Esempio:
In alcuni casi è possibile modificare l'url di un'applicazione web per accedere direttamente alle diectory del server nel quale è deployata (directory listing). Occorre disabilitare, a livello di application server, l'opzione di browsing delle directory.

Current Directory /pub/mirrors/perl/CPAN

```
The Comprehensive Perl Archive Network (http://www.cpan.org/)
master site has been from the very beginning (1995) hosted at FUNET,
the Finnish University NETwork.

Directory successfully changed.
```

```
[DIR] Parent Directory
[DIR] CPAN.html -> authors/id/J/JO/JONO/cpan.html          Feb 04 2010   Symbolic link
[FILE] ENDINGS                                3 KB     Mar 19 2017
[FILE] MIRRORED.BY                          124 KB     Nov 17 10:14
[FILE] MIRRORING.FROM                       335 bytes  Nov 24 14:10
[FILE] README                                 1 KB     Feb 13 1999
[DIR] README.html -> index.html                        Feb 04 2010   Symbolic link
[DIR] RECENT -> indices/RECENT-print                   Nov 24 08:34  Symbolic link
[FILE] RECENT-1M.json                         2 MB     Nov 24 02:05
[FILE] RECENT-1Q.json                         4 MB     Nov 19 00:47
[FILE] RECENT-1W.json                       310 KB     Nov 24 14:14
[FILE] RECENT-1Y.json                        15 MB     Nov 19 00:47
[FILE] RECENT-1d.json                        92 KB     Nov 24 14:14
```

In altri casi vengono sfruttate vulnerabilità connesse con le directory accessibili dall'esterno (path traversal): www.example.com/lmapp/../../../etc/hosts

In altri casi ancora le regole per il cambio password non sono sicure: ad esempio non viene richiesto l'inserimento della vecchia password o vengono poste domande di sicurezza le cui risposte sono intuitive o ricavabili attraverso il social engeenering.

Contromisure

È necessario:

- verificare i dati in input (filtrando i caratteri ".." e "/") per evitare i problemi del path traversal e disabilitare nell'application server il directory listing.
- garantire la robustezza delle password, seguendo regole precise sulla lunghezza, sulla complessità e sulla durata. Le password devono essere lunghe almeno otto caratteri e contenere lettere minuscole e maiuscole, numeri e simboli non alfanumerici; devono scadere a intervalli regolari, non devono essere inutitive, né devono essere simili alle ultime dodici inserite.

6.3 Crittografia

La crittografia rappresenta oggi uno degli strumenti più proficui per sviluppare applicazioni software sicure, capaci di rispondere alle necessità crescenti di preservazione dell'integrità e della riservatezza dei dati, sia in transito sia a riposo. Di seguito vengono riportare le tecniche più comunemente utilizzate dagli aggressori per appropriarsi in modo fraudolento d'informazioni private, invertendo il loro processo di cifratura e le vulnerabilità più comuni che permettono il verificarsi di tali condizioni.
Di seguito sono descritte le principali cause e vulnerabilità inerenti problematiche di crittografia.

6.3.1 Sniffing e algoritmi crittografici deboli

Uno dei principali motivi addotti a favore dell'uso della crittografia è quello di preservare la riservatezza dei dati che vengono scambiati in rete. Le applicazioni che non implementano alcun meccanismo crittografico sono le più esposte a tecniche di sniffing, il processo di monitoraggio e acquisizione di tutti i pacchetti di dati che attraversano una determinata rete. L'aggressore che riesce ad attestarsi in un punto qualsiasi fra i