4 MINACCE E TIPOLOGIE DI ATTACCO

4.1 Catalogo delle Minacce

Di seguito viene fornito un catalogo di massima delle minacce correlate alle informazioni e ai servizi erogati. L'elenco è stato costruito seguendo le linee guida dettate dallo standard ISO/IEC 27005:2011 "Information technology — Security techniques — Information security risk management", e più in generale lo standard ISO/IEC 27001:2013.

Le minacce sono state individuate e selezionate in base alla loro effettiva applicabilità nel contesto del presente documento, escludendo quindi quelle ritenute non applicabili.

ID	Minaccia
M01	Abuso di privilegi da parte dell'utente.
M02	Abuso di risorse.
M03	Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.).
M04	Accesso non autorizzato alle informazioni.
M05	Attacchi all'integrità dei sistemi (software e configurazioni).
M06	Attacchi all'integrità delle informazioni.
M07	Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.
M08	Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
M09	Compromissione delle comunicazioni.
M10	Crittografia debole o non validata.
M11	Divulgazione di informazioni riservate.
M12	Errori di amministrazione dei sistemi.
M13	Falsificazione di identità.
M14	Furto di credenziali di autenticazione.
M15	Generazione e/o gestione inadeguata delle chiavi crittografiche.
M16	Negazione dei servizi.
M17	Tentativi di frode.
M18	Uso non autorizzato di privilegi.
M19	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.)
M20	Violazione di leggi, di regolamenti, di obblighi contrattuali.
M21	Danneggiamento, perdita o furto di un asset fisico.

Tabella 3 - Catalogo delle Minacce

4.2 Catalogo delle tipologie di attacco

La tabella che segue fornisce una rassegna delle più note tipologie (meccanismi) di attacco.

Si sottolinea che i meccanismi di attacco sono sempre in evoluzione e spesso sfruttano vulnerabilità non note (i cosiddetti “zero-day”, descritti brevemente nel seguito), per cui un elenco di questo tipo, per sua stessa natura, non può ovviamente essere del tutto esaustivo.

ID	Tipologia	Descrizione
A01	BIOS rootkit attack	Un attacco di rootkit a livello di BIOS, noto anche come attacco persistente del BIOS, è un exploit in cui il BIOS viene aggiornato con codice dannoso. Il BIOS rootkit è un programma che risiede nella memoria fisica non volatile di un computer (in genera una EEPROM) e può consentire anche l'accesso e il monitoraggio del sistema da remoto.
A02	Brute Force Attack	Si definisce con il termine "Brute Force Attack" tratta di un attacco basato sul potere computazionale per decifrare le password o altre informazioni sensibili, o per “indovinare” password protette da hashing e crittografia.
A03	Buffer overflow	Si indica con il termine "Buffer overflow" tratta di una tecnica con cui un attaccante riesce ad eseguire uno “sfondamento” della memoria nel processo del sistema. Le vulnerabilità di buffer overflow possono portare ad attacchi di Denial of Service (DoS) o iniezione di codice (Code Injection). Un attacco di Denial of Service può causare un crash, uno stop o un rallentamento del processo; l'iniezione di codice invece, può modificare l'indirizzo di esecuzione del processo per eseguire il codice iniettato dall'aggressore.
A04	Cache poisoning	Il "cache poisoning", anche detto DNS poisoning o DNS cache poisoning, consiste nella compromissione di una tabella di sistema che memorizza gli indirizzi IP dei server internet dei nomi ottenuti dal server di dominio (DNS) Internet, sostituendo un indirizzo Internet corretto con quello di un altro indirizzo di un sito malevolo. Quando un utente Web cerca la pagina con tale indirizzo o nome host, la richiesta viene reindirizzata dalla voce all’indirizzo IP malevolo falsificato, presente nella tabella, verso un indirizzo diverso da quello reale. A quel punto è possibile che, un worm, uno spyware o un altro malware venga scaricato nel computer dell'utente direttamente dall'indirizzo malevolo, oppure è possibile che un sito contraffatto catturi le credenziali utente, eventualmente ponendosi come intermediario (man-in-the-middle) verso il sito legittimo.
A05	Clickjacking	Il Clickjacking (noto anche come reindirizzamento dell'interfaccia utente e “IFRAME overlay”) è un exploit in cui viene nascosto del codice dannoso nel codice dei pulsanti apparentemente innocui o di altri contenuti cliccabili presenti in un sito web.
A06	Clipboard hijacking	Il "clipboard hijacking" è un exploit in cui l'aggressore ottiene il controllo della clipboard della vittima e sostituisce i contenuti lì presenti con i propri dati, ad esempio un collegamento ad un sito Web dannoso.
A07	Code injection	È un attacco basato sull’inserimento nel codice dell’applicazione web di istruzioni, opportunamente modificate da un malintenzionato, finalizzate ad esempio, all'impersonificazione di un utente autenticato oppure nel furto di reperimento di credenziali di accesso.
A08	Cold boot attack	Un "cold boot attack" è un processo utilizzato per ottenere accesso non autorizzato alle chiavi di crittografia di un computer quando questo viene lasciato fisicamente incustodito. I ricercatori dell'Università di Princeton,

