l'attaccante riesce a manomettere il comportamento del programma che andrà quindi a scrivere nel file sbagliato.

Contromisure

La gestione della concorrenza fra diversi processi all'interno della stessa applicazione è una questione piuttosto delicata. Massima cura deve essere prestata, in fase di progettazione, al problema della competizione fra diversi thread per le stesse risorse. Non c'è una regola universale, ma i vari linguaggi di programmazione offrono diversi strumenti per la gestione di questo specifico aspetto.
La sincronizzazione di metodi e classi o l'uso di semafori sono di solito i rimedi adottati per prevenire questo problema.

6.4.6 Privilege Escalation e aggiramento dei permessi utente

Le eccezioni e le condizioni non previste o mal gestite sono sfruttate molto spesso dagli aggressori per ottenere un innalzamento dei privilegi (privilege escalation), ovvero la possibilità di svolgere operazioni sul sistema o sulla stessa applicazione con privilegi superiori rispetto a quelli posseduti prima dell'attacco. Ad esempio, sfruttando con successo uno Stack Overflow, l'aggressore che da remoto poteva unicamente godere dei privilegi di un utente anonimo o di basso profilo, può successivamente operare nel sistema come se fosse un utente locale a cui sono stati assegnati permessi amministrativi. Analogamente sfruttando una situazione di race condition, l'aggressore può modificare un file pur non possedendo come utenza originaria gli effettivi privilegi di scrittura. Nel caso di un Directory Listing può invece accedere ad aree riservate di un portale ancor prima di autenticarsi, bypassando il meccanismo con il quale l'applicazione assegna i permessi agli utenti regolari.
Le motivazioni che rendono solitamente possibile un Privilege Escalation sono menzionate di seguito:

- l'applicazione, il servizio o il singolo componente vengono avviati con i privilegi amministrativi;
- L'applicazione utilizza privilegi amministrativi anche quando svolge azioni per conto di un'utenza non privilegiata;
- Nei sistemi Unix o derivati il bit Set-User-ID è attivo.

Una privilege escalation non si definisce tale solo quando l'innalzamento dei privilegi riguarda direttamente il passaggio da un'utenza non privilegiata a una privilegiata, ma anche quando lo scambio di permessi avviene tra utenze non privilegiate.

Esempio:
Attraverso la tecnica del path traversal, l'attaccante è in grado di individuare le pagine che consentono l'accesso senza autenticazione:

```
/../.././userProfiles.html
```

Contromisure

È necessario progettare l'applicazione in modo tale da impedire che informazioni utili all'attacco possano essere svelate in caso di errore o di un'eventualità non gestita.

6.5 Bound checking e problematiche di overflow

Le problematiche di Overflow si verificano solitamente quando i dati provenienti da input utente, senza prima essere adeguatamente verificati, vengono memorizzati all'interno di buffer non abbastanza grandi per contenerli. Ciò è all'origine di differenti conseguenze, a seconda delle regioni di memoria in cui l'overflow si è manifestato e delle aree sovrascritte. In alcuni casi, l'aggressore può sfruttare l'area di memoria sovrascritta per eseguire comandi remoti finalizzati all'apertura di un canale di accesso al sistema vulnerabile. Altre volte viene semplicemente generato un crash dell'applicazione o del sistema, con conseguente interruzione nell'erogazione del servizio (DoS).