Risk Mapping						
Vulnerabilities scanning	**Risk ID**	**OWASP / Other Security risks**	**CWE**	**Burp Suite**	**NSlookup**	**Manual Test**
File path traversal, File path manipulation, Local file path manipulation	R01	Broken Access Control	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	V		
File path traversal, File path manipulation	R01	Broken Access Control	CWE-23 Relative Path Traversal	V		
File path traversal, File path manipulation	R01	Broken Access Control	CWE-35 Path Traversal: '.../...//'	V		
	R01	Broken Access Control	CWE-59 Improper Link Resolution Before File Access			
GraphQL (introspection enabled, suggestions enabled), Cross-domain Referer leakage, Session token in URL, Password field with autocomplete enable, Source code disclosure, Email address disclosed, Private IP address disclosed, Social security numbers disclosed, Credit card numbers disclosed, Private key disclosed, Robots.txt file, Json Web Key Set disclosed, JWT private key disclosed	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		V
	R01	Broken Access Control	CWE-201 Exposure of Sensitive Information Through			
	R01	Broken Access Control	CWE-219 Storage of File with Sensitive Data Under			
	R01	Broken Access Control	CWE-264 Permissions, Privileges, and Access			
	R01	Broken Access Control	CWE-275 Permission Issues			
	R01	Broken Access Control	CWE-276 Incorrect Default Permissions			
Broken Access Control	R01	Broken Access Control	CWE-284 Improper Access Control	V		
	R01	Broken Access Control	CWE-285 Improper Authorization			
GraphQL content type not validated, CSRF	R01	Broken Access Control	CWE-352 Cross-Site Request Forgery (CSRF)	V	V	
	R01	Broken Access Control	CWE-359 Exposure of Private Personal Information			
	R01	Broken Access Control	CWE-377 Insecure Temporary File			
	R01	Broken Access Control	CWE-402 Transmission of Private Resources into a			
	R01	Broken Access Control	CWE-425 Direct Request ('Forced Browsing')			
WebSocket URL poisoning	R01	Broken Access Control	CWE-441 Unintended Proxy or Intermediary	V		
Database connection string disclosed	R01	Broken Access Control	CWE-497 Exposure of Sensitive System Information to an Unauthorized Control Sphere	V		
Directory listing	R01	Broken Access Control	CWE-538 Insertion of Sensitive Information into Externally-Accessible File or Directory	V		
Source code disclosure	R01	Broken Access Control	CWE-540 Inclusion of Sensitive Information in Source	V		
Directory listing	R01	Broken Access Control	CWE-548 Exposure of Information Through Directory	V		
	R01	Broken Access Control	CWE-552 Files or Directories Accessible to External			
	R01	Broken Access Control	CWE-566 Authorization Bypass Through User-			
Open redirection	R01	Broken Access Control	CWE-601 URL Redirection to Untrusted Site ('Open	V		
	R01	Broken Access Control	CWE-639 Authorization Bypass Through User-			
	R01	Broken Access Control	CWE-651 Exposure of WSDL File Containing Sensitive			
	R01	Broken Access Control	CWE-668 Exposure of Resource to Wrong Sphere			
	R01	Broken Access Control	CWE-706 Use of Incorrectly-Resolved Name or			
	R01	Broken Access Control	CWE-862 Missing Authorization			
	R01	Broken Access Control	CWE-863 Incorrect Authorization			
	R01	Broken Access Control	CWE-913 Improper Control of Dynamically-Managed			
	R01	Broken Access Control	CWE-922 Insecure Storage of Sensitive Information			
	R01	Broken Access Control	CWE-1275 Sensitive Cookie with Improper SameSite			
	R02	Cryptographic Failures	CWE-259 Use of Hard-coded Password			
	R02	Cryptographic Failures	CWE-261 Weak Encoding for Password			