		della Electronic Frontier Foundation e Wind River Systems hanno scoperto che è possibile portare un attacco di questo tipo, dato che i chip di memoria ad accesso casuale dinamico (DRAM) conservano i dati per un breve periodo di tempo dopo lo spegnimento del computer su cui sono installate. Questa quantità di tempo può aumentare se i chip vengono rimossi dalla scheda madre e mantenuti a basse temperature. Ciò può essere fatto attraverso un raffreddamento con una canna invertita ad aria compressa. I chip possono quindi essere reinseriti rapidamente in un computer per poi leggerne il contenuto.
A09	Cracking	Con cracking si intende la modifica di un software per rimuovere la protezione dalla copia, oppure per ottenere accesso ad un'area altrimenti riservata. Per cracking si intende anche la violazione di sistemi informatici collegati ad Internet o ad un'altra rete, allo scopo di danneggiarli, di rubare informazioni oppure di sfruttare i servizi telematici della vittima (connessione ad Internet, traffico voce, sms, accesso a database etc..) senza la sua autorizzazione (thiefing).
A10	Cross-Frame Scripting (XFS)	Si tratta di un attacco che combina un codice JavaScript malizioso con un iframe che carica una pagina legittima allo scopo di rubare dati da un utente inconsapevole. In genere funziona in combinazione con il social engineering o il phishing. A titolo di esempio, un attaccante può convincere un utente a navigare su una pagina contenente il codice JavaScript e un iframe HTML che punta a un sito legittimo. Quando l'utente inserisce le credenziali sul sito legittimo, il codice JavaScript ne memorizza i caratteri.
A11	Cross-site request forgery (CSRF)	Un attacco "cross-site request forgery", detto anche brevemente CSRF e talvolta pronunciato "Sea-Surf", consiste nell'abuso della fiducia tra l'applicazione e un determinato client (la vittima) al fine di eseguire una transazione a livello applicativo, pilotata da un attaccante utilizzando l'identità del client. L'attacco è basato sull'incorporamento di URL, che rappresentano transazioni specifiche dell'applicazione di destinazione, all'interno di una pagina controllata dall' attaccante, che è già stata acceduta dalla vittima tramite browser dopo aver stabilito una relazione di fiducia con l'applicazione di destinazione (ad esempio tramite l'autenticazione). Esempi di tali richieste includono il trasferimento di fondi monetari e titoli, attività di provisioning, amministrazione di applicazioni e perfino operazioni di l'acquisto di beni e servizi.
A12	Cross-site scripting (XSS)	Esistono 3 tipi di Cross Site Scripting: - "Reflected": Il web server legge i dati dannosi (payload di attacco) direttamente dalla richiesta HTTP e li rimanda (riflette) indietro nella risposta HTTP (Il meccanismo più comune per distribuire i contenuti dannosi è quello di includerli come parametro in una URL che viene resa pubblica o inviata per e-mail direttamente alla vittima). - "Stored": Il web server memorizza i dati dannosi (payload di attacco) in un suo archivio. In un secondo momento, i dati dannosi vengono letti e inclusi in una risposta http. - "DOM based": A differenza dei due tipi precedenti, i dati dannosi (payload di attacco) non vengono inseriti nella risposta (a causa di un difetto lato server). L'attacco mira a modificare il DOM "environment" all'interno del browser della vittima in modo che uno script che gira lato client produca un esito diverso da quello atteso (a causa appunto della presenza dei dati dannosi che sono stati iniettati nel DOM

