

## iPhone 5S Jailbreak Yapma

### Gereksinimler

iTunes	// AltStore Server Gereksinimi I
iCloud	// AltStore Server Gereksinimi II
AltStore Server & Client	// Sideloadng Uygulaması
unc0ver Uygulaması	// Jailbreak Exploitation Uygulaması

*Not: Gereksinim dosyaları (veya aşağıda linklerde belirtilen kurulum dosyaları) "~/Downloads/iPhone 5S Jailbreak Materyalleri.zip" dosyasında mevcuttur.*

### a) Birinci Aşama: Bilgisayara ve iPhone 5S'e AltStore Yazılımı Kurma

Bilgisayara AltStore Server yazılımı gereksinimleri ve Altstore server yazılımının kendisi yüklenir. Ardından bilgisayardan iphone 5S mobil telefona Altstore client uygulaması yüklenir.

1. Bilgisayara "AltStore yazılımı" gereksinimi olan iTunes yüklenir.

İndirme Linki:

<https://discussions.apple.com/docs/DOC-6562#versions>

Not: iTunes açıldıktan sonra Help -> Check for Updates denmeli ve son sürüme güncellenmelidir.

2. Bilgisayara "AltStore yazılımı" gereksinimi olan iCloud yüklenir (Not: iCloud Microsoft Store'dan yükleme olmamalı. Setup.exe şeklinde yüklenmiş olmalı).

İndirme Linki:

<https://secure-appldnld.apple.com/windows/061-91601-20200323-974a39d0-41fc-4761-b571-318b7d9205ed/iCloudSetup.exe>

3. Bilgisayara AltStore gereksinimleri yüklendikten sonra AltStore Server yazılımı yüklenir.

İndirme Linki:

<https://altstore.io/>

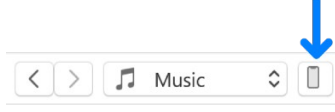
İnen altinstaller.zip klasörü zip'ten çıkarılır ve içerisindeki setup.exe ile kurulum sağlanır.

4. Bilgisayar windows başlat simgesinden AltStore Server yazılımı aranır ve başlatılır.

Not: AltServer başladığında sağ altta simgeler tepsisinde yerini alacaktır.

5. Bilgisayarda iTunes yazılımı başlatılır, bilgisayara iPhone 5S mobil cihazı usb kablo ile bağlanır ve iPhone 5s cihaz bilgilerinin iTunes yazılım ekranına gelmesi beklenir.

Not: iTunes yazılımının bağlanan iPhone 5S mobil cihazını gördüğünü doğrulamak için iTunes arayüzündeki küçük akıllı telefon simgesine tıklanmalıdır.



iPhone 5s cihaz bilgilerinin iTunes arayüzüne geldiği bu şekilde görülebilir.

6. Bilgisayarda iTunes yazılım ekranında sol sütundaki Summary seçeneğine gidilir, ve ekranın aşağısındaki Wi-fi Sync seçeneğine tick işareti konur.

7. Daha sonra bilgisayarın sağ alt köşesindeki simgeler tepsisinden AltServer ikonuna tıklanır ve

Install AltStore -> Hefese's iPhone 5S

denir.

Bu adım neticesinde bilgisayardaki Altstore Server yazılımı bilgisayara bağlı iphone 5s mobil cihazına Altstore Client uygulamasını yüklemeye başlayacaktır. Bu yüklemeye başlarken Apple ID hesap bilgilerinin girilmesini isteyecektir. Apple ID hesap bilgileri girildikten sonra ise sağ alta AltStore client uygulaması iphone 5s'e yükleniyor, ve yüklendi şeklinde iki ayrı windows bildirimini ekrana gelecektir. Bildirimler sonrası iPhone 5S mobil cihaza AltStore Client uygulaması yüklenmiş olacaktır.

8. iPhone 5S mobil cihaza geçilir ve cihaz ayarlarından apple store mağazası haricindeki yüklenen AltStore client uygulamasının çalışabilmesi için gerekli güven duy izni verilir:

iPhone 5S -> Settings -> General -> Profiles & Device Management -> AltStore -> (TRUST)

Bu adım neticesinde telefonun ana ekranında listelenmiş AltStore uygulaması simgesine tıkladığında uygulama açılabilir olur.

## **b) İkinci Aşama: iPhone 5S'e Jailbreak Exploit Uygulamasını Kurma**

iPhone 5S mobil telefona kendi sürümüyle (12.5.5 ile) ilintili olan jailbreak exploit uygulaması (unc0ver) safari web tarayıcısından indirilir, ve mobil cihazdaki Altstore Client uygulaması ile inen jailbreak exploit uygulaması unc0ver yüklenir.

iOS Version	Jailbreak provider/tool
11.0 → 14.3	unc0ver
10.0 → 10.3.4	doubleH3lix
9.3.5 → 9.3.6	Phoenix
9.1 → 9.3.4	Home Depot

#### UYARI:

iPhone 5S usb kablo ile halen bilgisayara baęlı durumda bırakılmalıdır ve çıkarılmamalıdır. Çünkü sonradan söylenecek Share işleminde bilgisayardaki Altstore Server ile irtibat kurulmaktadır.

1) iPhone 5S cihazında web tarayıcı Safari'den Unc0ver jailbreak uygulaması indirilir.

İndirme Linki:

<https://wettransfer.com/downloads/7e726f29552b814302e415b7be479d7020220228045330/b95a7e>

2) iPhone 5S cihazında indirilen unc0ver dosyasına Files'dan gidilir ve üzerine basılı tutup "Share" denir.

3) Share penceresinden AltStore uygulaması seçilir.

#### UYARI 1:

iPhone 5S'te share işleminden önce iphone 5S (altstore client) ile bilgisayar (altstore server) aynı wifi internete baęlı durumda olmalıdır. Bunun için Samsung Galaxy telefonunun hotspot'unu açabilirsin ve her ikisini de aynı wifi aęına dahil edebilirsin. Bu şekilde iphone 5s cihazda inen unc0ver kurulumu gerçekleşebilecektir. Dięer türlü kopyalama sırasında yükleme başarısız oluyor. Bu nedenle aynı wifi aęında olmalılar.

#### UYARI 2:

iPhone 5S'te share işleminden önce bilgisayarda Windows Defender kapatılmalıdır. Aksi takdirde iphone 5s'de cihaza indirilen unc0ver ipa kurulum dosyası paylaşımı Altstore Client uygulamasına yapılamıyor.

4) iPhone 5S'deki AltStore uygulaması otomatik olarak unc0ver uygulamasını (ipa kurulumunu) kurmaya başlayacaktır. Kurulum tamamlandığında AltStore sekmelerinden My Apps'de unc0ver listelenecektir ve iPhone 5S home tuşu ile ana ekranda unc0ver uygulamasının yer aldığı görülebilecektir.

### **c) Üçüncü Aşama: iPhone 5S'e Jailbreak Atma**

Jailbreak adımlarına başlanıp telefon jailbreak'li hale getirilecektir.

Uyarı:

Telefonda defalarca başarısız jailbreak teşebbüsü meydana gelecektir ve bu nedenle telefon elle sürekli yeniden başlatılıp tekrar jailbreak denemeleri yapılacaktır. Süreç bu şekilde işliyor. En sonunda başarılı olunuyor.

- 1) iPhone 5S uçak moduna alınır, ve arkaplandaki tüm pencereler kapatılır.
- 2) iPhone 5S'de ana ekranda listelenen unc0ver uygulaması açılır ve 1 dakika beklenilir. Ardından jailbreak butonuna basılır.
- 3) iPhone 5S'de unc0ver uygulaması hata verebilir. Bu durumda iPhone 5S kapatılıp açılır ve arkaplandaki açık unc0ver penceresine gelinip 1 dakika beklenilir ve tekrar Jailbreak butonuna basılır.

Not: Her hata verdiğinde iPhone 5S kapatılıp açılır ve arkaplandaki unc0ver uygulama penceresi açılıp bir dakika beklenilir ve tekrar Jailbreak butonuna basılır. Bu durum hata vermeyene kadar devam ettirilir.

