A3 – Sensitive Data Exposure	C10 - Handle All Errors and Exceptions	V8 - Error Handling and Logging
A6 – Security Missconfiguration	C10 - Handle All Errors and Exceptions	V19 - Configuration

Tabella 16 - Rischi di sicurezza OWASP relativi all'Information Disclosure

Alcuni esempi di minacce di information disclosure:

- Banner Grabbing/ricognizione attiva: Il Banner grabbing o ricognizione attiva è un tipo di attacco durante il quale gli aggressori inviano richieste al sistema che stanno tentando di attaccare per raccogliere maggiori informazioni riguardo il sistema stesso. Se il sistema non è ben configurato, può rivelare informazioni su se stesso, come la versione del server, la versione PHP/ASP.NET, la versione OpenSSH, ecc. Nella maggior parte dei casi, il banner grabbing non si traduce in una fuga di informazioni sensibili, ma piuttosto di informazioni che possono essere di aiuto per l'aggressore nella fase di sfruttamento dell'attacco. Ad esempio, se dal sistema target trapela la versione del PHP in esecuzione sul server, e tale versione risulta vulnerabile al Remote Command/Code Execution (RCE) in quanto non aggiornato, gli aggressori possono sfruttare la vulnerabilità nota e prendere il pieno controllo dell'applicazione web.
- Divulgazione del codice sorgente: I problemi di divulgazione del codice sorgente si verificano quando il codice dell'ambiente di backend di un'applicazione web viene pubblicamente esposto. La divulgazione del codice sorgente consente agli aggressori di comprendere come è fatta l'applicazione e come questa si comporta, semplicemente leggendo il codice e verificando le difettosità presenti nella logica applicativa, o rilevando le coppie username/password o le chiavi riservate delle API scolpite nel codice. La severità riguardo la sicurezza dell'applicazione web quindi dipende dal livello di esposizione del codice e dal livello di riservatezza delle linee di codice in esso contenute e divulgate. In breve, la divulgazione del codice sorgente trasforma un processo di penetration test black box in un approccio white box, dato che l'aggressore ha accesso al codice sorgente. Le problematiche di divulgazione del codice sorgente possono verificarsi in numerosi modi, di seguito se ne elencano alcuni:
  - **Repository di codice pubblico non protetto**: Numerose organizzazioni spesso ospitano il loro codice sorgente nel cloud per migliorare i metodi di sviluppo collaborativo. Tali repository a volte non vengono ben protetti e possono consentire agli aggressori di accedere al codice sorgente e alle informazioni in esso presenti. Inoltre, alcune organizzazioni che sviluppano software open source utilizzano repository pubblici in modo che chiunque possa contribuire allo sviluppo del progetto. In tal caso il codice sorgente è già pubblico, ma non è raro che il codice sorgente pubblicamente disponibile contiene informazioni sensibili.
  - **MIME Types non corretti**: I browser web sanno come analizzare le informazioni che ricevono dall'intestazione HTTP Content-Type, che viene inviata dal server web nella risposta HTTP. Per esempio se l'intestazione Content-Type è impostata su text/html, il browser analizzerà l'HTML e mostrerà il relativo output. Anche se il server web non è correttamente configurato, e ad esempio serve una pagina HTML inviando l'intestazione Content-Type: text/plain invece di Content-Type: text/html, tale pagina sarà resa come testo semplice nel browser web, permettendo all'attaccante di vedere il codice sorgente della pagina stessa.
- Trattamento inadeguato dei dati sensibili: Un altro errore comune è l'hardcoding di informazioni riservate o sensibili come le coppie username/password, gli indirizzi IP interni presenti negli script e i commenti nel codice e nelle pagine web. Nella maggior parte dei casi tali informazioni vengono lasciate all'interno dell'applicazione web di produzione. La divulgazione di tali informazioni può avere esiti devastanti per l'applicazione stessa; l'aggressore deve solo cercare queste informazioni nella fonte delle pagine (ad esempio, facendo un clic destro sulla pagina e selezionando "Visualizza fonte pagina", da non confondere con "Codice sorgente").
- Divulgazione di Nomi di file e di percorso: In alcune circostanze le applicazioni web possono rivelare nomi di file o percorsi di directory, divulgando così informazioni sulla struttura del sistema

sottostante. Questo può accadere a causa di un'errata gestione dell'input dell'utente, di eccezioni nel backend o di una configurazione inappropriata del server web. A volte tali informazioni possono essere individuate o identificate nell'output delle applicazioni web, pagine di errore, informazioni di debug, e quant'altro. Un esempio di divulgazione di nome di file e di percorso si ha quando a partire da un semplice test un attaccante può verificare se l'applicazione web rivela nomi di file o percorsi inviando un certo numero di richieste distinte che, a suo avviso, il server potrebbe gestire in modo diverso. Per esempio, quando si invia una richiesta del tipo che segue, l'applicazione web restituisce una risposta 403 (accesso negato):

https://www.esempio.org/%5C../etc/passwd

Ma quando l'attaccante invia la seguente richiesta, ottiene una risposta 404 (pagina non trovata):

https://www.esempio.org/%5C../etc/fake

Poiché per la prima richiesta l'attaccante ha ottenuto un errore 403 "accesso negato" e per la seconda un 404 "pagina non trovata", questo sa che nel primo caso il file in questione esiste. L'aggressore può quindi utilizzare a suo vantaggio il comportamento dell'applicazione web, come exploit per comprendere come è strutturato il server e per verificare se nel sistema esiste una certa directory o file. Un altro caso in cui il sistema è soggetto a divulgazione di informazioni riguardo gli elementi del file-system sottostante è rappresentato dal cosiddetto "Directory Listing" ovvero l'elenco delle directory e dei file presenti nel server web. Questa funzionalità viene normalmente fornita di default sui server web. Quando non viene definita una pagina web predefinita per il server web, nel momento in cui si tenta di accedere al server tramite una richiesta http, questo restituisce all'utente un elenco di file e directory presenti sul sito web. Quindi se il nome file predefinito su un server web Apache è index.php, e questo non è presente nella directory principale del sito web, il server mostrerà l'elenco di directory presenti nella directory principale invece di mostrare l'output del file php. Lasciare tale funzionalità abilitata negli ambienti di produzione è una cattiva pratica e può portare a numerosi problemi di sicurezza.

5.5.4.1.1.5 Indirizzamento del denial of service

La Tabella seguente mostra in elenco gli obiettivi del Denial Of Service, le strategie di mitigazione per indirizzare il Denial Of Service e le tecniche per attuare tali mitigazioni:

OBIETTIVO DELLA MINACCIA	STRATEGIA DI MITIGAZIONE	TECNICA DI MITIGAZIONE
Saturazione della rete (Network flooding)	Verificare le risorse esauribili	• Risorse flessibili (Elastic resources); • Progettare pensando che il consumo di risorse da parte di un futuro utilizzatore malintenzionato possa essere alto o comunque superiore a quello presunto.
		ACLs di rete.
Risorse utilizzate da un programma	Progettazione attenta e cautelativa	Gestione delle risorse flessibili.
	Evitare fattori moltiplicativi	Analizzare i punti in cui un eventuale attacco portato con uno sforzo minimo, potrebbe produrre una moltiplicazione nel consumo di CPU. Intervenire in modo tale da rendere maggiormente