		"environment"). Ad esempio, lo script che gira lato client usa il "document.location" –ossia l'url- e l'attaccante inserisce opportunamente uno script nell'url.
A13	CSV Injection	Questo attacco, noto anche come Formula Injection, avviene quando un sito web inserisce input malevoli in dati e formule (o anche delle macro maliziose) in un file CSV che viene scaricato dagli utenti. Quando un programma come Excel (o LibreOffice Calc) apre tale foglio CSV, "valuta" le formule presenti nelle celle e contenenti valori "maliziosi". Ci sono tre tipi di attacco di questo tipo: - quelli che sfruttano le vulnerabilità del foglio elettronico, come quella descritta in CVE-2014-3524; - quelli che compromettono il computer dell'utente sfruttando la tendenza degli utenti a non effettuare controlli antivirus e a ignorare gli avvisi di sicurezza sui fogli CSV scaricati; - quelli mirati al furto di informazioni da altri fogli elettronici aperti dall'utente o da qualsiasi file presente sul suo computer.
A14	Denial of Service	È un attacco mirato a che si perpetra portando al limite delle prestazioni il funzionamento di un sistema (ad es., un sito web) al limite delle prestazioni, (ad es., un sito web) causando il blocco del servizio. La variante distribuita (DDoS) si attua, invece, generando un numero molto elevato di richieste simultanee da parte di più macchine (a volte decine di migliaia) generalmente controllati attraverso un malware specifico, contemporaneamente dirette tutte al medesimo server, in modo da esaurirne le risorse e renderlo non più in grado di erogare i propri servizi. Come conseguenza, il server vittima non risulta più raggiungibile dall'esterno.
A15	Dictionary Attack	Con l'attacco Dictionary, un aggressore utilizza un programma per l'iterazione di tutte le parole presenti in un dizionario (o più dizionari in diverse lingue) e calcola l'hash per ogni parola. L'hash risultante viene confrontato con il valore presente nell'archivio delle password. Le password deboli come una squadra preferita o un'auto preferita, verranno decifrate rapidamente. Le password più forti come ad esempio quelle che combinano sequenze di caratteri differenti ("? BiolLNessFiNdMeyePasSWirt!"), sono meno probabili da decifrare.
A16	Direct Dynamic Code Evaluation ('Eval Injection')	L'attacco colpisce gli script che non validano correttamente l'input utente usato nel parametro page. Un utente remoto può fornire un input una URL opportunamente formata, per passare codice arbitrario a un'istruzione eval().
A17	Directory harvest attack (DHA)	Un attacco "directory harvest" (DHA) è un tentativo di determinare gli indirizzi di posta elettronica validi associati a un server di posta elettronica in modo tale da poterli aggiungere a un database di spam. Attraverso un attacco di brute force (a volte più o meno selettivo e mirato a una specifica organizzazione/evoluto nella composizione degli usernames) indirizzato verso l'e-mail Mail Server, il programma DHA alimenta il database di spam secondo il seguente criterio: se l'e-mail Mail Server ritorna restituisce un messaggio di replica errore di tipo "Not found" allora l'indirizzo provato è inesistente e va scartato, se l'e-mail server invece non restituisce nulla allora l'indirizzo provato è valido e va aggiunto al database.
A18	Drive-by-Downloads attack	In un attacco "Drive-by-Download", l'applicazione web viene modificata (ad esempio iniettando codice HTML) in modo tale da istruire il browser

