

Linee guida per lo sviluppo sicuro



SOMMARIO

1		
	1.1 SCOPO	
	1.2 STRUTTURA DEL DOCUMENTO	7
2	RIFERIMENTI	8
	2.1 DOCUMENTI DI RIFERIMENTO	
_	DEFINIZIONI E ACRONIMI	0
3	3.1 DEFINIZIONI	
	3.2 ACRONIMI	
4		
5		
3	5.1 PROGETTAZIONE E SVILOFFO DELL'APPLICAZIONE. DIRETTIVE STANDARD	
	5.2 SVILUPPO DELL'APPLICAZIONE — CRITERI GENERALI	
	5.2.1 Performance	
	5.2.2 Password nel codice sorgente	
	5.2.3 Privilegi esecutivi minimi	
	5.2.4 Metodi TRACE e TRACK	
	5.2.5 Assenza di codice malevolo	
	5.2.6 Fattore integrità	14
	5.2.7 Input character validation	14
	5.2.8 Gestione dell'output	15
	5.3 FORMATTAZIONE DEL CODICE	15
	5.3.1 Stile e sintassi	
	5.3.2 Algoritmi	16
	5.3.3 Utilizzo funzioni di gestione delle stringhe	16
	5.3.4 Specifica del formato delle stringhe	16
	5.3.5 Casting e variabili numeriche	
	5.4 TRACCIAMENTO E RACCOMANDAZIONI DI "ALARM DETECTION"	
	5.4.1 Tracciamento eventi	
	5.4.2 Tracciamento eventi di "Alarm Detection"	
	5.4.3 Scopo e campo di applicazione per eventi di "Alarm Detection"	
	5.4.4 Raccomandazioni generali per eventi di "Alarm Detection"	
	5.5 COMPILAZIONE DELL'APPLICAZIONE	
	5.5.1 Stack Canary	
	5.5.2 Correttezza del sorgente	
	5.6 AMBIENTE OPERATIVO DELL'APPLICAZIONE	
	5.6.1 Separazione degli ambienti	
	5.6.2 Test dell'Applicazione	
	5.6.3 Strumenti	
	5.6.4 Profili utente	
	5.6.5 Trattamento dei dati	
	5.6.6 Protezione dei sorgenti e delle librerie	
	5.7.1 Policy standard "Everything is generally forbidden unless expressly permitted"	
	5.7.2 Assegnazione dei privilegi utente	
	5.7.3 Procedura di accesso dell'applicazione	
	5.7.4 Account standard	
	5.7.5 Autorizzazione	
	5.7.6 Generazione dei token	
	5.7.7 Generazione dei cookie	
	5.7.8 Contenuto del cookie	
	5.7.9 Scadenza del cookie	



	5.7.10	Logout utente	20
	5.7.11	Timeout di sessione	
	5.7.12	Isolamento delle funzioni dall'applicazione	20
	5.8 P	ASSWORD, CHIAVI E CERTIFICATI	20
	5.8.1	Gestione di password, chiavi e certificati	21
	5.8.2	Trasmissione delle password in rete	21
	5.8.3	Generazione/conservazione delle password nel filesystem/DB	21
	5.8.4	Batch Job dell'applicazione	
	5.8.5	Storage dei dati applicativi	
	5.8.6	Integrità delle informazioni	
	5.8.7	Meccanismi di autenticazione	
	5.8.8	Non ripudio delle sessioni	21
	5.8.9	Schemi di sicurezza e crittografici	
	5.8.10	Weak Keys e Collision	
	5.8.11	URL cifrati	
	5.8.12	Normalizzazione dei dati cifrati	
6	PRINCI	PALI VULNERABILITÀ DERIVANTI DA ERRORI DI PROGRAMMAZIONE: OVERVIEW	23
	6.1 V	ALIDAZIONE DELL'INPUT	23
	6.1.1	Shell Execution Command	23
	6.1.2	File Inclusion	24
	6.1.3	XML external entity (XXE) injection	25
	6.1.4	Insecure Deserialization	26
	6.1.5	Cross Site Scripting (XSS)	26
	6.1.6	Directory Traversal	27
	6.1.7	SQL Injection	28
	6.2 Si	SSION MANAGEMENT	29
	6.2.1	Session Stealing e Hjihacking	29
	6.2.1	.1 Cookie	30
	6.2.1		
	6.2.1		
		RITTOGRAFIA	
	6.3.1	Sniffing e algoritmi crittografici deboli	
	6.3.2	Brute forcing	
	6.3.3	Rainbow table e salt value	
	6.3.4	Archiviazione insicura	
		ESTIONE DEGLI ERRORI, DELLE ECCEZIONI	
		User Enumeration	
	6.4.2	Information disclosure	
	6.4.3	Directory Listing	
	6.4.4	Denial of Service (DoS)	
	6.4.5	Race condition	
	6.4.6	Privilege Escalation e aggiramento dei permessi utente	
		DUND CHECKING E PROBLEMATICHE DI OVERFLOW	
	6.5.1	Stack overflow	
	6.5.2	Off-by-one/Off-by-few	
	6.5.3	Format string overflow	
	6.5.4	Heap overflow	
	6.5.5	Integer overflow ed altri errori logici di programmazione	
		ROCESSI DI TRACCIAMENTO	
	6.6.1	Agevolazione delle attività malevole dell'aggressore	
	6.6.2	Oscuramento delle attività dell'aggressore	46
7		RACTICES PER LO SVILUPPO IN SICUREZZA	
		/C++	
	7.1.1	Cross-site scripting (XSS)	
	7.1.2	Command Injection	
	7.1.3	Connection Strina Injection	49



