Risk Mapping

Vulnerabilities	Severity	Risk ID	OWASP / Other Security risks	CWE	Burp Suite	NSlookup	Manual Test
GraphQL introspection enabled	Low	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		
GraphQL suggestions enabled	Low	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		
Cross-domain Referer leakage	Information	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		
Session token in URL	Medium	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		
Password field with autocomplete enabled	Low	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		V
Email addresses disclosed	Information	R01 R13	Broken Access Control, GDPR	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		V
Private IP addresses disclosed	Information	R01 R13	Broken Access Control, GDPR	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		V
Social security numbers disclosed	Information	R01 R13	Broken Access Control, GDPR	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		V
Credit card numbers disclosed	Information	R01 R14	Broken Access Control, PCI DSS	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		V
Private key disclosed	Information	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		V
Robots.txt file	Information	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		
Json Web Key Set disclosed	Information	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		
JWT private key disclosed	High	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	V		
Source code disclosure	Low	R01	Broken Access Control	CWE-200 Exposure of Sensitive Information to an Unauthorized Actor CWE-540 Inclusion of Sensitive Information in Source Code CWE-615 Inclusion of Sensitive Information in Source Code Comments	V		V
Local file path manipulation (DOM-based)	High	R01	Broken Access Control	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	V		
Local file path manipulation (reflected DOM-based)	High	R01	Broken Access Control	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	V		
Local file path manipulation (stored DOM-based)	High	R01	Broken Access Control	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	V		
File path traversal	High	R01	Broken Access Control	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') CWE-23 Relative Path Traversal CWE-35 Path Traversal: '.../...//' CWE-36 Absolute Path Traversal	V		
File path manipulation	High	R01	Broken Access Control	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') CWE-23 Relative Path Traversal CWE-35 Path Traversal: '.../...//' CWE-36 Absolute Path Traversal	V		
Broken Access Control	Information	R01	Broken Access Control	CWE-284 Improper Access Control	V		V
GraphQL content type not validated	Low	R01	Broken Access Control	CWE-352 Cross-Site Request Forgery (CSRF)	V		
Cross-site request forgery	Medium	R01	Broken Access Control	CWE-352 Cross-Site Request Forgery (CSRF)	V	V	
WebSocket URL poisoning (DOM-based)	High	R01	Broken Access Control	CWE-441 Unintended Proxy or Intermediary ('Confused Deputy')	V		
WebSocket URL poisoning (reflected DOM-based)	High	R01	Broken Access Control	CWE-441 Unintended Proxy or Intermediary ('Confused Deputy')	V		
WebSocket URL poisoning (stored DOM-based)	High	R01	Broken Access Control	CWE-441 Unintended Proxy or Intermediary ('Confused Deputy')	V		
Database connection string disclosed	Medium	R01	Broken Access Control	CWE-497 Exposure of Sensitive System Information to an Unauthorized Control Sphere	V		
Directory listing	Information	R01	Broken Access Control	CWE-538 Insertion of Sensitive Information into Externally-Accessible File or Directory CWE-548 Exposure of Information Through Directory Listing	V		V
Open redirection (reflected)	Low	R01	Broken Access Control	CWE-601 URL Redirection to Untrusted Site ('Open Redirect')	V		
Open redirection (stored)	Medium	R01	Broken Access Control	CWE-601 URL Redirection to Untrusted Site ('Open Redirect')	V		
Open redirection (DOM-based)	Low	R01	Broken Access Control	CWE-601 URL Redirection to Untrusted Site ('Open Redirect')	V		