	R02	Cryptographic Failures	CWE-296 Improper Following of a Certificate's Chain			
Base64-encoded data in parameter	R02	Cryptographic Failures	CWE-310 Cryptographic Issues	V		
Cleartext submission of password, Mixed content	R02	Cryptographic Failures	CWE-319 Cleartext Transmission of Sensitive Information	V		
	R02	Cryptographic Failures	CWE-321 Use of Hard-coded Cryptographic Key			
	R02	Cryptographic Failures	CWE-322 Key Exchange without Entity			
	R02	Cryptographic Failures	CWE-323 Reusing a Nonce, Key Pair in Encryption			
	R02	Cryptographic Failures	CWE-324 Use of a Key Past its Expiration Date			
	R02	Cryptographic Failures	CWE-325 Missing Required Cryptographic Step			
TLS certificate, Unencrypted communications	R02	Cryptographic Failures	CWE-326 Inadequate Encryption Strength	V		
TLS certificate	R02	Cryptographic Failures	CWE-327 Use of a Broken or Risky Cryptographic	V		
	R02	Cryptographic Failures	CWE-328 Reversible One-Way Hash			
	R02	Cryptographic Failures	CWE-329 Not Using a Random IV with CBC Mode			
	R02	Cryptographic Failures	CWE-330 Use of Insufficiently Random Values			
	R02	Cryptographic Failures	CWE-331 Insufficient Entropy			
	R02	Cryptographic Failures	CWE-335 Incorrect Usage of Seeds in Pseudo-			
	R02	Cryptographic Failures	CWE-336 Same Seed in Pseudo-Random Number			
	R02	Cryptographic Failures	CWE-337 Predictable Seed in Pseudo-Random			
	R02	Cryptographic Failures	CWE-338 Use of Cryptographically Weak Pseudo-			
	R02	Cryptographic Failures	CWE-340 Generation of Predictable Numbers or			
JWT signature not verified	R02	Cryptographic Failures	CWE-347 Improper Verification of Cryptographic	V		
Strict transport security not enforced	R02	Cryptographic Failures	CWE-523 Unprotected Transport of Credentials	V		
	R02	Cryptographic Failures	CWE-720 OWASP Top Ten 2007 Category A9 -			

Risk Mapping						
Vulnerabilities scanning	**Risk ID**	**OWASP / Other Security risks**	**CWE**	**Burp Suite**	**NSlookup**	**Manual Test**
	R02	Cryptographic Failures	CWE-757 Selection of Less-Secure Algorithm During Negotiation('Algorithm Downgrade')			
	R02	Cryptographic Failures	CWE-759 Use of a One-Way Hash without a Salt			
	R02	Cryptographic Failures	CWE-760 Use of a One-Way Hash with a Predictable			
	R02	Cryptographic Failures	CWE-780 Use of RSA Algorithm without OAEP			
	R02	Cryptographic Failures	CWE-818 Insufficient Transport Layer Protection			
	R02	Cryptographic Failures	CWE-916 Use of Password Hash With Insufficient			
Input returned in response, Suspicious input transformation, HTML5 web message manipulation, Link manipulation, Document domain manipulation, DOM data manipulation, CSS injection, Client-side HTTP parameter pollution, Form action hijacking	R03	Injection	CWE-20 Improper Input Validation	V		
Link manipulation (reflected, stored), CSS injection, Form action hijacking	R03	Injection	CWE-73 External Control of File Name or Path	V		
	R03	Injection	in Output Used by a Downstream Component ('Injection')			
	R03	Injection	CWE-75 Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)			
OS Command injection	R03	Injection	CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')	V		
OS Command injection	R03	Injection	CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	V		
XSS(store, reflected, DOM-based, Client-side Xpath, Client-side JSON), Content security policy-allow untrusted source	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	V		
XSS(store, reflected, DOM-based), Content security policy-allow untrusted source	R03	Injection	CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	V		
	R03	Injection	CWE-83 Improper Neutralization of Script in			
	R03	Injection	CWE-87 Improper Neutralization of Alternate XSS			
	R03	Injection	CWE-88 Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')			
Injection (SQL, Client-side SQL)	R03	Injection	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	V		
LDAP Injection	R03	Injection	CWE-90 Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	V		
XML injection	R03	Injection	CWE-91 XML Injection (aka Blind XPath Injection)	V		
SMTP header injection	R03	Injection	CWE-93 Improper Neutralization of CRLF Sequences	V		
Injection (SQL, Xpath, PHP code, Server-side JavaScript code, Perl code, Ruby code, Python code, Unidentified code, Server-side template, JavaScript)	R03	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection')	V		
Injection (Server-side JavaScript code, Perl code, Ruby code, Python code, Unidentified code, Server-side template, JavaScript)	R03	Injection	CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	V		
SSI injection	R03	Injection	CWE-96 Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')	V		
	R03	Injection	CWE-97 Improper Neutralization of Server-Side			
	R03	Injection	Include/Require Statement in PHP Program ('PHP Remote File Inclusion')			
	R03	Injection	CWE-99 Improper Control of Resource Identifiers			
	R03	Injection	CWE-100 Deprecated: Was catch-all for input			
HTTP response header injection	R03	Injection	CWE-113 Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	V		
Injection (OS Command , SQL, LDAP, Xpath , XML , PHP code, Server-side JavaScript code , Perl code, Ruby code, Python code, Expression Language, Unidentified code injection, Server-side template, SSI, XSS, JavaScript, Client-side SQL, Client-side Xpath, Client-side JSON), Content security policy-allow untrused source, Input return in response, Ajax request header manipulation	R03	Injection	CWE-116 Improper Encoding or Escaping of Output	V		
	R03	Injection	CWE-138 Improper Neutralization of Special			
	R03	Injection	CWE-184 Incomplete List of Disallowed Inputs			
	R03	Injection	CWE-470 Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')			
	R03	Injection	CWE-471 Modification of Assumed-Immutable Data			
	R03	Injection	CWE-564 SQL Injection: Hibernate			
Out-of-band resource load (HTTP)	R03	Injection	CWE-610 Externally Controlled Reference to a	V		

Risk Mapping

Vulnerabilities scanning	Risk ID	OWASP / Other Security risks	CWE	Burp Suite	NSlookup	Manual Test
Xpath injection	R03	Injection	CWE-643 Improper Neutralization of Data within XPath Expressions ('XPath Injection')	V		
	R03	Injection	CWE-644 Improper Neutralization of HTTP Headers			
	R03	Injection	CWE-652 Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')			
Expression language injection	R03	Injection	Elements used in an Expression Language Statement ('Expression Language Injection')	V		
	R04	Insecure Design	CWE-73 External Control of File Name or Path			
	R04	Insecure Design	CWE-183 Permissive List of Allowed Inputs			
	R04	Insecure Design	CWE-209 Generation of Error Message Containing			
Referer-dependent response	R04	Insecure Design	CWE-213 Exposure of Sensitive Information Due to	V		
	R04	Insecure Design	CWE-235 Improper Handling of Extra Parameters			
	R04	Insecure Design	CWE-256 Unprotected Storage of Credentials			
	R04	Insecure Design	CWE-257 Storing Passwords in a Recoverable Format			
	R04	Insecure Design	CWE-266 Incorrect Privilege Assignment			
	R04	Insecure Design	CWE-269 Improper Privilege Management			
	R04	Insecure Design	CWE-280 Improper Handling of Insufficient			
Base64-encoded data in parameter	R04	Insecure Design	CWE-311 Missing Encryption of Sensitive Data	V		
	R04	Insecure Design	CWE-312 Cleartext Storage of Sensitive Information			
	R04	Insecure Design	CWE-313 Cleartext Storage in a File or on Disk			
	R04	Insecure Design	CWE-316 Cleartext Storage of Sensitive Information			
	R04	Insecure Design	CWE-419 Unprotected Primary Channel			
	R04	Insecure Design	CWE-430 Deployment of Wrong Handler			
File upload functionality	R04	Insecure Design	CWE-434 Unrestricted Upload of File with Dangerous	V		
HTTP request smuggling, Client-side desync	R04	Insecure Design	CWE-444 Inconsistent Interpretation of HTTP	V		
	R04	Insecure Design	CWE-451 User Interface (UI) Misrepresentation of			
	R04	Insecure Design	CWE-472 External Control of Assumed-Immutable			
	R04	Insecure Design	CWE-501 Trust Boundary Violation			
	R04	Insecure Design	CWE-522 Insufficiently Protected Credentials			
Cacheable HTTPS response	R04	Insecure Design	CWE-525 Use of Web Browser Cache Containing	V		
	R04	Insecure Design	CWE-539 Use of Persistent Cookies Containing			
	R04	Insecure Design	CWE-579 J2EE Bad Practices: Non-serializable Object			
Password submitted using GET method, Password returned in URL query string, SQL statement in request parameter, Session token in URL	R04	Insecure Design	CWE-598 Use of GET Request Method With Sensitive Query Strings	V		
	R04	Insecure Design	CWE-602 Client-Side Enforcement of Server-Side			
ASP.NET ViewState without MAC enabled	R04	Insecure Design	CWE-642 External Control of Critical State Data	V		
	R04	Insecure Design	CWE-646 Reliance on File Name or Extension of			
HTTP PUT method is enabled	R04	Insecure Design	CWE-650 Trusting HTTP Permission Methods on the	V		
	R04	Insecure Design	CWE-653 Insufficient Compartmentalization			
	R04	Insecure Design	CWE-656 Reliance on Security Through Obscurity			
	R04	Insecure Design	CWE-657 Violation of Secure Design Principles			
	R04	Insecure Design	CWE-799 Improper Control of Interaction Frequency			
	R04	Insecure Design	CWE-807 Reliance on Untrusted Inputs in a Security			
	R04	Insecure Design	CWE-840 Business Logic Errors			
	R04	Insecure Design	CWE-841 Improper Enforcement of Behavioral			
	R04	Insecure Design	CWE-927 Use of Implicit Intent for Sensitive			
Content security policy-allow clickjacking, Frameable response (potential Clickjacking)	R04	Insecure Design	CWE-1021 Improper Restriction of Rendered UI Layers or Frames	V		
	R04	Insecure Design	CWE-1173 Improper Use of Validation Framework			
	R05	Security Misconfiguration	CWE-2 7PK - Environment			
ASP.NET tracing enabled, ASP.NET debugging enabled	R05	Security Misconfiguration	CWE-11 ASP.NET Misconfiguration: Creating Debug Binary	V		
	R05	Security Misconfiguration	CWE-13 ASP.NET Misconfiguration: Password in			
Database connection string disclosed	R05	Security Misconfiguration	CWE-15 External Control of System or Configuration	V		
Path-relative style sheet import, External service interaction (SMTP), Referer-dependent response, Spoofable client IP address, User agent-dependent response, Cross-domain POST, Duplicate cookies set, Cookie scoped to parent domain, Cookie without HttpOnly flag set, Brower XSS filter disabled, HTTP TRACE method is enable, HTML does not specify charset, HTML uses unrecognized charset, Content type incorrectly stated, Content type is not specified, Mixed content	R05	Security Misconfiguration	CWE-16 Configuration	V		
	R05	Security Misconfiguration	CWE-260 Password in Configuration File			
	R05	Security Misconfiguration	CWE-315 Cleartext Storage of Sensitive Information			
	R05	Security Misconfiguration	CWE-520 .NET Misconfiguration: Use of			

Risk Mapping						
