6.2.1.2 Token di sessione

Un token è un identificativo che correla univocamente una sessione a un utente. Tale valore, una volta generato, viene collocato all'interno del cookie o propagato attraverso l'URL affinché l'applicazione riconosca con esattezza l'utenza e determini, in base ai suoi privilegi, le azioni che può svolgere sul portale. Un aggressore può appropriarsi di un token di sessione in almeno tre modi:

- Creandolo sul momento (ad esempio quando il meccanismo di generazione del token è banale, non si basa su valori randomici ed è facilmente ricostruibile a partire dal nome dell'utente).
- Forzando l'utente a rivelarlo con un copia e incolla dell'URL, se propagato con questa modalità. Spesso vengono utilizzate tecniche di Social Engineering, allo scopo.
- Indovinandolo attraverso tecniche di Brute Forcing. Ciò è possibile quando l'identificativo della sessione viene generato con valori non randomici o utilizzando una bassa entropia.

Esempio:
Un token, come quello che segue, può essere facilmente intercettato e analizzato:

```
"result":[
{
        "_id":"B663D248CE4C3B63A7422000B03B8F5E0F8E443B",
        "_rev":"",
        "token_id":"B663D248CE4C3B63A7422000B03B8F5E0F8E443B",
        "sts_id":"username-transformer",
        "principal_name":"demo",
        "token_type":"OPENIDCONNECT",
        "expiration_time":1459376096
}]
```

Contromisure

Una buona soluzione è di utilizzare la tecnologia JWT (JSON Web Token), per cui le informazioni vengono firmate in maniera digitale. Il token non viene memorizzato né nella sessione, né nel database, né altrove.
Un'altra tecnica si avvale del meccanismo conosciuto con l'acronimo OTP (One Time Password): il token è valido se attivato da una password temporanea, rilasciata in tempo reale, in concomitanza con l'operazione che s'intende effettuare.

6.2.1.3 Accesso ad aree non autorizzate

Un aggressore può in talune circostanze disinteressarsi dei cookie o dei token quando è in grado di aprire una nuova sessione con i privilegi dell'utente desiderato nei modi seguenti:

- bypassando il normale meccanismo di autenticazione dell'applicazione: l'aggressore può sfruttare problematiche di Directory Listing o Directory Traversal per accedere ad aree dell'applicazione che dovrebbero essere visibili solo previa autenticazione;
- facendo leva su alcuni errori logici dell'applicazione per ottenere la password corrente o sollecitarne un cambio. Questo caso si manifesta solitamente quando:
- la procedura di reset della password dell'applicazione fallisce nell'inviare la password al corretto utente o permette all'aggressore di cambiare impropriamente la casella e-mail alla quale la stessa viene trasmessa;
- la password è facilmente determinabile a partire dalla risposta che può essere fornita alla domanda posta per ricordarla (nel caso in cui sia questo il meccanismo di recupero adottato);
- le password di accesso possono essere recuperate in forma cifrata o in chiaro dal filesystem o dal database sfruttando problematiche di Directory Listing, Directory Traversal, SQL Injection, etc;
- con un attacco di brute forcing per ottenere la password direttamente dalla form di autenticazione dell'applicazione: l'aggressore può, di proposito o involontariamente, determinare il blocco dell'account utente a causa dei meccanismi di lock-out che potrebbero scattare quando l'applicazione rileva un certo numero di tentativi di login falliti. Questo genere di interventi è classificabile nella categoria degli attacchi DoS.