Risk Mapping

Vulnerabilities	Severity	Risk ID	OWASP / Other Security risks	CWE	Burp Suite	NSlookup	Manual Test
Open redirection (reflected DOM-based)	Low	R01	Broken Access Control	CWE-601 URL Redirection to Untrusted Site ('Open Redirect')	V		
Open redirection (stored DOM-based)	Medium	R01	Broken Access Control	CWE-601 URL Redirection to Untrusted Site ('Open Redirect')	V		
Base64-encoded data in parameter	Information	R02	Cryptographic Failures	CWE-310 Cryptographic Issues	V		
Cleartext submission of password	High	R02	Cryptographic Failures	CWE-319 Cleartext Transmission of Sensitive Information	V		
Mixed content	Information	R02	Cryptographic Failures	CWE-319 Cleartext Transmission of Sensitive Information	V		
Unencrypted communications	Low	R02	Cryptographic Failures	CWE-326 Inadequate Encryption Strength	V		
TLS certificate	Medium	R02	Cryptographic Failures	CWE-326 Inadequate Encryption Strength CWE-327 Use of a Broken or Risky Cryptographic Algorithm	V		
JWT signature not verified	High	R02	Cryptographic Failures	CWE-347 Improper Verification of Cryptographic Signature	V		
Strict transport security not enforced	Low	R02	Cryptographic Failures	CWE-523 Unprotected Transport of Credentials	V		
HTTP response header injection	High	R03	Injection	CWE-113 Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')	V		
Content security policy: allows form hijacking	Information	R03	Injection	CWE-116 Improper Encoding or Escaping of Output	V		
Ajax request header manipulation (DOM-based)	Low	R03	Injection	CWE-116 Improper Encoding or Escaping of Output	V		
Ajax request header manipulation (reflected DOM-based)	Low	R03	Injection	CWE-116 Improper Encoding or Escaping of Output	V		
Ajax request header manipulation (stored DOM-based)	Low	R03	Injection	CWE-116 Improper Encoding or Escaping of Output	V		
Client-side template injection	High	R03	Injection	CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Content security policy: allows untrusted style execution	Information	R03	Injection	CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Suspicious input transformation (reflected)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
Suspicious input transformation (stored)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
HTML5 web message manipulation (DOM-based)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
HTML5 web message manipulation (reflected DOM-based)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
HTML5 web message manipulation (stored DOM-based)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
HTML5 storage manipulation (DOM-based)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
HTML5 storage manipulation (reflected DOM-based)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
HTML5 storage manipulation (stored DOM-based)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
Link manipulation (DOM-based)	Low	R03	Injection	CWE-20 Improper Input Validation	V		
Link manipulation (reflected DOM-based)	Low	R03	Injection	CWE-20 Improper Input Validation	V		
Link manipulation (stored DOM-based)	Low	R03	Injection	CWE-20 Improper Input Validation	V		
Document domain manipulation (DOM-based)	Medium	R03	Injection	CWE-20 Improper Input Validation	V		
Document domain manipulation (reflected DOM-based)	Medium	R03	Injection	CWE-20 Improper Input Validation	V		
Document domain manipulation (stored DOM-based)	Medium	R03	Injection	CWE-20 Improper Input Validation	V		
DOM data manipulation (DOM-based)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
DOM data manipulation (reflected DOM-based)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
DOM data manipulation (stored DOM-based)	Information	R03	Injection	CWE-20 Improper Input Validation	V		
Client-side HTTP parameter pollution (reflected)	Low	R03	Injection	CWE-20 Improper Input Validation	V		
Client-side HTTP parameter pollution (stored)	Low	R03	Injection	CWE-20 Improper Input Validation	V		
Input returned in response (stored)	Information	R03	Injection	CWE-20 Improper Input Validation CWE-116 Improper Encoding or Escaping of Output	V		
Input returned in response (reflected)	Information	R03	Injection	CWE-20 Improper Input Validation CWE-116 Improper Encoding or Escaping of Output	V		
Out-of-band resource load (HTTP)	High	R03	Injection	CWE-610 Externally Controlled Reference to a Resource in Another Sphere	V		
Local file path manipulation (DOM-based)	High	R03	Injection	CWE-73 External Control of File Name or Path	V		

Risk Mapping							
Vulnerabilities	**Severity**	**Risk ID**	**OWASP / Other Security risks**	**CWE**	**Burp Suite**	**NSlookup**	**Manual Test**
Local file path manipulation (reflected DOM-based)	High	R03	Injection	CWE-73 External Control of File Name or Path	V		
Local file path manipulation (stored DOM-based)	High	R03	Injection	CWE-73 External Control of File Name or Path	V		
Link manipulation (reflected)	Information	R03	Injection	CWE-73 External Control of File Name or Path CWE-20 Improper Input Validation	V		
Link manipulation (stored)	Information	R03	Injection	CWE-73 External Control of File Name or Path CWE-20 Improper Input Validation	V		
CSS injection (reflected)	Medium	R03	Injection	CWE-73 External Control of File Name or Path CWE-20 Improper Input Validation	V		
CSS injection (stored)	Medium	R03	Injection	CWE-73 External Control of File Name or Path CWE-20 Improper Input Validation	V		
Form action hijacking (reflected)	Medium	R03	Injection	CWE-73 External Control of File Name or Path CWE-20 Improper Input Validation	V		
Form action hijacking (stored)	Medium	R03	Injection	CWE-73 External Control of File Name or Path CWE-20 Improper Input Validation	V		
OS command injection	High	R03	Injection	CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection') CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') CWE-116 Improper Encoding or Escaping of Output	V		
Client-side XPath injection (DOM-based)	Low	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Client-side XPath injection (reflected DOM-based)	Low	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Client-side XPath injection (stored DOM-based)	Low	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Client-side JSON injection (DOM-based)	Low	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Client-side JSON injection (reflected DOM-based)	Low	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Client-side JSON injection (stored DOM-based)	Low	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Cross-site scripting (stored)	High	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Cross-site scripting (reflected)	High	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Cross-site scripting (DOM-based)	High	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Cross-site scripting (reflected DOM-based)	High	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		

Risk Mapping

Vulnerabilities	Severity	Risk ID	OWASP / Other Security risks	CWE	Burp Suite	NSlookup	Manual Test
Cross-site scripting (stored DOM-based)	High	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Content security policy: allowlisted script resources	Information	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Content security policy: allows untrusted script execution	Information	R03	Injection	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Client-side SQL injection (DOM-based)	High	R03	Injection	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Client-side SQL injection (reflected DOM-based)	High	R03	Injection	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
Client-side SQL injection (stored DOM-based)	High	R03	Injection	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
SQL injection	High	R03	Injection	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-116 Improper Encoding or Escaping of Output	V		
SQL injection (second order)	High	R03	Injection	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-116 Improper Encoding or Escaping of Output	V		
LDAP injection	High	R03	Injection	CWE-90 Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') CWE-116 Improper Encoding or Escaping of Output	V		
XML injection	Medium	R03	Injection	CWE-91 XML Injection (aka Blind XPath Injection) CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
SMTP header injection	Medium	R03	Injection	CWE-93 Improper Neutralization of CRLF Sequences ('CRLF Injection') CWE-159 Improper Handling of Invalid Use of Special Elements	V		
PHP code injection	High	R03	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
XPath injection	High	R03	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements CWE-643 Improper Neutralization of Data within XPath Expressions ('XPath Injection')	V		
JavaScript injection (DOM-based)	High	R03	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') CWE-116 Improper Encoding or Escaping of Output	V		
JavaScript injection (reflected DOM-based)	High	R03	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') CWE-116 Improper Encoding or Escaping of Output	V		
JavaScript injection (stored DOM-based)	High	R03	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') CWE-116 Improper Encoding or Escaping of Output	V		
Frameable response (potential Clickjacking)	Information	R04	Insecure Design	CWE-1021 Improper Restriction of Rendered UI Layers or Frames	V		
Content security policy: allows clickjacking	Information	R04	Insecure Design	CWE-1021 Improper Restriction of Rendered UI Layers or Frames CWE-693 Protection Mechanism Failure	V		
Referer-dependent response	Information	R04	Insecure Design	CWE-213 Exposure of Sensitive Information Due to Incompatible Policies	V		
Base64-encoded data in parameter	Information	R04	Insecure Design	CWE-311 Missing Encryption of Sensitive Data	V		
File upload functionality	Information	R04	Insecure Design	CWE-434 Unrestricted Upload of File with Dangerous Type	V		