Vulnerabilities scanning	**Risk ID**	**OWASP / Other Security risks**	**CWE**	**Burp Suite**	**NSlookup**	**Manual Test**
	R05	Security Misconfiguration	CWE-526 Exposure of Sensitive Information Through			
	R05	Security Misconfiguration	CWE-537 Java Runtime Error Message Containing			
Source code disclosure	R05	Security Misconfiguration	CWE-541 Inclusion of Sensitive Information in an	V		
	R05	Security Misconfiguration	CWE-547 Use of Hard-coded, Security-relevant			
XML external entity injection, XML injection	R05	Security Misconfiguration	CWE-611 Improper Restriction of XML External	V		
TLS cookie without secure flat set	R05	Security Misconfiguration	CWE-614 Sensitive Cookie in HTTPS Session Without	V		
	R05	Security Misconfiguration	CWE-756 Missing Custom Error Page			
XML injection, XML entity expansion	R05	Security Misconfiguration	CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	V		
Flash cross-domain policy, Sliverlight cross-domain policy, Cross-origin resource sharing (arbitrary origin trusted, unencrypted orgin trusted, all subdomain trusted)	R05	Security Misconfiguration	CWE-942 Permissive Cross-domain Policy with Untrusted Domains	V		
	R05	Security Misconfiguration	CWE-1004 Sensitive Cookie Without 'HttpOnly' Flag			
	R05	Security Misconfiguration	CWE-1032 OWASP Top Ten 2017 Category A6 -			
	R05	Security Misconfiguration	CWE-1174 ASP.NET Misconfiguration: Improper			
	R06	Vulnerable and Outdated Components	CWE-937 OWASP Top 10 2013: Using Components with Known Vulnerabilities			
	R06	Vulnerable and Outdated Components	CWE-1035 2017 Top 10 A9: Using Components with Known Vulnerabilities			
Vulnerable JavaScript dependency	R06	Vulnerable and Outdated Components	CWE-1104 Use of Unmaintained Third Party Components	V		
	R07	Identification and Authentication Failures	CWE-255 Credentials Management Errors			
	R07	Identification and Authentication Failures	CWE-259 Use of Hard-coded Password			V
Password value set in cookie	R07	Identification and Authentication Failures	CWE-287 Improper Authentication	V		V
	R07	Identification and Authentication Failures	CWE-288 Authentication Bypass Using an Alternate Path or Channel			V
	R07	Identification and Authentication Failures	CWE-290 Authentication Bypass by Spoofing			
	R07	Identification and Authentication Failures	CWE-294 Authentication Bypass by Capture-replay			
TLS certificate	R07	Identification and Authentication Failures	CWE-295 Improper Certificate Validation	V		
	R07	Identification and Authentication Failures	CWE-297 Improper Validation of Certificate with Host Mismatch			
	R07	Identification and Authentication Failures	CWE-300 Channel Accessible by Non-Endpoint			
	R07	Identification and Authentication Failures	CWE-302 Authentication Bypass by Assumed-Immutable Data			
	R07	Identification and Authentication Failures	CWE-304 Missing Critical Step in Authentication			V
	R07	Identification and Authentication Failures	CWE-306 Missing Authentication for Critical Function			V
	R07	Identification and Authentication Failures	CWE-307 Improper Restriction of Excessive Authentication Attempts		V	
WebSocket URL poisoning	R07	Identification and Authentication Failures	CWE-346 Origin Validation Error	V		
Session token in URL	R07	Identification and Authentication Failures	CWE-384 Session Fixation	V		V
	R07	Identification and Authentication Failures	CWE-521 Weak Password Requirements			V
	R07	Identification and Authentication Failures	CWE-613 Insufficient Session Expiration			V
	R07	Identification and Authentication Failures	CWE-620 Unverified Password Change			V
	R07	Identification and Authentication Failures	CWE-640 Weak Password Recovery Mechanism for Forgotten Password			V
