Testing for Host Header Injection (Ana Bilgisayar Başlığı Enjeksiyonu Testi)

Summary (Özet)

Bir web sunucusu genellikle aynı IP adresinde birkaç web uygulamasına ev sahipliği yapar ve her uygulamaya sanal ana bilgisayar aracılığıyla atıfta bulunur. Gelen bir HTTP talebinde, web sunucuları genellikle Host başlığında sağlanan değere bağlı olarak hedef sanal ana bilgisayara
talebi gönderir. Başlık değerinin uygun şekilde doğrulanması olmadan, saldırgan web sunucusuna neden olmak için geçersiz giriş sağlayabilir:

- Listedeki ilk sanal ev sahibine talepler gönderin
- Saldırgan kontrollü bir alana yönlendirmeye neden olur
- Web önbelleği zehirlenmesini gerçekleştirin
- Şifre sıfırlama işlevselliğini manipüle edin

Test Objectives (Test Hedefleri)

- Host başlığının uygulamada dinamik olarak ayrıştırılıp ayrıştırılmadığını değerlendirin.
- Başlıka dayanan güvenlik kontrollerini atlayın.

How To Test (Nasıl Test Edilir)

İlk test, başka bir alan adı sağlamak kadar basittir (yani. `attacker.com`) Host başlığı alanına. Web sunucusunun etkiyi belirleyen başlık değerini nasıl işlediğidir. Saldırı, web sunucusu, talebi sağlanan etki alanında bulunan saldırgan kontrollü bir ana bilgisayara göndermek için girişi
işlerken ve web sunucusunda bulunan dahili bir sanal ana bilgisayara değil geçerlidir.

```
GET / HTTP/1.1
Host: www.attacker.com
[...]
```

En basit durumda, bu, tedarik edilen alana 302 yönlendirmeye neden olabilir.

```
HTTP/1.1 302 Found
[...]
Location: http://www.attacker.com/login.php
```

Alternatif olarak, web sunucusu isteği listedeki ilk sanal ana bilgisayara gönderebilir.

X-Forwarded Host Header Bypass (X-İleri Ev Sahibi Başlık Bypass)

Host başlığı enjeksiyonunun, Host başlığı aracılığıyla enjekte edilen geçersiz girdiyi kontrol ederek hafifletilmesi durumunda, değeri ona sağlayabilirsiniz. `X-Forwarded-Host` Başlık.

```
GET / HTTP/1.1
Host: www.example.com
X-Forwarded-Host: www.attacker.com
...
```

Potansiyel olarak aşağıdaki gibi istemci tarafı çıktısı üretmek gibi:

```
...
<link src="http://www.attacker.com/link" />
...
```

Bir kez daha, bu web sunucusunun başlık değerini nasıl işlediğine bağlıdır.

Web Cache Poisoning (Web Önbelleği Zehirlenmesi)

Bu tekniği kullanarak, bir saldırgan, isteyen herkese zehirli içerik sunmak için bir web-cache'yi manipüle edebilir. Bu, uygulamanın kendisi, CDN'ler veya diğer aşağı

akış sağlayıcıları tarafından yürütülen önbellekleme vekili zehirleme yeteneğine dayanır. Sonuç olarak, mağdur, savunmasız başvuruyu talep ederken kötü amaçlı içeriğin alınması üzerinde hiçbir kontrole sahip olmayacaktır.

```
GET / HTTP/1.1
Host: www.attacker.com
...
```

Aşağıdakiler, bir mağdur savunmasız uygulamayı ziyaret ettiğinde web önbelleğinden servis edilecektir.

```
...
<link src="http://www.attacker.com/link" />
...
```

Password Reset Poisoning (Şifre Sıfırlama Zehirlenmesi)

Parola sıfırlama işlevselliğinin, oluşturulan bir gizli belirteç kullanan şifre sıfırlama bağlantıları oluştururken Host başlığı değerini içermesi yaygındır. Uygulama, bir şifre sıfırlama bağlantısı oluşturmak için saldırgan kontrollü bir etki alanını işlerse, kurban e-postadaki bağlantıya tıklayabilir ve saldırganın sıfırlama belirteciyi almasına izin verebilir ve böylece kurbanın şifresini sıfırlayabilir.

```
... Email snippet ...

Click on the following link to reset your password:

http://www.attacker.com/index.php?module=Login&action=resetPassword&toker
CRET_TOKEN>

... Email snippet ...
```

Referances (Referanslar)

- What is a Host Header Attack?

- Host Header Attack
- Practical HTTP Host Header Attacks