Risk Mapping

Vulnerabilities	Severity	Risk ID	OWASP / Other Security risks	CWE	Burp Suite	NSlookup	Manual Test
HTTP request smuggling	High	R04	Insecure Design	CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	V		
Client-side desync	High	R04	Insecure Design	CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	V		
Cacheable HTTPS response	Information	R04	Insecure Design	CWE-525 Use of Web Browser Cache Containing Sensitive Information	V		
Password submitted using GET method	Low	R04	Insecure Design	CWE-598 Use of GET Request Method With Sensitive Query Strings	V		
Password returned in URL query string	Low	R04	Insecure Design	CWE-598 Use of GET Request Method With Sensitive Query Strings	V		
SQL statement in request parameter	Medium	R04	Insecure Design	CWE-598 Use of GET Request Method With Sensitive Query Strings	V		
Session token in URL	Medium	R04	Insecure Design	CWE-598 Use of GET Request Method With Sensitive Query Strings	V		
ASP.NET ViewState without MAC enabled	High	R04	Insecure Design	CWE-642 External Control of Critical State Data	V		
HTTP PUT method is enabled	High	R04	Insecure Design	CWE-650 Trusting HTTP Permission Methods on the Server Side	V		
Server-side JavaScript code injection	High	R04	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') CWE-116 Improper Encoding or Escaping of Output	V		
ASP.NET tracing enabled	High	R05	Security Misconfiguration	CWE-11 ASP.NET Misconfiguration: Creating Debug Binary	V		
ASP.NET debugging enabled	Medium	R05	Security Misconfiguration	CWE-11 ASP.NET Misconfiguration: Creating Debug Binary	V		
Database connection string disclosed	Medium	R05	Security Misconfiguration	CWE-15 External Control of System or Configuration Setting	V		
Path-relative style sheet import	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
External service interaction (SMTP)	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
Referer-dependent response	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
Spoofable client IP address	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
User agent-dependent response	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
Cross-domain POST	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
Duplicate cookies set	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
Cookie scoped to parent domain	Low	R05	Security Misconfiguration	CWE-16 Configuration	V		
Cookie without HttpOnly flag set	Low	R05	Security Misconfiguration	CWE-16 Configuration	V		
Browser cross-site scripting filter disabled	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
HTTP TRACE method is enabled	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
Content type is not specified	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
Mixed content	Information	R05	Security Misconfiguration	CWE-16 Configuration	V		
HTML does not specify charset	Information	R05	Security Misconfiguration	CWE-16 Configuration CWE-436 Interpretation Conflict	V		
HTML uses unrecognized charset	Information	R05	Security Misconfiguration	CWE-16 Configuration CWE-436 Interpretation Conflict	V		
Content type incorrectly stated	Low	R05	Security Misconfiguration	CWE-16 Configuration CWE-436 Interpretation Conflict	V		
Source code disclosure	Low	R05	Security Misconfiguration	CWE-541 Inclusion of Sensitive Information in an Include File	V		V
XML external entity injection	High	R05	Security Misconfiguration	CWE-611 Improper Restriction of XML External Entity Reference	V		
XML injection	Medium	R05	Security Misconfiguration	CWE-611 Improper Restriction of XML External Entity Reference CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	V		
TLS cookie without secure flag set	Medium	R05	Security Misconfiguration	CWE-614 Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	V		
XML entity expansion	Medium	R05	Security Misconfiguration	CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XM	V		
Perl code injection	High	R05	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') CWE-116 Improper Encoding or Escaping of Output	V		
Flash cross-domain policy	High	R05	Security Misconfiguration	CWE-942 Permissive Cross-domain Policy with Untrusted Domains	V		
Silverlight cross-domain policy	High	R05	Security Misconfiguration	CWE-942 Permissive Cross-domain Policy with Untrusted Domains	V		

