- Scoprire la password dell'account di sistema nel database (tramite un brute-force attack).

Per comunicare con il proprio database o con un altro server (ad esempio Active Directory), l'applicazione costruisce dinamicamente una sua stringa di connessione. Questa stringa di connessione viene costruita dinamicamente con l'input inserito dall'utente per l'autenticazione stessa. Se i valori immessi sono stati verificati in misura insufficiente o non sono stati affatto verificati, la stringa di connessione potrebbe essere manipolata ad arte a vantaggio dell'attaccante.

Come difendersi

Validare tutti gli input, indipendentemente dalla loro provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati che adottano una struttura specificata nella white list, scartando quelli che non la rispettano). In generale, è necessario controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
Evitare di costruire dinamicamente stringhe di connessione. Se è necessario creare dinamicamente una stringa di connessione evitare di includere l'input dell'utente. In ogni caso, utilizzare utilità basate sulla piattaforma per validarlo.

Esempio:
Forma non corretta: L'applicazione crea una stringa di connessione usando l'input dell'utente:

```
from sys import stdin
import cx_Oracle
print 'Insert your ID: '
userInput = stdin.readline()
connection = cx_Oracle.connect(userInput + '/password@99.999.9.99:PORT/SID')
```

L'input deve essere validato prima di utilizzarlo all'interno della costruzione di una stringa di connessione. Se si riesce a fare a meno dell'input utente per questo scopo è ancora meglio.

Per ulteriori informazioni si veda: http://cwe.mitre.org/data/definitions/99.html,
CWE-99: Improper Control of Resource Identifiers ('Resource Injection').

7.5.5 LDAP Injection

Come riconoscerla

Si verifica quando l'applicazione comopne dinamicamente query LDAP utilizzando l'input utente, senza preventivamente verificarlo e validarlo.
Un attacco del genere permette:

- il login con un'utenza diversa (spoofing);
- l'acquisizione di privilegi di sistema (escalation of privileges);
- Il furto di informazioni.

Per comunicare con il proprio servizio di directory (ad esempio Active Directory), l'applicazione costruisce dinamicamente una stringa di connessione, includendo valori inseriti dall'utente in fase di autenticazione. Se i valori immessi dall'utente non sono stati verificati, né tantomeno sanificati, l'input potrebbe essere utilizzato per manipolare ad arte la stringa di connessione.

Come difendersi

Validare tutti gli input, indipendentemente dalla provenienza. Per la validazione, si consiglia l'approccio white list (sono accettati solo i dati specificati nella white list, scartando quelli che non la rispettano). Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).

Per ulteriori informazioni si veda: http://cwe.mitre.org/data/definitions/90.html,
CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection').