OWASP TOP-10 2017 (Rischi di sicurezza delle applicazioni)	OWASP Proactive Controls 2018 v 3.0 (Pratiche di sicurezza proattive)	OWASP ASVS 3.0 (Requisiti di sicurezza applicativa)
A2 – Broken Authentication	C6 – Implementing Digital Identity	V2 - Authentication
		V3 - Session Management

Tabella 10 - Rischi di sicurezza OWASP relativi allo Spoofing

Esempi di minacce di spoofing:

- ARP Spoofing: Un attacco di spoofing ARP è un attacco che utilizza il protocollo di risoluzione degli indirizzi per catturare informazioni. In un attacco ARP spoofing l'aggressore invia messaggi ARP attraverso una rete nel tentativo di collegare il proprio indirizzo MAC con un indirizzo IP target. L'aggressore rimane in attesa sulla rete finché non riesce a violare l'indirizzo IP. Una volta che l'indirizzo IP è stato violato, l'aggressore può intercettare i dati in transito tra il computer relativo all'IP violato e il router. I dati inviati al target vengono quindi inviati all'indirizzo IP dell'aggressore. Il risultato finale è che i dati destinati al legittimo destinatario arrivano nelle mani dell'aggressore. L'aggressore può quindi utilizzare gli indirizzi IP della rete per lanciare un attacco DOS denial-of-service. Una cosa molto importante da tener presente sugli attacchi di ARP spoofing è che questi possono funzionare solo su LAN che utilizzano il protocollo ARP.
- IP Spoofing: Un attacco di IP spoofing si ha quando un aggressore tenta di impersonare un indirizzo IP in modo da poter fingere di essere un altro utente. Durante un attacco di spoofing dell'indirizzo IP, l'aggressore invia pacchetti da un falso indirizzo di origine.
- DNS Spoofing: Gli attacchi DNS o dei nomi di dominio di sistema sono quelli in cui gli aggressori confondono l'elenco degli indirizzi IP pubblici o dei nomi corrispondenti. I server DNS dispongono di un database di indirizzi IP pubblici e hostname che vengono utilizzati per facilitare la navigazione in rete. Quando si verifica un attacco DNS, l'aggressore modifica i nomi di dominio in modo che vengano reindirizzati a un nuovo indirizzo IP. Un esempio di ciò si ha quando s'inserisce un URL di un sito Web e si viene re diretti verso un dominio spoofed piuttosto che verso il sito Web atteso. Ciò rappresenta un mezzo comune per gli aggressori per diffondere worm e virus nelle reti.
- Email Spoofing: Gli attacchi di spoofing delle e-mail sono quelli in cui un attaccante invia un'e-mail emulando un altro mittente. In questi attacchi, il campo mittente viene alterato per mostrare dettagli falsificati di contatto. L'aggressore impersonifica il mittente scelto e poi invia un'e-mail con una richiesta di informazioni. Questi attacchi vengono spesso impiegati per spacciarsi come amministratori e chiedere agli altri membri dell'organizzazione dettagli sui propri account.

5.5.4.1.1.2 Indirizzamento del Tampering

La Tabella seguente mostra in elenco gli obiettivi di tampering, le strategie di mitigazione per indirizzare il tampering e le tecniche per attuare tali mitigazioni.

OBIETTIVO DELLA MINACCIA	STRATEGIA DI MITIGAZIONE	TECNICA DI MITIGAZIONE
Tampering di un file	Sfruttare le funzionalità messe a disposizione dal Sistema Operativo	ACLs.
	Crittografia	• Firme digitali; • Keyed MAC.
Concorrenza nella creazione di un file (tampering del file system)	Utilizzo di una directory protetta da manipolazione arbitraria di un utente	• ACLs; • Utilizzo di strutture private di directory;