		del visitatore a scaricare il malware situato nel server controllato da un aggressore. Spesso, la manomissione non è visibile ai visitatori, quindi le vittime innocenti non sono a conoscenza dell'operazione di download che avviene in background. Pertanto l'attacco "Drive-by-Download" si svolge su 3 fronti: - compromissione di un web server legittimo per hostare il contenuto malevolo capace di avviare il download sul client della vittima o utilizzare, per lo stesso scopo, un *third party service* (ad es. un banner pubblicitario) che il web server legittimo (inconsapevolmente) espone; - compromissione del client per avviare il download del malware vero e proprio; - esecuzione del malware sul client.
A19	Esecuzione arbitraria di codice	Se un utente malintenzionato riesce a eseguire codice dannoso sul server, questo può compromettere le risorse del server o installare ulteriore software capace di portare attacchi contro i sistemi a valle dell'infrastruttura. I rischi derivanti dall'esecuzione arbitraria di codice aumentano se il processo server in cui viene eseguito il codice dell'attaccante ha privilegi elevati. Le vulnerabilità più comuni che consentono l'esecuzione arbitraria di codice sono legate a sistemi server mal configurati (privi di hardening) o non aggiornati (privi delle patch di sicurezza), oppure alla mancata validazione dell'input utente, specie in applicazioni scritte in linguaggi in cui la memoria dinamica non è gestita automaticamente e l'accesso diretto alla memoria tramite puntatori non viene impedito a causa di configurazioni deboli dell'application server e da server non sottoposti agli ultimi aggiornamenti che consentono l'attraversamento di percorsi non protetti (path traversal) e attacchi di buffer overflow, dove entrambi comunque, possono portare all'esecuzione di codice arbitrario.
A20	Format String Attack	Questo attacco si verifica quando i dati forniti in input e copiati in una stringa vengono in realtà "valutati" come un comando che viene eseguito dall'applicazione. In tal modo un attaccante può iniettare codice arbitrario, leggere lo stack o causare un "segmentation fault".
A21	Heap Overflow	Consiste in un tipo particolare di buffer overflow che avviene però nell'area di memoria dello "heap". La memoria nello heap è allocata dinamicamente dall'applicazione a run-time e tipicamente contiene le strutture dati allocate dinamicamente dal programma. L'attacco mira a corrompere queste strutture in vari modi, come ad es. sovrascrivendole attraverso i relativi puntatori, usati per accedere ad indirizzi che vanno oltre la fine di una determinata struttura memorizzata.
A22	Heartbleed	Si tratta di un attacco che sfrutta un bug della libreria crittografica fornita da OpenSSL, usata da innumerevoli applicazioni, compresi client e server Web, VPN, LDAP(S), IMAP(S), SMTP(S), SFTP, RDBMS, ecc. La vulnerabilità è dovuta a una impropria validazione dell'input da parte della libreria, in particolare nell'estensione TLS heartbeat, che comporta un "buffer over-read" in grado di esporre la chiave crittografica del server. È descritto in CVE-2014-0160.
A23	HTML Injection	L'HTML injection è una tecnica utilizzata per sfruttare input non validati al

		fine di modificare una pagina web fornita da un'applicazione web ai propri utenti. Gli aggressori sfruttano il fatto che il contenuto di una pagina web è spesso legato ad una precedente interazione con gli utenti. Quando l'applicazione non riesce a convalidare i dati forniti dall'utente, un utente malintenzionato può inviare un testo HTML opportunamente modificato per alterare quei contenuti del sito che vengono poi presentati ad altri utenti. Una query creata ad-hoc può portare all'inserimento nella pagina web di elementi HTML controllati dall'attaccante che modificano il modo in cui il contenuto dell'applicazione viene esposto sul web.
A24	HTTP response splitting	Un attaccante passa dati “maliziosi” a una applicazione che non li valida e li include immutati in una HTTP Response Header. L’applicazione è vulnerabile se consente l’input di caratteri contenenti CR (carriage return, ovvero %0d o \r) ed LF (line feed, ovvero %0a o \n) nell’header http e se contemporaneamente la piattaforma su cui gira il sistema è a sua volta vulnerabile alla injection di tali caratteri. Con questo attacco l’aggressore ha la possibilità di controllare le successive http response dell’applicazione, incluse l’HEADER e il BODY, e inoltre di creare altre response a suo piacimento.
A25	Infezione da malware	Per compromissione di un sistema di elaborazione causata da un software malevolo, si intende il malfunzionamento di un sistema di elaborazione causato da software che esegue funzioni "nocive" (ad esempio, virus, worm, cavalli di Troia).
A26	Information gathering	Si indica con il termine "Information gathering" una tecnica mirata a individuare, identificare e caratterizzare i dispositivi di rete che possono essere scoperti e profilati. Ciò avviene attraverso la scansione delle porte. Dopo aver identificato le porte aperte, si rilevano i tipi di periferica e si determinano le versioni del sistema operativo e delle applicazioni. Con queste informazioni, un aggressore può successivamente attaccare le vulnerabilità note che potrebbero non essere state risolte con patch di protezione.
A27	Integer Overflow	Un integer overflow avviene quando un’operazione aritmetica cerca di calcolare un valore numerico che supera il range che può essere rappresentato con un dato numero di bit. In tal modo si ottiene un risultato imprevisto che può compromettere la stabilità e l’integrità dell’applicazione, laddove l’errore non sia intercettato e gestito.
A28	Keylogging	Un keylogger è uno strumento hardware o software in grado di effettuare lo sniffing della registrazione dei caratteri premuti sulla della tastiera di un computer, cioè è in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente si accorga di essere monitorato.
A29	KRACK	L’attacco Key Reinstallation AttaCK (KRACK), e un attacco di “replay” mirato allo standard Wi-Fi Protected Access protocol (WPA / WPA2), che si suppone metta in sicurezza le connessioni WiFi. L’attacco consiste nel resettare ripetutamente il “nonce” trasmesso in una specifica fase dell’handshake WPA2, consentendo di analizzare e decifrare gradualmente i pacchetti attraverso la comparazione con quelli precedenti, fino a ottenere la chiave crittografica utilizzata per cifrare il traffico. L’attacco sfrutta una vulnerabilità insita nello standard e non in specifici prodotti, e colpisce tutti i principali sistemi operativi compresi quelli usati