7.1.6 LDAP Injection 7.1.7 Process control. 7.1.8 Ulterior indication per lo sviluppo sicuro 7.1.8 Ulterior indication per lo sviluppo sicuro 7.1.8.1 Utilizzo dei tipi di dati 7.1.8.2 Utilizzo dei tipi di dati 7.1.8.3 Utilizzo dei tipi di dati 7.1.8.4 Macro. 7.1.8.6 Alfocazione dinamica 7.1.8.6 Alfocazione dinamica 7.1.8.7 Deallocazione 7.1.8.7 Postalocazione 7.1.8.9 Puntatori. 7.1.8.9 Puntatori. 7.1.8.10 Computazione e condizionali. 7.1.8.11 Computazione e condizionali. 7.1.8.11 Computazione e condizionali. 7.1.8.12 Passaggio di argomenti. 7.1.8.13 Passaggio di argomenti. 7.1.8.14 Chiamate a funzioni. 7.1.8.15 Files 7.1.8.16 Gestione degli errori 7.1.8.17 Sicurezza dell'applicazione 7.1.8.17 Sicurezza dell'applicazione 7.1.8.18 Computazione dell'applicazione 7.1.8.19 Computazione dell'applicazione 7.1.8.10 Cross-site scripting (XSS). 7.2.1 Cross-site scripting (PSS). 7.2.2 Code injection. 7.2.3 Command injection. 7.2.4 Connection string injection 7.2.5 Coli injection. 7.2.6 Resource injection. 7.2.7 SQL injection. 7.2.8 XPath injection. 7.2.10 Ulterior indicazioni per lo sviluppo sicuro 7.2.10.1 Ulterior indicazioni dei comandi di sistema 7.2.10.2 Visibilità 7.2.10.3 Serializzazione dei deserializzazione. 7.2.10.1 Peckages 7.2.10.1 Peckages 7.2.2 Injection. 7.2.3 Resource injection. 7.2.3 Resource injection. 7.2.4.1 Cross-site scripting (XSS). 7.2.10.1 Peckages 7.2.10.1 Peckages 7.2.2 Injection dei comandi di sistema 7.2.10.2 Visibilità 7.2.10.3 Java Serviet 7.2.10.1 Peckages 7.2.2 Injection dei comandi di sistema 7.2.2.10.2 Gestione delle eccezioni 7.2.2.10.3 Java Serviet 7.2.3 Tipologe di procedure vlySQL 7.3.4 Tipologe di procedure vlySQL 7.3.4 Tipologe di procedure vlyGQL 7.3.4.1 Cross-site scripting (XSS). 7.3.4 Tipologe di procedure vlyGQL 7.3.4.2 Tipologe di procedure vlyGQL 7.3.4.3 Client DOM Code Injection. 7.4.3 Client DOM Code Injection.	7.1.4	Resource Injection	51
7.1.8 Ulteriori indicazioni per lo sviluppo sicuro 7.1.8.1 Ultitiza del tipi di dati 7.1.8.2 Utilizza del tipi di dati 7.1.8.2 Striebe si di	7.1.5	SQL Injection	52
7.1.8 Ulteriori indicazioni per lo sviluppo sicuro 7.1.8.1 Ultitiza del tipi di dati 7.1.8.2 Utilizza del tipi di dati 7.1.8.2 Striebe si di	7.1.6	LDAP Injection	53
7.1.8.1 Dichiarazioni		· · ·	
7.18.1 Dichiarazioni. 7.18.3 Bitfields. 7.18.3 Bitfields. 7.18.6 Alfocazione dinamica. 7.18.6 Alfocazione dinamica. 7.18.6 Poellocazione. 7.18.7 Poellocazione. 7.18.7 Poellocazione. 7.18.8 Puntatori. 7.18.8 Puntatori. 7.18.9 Puntatori. 7.18.9 Puntatori. 7.18.10 Computazione e condizionali. 7.18.11 Corrollo del flusso. 7.18.12 Passaggio di argomenti. 7.18.13 Passaggio di argomenti. 7.18.14 Chiamate a funzioni. 7.18.15 Files. 7.18.16 Gestione degli errori. 7.18.17 Sicurezza dell'applicazione. 7.18.17 Sicurezza dell'applicazione. 7.18.18 Gestione degli errori. 7.18.19 Sicurezza dell'applicazione. 7.18.10 Computatione e condizione. 7.18.10 Computatione e condizione. 7.18.11 Cross-site scripting (XSS). 7.18.12 Cross-site scripting (XSS). 7.18.13 Cross-site scripting (XSS). 7.18.14 Cross-site scripting (XSS). 7.18.15 Cude injection. 7.18.16 Gestion e degli errori. 7.18.17 Cross-site scripting (XSS). 7.18.18 Cross-site scripting (XSS). 7.18.19 Cude injection. 7.19 Cude injection. 7.20 Code injection. 7.21 Cude injection. 7.22 Sour injection. 7.23 Command injection. 7.24 Connection string injection. 7.25 SQL injection. 7.26 Resource Injection. 7.27 SQL injection. 7.28 XPath injection. 7.29 XML External Entity (XXE) injection. 7.210 Ulteriori indicazioni per lo sviluppo sicuro. 7.210.1 Ulteriori indicazioni per lo sviluppo sicuro. 7.210.2 Visibilità. 7.210.3 Definizione delle classi. 7.210.4 Codice e permessi speciali. 7.210.5 Definizione delle classi. 7.210.7 Esecuzione del comandi di sistema. 7.210.8 Serializzazione e deserializzazione. 7.210.11 Packages. 7.210.12 Gestione delle eccezioni. 7.210.13 Java Servlet. 7.210.14 Cross-site scripting (XSS). 7.32 Resource injection. 7.33 Cla Injection. 7.34.1 Piotogie di procedure vulnerabili. 7.34.2 Direction polici pid input interbalie. 7.34.3 Tipologie di procedure vulnerabili. 7.34.2 Direction polici pid input interbalie. 7.34.2 Direction DOM Code lejecticon.			
