Summary	IssueType	Issue ID	Parent ID
Information Gathering	Task	1	
Manually explore the site	Sub-task	2	1
Spider/crawl for missed or hidden content	Sub-task	3	1
Check for files that expose content, such as robots.txt, sitemap.xml, .DS_Store	Sub-task	4	1
Check the caches of major search engines for publicly accessible sites	Sub-task	5	1
Check for differences in content based on User Agent (eg, Mobile sites, access as a Search engine Crawler)	Sub-task	6	1
Perform Web Application Fingerprinting	Sub-task	7	1
Identify technologies used	Sub-task	8	1
Identify user roles	Sub-task	9	1
Identify application entry points	Sub-task	10	1
Identify client-side code	Sub-task	11	1
Identify multiple versions/channels (e.g. web, mobile web, mobile app, web services)	Sub-task	12	1
Identify co-hosted and related applications	Sub-task	13	1
Identify all hostnames and ports	Sub-task	14	1
Identify third-party hosted content	Sub-task	15	1
Configuration Management	Task	16	
Check for commonly used application and administrative URLs	Sub-task	17	16
Check for old, backup and unreferenced files	Sub-task	18	16
Check HTTP methods supported and Cross Site Tracing (XST)	Sub-task	19	16
Test file extensions handling	Sub-task	20	16
Test for security HTTP headers (e.g. CSP, X-Frame-Options, HSTS)	Sub-task	21	16
Test for policies (e.g. Flash, Silverlight, robots)	Sub-task	22	16
Test for non-production data in live environment, and vice-versa	Sub-task	23	16
Check for sensitive data in client-side code (e.g. API keys, credentials)	Sub-task	24	16
Secure Transmission	Task	25	
Check SSL Version, Algorithms, Key length	Sub-task	26	25
Check for Digital Certificate Validity (Duration, Signature and CN)	Sub-task	27	25
Check credentials only delivered over HTTPS	Sub-task	28	25
Check that the login form is delivered over HTTPS	Sub-task	29	25
Check session tokens only delivered over HTTPS	Sub-task	30	25
Check if HTTP Strict Transport Security (HSTS) in use	Sub-task	31	25
Authentication	Task	32	
Test for user enumeration	Sub-task	33	32
Test for authentication bypass	Sub-task	34	32
Test for bruteforce protection	Sub-task	35	32
Test password quality rules	Sub-task	36	32
Test remember me functionality	Sub-task	37	32
Test for autocomplete on password forms/input	Sub-task	38	32
Test password reset and/or recovery	Sub-task	39	32
Test password change process	Sub-task	40	32
Test CAPTCHA	Sub-task	41	32
Test multi factor authentication	Sub-task	42	32
Test for logout functionality presence	Sub-task	43	32
Test for cache management on HTTP (eg Pragma, Expires, Max-age)	Sub-task	44	32
Test for default logins	Sub-task	45	32
Test for user-accessible authentication history	Sub-task	46	32
Test for out-of channel notification of account lockouts and successful password changes	Sub-task	47	32
Test for consistent authentication across applications with shared authentication schema / SSO	Sub-task	48	32
Session Management	Task	49	
Establish how session management is handled in the application (eg, tokens in cookies, token in URL)	Sub-task	50	49
Check session tokens for cookie flags (httpOnly and secure)	Sub-task	51	49
Check session cookie scope (path and domain)	Sub-task	52	49
Check session cookie duration (expires and max-age)	Sub-task	53	49
Check session termination after a maximum lifetime	Sub-task	54	49
Check session termination after relative timeout	Sub-task	55	49
Check session termination after logout	Sub-task	56	49
Test to see if users can have multiple simultaneous sessions	Sub-task	57	49
Test session cookies for randomness	Sub-task	58	49
Confirm that new session tokens are issued on login, role change and logout	Sub-task	59	49
Test for consistent session management across applications with shared session management	Sub-task	60	49
Test for session puzzling	Sub-task	61	49
Test for CSRF and clickjacking	Sub-task	62	49
Authorization	Task	63	
Test for path traversal	Sub-task	64	63
Test for bypassing authorization schema	Sub-task	65	63
Test for vertical Access control problems (a.k.a. Privilege Escalation)	Sub-task	66	63

