Test for Subdomain Takeover (Alt Alan Adının Ele Geçirilmesini Test Etme)

Summary (Özet)

Bu tür bir güvenlik açığının başarılı bir şekilde sömürülmesi, bir hasımın kurbanın alt yapısının kontrolünü talep etmesine ve ele geçirmesine izin verir. Bu saldırı aşağıdakilere dayanır:

1. Maktulün harici DNS sunucusu alt domaın kaydı, mevcut olmayan veya aktif olmayan bir kaynak / dış hizmet / bitiş noktasına işaret edecek şekilde yapılandırılmıştır. XaaS (Hizmet olarak Her Şey) ürünlerinin ve genel bulut hizmetlerinin çoğalması, dikkate alınması gereken birçok potansiyel hedef sunar.
2. Kaynak / dış hizmet / uç noktaya ev sahipliği yapan servis sağlayıcı, subdomina mülkiyet doğrulamasını düzgün bir şekilde ele almaz.

Subdomain devralınması başarılı olursa çok çeşitli saldırılar mümkündür (kötü amaçlı içeriğe hizmet etmek, yemek pişirmek, kullanıcı oturum çerezleri, kimlik bilgileri vb.). Bu güvenlik açığı, aşağıdakiler de dahil olmak üzere çok çeşitli DNS kaynak kayıtları için kullanılabilir: `A`, `CNAME`, `MX`, `NS`, `TXT` vs. Saldırı şiddeti açısından bir `NS` Subdomain devralma (daha az olası olsa da) en yüksek etkiye sahiptir, çünkü başarılı bir saldırı tüm DNS bölgesi ve kurbanın etki alanı üzerinde tam kontrole neden olabilir.

GitHub

1. Kurban (victim.com) geliştirme için GitHub kullanır ve bir DNS kaydını yapılandırır (`coderepo.victim.com`) ona erişmek için.
2. Mağdur, kod deposunu GitHub'dan ticari bir platforma taşımaya karar verir ve kaldırmaz `coderepo.victim.com` DNS sunucusundan.

3. Bir düşman bunu öğrenir `coderepo.victim.com` GitHub'da barındırılır ve iddia etmek için GitHub Pages'i kullanır `coderepo.victim.com` GitHub hesabını kullanarak.

Expired Domain (Süresi Doldurulmuş Alan)

1. Kurban (victim.com) başka bir alana (victimotherdomain.com) sahiptir ve diğer alan adını ifade etmek için bir CNAME kaydı (www) kullanır (`www.victim.com` > `victimotherdomain.com`)
2. Bir noktada, mağdurotherdomain.com sona erer ve herkes tarafından kayıt için kullanılabilir. CNAME kaydı kurban.com DNS bölgesinden silinmediği için kayıt yapan herkes `victimotherdomain.com` Üzerinde tam kontrole sahip `www.victim.com` DNS kaydı bulunana kadar.

Test Objectives (Test Hedefleri)

- Tüm olası alanlara (önceden ve güncel) numaralandırın.
- Unutulmuş veya yanlış yapılandırılmış alanları belirleyin.

How to Test (Nasıl Test Edilir)

Black-Box Testing (Siyah-Kutu Testi)

İlk adım, mağdur DNS sunucularını ve kaynak kayıtlarını numaralandırmaktır. Bu görevi yerine getirmenin birden fazla yolu vardır, örneğin DNS numaralandırması, ortak subdominalar sözlüğü, DNS brute kuvveti veya web arama motorlarını ve diğer OSINT veri kaynaklarını kullanarak DNS numaralandırması.

Kazı komutunu kullanarak test cihazı, daha fazla soruşturmayı gerektiren aşağıdaki DNS sunucusu yanıt mesajlarını arar:

- `NXDOMAIN`
- `SERVFAIL`
- `REFUSED`
- `no servers could be reached.`

Testing DNS A, CNAME Record Subdomain Takeover (Test DNS A, CNAME Rekorsu Alt Dolaşımı Devralma)

Kurbanın etki alanında temel bir DNS numaralandırması yapın (`victim.com`) kullanımı `dnsrecon` : :

```
$ ./dnsrecon.py -d victim.com
[*] Performing General Enumeration of Domain: victim.com
...
[-] DNSSEC is not configured for victim.com
[*]     A subdomain.victim.com 192.30.252.153
[*]     CNAME subdomain1.victim.com fictioussubdomain.victim.com
...
```

Hangi DNS kaynak kayıtlarının öldüğünü belirleyin ve aktif olmayan / kullanılmayan hizmetlere işaret edin. Kazı komutunu kullanmak için `CNAME` Rekor:

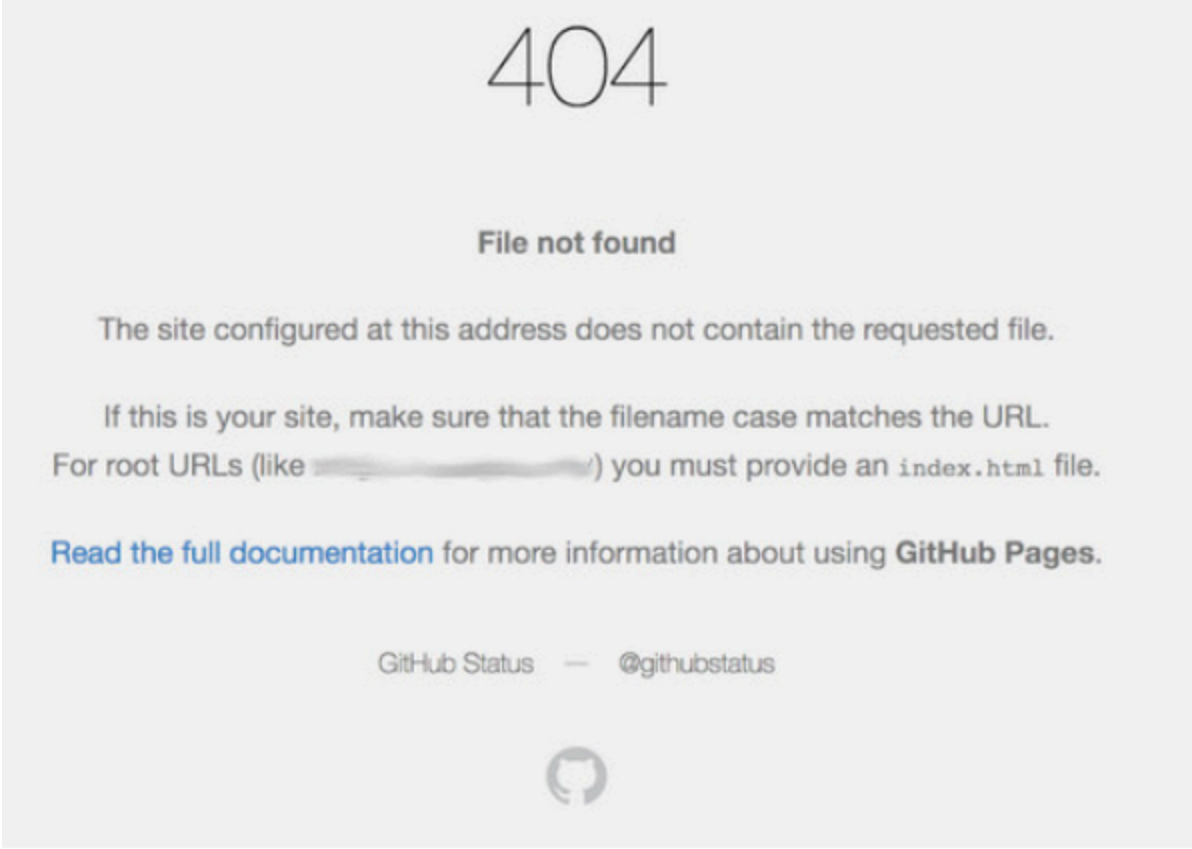
```
$ dig CNAME fictioussubdomain.victim.com
; <<>> DiG 9.10.3-P4-Ubuntu <<>> ns victim.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 42950
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
```

Aşağıdaki DNS yanıtları daha fazla soruşturmayı gerektirir: `NXDOMAIN` . .

Testi yapmak için `A` Test cihazının tüm veri tabanı aramasını gerçekleştirdiğini ve GitHub'ı servis sağlayıcı olarak tanımladığını kaydedin:

