A8 - Insecure Deserialization	C5 – Validate All Inputs	V5 - Malicious Input Handling
	C4 – Encode and Escape Data	V5 - Malicious Input Handling

Tabella 12 - Rischi di sicurezza OWASP relativi al Tampering

Esempi di minacce di Tampering:

- Manomissione dei Cookie: I cookie vengono utilizzati come meccanismo per memorizzare informazioni di dettaglio e preferenze dell'utente nonché altri dati, come i token di sessione. I cookie di tipo persistente e non, sicuri o non, possono essere manomessi dall'utente e inviati al server tramite richieste di Uniform Resource Locator, pertanto qualsiasi utente o hacker malintenzionato può modificare il contenuto dei cookie a suo vantaggio consentendo a se stesso di accedere ai file desiderati.
- Manomissione dei campi di Form HTML: Quando un utente effettua selezioni o modifiche su una pagina web o HTML, la selezione viene memorizzata come valore di un campo del form, che viene poi inviato all'applicazione attraverso una richiesta HTTP. L'HTML solitamente memorizza tali valori come campi nascosti (Hidden Fields), che non vengono mostrati sullo schermo dell'utente, ma vengono raccolti e inviati come stringhe o parametri durante la trasmissione del form. Se tali campi possono essere nascosti, preselezionati o liberi, possono anche essere manomessi o manipolati dall'hacker per inviare valori a sua scelta.
- Manomissione della stringa di Query URL: La manomissione degli URL comporta tutta una serie di problemi legati alla presenza di campi nascosti nei Form. Per sottomettere i dati all'applicazione viene utilizzato uno dei due metodi usati dai form HTML, POST o GET. Di solito viene usato il metodo GET, il quale mostra tutti i nomi degli elementi dei form e i relativi valori nella stringa di query dell'URL che l'hacker è in grado di vedere. Gli hacker trovano più facile manomettere le stringhe di query che manomettere i campi nascosti del form. Tutto quello che l'hacker deve fare è guardare l'URL presente nella barra degli indirizzi dell'utente. Ad esempio, una pagina web potrebbe consentire all'utente autenticato di selezionare uno dei suoi account pre-caricati da un campo con valori multipli e di addebitare all'account selezionato un importo unitario fisso. La scelta viene registrata premendo un pulsante di invio. La pagina memorizza effettivamente i valori scelti nei relativi campi del form e invia tali valori all'applicazione utilizzando un comando di submit del form. Tale comando sottomette la seguente richiesta HTTP: http://www.vittima.org/esempio?numeroconto=12345&addebito=1, ora tutto ciò che l'hacker deve fare è costruire il proprio numero di conto e modificare i parametri come segue: http://www.vittima.org/esempio?numeroconto=98760&addebito=100000000.
- Password Cracking: Un password cracker è un programma applicativo che viene utilizzato per supportare un hacker o un utente malintenzionato a identificare una password sconosciuta di accesso a un computer o a un dispositivo di rete con il fine di ottenere o consentire l'accesso non autorizzato alle sue risorse. L'hacker tenterebbe di ottenere le credenziali valide dal sistema di autenticazione attraverso un numero elevato di tentativi di autenticazione con password diverse ripetuti nel tempo. Il programma di Password cracking utilizza principalmente due metodi per cercare o identificare le password valide, che sono: la "forza bruta" e le "ricerche basate su dizionario". Quando il programma utilizza la "forza bruta", questo sottomette al sistema di autenticazione diverse combinazioni di tutti i tipi di caratteri con una lunghezza predeterminata fino a quando non viene identifica la combinazione corretta per il sistema informatico. Quando invece utilizza la "ricerca basata su dizionario", il programma applicativo utilizza ogni parola presente nel dizionario alla ricerca della password che il sistema informatico riconosce come valida.
- Manomissione dell'intestazione HTTP: Le intestazioni HTTP vengono utilizzate dal software del server web e dal client. Nella maggior parte delle applicazioni web tali intestazioni non vengono usate. Alcuni sviluppatori web scelgono di monitorare le intestazioni in entrata ed è importante notare che le intestazioni di richiesta provengono originariamente dal client, e come tali potrebbero essere manipolate da un potenziale aggressore. Normalmente le applicazioni web non consentono l'alterazione o la modifica delle intestazioni HTTP. Un hacker dovrà dunque scrivere il proprio