7.18.2 Utilizzo dei tipi di dati . 7.18.5 Li Spirio di Computation di dati come parametri . 7.18.6 Allocazione dinamice . 7.18.7 Deallocazione . 7.18.9 Casting e problematiche di gestione delle variabili numeriche . 7.18.9 Casting e problematiche di gestione delle variabili numeriche . 7.18.10 Computazione e condizionali . 7.18.11 Controllo del flusso . 7.18.12 Passaggio di argoment . 7.18.13 Valori di ritorno . 7.18.14 Valori di ritorno . 7.18.15 Files . 7.18.15 Files . 7.18.16 Gestione degli errori . 7.18.17 Sicurezza dell'applicazione . 7.18.17 Sicurezza dell'applicazione . 7.18.17 Sicurezza dell'applicazione . 7.18.18 Casting degli errori . 7.18.19 Seriali esti controli di controli . 7.18.19 Seriali esti controli . 7.18.10 Java . 7.2.1 Cross-site scripting (XSS) . 7.2.2 Code injection . 7.2.3 Command injection . 7.2.4 Connection string injection . 7.2.5 LDAP Injection . 7.2.6 Resource Injection . 7.2.7 SQL injection . 7.2.8 Yabit injection . 7.2.9 XML External Entity (XXE) injection . 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro . 7.2.10.1 Inizializzazione . 7.2.10.2 Visibilità . 7.2.10.3 Oggetti mutevoli . 7.2.10.4 Utilizzo degli oggetti mutevoli . 7.2.10.5 Definizione delle ciassi . 7.2.10.6 Godice e permessi speciali . 7.2.10.7 Pescure e diece comandi di sistema . 7.2.10.8 Serializzazione de delle informazioni riservate . 7.2.10.1 Packages . 7.2.10.1 Packages . 7.2.10.1 Packages . 7.2.10.2 Gestione delle eccezioni . 7.2.20.3 Sul Injection . 7.3.3 SQL Injection . 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro . 7.3.5 Purico delle indicazioni per lo sviluppo sicuro . 7.3.6 Purico delle indicazioni per lo sviluppo sicuro . 7.3.7 Purico delle indicazioni e delle procedure PUSQL . 7.3.1 Pross siste scripting (XSS) . 7.3.2 Prossoure Injection . 7.3.3 SQL Injection . 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro . 7.3.5 Purico delle indicazioni per lo sviluppo sicuro . 7.3.6 Purico delle indicazioni per lo sviluppo sicuro . 7.3.7 Purico delle indicazioni per lo sviluppo sicuro . 7.3.3 SQL Inject		·	
7.18.3 Bitfields. 7.18.5 L'operatore sizeof e il passaggio di dati come parametri 7.18.6 Allocazione dinamica. 7.18.7 Deallocazione. 7.18.8 Puntatori. 7.18.8 Puntatori. 7.18.9 Casting e problematiche di gestione delle variabili numeriche 7.18.9 Casting e problematiche di gestione delle variabili numeriche 7.18.10 Computazione e condizionali 7.18.11 Controllo def flusso. 7.18.12 Passaggio di argomenti 7.18.13 Chiamate a funzioni 7.18.14 Chiamate a funzioni 7.18.15 Files. 7.18.16 Gestione degli errori. 7.18.17 Sicurezza dell'applicazione. 7.18.17 Sicurezza dell'applicazione. 7.2 Java. 7.2.1 Cross-site scripting (XSS). 7.2.2 Code injection. 7.2.3 Command injection. 7.2.4 Connection string injection. 7.2.5 LDAP Injection. 7.2.6 Resource Injection. 7.2.7 SQL injection. 7.2.8 XPath injection. 7.2.9 XML External Entity (XXE) injection. 7.2.10.1 Inizializzazione. 7.2.10.2 Utilizza degli oggetti mutevoli. 7.2.10.3 Modificatori. 7.2.10.4 Utilizza degli oggetti mutevoli. 7.2.10.5 Definizione delle classi. 7.2.10.6 Codice e permessi speciali. 7.2.10.7 Poscioni pare lo sviluppo sicuro 7.2.10.1 Inizializzazione degle classi. 7.2.10.2 Secretario gle scerializzazione 7.2.10.1 Packages. 7.2.10.2 Gestione delle eccezioni. 7.2.10.3 Java Servlet. 7.2.10.1 Packages. 7.2.10.1 Packages. 7.2.10.2 Gestione delle eccezioni. 7.2.2.10.3 Gestione delle eccezioni. 7.2.2.10.4 Utilizza degli oggetti mutevoli. 7.2.10.5 Secretario delle eccezioni. 7.2.10.6 Godice a permessi speciali. 7.2.10.7 Packages. 7.2.10.1 Packages. 7.2.10.2 Gestione delle eccezioni. 7.2.2.2 Packages. 7.2.10.3 Java Servlet. 7.2.10.4 Utilizza degli oggetti mutevoli. 7.2.2 Poscionamento delle procedure PUSQ. 7.3.3 Filtraggio del tripi di input interbabile. 7.3.4.1 Piotogic di procedure vulnerabili. 7.3.4.2 Directio per Cracle. 7.4.1 Lavascript in Dom Code la jection.	_		
7.18.4 Macro 7.18.5 L'Operatore sizeof e il passaggio di dati come parametri 7.18.6 Allocazione dinamica 7.18.7 Deallocazione. 7.18.8 Puntatori 7.18.9 Casting e problematiche di gestione delle variabili numeriche 7.18.10 Controllo del flusso 7.18.11 Controllo del flusso 7.18.12 Passaggio di argomenti 7.18.13 Valori di ritorno. 7.18.14 Chiamate a funzioni 7.18.15 Files. 7.18.16 Gestione degli errori. 7.18.17 Sicurezza dell'applicazione. 7.18.17 Sicurezza dell'applicazione. 7.18.18 Cross-site scripting (XSS). 7.18.19 Cross-site scripting (XSS). 7.2 Code injection. 7.2.1 Cross-site scripting injection. 7.2.2 Command injection. 7.2.3 Command injection. 7.2.4 Connection string injection. 7.2.5 LOAP Injection. 7.2.6 Resource Injection. 7.2.7 SQL injection. 7.2.8 XPath injection. 7.2.9 XML External Entity (XXE) injection. 