		da smartphone e tablet. Particolarmente grave è il fatto che sui sistemi linux-based, il client wpa-supplicant usato per connettersi alla rete WiFi con il WPA2 consente addirittura l'inserimento di una chiave "nulla".
A30	LDAP Injection	L'LDAP Injection è un tipo di attacco portato verso un'applicazione web dove gli hacker introducono del codice malevolo in un campo di input dell'interfaccia utente nel tentativo di ottenere accesso a informazioni non autorizzate. L'LDAP Injection utilizza i dati forniti nella richiesta proveniente dal client, nella costruzione di istruzioni LDAP (Lightweight Directory Access Protocol), quando questi non vengono controllati e validati al fine di rimuovere codice potenzialmente dannoso. Quando un'applicazione web non applica adeguati controlli sull'input fornito dall'utente, gli hacker possono essere in grado di modificare la costruzione di un'istruzione LDAP che verrà poi eseguita con le stesse autorizzazioni del componente destinato all'esecuzione del comando. Un LDAP Injection può causare seri problemi di protezione se le autorizzazioni consentono di interrogare, modificare o rimuovere qualsiasi oggetto presente all'interno dell'albero LDAP.
A31	Man-in-the-browser	È un attacco simile al man-in-the-middle, ma agisce all'interno del browser utente. Generalmente è basato su un "Trojan Horse" che si installa nel browser per intercettare e manipolare richieste e risposte http. Spesso questa tecnica è usata da malware mirati a specifici siti di Home Banking, in grado di rubare denaro modificando "al volo" le transazioni finanziarie (es. i bonifici). Il malware può insediarsi nei "Browser Helper Objects" di Internet Explorer (librerie caricate dinamicamente all'avvio del browser), nelle Estensioni dei browser più recenti o attraverso "API-Hooking" in un eseguibile o una libreria DLL, o ancora tramite Javascript (ad es. attraverso uno "worm" basato su Ajax).
A32	Man-in-the-middle	Questo attacco consiste nell'intercettare la comunicazione tra due sistemi ponendosi in mezzo e fingendo con ciascuno degli interlocutori di essere l'altro. Ad es. in una connessione http l'attaccante rompe la connessione originale in due parti: una connessione dal client a sé stesso (fingendosi il server) e una da sé stesso al server (fingendosi il client), inoltrando dopo averle intercettate ed eventualmente manipolate, le richieste del client al server e le risposte del server al client.
A33	Manipolazione dei campi di Form	I valori dei campi presenti in una form HTML vengono inviati in chiaro al server utilizzando il protocollo HTTP POST. Ciò può includere campi di form visibili e nascosti. Indipendentemente dalla tipologia, questi campi possono essere facilmente modificati ignorando le routine di convalida lato client. Di conseguenza, le applicazioni che si basano sui valori di input di un campo di una form per prendere decisioni di sicurezza lato server sono vulnerabili all'attacco in oggetto.
A34	Manipolazione dei Cookie	I cookie sono suscettibili a modifiche da parte del client. Ciò è vero sia per i cookie persistenti che per quelli che risiedono in memoria. Sono disponibili diversi strumenti per supportare un aggressore nella modifica del contenuto di un cookie residente in memoria. La manipolazione del cookie è l'attacco che si riferisce alla modifica di un cookie, si effettua di solito per