Test for horizontal Access control problems (between two users at the same privilege level)	Sub-task	67	63
Test for missing authorization	Sub-task	68	63
Data Validation	Task	69	
Test for Reflected Cross Site Scripting	Sub-task	70	69
Test for Stored Cross Site Scripting	Sub-task	71	69
Test for DOM based Cross Site Scripting	Sub-task	72	69
Test for Cross Site Flashing	Sub-task	73	69
Test for HTML Injection	Sub-task	74	69
Test for SQL Injection	Sub-task	75	69
Test for SOQL Injection	Sub-task	76	69
Test for LDAP Injection	Sub-task	77	69
Test for ORM Injection	Sub-task	78	69
Test for XML Injection	Sub-task	79	69
Test for XXE Injection	Sub-task	80	69
Test for SSI Injection	Sub-task	81	69
Test for XPath Injection	Sub-task	82	69
Test for XQuery Injection	Sub-task	83	69
Test for IMAP/SMTP Injection	Sub-task	84	69
Test for Code Injection	Sub-task	85	69
Test for Expression Language Injection	Sub-task	86	69
Test for Command Injection	Sub-task	87	69
Test for Overflow (Stack, Heap and Integer)	Sub-task	88	69
Test for Format String	Sub-task	89	69
Test for incubated vulnerabilities	Sub-task	90	69
Test for HTTP Splitting/Smuggling	Sub-task	91	69
Test for HTTP Verb Tampering	Sub-task	92	69
Test for Open Redirection	Sub-task	93	69
Test for Local File Inclusion	Sub-task	94	69
Test for Remote File Inclusion	Sub-task	95	69
Compare client-side and server-side validation rules	Sub-task	96	69
Test for NoSQL injection	Sub-task	97	69
Test for HTTP parameter pollution	Sub-task	98	69
Test for auto-binding	Sub-task	99	69
Test for Mass Assignment	Sub-task	100	69
Test for NULL/Invalid Session Cookie	Sub-task	101	69
Denial of Service	Task	102	
Test for anti-automation	Sub-task	103	102
Test for account lockout	Sub-task	104	102
Test for HTTP protocol DoS	Sub-task	105	102
Test for SQL wildcard DoS	Sub-task	106	102
Business Logic	Task	107	
Test for feature misuse	Sub-task	108	107
Test for lack of non-repudiation	Sub-task	109	107
Test for trust relationships	Sub-task	110	107
Test for integrity of data	Sub-task	111	107
Test segregation of duties	Sub-task	112	107
Cryptography	Task	113	
Check if data which should be encrypted is not	Sub-task	114	113
Check for wrong algorithms usage depending on context	Sub-task	115	113
Check for weak algorithms usage	Sub-task	116	113
Check for proper use of salting	Sub-task	117	113
Check for randomness functions	Sub-task	118	113
Risky Functionality - File Uploads	Task	119	
Test that acceptable file types are whitelisted	Sub-task	120	119
Test that file size limits, upload frequency and total file counts are defined and are enforced	Sub-task	121	119
Test that file contents match the defined file type	Sub-task	122	119
Test that all file uploads have Anti-Virus scanning in-place.	Sub-task	123	119
Test that unsafe filenames are sanitised	Sub-task	124	119
Test that uploaded files are not directly accessible within the web root	Sub-task	125	119
Test that uploaded files are not served on the same hostname/port	Sub-task	126	119
Test that files and other media are integrated with the authentication and authorisation schemas	Sub-task	127	119
Risky Functionality - Card Payment	Task	128	
Test for known vulnerabilities and configuration issues on Web Server and Web Application	Sub-task	129	128
Test for default or guessable password	Sub-task	130	128
Test for non-production data in live environment, and vice-versa	Sub-task	131	128
Test for Injection vulnerabilities	Sub-task	132	128

Test for Buffer Overflows	Sub-task	133	128
Test for Insecure Cryptographic Storage	Sub-task	134	128
Test for Insufficient Transport Layer Protection	Sub-task	135	128
Test for Improper Error Handling	Sub-task	136	128
Test for all vulnerabilities with a CVSS v2 score > 4.0	Sub-task	137	128
Test for Authentication and Authorization issues	Sub-task	138	128
Test for CSRF	Sub-task	139	128
HTML 5	Task	140	
Test Web Messaging	Sub-task	141	140
Test for Web Storage SQL injection	Sub-task	142	140
Check CORS implementation	Sub-task	143	140
Check Offline Web Application	Sub-task	144	140