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro. 7.2.10.1 Inizializzazione. 7.2.10.2 Ulteriori undicazioni per lo sviluppo sicuro. 7.2.10.3 Modificatori 7.2.10.4 Ultilizo degli oggetti mutevoli. 7.2.10.5 Definizione delle classi. 7.2.10.6 Codice e permessi speciali. 7.2.10.7 Escuzione del comandi di sistema 7.2.10.8 Oggetti . 7.2.10.1 Packagges 7.2.10.1 Packagges 7.2.10.2 Injection. 7.3.1 Cross-site scripting (XSS). 7.3.2 Resource Injection. 7.3.3 Ulteriori indicazioni per lo sviluppo sicuro. 7.3.4 Ulteriori deli cazioni per lo sviluppo sicuro. 7.3.5 Parametrio deli encerioni. 7.3.6 Resource Injection. 7.3.7 Specializzazione deli encerioni. 7.3.8 Jungettion. 7.3.9 Visibilità . 7.3.1 Cross-site scripting (XSS). 7.3.2 Resource Injection. 7.3.3 Il Tross-site scripting (XSS). 7.3.4 Tipologie di procedure PL/SQ. 7.3.4.1 Posizionamento delle procedure PL/SQ. 7.3.4.2 Tipologie di procedure vulnerabili . 7.3.4.2 Tipologie di procedure vulnerabili . 7.3.4.3 Filtro dei caratteri potenzialimente dannosi . 7.3.4.1 Cross site Scripting (XSS). 7.4.1 Cross site Scripting (XSS). 7.4.2 Cilent DOM Code Injection.	_	·	
7.1.8.5 L'operatore sizeof e il passaggio di dati come parametri 7.1.8.7 Deallocazione. 7.1.8.8 Puntatori. 7.1.8.9 Puntatori. 7.1.8.10 Computazione e condizionali. 7.1.8.11 Controllo del flusso. 7.1.8.12 Passaggio di argomenti. 7.1.8.12 Passaggio di argomenti. 7.1.8.13 Valori di ritorno. 7.1.8.14 Chiamate a funzioni. 7.1.8.15 Files. 7.1.8.16 Gestione degli errori. 7.1.8.17 Sicurezza dell'applicazione. 7.2. JAVA. 7.2.1 Cross-site scripting (XSS). 7.2.2 Code injection. 7.2.3 Command injection. 7.2.4 Connection string injection. 7.2.5 LDAP injection. 7.2.6 Resource injection. 7.2.7 SQL injection. 7.2.8 XPath injection. 7.2.9 XML External Entity (XXE) injection. 7.2.10 Intrializzazione. 7.2.10.1 Inizializzazione delle informazione. 7.2.10.2 Utileriori indicazioni per lo sviluppo sicuro. 7.2.10.1 Inizializzazione. 7.2.10.2 Utilizzo degli oggetti mutevoli. 7.2.10.3 Validicatori. 7.2.10.4 Utilizzo degli oggetti mutevoli. 7.2.10.5 Pefinizione delle classi. 7.2.10.6 Codice e permessi spicalil 7.2.10.7 Secuzione dei comandi di sistema. 7.2.10.1 Packagges. 7.2.10.1 Packagges. 7.2.10.1 Packagges. 7.2.10.2 Gestione delle conandi di sistema. 7.2.10.1 Packagges. 7.2.10.1 Packagges. 7.2.10.2 Gestione delle conandi di sistema. 7.2.10.3 Servicion. 7.2.3 Vilteriori indicazioni per lo sviluppo sicuro. 7.2.3 PISSI. 7.3.1 Poss-site scripting (XSS). 7.3.2 Resource Injection. 7.3.3 Qual Injection. 7.3.4 Utileriori indicazioni per lo sviluppo sicuro. 7.3.4.1 Posisionamento delle procedure PUSQ. 7.3.4.2 Tipologie di procedure vulnerabili. 7.3.4.3 Filtro dei caratteri potenzialmente dannosi. 7.3.4.1 Posisionamento delle procedure PUSQ. 7.3.4.2 Directive per Oracle. 7.4.1 AVASCRIPT. 7.4.1 Cross Site Scripting (XSS). 7.4.2 Cient DOM Code Injection.			
7.1.8.6 Allocazione dinamica 7.1.8.7 Deallocazione. 7.1.8.8 Puntatori. 7.1.8.9 Casting e problematiche di gestione delle variabili numeriche. 7.1.8.10 Computazione e condizionali. 7.1.8.11 Controllo del flusso. 7.1.8.12 Passaggio di argomenti. 7.1.8.13 Valori di ritorno. 7.1.8.15 Files. 7.1.8.16 Gestione degli errori. 7.1.8.17 Sicurezza dell'applicazione. 7.2.1 Cross-site scripting (XSS) 7.2.2 Code injection. 7.2.3 Command injection. 7.2.4 Connection string injection. 7.2.5 LDAP Injection. 7.2.6 Resource Injection. 7.2.7 SQL injection. 7.2.8 XPath injection. 7.2.9 XML External Entity (XXE) injection. 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro. 7.2.10.1 Ultiziori indicazioni per lo sviluppo sicuro. 7.2.10.1 Ultiziori indicazioni del consultati di Sistema. 7.2.10.1 Secuzione delle enticasi. 7.2.10.2 Squincione. 7.2.10.3 Modificatori. 7.2.10.4 Secuzione delle informazioni riservate. 7.2.10.7 Secuzione delle delle informazioni riservate. 7.2.10.1 Packages. 7.2.10.2 Gestione delle enticormazioni riservate. 7.2.10.1 Packages. 7.2.10.2 Secuzione delle informazioni riservate. 7.2.10.1 Packages. 7.2.10.1 Packages. 7.2.10.1 Packages. 7.2.10.1 Packages. 7.2.10.2 Ulteriori indicazioni per lo sviluppo sicuro. 7.2.10.1 Packages. 7.2.10.2 Secuzione delle encerializzazione. 7.2.10.1 Packages. 7.2.10.2 Secuzione delle encerializzazione. 7.2.10.1 Packages. 7.2.10.2 Fascuzione delle encerializzazione. 7.2.10.1 Packages. 7.2.10.2 Fascuzione delle encerializzazione. 7.2.10.3 Secuzione delle encerializzazione. 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro. 7.3.4.1 Posizionamento delle procedure PUSQL. 7.3.4.2 Tipologie di procedure vulnerabili. 7.3.4.3 Filtrogio del tipi di input intitatabile. 7.3.4.4 Filtro dei caratteri potenzialmente dannosi. 7.4.1 Cross Sice Scripting (XSS). 7.4.2 Cient DOM Code Injection.			