		ottenere un accesso non autorizzato ad un sito Web.
A35	Manipolazione della Query String	Gli utenti possono facilmente manipolare i valori della stringa di query passati tramite HTTP GET da client a server in quanto vengono visualizzati nella barra degli indirizzi URL del browser Web. Se l'applicazione si basa su valori della stringa di query per prendere decisioni di sicurezza o se i valori rappresentano dati sensibili o parametri critici di una transazione come importi monetari, l'applicazione è vulnerabile all'attacco in oggetto.
A36	Manipolazione dell'intestazione HTTP	Le headers HTTP passano le informazioni tra il client e il server. Il client costruisce le headers di richiesta mentre il server costruisce le headers di risposta. Se l'applicazione si basa sulle headers di richiesta per prendere una decisione, questa allora è vulnerabile all'attacco in oggetto.
A37	Memory dump attack	Un attacco di dump di memoria consiste nella cattura e nell'utilizzo di contenuti RAM che sono stati scritti su un'unità di memorizzazione durante un errore irreversibile (a scopo di diagnostica), tipicamente innescato dall'attaccante.
A38	Path Manipulation	Simile alla Resource Injection, salvo che si focalizza sul re-indirizzamento verso risorse di file system locali del server, forzandolo a caricare risorse diverse da quelle previste.
A39	Path traversal	Accesso alla struttura del file system non di pertinenza dell'applicativo web. Un aggressore avendo accesso alla gerarchia del file system (ad es. mediante la notazione "../") potrebbe prelevare informazioni riservate presenti all'interno della struttura di file e delle cartelle esterne all'applicazione.
A40	Pharming	Il phishing ed il pharming sono due tecniche utilizzate per ottenere l'accesso a informazioni personali o riservate. Nel primo caso un utente incauto viene indotto, tramite tecniche di social engineering, ad accedere ad un sito web contraffatto in modo tale da sembrare ufficiale ed a inserirvi dati personali e/o sensibili. Nel secondo caso, l'utente viene reindirizzato automaticamente, tramite alterazione delle richieste DNS (che possono coinvolgere direttamente il DNS server o la PdL vittima, tramite l'installazione di trojan) al sito web contraffatto, anche nel caso in cui digiti nel browser l'indirizzo corretto del server autentico.
A41	Phishing	Per "phishing" si intende un qualsiasi tentativo (per telefono, e-mail, messaggistica immediata o fax) di ottenere informazioni di identificazione personale a scopo di furto di identità. Un tipico attacco di phishing elettronico comprende due componenti: un messaggio e-mail dall'aspetto autentico e una pagina web fraudolenta. I collegamenti web inclusi in questi messaggi e-mail quasi sempre hanno l'aspetto e il funzionamento dei siti legittimi copiati, rendendo la frode quasi impossibile da rilevare.
A42	POODLE attack	Il POODLE (Padding Oracle On Downgraded Legacy Encryption) è una vulnerabilità che riguarda la sicurezza di una vecchia versione del protocollo SSL, la 3.0, che potrebbe essere sfruttata per intercettare i dati in transito fra client e server. La vulnerabilità, rivolta al lato client e non a quello server, potrebbe ad esempio consentire a un utente malintenzionato di decifrare i cookie che corrispondono a servizi come Twitter o Google, per entrare negli account degli utenti senza la necessità di conoscere la password di accesso. Il protocollo SSL 3.0, così come utilizzato in molti prodotti (es. OpenSSL 1.0.1i), usa un padding CBC non deterministico che consente a un attacco

