA	
6.13 Test for regular expression injection	NA	
6.14 Test for data property/field injection	NA	
6.15 Test for protocol specific injection	NA	
6.16 Test for expression language injection	NA	
7.0 Sessions		
7.1 Test for cross-site request forgery (CSRF)	P	
7.2 Test for predictable CSRF tokens	P	
7.3 Test for missing session revocation on logout	P	
7.4 Test for missing session regeneration on login	P	
7.5 Test for missing session regeneration when changing credentials	P	
7.6 Test for missing revocation of other sessions when changing credentials	P	
7.7 Test for missing Secure flag on session cookies	P	

House 1, Avenue 1, Block D, Section 11, Mirpur.. Dhaka 1216
e-mail: info@activationltd.com website: activationltd.com

7.8 Test for missing HttpOnly Flag on session cookies	P	
7.9 Test for non-restrictive domain on session cookies	P	
7.10 Test for non-restrictive or missing path on session cookies	P	
7.11 Test for predictable session identifiers	NA	
7.12 Test for session identifier collisions	NA	
7.13 Test for session fixation	NA	
7.14 Test for insecure transmission of session identifiers	P	
7.15 Test for external session hijacking	P	
7.16 Test for missing periodic expiration of sessions	P	
8.0 File Uploads		
8.1 Test for storage of uploaded files in the document root	P	
8.2 Test for execution or interpretation of uploaded files	P	
8.3 Test for uploading outside of designated upload directory	P	
8.4 Test for missing size restrictions on uploaded files	P	
8.5 Test for missing type validation on uploaded files	P	
9.0 Content		
9.1 Test for missing or non-specific content type definitions	NA	
9.2 Test for missing character set definitions	P	
9.3 Test for missing anti content sniffing measures	NA	
10.0 XML Processing		
10.1 Test for XML external entity expansion	NA	
10.2 Test for external DTD parsing	NA	
10.3 Test for extraneous or dangerous XML extensions	NA	
10.4 Test for recursive entity expansion	NA	
11.0 Miscellaneous		
11.1 Test for missing anti-clickjacking measures	NA	
11.2 Test for open redirection	P	
11.3 Test for insecure cross-domain access policy	P	
11.4 Test for missing rate limiting on e-mail functionality	P	Server restriction
11.5 Test for missing rate limiting on resource intensive functionality	P	
11.6 Test for inappropriate rate limiting resulting in a denial of service	P	
11.7 Test for application or setup specific problems	P	

House 1, Avenue 1, Block D, Section 11, Mirpur.. Dhaka 1216
e-mail: info@activationltd.com website: activationltd.com

House 1, Avenue 1, Block D, Section 11, Mirpur.. Dhaka 1216
e-mail: info@activationltd.com website: activationltd.com

Server security summary

In current deployment (DHS-MIS data center) Server and network infrastructures are deployed and maintained by a separate vendor. Hence this is out of scope of Activation. However we are attaching the following checklist that should be performed by Server and Network vendors in a pre-defined frequency to ensure proper security

This checklist can be used as a standard when performing a remote security test on a server.

Certified Secure Server Security Test Checklist	Result	Comment
1.0 Version Management		
1.1 Test all services for missing security updates		
1.2 Test all services for unsupported or end-of-life software versions		
2.0 Network Security		
2.1 Test for extraneous services		
2.2 Test for extraneous ICMP functionality		
2.3 Test for extraneous enabled networks protocols		
2.4 Test for firewall evasion using common techniques		
3.0 Authentication and Authorization		
3.1 Test all services for missing authentication or authorization		
3.2 Test all services for predictable credentials		
3.3 Test all services for default, test, guest and obsolete accounts		
3.4 Test all services for missing rate limiting on authentication functionality		
4.0 Privacy and Confidentiality		
4.1 Test all services for disclosure of extraneous information		
4.2 Test all services for insecure transmission of sensitive information		
4.3 Test all services for weak, untrusted or expired SSL certificates		
4.4 Test all services for known vulnerabilities in SSL/TLS		
4.5 Test all services for the usage of unproven cryptographic primitives		
4.6 Test all services for incorrect usage of cryptographic primitives		
4.7 Test for publicly accessible test, development and acceptance systems		
5.0 Service Specific		
5.1 Test web services using the Web Application Security Test Checklist		

House 1, Avenue 1, Block D, Section 11, Mirpur.. Dhaka 1216
e-mail: info@activationltd.com website: activationltd.com

5.2 Test mail services for open relaying		
5.3 Test mail services for e-mail address enumeration		
5.4 Test FTP services for anonymous file uploading		
5.5 Test DNS services for unauthorized AXFR transfers		
6.0 Miscellaneous		
6.1 Test for missing rate limiting on resource intensive functionality		
6.2 Test for inappropriate rate limiting resulting in a denial of service		
6.3 Test all services for service specific issues		
6.4 Test for server or setup specific problems		
5.6 Test for identifier-based authorization		
5.7 Test for acceptance of weak passwords		
5.8 Test for plaintext retrieval of passwords		
5.9 Test for missing rate limiting on authentication functionality		
5.10 Test for missing re-authentication when changing credentials		
5.11 Test for missing logout functionality		
6.0 User Input		
6.1 Test for SQL injection		
6.2 Test for path traversal and filename injection		
6.3 Test for cross-site scripting		
6.4 Test for system command injection		

House 1, Avenue 1, Block D, Section 11, Mirpur.. Dhaka 1216
e-mail: info@activationltd.com website: activationltd.com