7.1.8.7 Deallocazione. 7.1.8.8 Puntatori 7.1.8.9 Casting e problematiche di gestione delle variabili numeriche 7.1.8.10 Computazione e condizionali. 7.1.8.11 Passaggio di argomenti. 7.1.8.12 Passaggio di argomenti. 7.1.8.13 Valori di ritorio 7.1.8.14 Chiamate a funzioni. 7.1.8.15 Files. 7.1.8.16 Gestione degli errori. 7.1.8.17 Sicurezza dell'applicazione. 7.2 Javv. 7.2 Javv. 7.2 Javv. 7.2 Jav. 7.2 Jav. 7.2 Jav. 7.3 Command injection 7.4 Connection string injection 7.5 LDAP injection 7.6 Resource Injection 7.7.6 Resource Injection 7.7.7 SQL injection 7.7.8 XPAth injection 7.7.9 XML External Entity (XXE) injection 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro 7.2.10.1 Initializzazione 7.2.10.1 Visibilità 7.2.10.1 Visibilità 7.2.10.1 Secuzione delle celassi 7.2.10.1 Gestione delle celassi 7.2.10.1 Secuzione del comandi di sistema 7.2.10.1 Gestione delle celassi 7.2.10.1 Gestione delle celassi 7.2.10.2 Serializzazione de delle informazioni riservate 7.2.10.1 Packages 7.2.10.2 Gestione delle eccezion 7.2.10.3 Java Servitti 7.2.10.4 Horizzazione delle eccezion 7.2.10.7 Escuzione delle cecezion 7.2.10.1 Packages 7.2.10.1 Demonstrazione delle eccezion 7.2.10.1 Packages 7.2.10.2 Serializzazione delle eccezion 7.2.10.3 Java Servitti 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 QL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.3 Iltraggio dei tipi di input injectionilia 7.3.4 Iltrediori indicazioni per lo sviluppo sicuro 7.3.3 Filtraggio dei tipi di input injectionilia 7.3.4 Iltrediori indicazioni per lo svilupo sicuro 7.3.5 Diettive per poracle 7.4.1 Cross Site Scripting (XSS) 7.4.2 Cient DOM Code Injection 7.4.1 Cross Site Scripting (XSS) 7.4.2 Cient DOM Code Injection		, , , , , , , , , , , , , , , , , , , ,	
7.1.8.8 Puntatori. 7.1.8.10 Costing e problematiche di gestione delle variabili numeriche. 7.1.8.11 Computazione e condizionali. 7.1.8.12 Passaggio di argomenti. 7.1.8.13 Valori di ritorno. 7.1.8.14 Chiamate a funzioni. 7.1.8.15 Files. 7.1.8.16 Gestione degli errori. 7.1.8.17 Sicurezza dell'applicazione. 7.1.8.17 Sicurezza dell'applicazione. 7.2.1 Cross-site scripting (XSS). 7.2.2 Code injection. 7.2.3 Command injection. 7.2.4 Connection string injection. 7.2.5 LDAP Injection. 7.2.6 Resource Injection. 7.2.7 SQL injection. 7.2.8 XPath injection. 7.2.9 XML External Entity (XXE) injection. 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro. 7.2.10.1 Inizializzazione. 7.2.10.1 Visibilità. 7.2.10.2 Visibilità. 7.2.10.3 Modificatori. 7.2.10.4 Ultilizzo degli oggetti mutevoli. 7.2.10.5 Definizione delle encessi speciali. 7.2.10.7 Secuzione dei comandi di sistema. 7.2.10.8 Segetti. 7.2.10.9 Serializzazione deserializzazione. 7.2.10.1 Packagges. 7.2.10.1 Packagges. 7.2.10.2 Packagione. 7.2.10.3 Soggetti. 7.2.10.4 Segetti. 7.2.10.5 Packagione. 7.2.10.6 Segetti. 7.2.10.7 Packagges. 7.2.10.8 Segetti. 7.2.10.9 Serializzazione delle enformazioni riservate. 7.2.10.10 Packagges. 7.2.10.11 Packagges. 7.2.10.12 Gestione delle eccezioni. 7.2.10.13 Java Serviet. 7.3.1 Cross-site scripting (XSS). 7.3.2 Resource Injection. 7.3.3 QL Injection. 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro. 7.3.4.1 Posizionamento delle procedure Pt/SQL. 7.3.3.2 Tipologi di procedure vulnerabili. 7.3.4.2 Tipologi di procedure vulnerabili. 7.3.4.3 Filtroggio dei tipi di input i hietabile. 7.3.4.1 Posizionamento delle procedure Pt/SQL. 7.3.4.2 Filtroggio dei tipi di input i hietabile. 7.3.4.1 Filtrogio dei cipi di prote tinictabile. 7.3.4.1 Posizionamento delle procedure Pt/SQL. 7.3.4.2 Filtrogio dei tipi di prote tinictabile. 7.3.4.1 Cross site Scripting (XSS). 7.4.2 Cient DOM Code Injection.			
7.1.8.9 Casting e problematiche di gestione delle variabili numeriche. 7.1.8.11 Controllo del flusso. 7.1.8.12 Passaggio di argomenti. 7.1.8.13 Valori di ritorno. 7.1.8.14 Chiamate a funzioni 7.1.8.15 Files 7.1.8.16 Gestione degli errori. 7.1.8.17 Sicurezza dell'applicazione. 7.2 JAVA. 7.2.1 Cross-site scripting (XSS). 7.2.2 Code injection. 7.2.3 Command injection. 7.2.4 Connection string injection. 7.2.5 LDAP Injection. 7.2.6 Resource Injection. 7.2.7 SQL injection. 7.2.8 XPML External Entity (XXE) injection. 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro 7.2.10.1 Inizializzazione. 7.2.10.1 Ulteriori indicazioni per lo sviluppo sicuro 7.2.10.1 Ulteriori indicazioni generali sulpida i sistema 7.2.10.1 Ulteriori indicazioni per lo svilupo in sicure. 7.2.10.1 Ulteriori indicazioni generali sistema 7.2.10.2 Sepalitzazione e deserializzazione. 7.2.10.1 Definizione delle classi. 7.2.10.1 Secuzione del comandi di sistema 7.2.10.2 Serializzazione delle informazioni riservate 7.2.10.11 Packages 7.2.10.12 Gestione delle edecezioni 7.2.10.13 Java Servitori (XSS). 7.3.2 Resource Injection 7.3.3 QL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4 Iteriori indicazioni per lo sviluppo sicuro 7.3.4 Iteriori indicazioni per lo sviluppo sicuro 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.5 Definizione delle procedure vulnerabili . 7.3.6 Definizione delle procedure v			
7.18.10 Computazione e condizionali. 7.18.11 Controllo del flusso. 7.18.12 Passaggio di argomenti. 7.18.13 Valori di ritorno. 7.18.14 Chiamate a funzioni. 7.18.15 Files 7.18.16 Gestione degli errori. 7.18.17 Sicurezza dell'applicazione. 7.18.17 Sicurezza dell'applicazione. 7.2 JAVA. 7.2 JAVA. 7.2 JAVA. 7.2.1 Cross-site scripting (XSS). 7.2.2 Code injection. 7.2.3 Command injection. 7.2.4 Connection string injection. 7.2.5 LDAP Injection. 7.2.6 Resource injection. 7.2.7 SQL Injection. 7.2.8 XPath injection. 7.2.9 XML External Entity (XXE) injection. 7.2.10 Utterior indicazioni per lo sviluppo sicuro. 7.2.10.1 Inizializazione 7.2.10.2 Utilizzo degli oggetti mutevoli. 7.2.10.3 Modificatori. 7.2.10.4 Utilizzo degli oggetti mutevoli. 7.2.10.5 Definizione delle classi. 7.2.10.6 Codice e permessi speciali. 7.2.10.7 Secuzione delle classi. 7.2.10.8 Oggetti. 7.2.10.9 Senalizzazione e deserializzazione. 7.2.10.1 Secuzione delle ecezzioni. 7.2.10.1 Packages 7.2.10.1 Packages 7.2.10.1 Java Serviet. 7.3.1 Cross-site scripting (XSS). 7.3.2 Resource Injection. 7.3.3 SQL Injection. 7.3.4 Posicionamento delle procedure PL/SQL 7.3.4.2 Filtro dei caratteri potenzialmente dannosi. 7.3.4.3 Filtraggio dei tipi di input iniettabile. 7.3.4.4 Filtro dei caratteri potenzialmente dannosi. 7.3.4.5 Dierttive per Oracle. 7.4.1 LAVASCRIPT. 7.4.1 Cross Site Scripting (XSS). 7.4.2 Client DOM Code Injection.			
7.1.8.11 Controllo del flusso 7.1.8.12 Passaggio di argomenti 7.1.8.13 Valori di ritorno 7.1.8.14 Chiamate a funzioni 7.1.8.15 Files 7.1.8.16 Gestione degli errori 7.1.8.17 Sicurezza dell'applicazione 7.2 JAVA 7.2 1 Cross-site scripting (XSS) 7.2.2 Code injection 7.2.3 Command injection 7.2.4 Connection string injection 7.2.5 LDAP injection 7.2.6 Resource Injection 7.2.7 SQL injection 7.2.8 XPath injection 7.2.9 XML External Entity (XXE) injection 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro 7.2.10.1 Inizializzazione 7.2.10.2 Visibilità 7.2.10.3 Modificatori 7.2.10.4 Utilizzo degli oggetti mutevoli 7.2.10.5 Definizione delle classi 7.2.10.6 Codice e permessi speciali 7.2.10.7 Esecuzione del comandi di sistema 7.2.10.8 Oggetti 7.2.10.1 Packages 7.2.10.1 Packages 7.2.10.1 Packages 7.2.10.1 Packages 7.2.10.2 Gestione delle eccezioni 7.2.10.1 Packages 7.2.10.1 Packages 7.2.10.1 Packages 7.2.10.2 Gestione delle eccezioni 7.2.10.3 Al Viteriori indicazioni per lo sviluppo sicuro 7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4 Ilteriori indicazioni per lo sviluppo sicuro 7.4.1 Cross Site Sc			
7.1.8.14 Valori di ritorno 7.1.8.15 Files	7.1.8.1	·	
7.1.8.14 Valori di ritorno 7.1.8.15 Files	7.1.8.1	.2 Passaggio di argomenti	59
7.18.15 Files. 7.18.16 Gestione degli errori. 7.18.17 Sicurezza dell'applicazione. 7.2 JAVA. 7.2.1 Cross-site scripting (XSS). 7.2.2 Code injection. 7.2.3 Command injection. 7.2.4 Connection string injection. 7.2.5 LDAP Injection. 7.2.6 Resource Injection. 7.2.7 SQL injection. 7.2.8 YPath injection. 7.2.9 XML External Entity (XXE) injection. 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro. 7.2.10.1 Inizializzazione. 7.2.10.2 Visibilità 7.2.10.3 Modificatori. 7.2.10.4 Utilizzo degli oggetti mutevoli. 7.2.10.5 Definizione delle classi. 7.2.10.6 Codice e permessi speciali. 7.2.10.7 Esecuzione dei comandi di sistema 7.2.10.8 Oggetti. 7.2.10.10 Gegetti. 7.2.10.10 Memorizzazione deserializzazione. 7.2.10.10 Memorizzazione delle informazioni riservate. 7.2.10.11 Packages. 7.2.10.12 Gestione delle eccezioni. 7.2.10.12 Gestione delle eccezioni. 7.2.10.13 Java Serviet. 7.3.1 Cross-site scripting (XSS). 7.3.2 Resource Injection. 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL. 7.3.4.2 Tipologie di procedure vulnerabili. 7.3.4.3 Filtraggio dei tipi di input iniettabile. 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle. 7.4.1 AVASCRIPT. 7.4.1 Cross Site Scripting (XSS). 7.4.2 Client DOM Code Injection.	7.1.8.1	l3 Valori di ritorno	59
7.18.16 Gestione degli errori 7.2 Java 7.2.1 Cross-site scripting (XSS) 7.2.2 Code injection 7.2.3 Command injection 7.2.4 Connection string injection 7.2.4 Connection string injection 7.2.5 LDAP Injection 7.2.6 Resource Injection 7.2.7 SQL injection 7.2.8 XPath injection 7.2.9 XML External Entity (XXE) injection 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro 7.2.10.1 Inizializzazione 7.2.10.2 Visibilità 7.2.10.3 Modificatori 7.2.10.4 Utilizzo degli oggetti mutevoli 7.2.10.5 Definizione delle classis. 7.2.10.6 Codice e permessi speciali 7.2.10.7 Secuzione del comandi di sistema 7.2.10.8 Oggetti 7.2.10.9 Serializzazione delle informazioni riservate 7.2.10.1 Packages 7.2.10.1 Packages 7.2.10.1 Packages 7.2.10.1 Packages 7.2.10.2 Gestione delle eccezioni 7.2.10.3 Java Servlet 7.2.10.1 Packages 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtro dei caratteri potenzialmente dannosi 7.3.4.3 Filtro dei caratteri potenzialmente dannosi 7.3.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection	7.1.8.1	L4 Chiamate a funzioni	60
7.1.8.17 Sicurezza dell'applicazione 7.2.1 Cross-site scripting (XSS) 7.2.2 Code injection	7.1.8.1	.5 Files	60
7.2.1 AVA	7.1.8.1	L6 Gestione degli errori	60
7.2.1 Cross-site scripting (XSS)	7.1.8.1	.7 Sicurezza dell'applicazione	60
7.2.2 Code injection	7.2 JAV	Α	60
7.2.3 Command injection 7.2.4 Connection string injection 7.2.5 LDAP Injection 7.2.6 Resource Injection 7.2.7 SQL injection 7.2.8 XPath injection 7.2.9 XML External Entity (XXE) injection 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro 7.2.10.1 Inizializzazione 7.2.10.2 Visibilità 7.2.10.3 Modificatori 7.2.10.4 Utilizzo degli oggetti mutevoli 7.2.10.5 Definizione delle classi 7.2.10.6 Codice e permessi speciali 7.2.10.7 Esecuzione dei comandi di sistema 7.2.10.9 Serializzazione deserializzazione 7.2.10.10 Memorizzazione delle informazioni riservate 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tiploogle di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection	7.2.1	Cross-site scripting (XSS)	60
7.2.3 Command injection 7.2.4 Connection string injection 7.2.5 LDAP Injection 7.2.6 Resource Injection 7.2.7 SQL injection 7.2.8 XPath injection 7.2.9 XML External Entity (XXE) injection 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro 7.2.10.1 Inizializzazione 7.2.10.2 Visibilità 7.2.10.3 Modificatori 7.2.10.4 Utilizzo degli oggetti mutevoli 7.2.10.5 Definizione delle classi 7.2.10.6 Codice e permessi speciali 7.2.10.7 Esecuzione dei comandi di sistema 7.2.10.9 Serializzazione deserializzazione 7.2.10.10 Memorizzazione delle informazioni riservate 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tiploogle di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection	7.2.2	Code injection	61