- 4) Jailbreak ilk aşaması başarılı olduğunda iPhone 5S otomatik olarak yeniden başlar ve arkaplan penceresindeki unc0ver açılarak 1 dakika beklenilir ve tekrar Jailbreak butonuna basılır.

Not: Hata verdiğinde iPhone 5S kapatılıp açılır ve arkaplandaki unc0ver uygulama penceresi açılıp bir dakika beklenilir ve tekrar Jailbreak butonuna basılır. Bu durum hata vermeyene kadar devam eder.

- 5) Bir yeniden başlatma sonrası denemede hata vermeden devam edildiğinde Jailbreak tamamlanmak üzereyken gelen popup'a "Always Allow" denir.

Not: Jailbreak tamamlandığında da böyle bir popup gelirse Always Allow denir.

- 6) En nihayetinde bir popup daha gelir. iPhone 5S'in yeniden başlayacağını ve yeniden başladığında jailbreak'li olacağını söyler. Bu popup'a OK denir ve iPhone 5S yeniden başlar.

Not: Yeniden başlama 5 dakikadan fazla sürerse sorun vardır. Bu durumda telefon bir türlü başlayamayacaktır ve o başlama ekranı şarj bitene kadar kalacaktır. Ve telefon elle başlatıldığında jailbreak olmadığı görülecektir. Bu nedenle telefon başlıyor ekranında uzun süre kaldığında kapat aç ve home düğmesine birlikte basılmalıdır ve telefon başlama ekranındayken kapatılıp yeniden başlatılmalıdır. Ardından unc0ver ile jailbreak butonuna basarak

jailbreak tekrarlanmalıdır. Bunun için uçak moduna geçilir, tüm arkaplandaki pencereler kapatılır, unc0ver açılır, 1 dk beklenilir ve jailbreak butonuyla jailbreak'e başlanır. Başarısız olduğunda unc0ver uygulamasında jailbreak butonu ile jailbreak tekrarlanır. Telefon jailbreak'li başlayacak mesajı sonrası telefon eğer başarılı şekilde jailbreak'lenmişse yeniden başlamada en fazla 1 dakika içerisinde telefonu uygun şekilde başlatacaktır.

7) iPhone 5S yeniden başladığında jailbreak böylece tamamlanır. unc0ver uygulamasına gelindiğinde Jailbreak yerine "Re-jailbreak" yazıyorsa jailbreak'in tamam olduğu anlaşılır. Bu noktadan sonra jailbreak sonucu yüklenen cydia mağaza uygulaması ile openssh, terminal gibi uygulamalar indirilip kullanılabilir.

Not: Eğer işlem sonrası unc0ver uygulamasına gelindiğinde buton "Re-Jailbreak" yerine halen Jailbreak şeklindeyse jailbreak tamamlanmamıştır. Dolayısıyla tekrar Jailbreak denenmelidir. Bunun için telefon uçak modunda olmalıdır ve arkaplandaki tüm pencereler kapatılmalıdır. Unc0ver açıldığında 1 dk beklenilerek jailbreak yapma işlemine başlanmalıdır. Başarısız olduğunda aynı işlem tekrarlanmalıdır.

Uyarı: Telefon yeniden başlatıldığında jailbreak gitmektedir. Bu ise jailbreak ile yüklenen cydia mağaza uygulaması ve cydia mağazası ile yüklenen uygulamalarının kullanılamamasına sebep olmaktadır. Eğer telefon yeniden başlatılırsa veya şarjı biterse yeniden jailbreak yapılmalıdır. Bunun için telefon uçak modunda olmalıdır ve arkaplandaki tüm pencereler kapatılmalıdır. Unc0ver açıldığında 1 dk beklenilerek jailbreak yapma işlemine başlanmalıdır. Başarısız olduğunda aynı işlem tekrarlanmalıdır.