	R07	Identification and Authentication Failures	CWE-798 Use of Hard-coded Credentials			V
	R07	Identification and Authentication Failures	CWE-940 Improper Verification of Source of a Communication Channel			
	R07	Identification and Authentication Failures	CWE-1216 Lockout Mechanism Errors			V
WebSocket URL poisoning, JWT signature not verified, JWT none algorithm supported	R08	Software and Data Integrity Failures	CWE-345 Insufficient Verification of Data Authenticity	V		
	R08	Software and Data Integrity Failures	CWE-353 Missing Support for Integrity Check			

Risk Mapping

Vulnerabilities scanning	Risk ID	OWASP / Other Security risks	CWE	Burp Suite	NSlookup	Manual Test
	R08	Software and Data Integrity Failures	CWE-426 Untrusted Search Path			
	R08	Software and Data Integrity Failures	CWE-494 Download of Code Without Integrity Check			
Serialized object in HTTP message	R08	Software and Data Integrity Failures	CWE-502 Deserialization of Untrusted Data	V		
Cookie manipulation	R08	Software and Data Integrity Failures	CWE-565 Reliance on Cookies without Validation and Integrity Checking	V		
	R08	Software and Data Integrity Failures	CWE-784 Reliance on Cookies without Validation and Integrity Checking in a Security Decision			
Cross-domain script include, Cookie manipulation	R08	Software and Data Integrity Failures	CWE-829 Inclusion of Functionality from Untrusted Control Sphere	V		
	R08	Software and Data Integrity Failures	CWE-830 Inclusion of Web Functionality from an Untrusted Source			
	R08	Software and Data Integrity Failures	CWE-915 Improperly Controlled Modification of Dynamically-Determined Object Attributes			
	R09	Security Logging and Monitoring Failures	CWE-117 Improper Output Neutralization for Logs			
	R09	Security Logging and Monitoring Failures	CWE-223 Omission of Security-relevant Information			
	R09	Security Logging and Monitoring Failures	CWE-532 Insertion of Sensitive Information into Log File			
	R09	Security Logging and Monitoring Failures	CWE-778 Insufficient Logging			V
	R10	CSRF	CWE-352 Cross-Site Request Forgery (CSRF)	V		
Out-of-band resource load (HTTP), External service interaction (DNS, HTTP)	R10	SSRF	CWE-918 Server-Side Request Forgery (SSRF)	V		
DoS	R11	DoS, DDoS	CWE-400 Uncontrolled Resource Consumption	V		
	R11	DoS, DDoS	CWE-405 Asymmetric Resource Consumption			
External service interaction (DNS, HTTP, SMTP)	R11	DoS, DDoS	CWE-406 Insufficient Control of Network Message Volume (Network Amplification)	V		
	R11	DoS, DDoS	CWE-410 Insufficient Resource Pool			
	R11	DoS, DDoS	CWE-664 Improper Control of a Resource Through its			
	R11	DoS, DDoS	CWE-674 Uncontrolled Recursion			
	R11	DoS, DDoS	CWE-770 Allocation of Resources Without Limits or			
	R11	DoS, DDoS	CWE-771 Missing Reference to Active Allocated			
	R11	DoS, DDoS	CWE-779 Logging of Excessive Data			
	R11	DoS, DDoS	CWE-920 Improper Restriction of Power			
	R11	DoS, DDoS	CWE-1235 Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations			
	R11	DoS, DDoS	CWE-1246 Improper Write Handling in Limited-write			
DNS misconfigurations	R05				V	
DNS cache poisoning	R05				V	
	R12	WCAG				V
Email address disclosed, Private IP address disclosed, Social security numbers disclosed, Credit card numbers disclosed, Private key diclosed	R13	GDPR		V		V
Credit card numbers disclosed	R14	PCI DSS		V		V
Web cache poisoning, Request URL override, Multiple content types specified, HTML does not specify charset, HTML uses unrecognized charset, Content type incorrectly stated		Automated Threats to Web Applications	CWE 436 Interpretation Conflict	V		