7.2.4 Connection string injection 7.2.5 LDAP Injection 7.2.6 Resource Injection 7.2.7 SQL injection 7.2.8 XPath injection 7.2.9 XML External Entity (XXE) injection 7.2.10 Ulterior indicazioni per lo sviluppo sicuro 7.2.10.1 Inizializzazione 7.2.10.2 Visibilità 7.2.10.3 Modificatori 7.2.10.4 Utilizzo degli oggetti mutevoli 7.2.10.5 Definizione delle classi 7.2.10.6 Codice e permessi speciali 7.2.10.7 Esecuzione dei comandi di sistema 7.2.10.8 Oggetti 7.2.10.9 Serializzazione e deserializzazione 7.2.10.1 Packages 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3. Pl/SQL 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.4.1 Posizionamento delle procedure vulnerabili 7.3.4.2 Tipologie di procedu			
7.2.5 LDAP Injection		· · · · · · · · · · · · · · · · · · ·	
7.2.6 Resource Injection		<u> </u>	
7.2.7 SQL injection 7.2.8 XPath injection 7.2.9 XML External Entity (XXE) injection 7.2.10 Ulteriori indicazioni per lo sviluppo sicuro 7.2.10.1 Inizializzazione 7.2.10.2 Visibilità 7.2.10.3 Modificatori 7.2.10.4 Utilizzo degli oggetti mutevoli 7.2.10.5 Definizione delle classi 7.2.10.6 Codice e permessi speciali 7.2.10.7 Esecuzione dei comandi di sistema 7.2.10.8 Oggetti 7.2.10.9 Serializzazione e deserializzazione 7.2.10.10 Memorizzazione delle informazioni riservate 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Direttive per Oracle. 7.4.1 Loross Site Scripting (XSS) 7.4.2 Client DOM Code Injection 7.5.4.5 Direttive per Oracle 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection		•	
7.2.8 XPath injection		•	
7.2.9 XML External Entity (XXE) injection		· · · · · · · · · · · · · · · · · · ·	
7.2.10 Ulteriori indicazioni per lo sviluppo sicuro		·	
7.2.10.1 Inizializzazione 7.2.10.2 Visibilità 7.2.10.3 Modificatori 7.2.10.4 Utilizzo degli oggetti mutevoli 7.2.10.5 Definizione delle classi 7.2.10.6 Codice e permessi speciali 7.2.10.7 Esecuzione dei comandi di sistema 7.2.10.8 Oggetti 7.2.10.9 Serializzazione e deserializzazione 7.2.10.10 Memorizzazione delle informazioni riservate 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3 PL/SQL 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4 JAVASCRIPT 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection			
7.2.10.2 Visibilità 7.2.10.3 Modificatori 7.2.10.4 Utilizzo degli oggetti mutevoli 7.2.10.5 Definizione delle classi 7.2.10.6 Codice e permessi speciali 7.2.10.7 Esecuzione dei comandi di sistema 7.2.10.8 Oggetti 7.2.10.9 Serializzazione e deserializzazione 7.2.10.10 Memorizzazione delle informazioni riservate 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4 JAVASCRIPT 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection	_	· · · · · · · · · · · · · · · · · · ·	
7.2.10.3 Modificatori 7.2.10.4 Utilizzo degli oggetti mutevoli 7.2.10.5 Definizione delle classi 7.2.10.6 Codice e permessi speciali 7.2.10.7 Esecuzione dei comandi di sistema 7.2.10.8 Oggetti 7.2.10.9 Serializzazione e deserializzazione 7.2.10.10 Memorizzazione delle informazioni riservate 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection			
7.2.10.4 Utilizzo degli oggetti mutevoli 7.2.10.5 Definizione delle classi 7.2.10.6 Codice e permessi speciali 7.2.10.7 Esecuzione dei comandi di sistema 7.2.10.8 Oggetti 7.2.10.9 Serializzazione e deserializzazione 7.2.10.10 Memorizzazione delle informazioni riservate 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3 PL/SQL 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection	_		
7.2.10.5 Definizione delle classi			
7.2.10.6 Codice e permessi speciali		0 00	
7.2.10.7 Esecuzione dei comandi di sistema 7.2.10.8 Oggetti 7.2.10.9 Serializzazione e deserializzazione. 7.2.10.10 Memorizzazione delle informazioni riservate. 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3. PL/SQL			
7.2.10.8 Oggetti 7.2.10.9 Serializzazione e deserializzazione 7.2.10.10 Memorizzazione delle informazioni riservate 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3 PL/SQL			
7.2.10.9 Serializzazione e deserializzazione 7.2.10.10 Memorizzazione delle informazioni riservate 7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3 PL/SQL 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4 JAVASCRIPT			
7.2.10.10 Memorizzazione delle informazioni riservate	_		
7.2.10.11 Packages 7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3 PL/SQL 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4 JAVASCRIPT 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection	_		
7.2.10.12 Gestione delle eccezioni 7.2.10.13 Java Servlet 7.3 PL/SQL 7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4 JAVASCRIPT 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection			
7.2.10.13 Java Servlet 7.3 PL/SQL			
7.3.1 Cross-site scripting (XSS) 7.3.2 Resource Injection 7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL 7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4 JAVASCRIPT 7.4.1 Cross Site Scripting (XSS) 7.4.2 Client DOM Code Injection	7.2.10	.13 Java Servlet	75
7.3.2 Resource Injection	7.3 PL/	'SQL	78
7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL. 7.3.4.2 Tipologie di procedure vulnerabili. 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi. 7.3.4.5 Direttive per Oracle 7.4 JAVASCRIPT 7.4.1 Cross Site Scripting (XSS)	7.3.1	Cross-site scripting (XSS)	78
7.3.3 SQL Injection 7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL. 7.3.4.2 Tipologie di procedure vulnerabili. 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi. 7.3.4.5 Direttive per Oracle 7.4 JAVASCRIPT 7.4.1 Cross Site Scripting (XSS)	7.3.2	Resource Injection	<i>79</i>
7.3.4 Ulteriori indicazioni per lo sviluppo sicuro 7.3.4.1 Posizionamento delle procedure PL/SQL		·	
7.3.4.1 Posizionamento delle procedure PL/SQL		·	
7.3.4.2 Tipologie di procedure vulnerabili 7.3.4.3 Filtraggio dei tipi di input iniettabile 7.3.4.4 Filtro dei caratteri potenzialmente dannosi 7.3.4.5 Direttive per Oracle 7.4 JAVASCRIPT		· · · · · · · · · · · · · · · · · · ·	
7.3.4.3 Filtraggio dei tipi di input iniettabile		•	
7.3.4.4 Filtro dei caratteri potenzialmente dannosi	_		
7.3.4.5 Direttive per Oracle			
7.4 JAVASCRIPT			
7.4.1 Cross Site Scripting (XSS)	7.4 JAV	·	
7.4.2 Client DOM Code Injection			
·		• • • •	



7.4.4	Client DOM Stored XSS	85
7.4.5	Client DOM XSS	87
7.5 F	PYTHON	
7.5.1	Cross-site scripting (XSS)	
7.5.2	Code Injection	
7.5.3	Command Injection	
7.5.4	Connection String Injection	
7.5.4 7.5.5	LDAP Injection	
	•	
7.5.6	Resource Injection	
7.5.7	SQL Injection	
7.5.8	XPath Injection	
7.5.9	XML External Entity (XXE) injection	
7.5.10		
7.5.11		
7.6	`#	
7.6.1	Cross-site scripting (XSS)	
7.6.2	Code Injection	97
7.6.3	Command Injection	98
7.6.4	Connection String Injection	99
7.6.5	LDAP Injection	101
7.6.6	Resource Injection	
7.6.7	SQL Injection	
7.6.8	XPath Injection	
7.6.9	XML External Entity (XXE) injection	
7.6.10		
	10.1 Managed Wrapper per l'implementazione del codice nativo	
	10.2 Library Code che espone risorse protette	
	10.3 Richieste di autorizzazione	
	10.4 Protezione dell'accesso ai metodi	
	10.5 Protezione e campi pubblici di sola lettura	
7.6.	10.6 Esclusione di classi e membri utilizzati da codice non attendibile	
7.6.	10.7 Definizione delle classi	108
7.6.	10.8 User input	108
7.6.	10.9 Concorrenza	108
7.6.	10.10 Serializzazione e deserializzazione	109
7.7 A	ASP	
7.7.1	Cross-site scripting (XSS)	109
7.7.2	Code Injection	111
7.7.3	Command Injection	
7.7.4	Connection String Injection	112
7.7.5	LDAP Injection	
7.7.6	XPath Injection	
7.7.7	Resource Injection	
7.7.8	SQL Injection	
_	SQL Injection	
7.8.1		
	Cross-site scripting (XSS)	
7.8.2	Code Injection	
7.8.3	Command Injection	
7.8.4	Connection String Injection	
7.8.5	LDAP Injection	119
7.8.6	Resource Injection	120
7.8.7	SQL Injection	120
7.8.8	XPath Injection	120
7.8.9	Ulteriori indicazioni per lo sviluppo sicuro	121
7.8.	• • • • • • • • • • • • • • • • • • • •	
7.8.	9.2 ASP.NET MVC	122
7.9 F	PHP	123
7.9.1	Cross-site scripting (XSS)	123



7.9.2	Code Injection	
7.9.3	Command Injection	126
7.9.4	File Disclosure	127
7.9.5	Remote File Inclusion	127
7.9.6	File Manipulation	128
7.9.7	LDAP Injection	129
	Reflected Injection	
	SQL Injection	
7.9.10	XPath Injection	
7.9.11	XML External Entity (XXE) injection	
7.9.12	Unsecure deserialization	
	NET	
7.10.1	Cross-site scripting (XSS)	
7.10.2	Code Injection	
7.10.3	Command Injection	
7.10.4	Connection String Injection	
7.10.5	LDAP Injection	
7.10.5	Resource Injection	
7.10.0	SQL Injection	
7.10.7	XPath Injection	
	AX	
7.11 AJ/ 7.11.1	Client Dom Code Injection	
7.11.1 7.11.2	Client DOM Stored Code Injection	
7.11.2 7.11.3	Client Dom Stored XSS	
_		
7.11.4 7.11.5	Client Dom XSSClient Resource Injection	
_	Client Second Order Sql Injection	
7.11.6	Client Sql Injection	
7.11.7	· ·	
7.11.8	Cross-Site Request Forgery (CSRF)	
	Client Devices the read VCC	
7.12.1	Client Dom Stored XSS	
7.12.2	SQL Injection	
7.12.3	Ulteriori indicazioni per lo sviluppo sicuro	
7.12.3 7.12.3		
7.12.3 7.12.3		
7.12.3	· · · · · · · · · · · · · · · · · · ·	
7.12.3	-	
25		
LISTA DELLE	TABELLE ocumenti di Riferimento	Q
	efinizioni	
	ronimi	
Tabella 5 - AC		11
LISTA DELLE	FIGURE	
LIGUED 1 CCh	iama nar ia cicuratta dall'annicationa	12



1 INTRODUZIONE

1.1 Scopo

Scopo del presente documento è supportare, attraverso opportune linee guida, lo sviluppo di applicazioni software sicure. Queste linee guida, costituiscono un insieme di best practices da seguire, al fine prevenire eventuali problematiche di sicurezza nel codice, e forniscono nel contempo uno strumento utile nell'individuazione di possibili vulnerabilità presenti nel codice sorgente e le relative contromisure da applicare.

1.2 Struttura del documento

Il presente documento è articolato come segue:

- Il Capitolo 1 riporta le generalità e lo scopo del documento;
- Il Capitolo 2 riporta la documentazione applicabile e di riferimento al presente documento;
- Il Capitolo 3 riporta le definizioni e gli acronimi utili per la lettura del documento;
- Il Capitolo 4 riporta un'introduzione alle applicazioni sicure;
- Il Capitolo 5 fornisce un insieme di raccomandazioni generali e trasversali alle scelte implementative;
- Il Capitolo 6 fornisce un elenco delle principali vulnerabilità software, corredate da esempi puntuali e delle relative contromisure da adottare;
- Il Capitolo 7 fornisce le best practices per i linguaggi di sviluppo utilizzati (C/C++, Java, PL/SQL, Javascript, PyThon, C#, ASP, ASP.NET, PHP, VBNET, AJAX, GO) e delle misure da adottare al fine di diminuire l'esposizione verso problematiche di sicurezza applicativa.