Uyarı 2: Eğer telefon başladıktan sonra cydia uygulaması açılmıyorsa (başlatıldığında kendiliğinden otomatikmen programdan atıyorsa) uçak modunda ve tüm arkaplandaki pencereler kapalıyken unc0ver'a gelinir. 1 dk beklenilir. Settings'den Re-install cydia seçilir ve tekrar telefona jailbreak yapılır. Jailbreak hata vermezse telefon yeniden başlayacaktır ve cydia uygulaması çalışır şekilde jailbreak tamamlanacaktır. Hata verirse telefon kapatılıp açılır, arkaplandaki pencereler kapatılır ve arkaplandaki açık unc0ver penceresine gelinip tekrar 1dk bekleme sonrası jailbreak denir. Jailbreak başarısız olursa aynı işlem tekrarlanır. Başarıya ulaşına kadar bu jailbreak denemelerine devam edilir. En nihayetinde olduğunda ise Cydia uygulaması açılır.

## **Sonuç**

iPhone 5S'e jailbreak atmak için bilgisayara iTunes, iCloud ve AltStore Server yazılımı kurulmuştur. Ardından iphone 5s cihazı bilgisayara usb kablo ile bağlandıktan sonra bilgisayardaki AltStore Server yazılımı üzerinden iphone 5s cihaza AltStore Client uygulaması kurulmuştur. iPhone 5S cihaz ayarlarından kurulan AltStore Client uygulamasına çalıştırılabilir izni (güven izni) tanımlanmıştır. AltStore Client uygulaması iphone 5S cihaza apple store mağazası haricindeki kaynaklardan

indirilen uygulama kurulum dosyalarının kurulumunu sađlayan bir uygulamadır. Bu şekilde apple mađaza store'unda yer almayan jailbreak uygulaması kurulabilecektir.

iPhone 5S cihazına safari web tarayıcıdan jailbreak exploit işlemini yapacak unc0ver uygulaması kurulum dosyası indirilmiştir. Bu kurulum dosyası indikten sonra iPhone Share seçeneđi ile AltStore Client uygulamasına paylaşılmıştır. AltStore Client uygulaması ise bu gelen dosyayı iPhone 5S cihazına kurmuştur ve iPhone 5S cihazında ana ekranda uygulamalar arasında unc0ver yerini almıştır. Son olarak unc0ver uygulaması ana ekranda başlatılıp çalıştırılarak exploitation uygulanmıştır ve telefon tekrarlı jailbreak denemeleri sonunda jailbreak'lenmiştir.

### **EK: AltStore Client ile Kurulu Uygulamaların Süresi Dolduđunda Refresh'leme**

iPhone 5S'teki AltStore Client'ta kurulan uygulamaların expire'ı dolduđunda uygulamaların kurulumlarının refresh'lenmesi gerekmektedir. Bunun için;

- 1) Bilgisayar ve iPhone 5S wifi ile aynı internet ađına bađlanmalıdır.
- 2) Bilgisayarda AltStore Server, iCloud ve iTunes açık olmalıdır.
- 3) Ardından iPhone 5S usb kablo ile bilgisayara bađlanmalıdır.
- 3) Sonra bilgisayarda Başlat çubuđunun sađındaki simgeler bölümünden AltStore Server ikonuna tıklanmalıdır ve Check For Updates denmelidir.
- 4) Son olarak iPhone 5S'te AltStore Client uygulamasında Refresh All butonuna basılmalıdır.

Böylece uygulamaların dolan süresi yenilenecektir ve uygulamalar iPhone 5S'te kullanılmaya devam edebilecektir.

### **Kaynaklar**

<https://cybertips.io/how-to-install-altstore/>

<https://support.apple.com/en-ca/guide/itunes/itns3751d862/windows>

<https://cybertips.io/download-unc0ver-jailbreak-ipa/>

<https://www.jailbreaktr.com/konular/ios-12-4-unc0ver-hatasi.8308/#post-106307>

[https://www.youtube.com/watch?v=3\\_f9drcETA](https://www.youtube.com/watch?v=3_f9drcETA)

<https://cobalt.io/blog/ios-pentesting-101>

<https://www.jailbreaktr.com/konular/cydia-acilmiyor.5085/>

<https://tweak-box.com/tr/altstore-indir/>

[https://www.reddit.com/r/AltStore/comments/eqlaxl/invalid\\_anisette\\_data/](https://www.reddit.com/r/AltStore/comments/eqlaxl/invalid_anisette_data/)