		di tipo man-in-the-middle di decifrare facilmente i dati trasmessi utilizzando un attacco "padding-oracle". Il protocollo TLS (Transport Layer Security) ha largamente sostituito il protocollo SSL per la comunicazione sicura su Internet, ma molti browser tornano ad utilizzare SSL 3.0 quando non è disponibile una connessione TLS. Un aggressore che vuole sfruttare il POODLE approfitta di questa vulnerabilità inserendosi nella sessione di comunicazione e costringendo il browser a utilizzare SSL 3.0.
A43	Privilege horizontal escalation attack	Un attacco di "privilege escalation" è un tipo di intrusione di rete che sfrutta gli errori di programmazione o i difetti di progettazione per concedere all'attaccante un accesso privilegiato alla rete, ai dati e alle applicazioni ad essa associati. Nel caso di "horizontal esclation", per "accesso privilegiato" si intende un accesso nel quale un utente con certi privilegi accede alle funzioni e/o contenuti riservati a un altro utente che gode degli stessi privilegi.
A44	Privilege vertical escalation attack	Un attacco di "privilege escalation" è un tipo di intrusione di rete che sfrutta gli errori di programmazione o i difetti di progettazione per concedere all'attaccante un accesso privilegiato alla rete, ai dati e alle applicazioni ad essa associati. Nel caso di "vertical escalation", per "accesso privilegiato" si intende un accesso più alto di quello previsto dall'amministratore o dallo sviluppatore dell'applicazione.
A45	Proxy hijacking attack	Il "proxy hijacking" è una tecnica di attacco in cui il codice malevolo non installa un malware ma configura il browser presente sul sistema della macchina vittima per usare un web proxy controllato dall'attaccante stesso. Oltre a eseguire il deploy dei proxy settings fraudolenti, l'attacco installa un "self-signed root certificate" sul sistema in modo che l'attaccante possa leggere il traffico HTTPS che passa attraverso il proxy server fraudolento (man-in-the-middle MITM Attack). Tipicamente l'attacco parte da spam email con un attachment malevolo che esegue le operazioni di cui sopra.
A46	Remote File Inclusion (RFI)	Il "Remote File Inclusion (RFI)" è un attacco che punta ad un server di computer su cui sono in esecuzione siti e applicazioni web. Gli exploit RFI sono spesso attribuiti al linguaggio di programmazione PHP utilizzato da molte grandi aziende, tra cui Facebook e SugarCRM. Tuttavia, l'RFI può manifestarsi in altri ambienti ed è stato infatti introdotto inizialmente come "SHTML injection". RFI funziona sfruttando applicazioni che dinamicamente fanno riferimento a script esterni indicati da input dell'utente, senza adeguati controlli. Di conseguenza, l'applicazione può essere istruita per includere uno script ospitato su un server remoto e quindi eseguire codice controllato da un utente malintenzionato. Gli script eseguiti possono essere utilizzati per il furto temporaneo o l'accesso non autorizzato ai dati, la loro manipolazione o anche la loro sottrazione, per una acquisizione dati a lungo termine.
A47	Resource Injection	Questo attacco consiste nel modificare il tipo o l'identificatore di una risorsa usato da un'applicazione, attraverso un input non validato, i cui caratteri vengono usati dall'applicazione vulnerabile per determinare la risorsa da accedere (es. un nome file su uno share remoto, una porta TCP/IP, una URL, ecc.). In tal modo l'attaccante forza il server a caricare una risorsa arbitraria dalla rete, potenzialmente contenente codice dannoso, che in alcuni casi può essere persino memorizzato sul server ed essere inviato ad altri utenti.