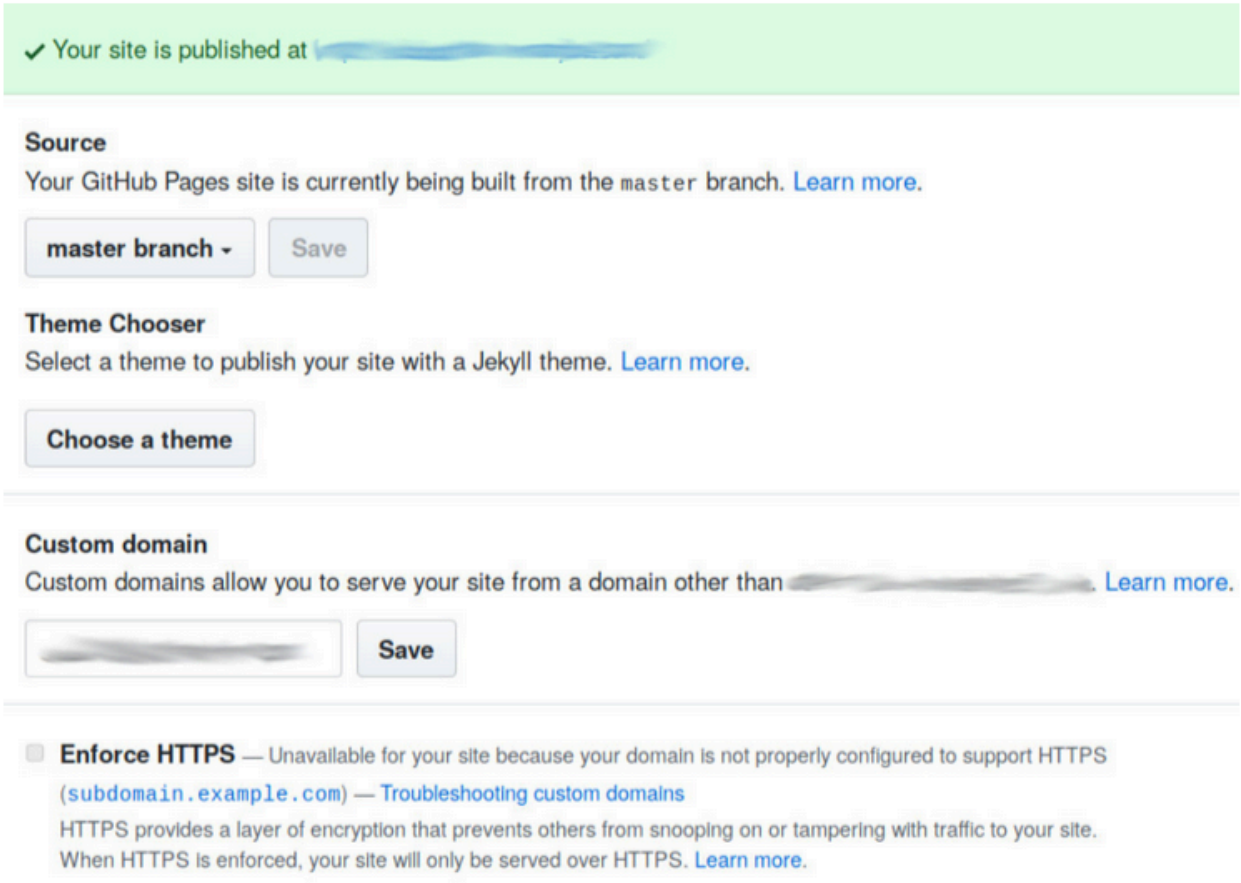
```
$ whois 192.30.252.153 | grep "OrgName"
OrgName: GitHub, Inc.
```

Testçi ziyaretleri `subdomain.victim.com` veya güvenlik açığının açık bir göstergesi olan bir “404 - Dosya bulunmayın” yanıtını döndüren bir HTTP GET talebinde bulunur.



Şekil 4.2.10-1: GitHub 404 Dosya Bulunmadı yanıt

Test cihazı, GitHub Sayfalarını kullanarak etki alanını iddia ediyor:



Şekil 4.2.10-2: GitHub iddia alanı

Testing NS Record Subdomain Takeover (Test NS Rekorsu Subdomain Devralma)

Alan için tüm isim sunucularını tespit edin:

```
$ dig ns victim.com +short
ns1.victim.com
nameserver.expireddomain.com
```

Bu uyduruk örnekte, test cihazı etki alanı olup olmadığını kontrol eder `expireddomain.com` Bir domain kayıt cihazı arama ile aktiftir. Etki alanı satın alınabilirse, subdomain savunmasızdır.

Aşağıdaki DNS yanıtları daha fazla soruşturmayı gerektirir: `SERVFAIL` ya da `REFUSED` .
.

Gray-Box Testing (Gri-Kutu Testi)

Test cihazı, DNS ışınlanmasının gerekli olmadığı anlamına gelen DNS bölge dosyasına sahiptir. Test metodolojisi de aynıdır.

Remediation (Düzeltme)

Alt alan adının ele geçirilmesi riskini azaltmak için savunmasız DNS kaynak kayıt(lar)ı DNS bölgesinden kaldırılmalıdır. En iyi uygulama olarak sürekli izleme ve periyodik kontroller önerilir.

Tools (Araçlar)

- dig - man page
- recon-ng - Web Reconnaissance framework
- theHarvester - OSINT intelligence gathering tool
- Sublist3r - OSINT subdomain enumeration tool
- dnsrecon - DNS Enumeration Script
- OWASP Amass DNS enumeration

References (Referanslar)

- HackerOne - A Guide To Subdomain Takeovers
- Subdomain Takeover: Basics
- Subdomain Takeover: Going beyond CNAME
- OWASP AppSec Europe 2017 - Frans Rosén: DNS hijacking using cloud providers – no verification needed