Risk Mapping

Vulnerabilities	Severity	Risk ID	OWASP / Other Security risks	CWE	Burp Suite	NSlookup	Manual Test
Cross-origin resource sharing	Information	R05	Security Misconfiguration	CWE-942 Permissive Cross-domain Policy with Untrusted Domains	V		
Cross-origin resource sharing: arbitrary origin trusted	High	R05	Security Misconfiguration	CWE-942 Permissive Cross-domain Policy with Untrusted Domains	V		
Cross-origin resource sharing: unencrypted origin trusted	Low	R05	Security Misconfiguration	CWE-942 Permissive Cross-domain Policy with Untrusted Domains	V		
Cross-origin resource sharing: all subdomains trusted	Low	R05	Security Misconfiguration	CWE-942 Permissive Cross-domain Policy with Untrusted Domains	V		
DNS misconfigurations		R05	Security Misconfiguration			V	
DNS cache poisoning		R05	Security Misconfiguration			V	
Vulnerable JavaScript dependency	Low	R06	Vulnerable and Outdated Components	CWE-1104 Use of Unmaintained Third Party Components	V		
Ruby code injection	High	R06	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') CWE-116 Improper Encoding or Escaping of Output	V		
Lockout Mechanism Errors		R07	Identification and Authentication Failures	CWE-1216 Lockout Mechanism Errors			V
Use of Hard-coded Password		R07	Identification and Authentication Failures	CWE-259 Use of Hard-coded Password			V
Password value set in cookie	Medium	R07	Identification and Authentication Failures	CWE-287 Improper Authentication	V		
Authentication Bypass Using an Alternate Path or Channel		R07	Identification and Authentication Failures	CWE-288 Authentication Bypass Using an Alternate Path or Channel			V
TLS certificate	Medium	R07	Identification and Authentication Failures	CWE-295 Improper Certificate Validation	V		
Missing Critical Step in Authentication		R07	Identification and Authentication Failures	CWE-304 Missing Critical Step in Authentication			V
Missing Authentication for Critical Function		R07	Identification and Authentication Failures	CWE-306 Missing Authentication for Critical Function			V
Improper Restriction of Excessive Authentication Attempts		R07	Identification and Authentication Failures	CWE-307 Improper Restriction of Excessive Authentication Attempts		V	
WebSocket URL poisoning (DOM-based)	High	R07	Identification and Authentication Failures	CWE-346 Origin Validation Error	V		
WebSocket URL poisoning (reflected DOM-based)	High	R07	Identification and Authentication Failures	CWE-346 Origin Validation Error	V		
WebSocket URL poisoning (stored DOM-based)	High	R07	Identification and Authentication Failures	CWE-346 Origin Validation Error	V		
Session token in URL	Medium	R07	Identification and Authentication Failures	CWE-384 Session Fixation	V		
Weak Password Requirements		R07	Identification and Authentication Failures	CWE-521 Weak Password Requirements			V
Insufficient Session Expiration		R07	Identification and Authentication Failures	CWE-613 Insufficient Session Expiration			V
Unverified Password Change		R07	Identification and Authentication Failures	CWE-620 Unverified Password Change			V
Weak Password Recovery Mechanism for Forgotten Password		R07	Identification and Authentication Failures	CWE-640 Weak Password Recovery Mechanism for Forgotten Password			V
Use of Hard-coded Credentials		R07	Identification and Authentication Failures	CWE-798 Use of Hard-coded Credentials			V

Risk Mapping

Vulnerabilities	Severity	Risk ID	OWASP / Other Security risks	CWE	Burp Suite	NSlookup	Manual Test
Python code injection	High	R07	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') CWE-116 Improper Encoding or Escaping of Output	V		
Expression Language injection	High	R08	Injection	CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	V		
WebSocket URL poisoning (DOM-based)	High	R08	Software and Data Integrity Failures	CWE-345 Insufficient Verification of Data Authenticity	V		
WebSocket URL poisoning (reflected DOM-based)	High	R08	Software and Data Integrity Failures	CWE-345 Insufficient Verification of Data Authenticity	V		
WebSocket URL poisoning (stored DOM-based)	High	R08	Software and Data Integrity Failures	CWE-345 Insufficient Verification of Data Authenticity	V		
JWT signature not verified	High	R08	Software and Data Integrity Failures	CWE-345 Insufficient Verification of Data Authenticity	V		
JWT none algorithm supported	High	R08	Software and Data Integrity Failures	CWE-345 Insufficient Verification of Data Authenticity	V		
Serialized object in HTTP message	High	R08	Software and Data Integrity Failures	CWE-502 Deserialization of Untrusted Data	V		
Cookie manipulation (DOM-based)	Low	R08	Software and Data Integrity Failures	CWE-565 Reliance on Cookies without Validation and Integrity Checking CWE-829 Inclusion of Functionality from Untrusted Control Sphere	V		
Cookie manipulation (reflected DOM-based)	Low	R08	Software and Data Integrity Failures	CWE-565 Reliance on Cookies without Validation and Integrity Checking CWE-829 Inclusion of Functionality from Untrusted Control Sphere	V		
Cookie manipulation (stored DOM-based)	Low	R08	Software and Data Integrity Failures	CWE-565 Reliance on Cookies without Validation and Integrity Checking CWE-829 Inclusion of Functionality from Untrusted Control Sphere	V		
Cross-domain script include	Information	R08	Software and Data Integrity Failures	CWE-829 Inclusion of Functionality from Untrusted Control Sphere	V		
Insufficient Logging		R09	Security Logging and Monitoring Failures	CWE-778 Insufficient Logging			V
Unidentified code injection	High	R09	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') CWE-116 Improper Encoding or Escaping of Output	V		
Out-of-band resource load (HTTP)	High	R10	SSRF	CWE-918 Server-Side Request Forgery (SSRF)	V		
External service interaction (DNS)	Information	R10	SSRF	CWE-918 Server-Side Request Forgery (SSRF)	V		
External service interaction (HTTP)	High	R10	SSRF	CWE-918 Server-Side Request Forgery (SSRF)	V		
Server-side template injection	High	R10	Injection	CWE-94 Improper Control of Generation of Code ('Code Injection') CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') CWE-116 Improper Encoding or Escaping of Output	V		
Denial of service (DOM-based)	Information	R11	DoS, DDoS	CWE-400 Uncontrolled Resource Consumption	V		
Denial of service (reflected DOM-based)	Information	R11	DoS, DDoS	CWE-400 Uncontrolled Resource Consumption	V		
Denial of service (stored DOM-based)	Low	R11	DoS, DDoS	CWE-400 Uncontrolled Resource Consumption	V		
External service interaction (DNS)	Information	R11	DoS, DDoS	CWE-406 Insufficient Control of Network Message Volume (Network Amplification)	V		
External service interaction (HTTP)	High	R11	DoS, DDoS	CWE-406 Insufficient Control of Network Message Volume (Network Amplification)	V		
External service interaction (SMTP)	Information	R11	DoS, DDoS	CWE-406 Insufficient Control of Network Message Volume (Network Amplification)	V		
SSI injection	High	R11	Injection	CWE-96 Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') CWE-116 Improper Encoding or Escaping of Output CWE-159 Improper Handling of Invalid Use of Special Elements	V		
BCheck generated issue	Information				V		
Web cache poisoning	High			CWE-436 Interpretation Conflict	V		
Request URL override	Information			CWE-436 Interpretation Conflict	V		
Multiple content types specified	Information			CWE-436 Interpretation Conflict	V		
Content security policy: malformed syntax	Information				V		
Content security policy: not enforced	Information				V		
GraphQL endpoint found	Information				V		
GraphQL endpoint discovered	Information				V		
Web cache deception	Medium				V		
JWT self-signed JWK header supported	High				V		
JWT weak HMAC secret	High				V		
JWT arbitrary jku header supported	High				V		
JWT arbitrary x5u header supported	High				V		
Extension generated issue	Information				V		
Client-side prototype pollution	Information			CWE-1321	V		
Password returned in later response	Medium			CWE-204 Observable Response Discrepancy	V		V
Backup file	Information			CWE-530 Exposure of Backup File to an Unauthorized Control Sphere	V		V

Risk Mapping

Vulnerabilities	Severity	Risk ID	OWASP / Other Security risks	CWE	Burp Suite	NSlookup	Manual Test
Long redirection response	Information			CWE-698 Execution After Redirect (EAR)	V		V
Hidden HTTP 2	Information			CWE-912	V		
Failing to provide alternative text (Alt Text) for images.		R12	WCAG 1.1 Text Alternatives				V
Failure to include captions or transcripts for videos.		R12	WCAG 1.2 Time-based Media				V
Not meeting the minimum contrast requirements.		R12	WCAG 1.4 Distinguishable				V
Failure to ensure keyboard accessibility for all site functions.		R12	WCAG 2.1 Keyboard Accessible				V
No warning about the duration of user inactivity during checkout process.		R12	WCAG 2.2 Enough Time				V
No status message when shopping cart data or the checkout process is successfully submitted.		R12	WCAG 4.1 Compatible				V
Lack of consent mechanisms.		R13	GDPR Art. 7 Conditions for consent				V
Inadequate data security measures to safeguard users' personal data from data breaches.		R13	GDPR Art. 32 Security of processing				V
No documented records of data processing activities, including website and web shop.		R13	GDPR Art. 30 Records of processing activities				V
Lack of mechanisms for users to exercise their rights, such as restricting or objecting to processing their personal data.		R13	GDPR Art. 12-23 Rights of the data subject				V
Accepting credit card payments without complying with requirements for protecting cardholder data, implementing data encryption, etc.		R14	PCI DSS 4.0 requirements				V