WHITE HAT REPORT

FACEBOOK CONFIRMATION CODE
URL INJECTION ATTACK

Araştırmacı: Aydın Keskin
Tür: Kaba kuvvet (Bruteforce)
Tehlike Seviyesi: Orta
Tanım: Parola değiştirme işleminin HTTP GET aracılığıyla yapılmasının istismar edilmesi.

ADIMLAR

1-)Profil ismi veya ID si bilinen facebook hesabı şu link üzerinden bulunur.

https://www.facebook.com/login/identify?ctx=recover (hesap bulma)

2-)Mail adresi ile kurtarma seçeneğine tıklanır (mail adresini açık olarak görmüyoruz, ama bu önemli değil)

3-)Mailde ki kodun geçerlilik süresi 24 saat.

4-)Parola girmemiz gereken facebookda 1 sayfa açılır. Rastgele bir parola denediğimizde, parola yanlıştır diyecek. Fakat adres çubuğuna baktığımızda bu isteğin GET methodu ile alındığını görüyoruz.

https://www.facebook.com/recover/password?u=FACEBOOK_ID&n=ONAYKODU&sih=0

5-)Hesap kurtarma kodu 6 haneli rakamlardan oluşuyor (000000-999999).

10^6=1,000,000 gibi çok küçük bir rakamsal kombinasyon oluyor.

6-)Adres çubuğunda ONAYKODU yazan kısım için bruteforce uyguluyoruz. Ben aşağıdaki modüller yardımıyla mini bir script yazdım.

```
import urllib
import requests
import webbrowser
```

7-)10-15 request den sonra facebook güvenlik engellemesi yaptığı için script üzerinde tor proxy kullandım.

8-)Tek bir bilgisayar ile 8-9 saat gibi sürede hedef hesabın onay koduna ulaşılıyor ve parola değiştirme şansı doğuyor (network isteklerine dayalı olduğu için 1 saniyede ortalama 15-20 deneme yapma imkanı oluyor).

FACEBOOK EKİBİ İÇİN ÇÖZÜM ÖNERİLERİ

1-)Kurtarma kodunun geçerlilik süresinin 30 dk gibi makul sürelere indirilmesi.

2-)Kurtarma kodunun çok daha uzun alfanumerik+özel karakter ile kombine edilmesi.

3-)Facebook güvenlik engellemesinin kontrolünü client tabanlı değil de server tabanlı yapmalı (böylece IP değiştirilse bile 15 denemeden sonra erişim geçici olarak bloke olacaktır).

KULLANICILAR İÇİN ÖNERİLER

1-)Multi factor korumalarını kullanmak.

2-)Mail adresi üzerinde şüpheli bir işlem varsa, linke tıklamadan doğrudan facebooka giriş yapıp parola değiştirmesi.