A48	SEO poisoning attack	Il "SEO poisoning", noto anche come "search poisoning", è un metodo di attacco in cui i cyber criminali creano siti web dannosi e utilizzano tattiche di ottimizzazione dei motori di ricerca per renderli prominenti nei risultati della ricerca. Tali siti vengono associati a termini presumibilmente utilizzati nella ricerca da un numero elevato di persone in un dato momento, ad esempio frasi correlate a festività, news e video virali. Secondo i Websense Security Labs, in questi casi, fino ad un quarto della prima pagina dei risultati della ricerca, questi possono essere collegati a siti web dannosi. Gli aggressori creano siti web con nomi e descrizioni associate a temi popolari o ad argomenti di tendenza. Ad esempio, nelle settimane precedenti a Halloween, gli aggressori potrebbero attivare siti che offrono modelli gratuiti per i costumi di Halloween. Tuttavia, il vero scopo è quello di infettare i visitatori con malware o accedere in modo fraudolento a informazioni sensibili da utilizzare poi per il furto di identità.
A49	Sfruttamento delle sessioni	Ogni applicazione web che si avvale di un meccanismo di login di autenticazione, basato sul logon gestisce delle sessioni con le quali tracciare l'utente, che si attua con l'assegnazione di un token (ad es. un cookie, un parametro di sessione) univoco. L'attacco si perpetra dopo aver determinato il funzionamento dell'algoritmo di generazione del token e, in genere, comporta la sostituzione di identità, dando all'aggressore l'opportunità di accedere all'applicazione web poiché da essa ritenuto un utente accreditato.
A50	Shellcode	Uno shellcode è un programma in linguaggio assembly che tradizionalmente esegue una shell, come la shell Unix '/bin/sh' oppure la shell "command.com" sui sistemi operativi DOS e Microsoft Windows. Uno shellcode può essere utilizzato per sfruttare un bug mediante un exploit, consentendo ad un hacker o un cracker di acquisire l'accesso alla riga di comando di un computer, o più in generale di eseguire codice arbitrario.
A51	Spam	Il termine "spam" descrive una comunicazione non sollecitata (inviata per e-mail o messaggi/chat immediata) e destinata al lucro commerciale. Il termine spam comprende un'ampia gamma di attività, molte delle quali sono dannose (come la distribuzione di e-mail di phishing). Una variante di tale attacco è lo spam per immagini (spam in cui il messaggio è testo sotto forma di immagine, anziché testo effettivo) come mezzo usato per evadere il rilevamento.
A52	Spim (Instant Messaging Spam)	Lo Spim è una forma di spam distribuito tramite messaggistica istantanea (IM) anziché tramite messaggistica di posta elettronica. Anche se meno diffuso rispetto alla sua controparte di posta elettronica, lo Spim sta raggiungendo sempre più utenti. l'IM è un canale particolarmente adatto per gli spammer. Per prima cosa, l'immediatezza nello scambio di messaggi fornita dall'IM rende probabilmente gli utenti meno riflessivi nel cliccare sui link. Inoltre, con il fatto che l'IM bypassa il software antivirus e i firewall, questo rappresenta un mezzo facile per passare non solo messaggi commerciali, ma anche virus e altri malware.
A53	SQL injection	"SQL injection" è una tecnica di hacking che mira a colpire le applicazioni web connesse ad un database di tipo SQL. Tale attacco sfrutta l'inefficienza dei controlli sui dati ricevuti in input ed inserisce codice maligno all'interno di una query SQL. La tecnica permette al malintenzionato di autenticarsi con ampi privilegi in aree protette dell'applicazione e di visualizzare e/o alterare dati sensibili.
A54	Stack overflow	Lo stack overflow si verifica quando il puntatore di stack di chiamata,

		supera lo spazio di memoria associato allo stack. Lo stack delle chiamate può occupare uno spazio di memoria di dimensioni ridotte, in genere questa spesso viene determinata all'avvio del programma. La dimensione dello stack di chiamata dipende da molti fattori, tra cui il linguaggio di programmazione, l'architettura della macchina, il multi-threading e la quantità di memoria disponibile. Quando un programma tenta di utilizzare più spazio di quanto non sia disponibile nello stack di chiamata (ovvero quando tenta di accedere alla memoria oltre i limiti dello stack di chiamata, che è essenzialmente un buffer overflow), si parla di overflow dello stack, che porta al crash del programma. Questo si verifica in genere in caso di errori di programmazione quali la ricorsione infinita o l'uso di variabili di stack troppo grandi.
A55	XPath Injection	XPath è un linguaggio di query che consente di accedere a qualsiasi parte di un documento XML senza alcuna restrizione nel controllo di accesso (chi può accedere a cosa). Con un attacco di XPATH Injection, un malintenzionato può modificare una query XPATH per eseguire un'azione differente da quella prevista. La XPath Injection può essere usata per estrarre da un'applicazione, dati forniti dagli utenti, memorizzati in modo non sicuro. Questo può avvenire se l'applicazione non valida correttamente l'input usato per comporre una query XPATH.
A56	Zero-day exploit	Un exploit "zero-day" consiste nello sfruttamento di una vulnerabilità di sicurezza nello stesso giorno in cui questa generalmente diventa nota. Ci sono zero giorni tra il momento della scoperta della vulnerabilità e il primo attacco. Normalmente, quando qualcuno rileva che un programma software contiene un potenziale problema di sicurezza, la persona o l'azienda notificano il problema riscontrato alla società che ha realizzato il software (e talvolta al mondo in generale) in modo da poter intraprendere azioni di correzione. Passa del tempo prima che, la società che ha realizzato il software, possa correggere il codice e distribuire una patch o un aggiornamento software. Anche se potenziali aggressori sono a conoscenza della vulnerabilità, potrebbe essere necessario un certo tempo per poterla sfruttare a loro vantaggio. Nel frattempo, si spera che la soluzione di correzione sia disponibile prima che ciò avvenga.