

Command Injection

Command Injection, uygulamanın kötü niyetli kullanıcılar tarafından komut çalıştırmasına olanak sağlayan bir zafiyettir. Genelde kullanıcıdan aldığı veriyi sistemde komut ile çalıştırmaktan kaynaklanır. Ve başlıca nedenlerinden biri yetersiz input doğrulaması. Bir php uygulaması düşünelim düşünelim,

```
<?php
```

```
$filename = $_GET['filename'];
```

```
system("cat " . $filename);
```

```
?>
```

Kullanıcı girdiye ; yerleştirerek komutu kapatıp kendi istediği komutları çalıştırabilir. Buradaki labımızda command injection zafiyeti var.

Bu laboratuvar, uzaktan komut çalıştırmaya yol açan bir Komut Enjeksiyonu güvenlik açığı içerir.

Web uygulaması, kontrol etmek istediğiniz alan adını terminalde çalışan "nslookup" aracına parametre olarak verir. Sistem üzerinde bir komut çalıştırmanın bir yolunu bulun.

Web sitesinin çalıştığı sunucunun ana bilgisayar adı adresi nedir?

Bizden bu zafiyeti kullanarak sitenin çalıştığı sunucunun ana bilgisayar adını bulmamız isteniyor.

DNS Lookup

;ls

Search

;ls ile zafiyet belirlemeye çalışıyorum. Eğer herhangi bir listeleme gelirse ilk adım için oldukça başarılı sonuçlar elde etmiş olacağız.

DNS Lookup

Search

assets

index.php

Başarılı bir aşama! Şimdi ise ; ile kapatıp hostname komutunu çalıştırmayı deniyoruz...

DNS Lookup

Search

squirrel

Görev başarılı!

Bir diğer örneğimizde ise yaygın komutları ve operatörleri engelleyen bir sistem kurulmuştur.

Command Injection Filter Bypass

Bu laboratuvar, uzaktan komut çalıştırmaya yol açan bir Command Injection zafiyeti içerir.

Web uygulaması, kontrol etmek istediğiniz alan adını terminalde çalışan "nslookup" isimli araca parametre olarak verir. Gönderdiğiniz alan adı yaygın komutlar veya operatörler içeriyorsa, sorgunuz engellenecektir. Sistem üzerinde komut çalıştırmanın bir yolunu bulun.

Web sitesinin çalıştığı sunucunun ana bilgisayar adı adresi nedir?

DNS Lookup

Search

Error: Command contains blacklisted keyword.

Görüldüğü gibi bu sefer ls komutumuz işe yaramadı.

Peki burada bir örnekle gidelim...

echo Hello Yavuz || ls komutunun ne işe yaradığını açıklayalım || operatörü sayesinde eğer ilk komut bir şekilde başarısız olursa ikinci komutu çalıştır demektir. Kısacası eğer echo herhangi bir nedenden kaynaklı çalışmazsa bize ls komutunu çalıştıracak. Hemen bu operatör yasaklanmış mı diye deniyorum.

DNS Lookup

||hostname

||hostname

Search

legend

Tahmin ettiğimiz gibi. || komutu sayesinde başarılı bir şekilde labımızı tamamlıyoruz.