SATELLITE WRİTE-UP

Merhaba arkadaşlar. Bugün sizlerle Hackviser platformunda bulunan Satellite adlı Warmup' ını yazacağım.

SORU 1: Web sitesinin alan adı nedir?

Makineyi ayağa kaldırmak için bize ip ve alan adı veriyor. Cevap: **beyondbound.hv**

SORU 2: Hangi CMS yazılımı kullanılıyor?

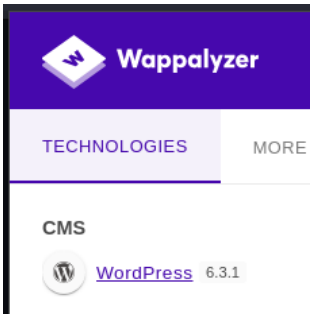
CMS yazılımları: İçerik yönetim sistemidir. (Wordpress, shopify, wix vb.)

Bu sorunun cevabı için whatweb toolunu kullanalım.

```
└─# whatweb 172.20.15.46
http://172.20.15.46 [200 OK] Country[RESERVED][ZZ], Email[info@beyondbound.hv], HTML5, HTTPServer[nginx/1.18.0], IP[172
.20.15.46], MetaGenerator[WordPress 6.3.1], Script, Title[BeyondBound &#8211; Beyond Earth, Toward Infinity], UncommonH
eaders[link], WordPress[6.3.1], nginx[1.18.0]
```

Cevap: **Wordpress**

Ayrıca bu sorunun cevabı için Wappalyzer'da kullanabiliriz.



SORU 3: WordPress güvenlik taraması için hangi araç kullanılabilir?

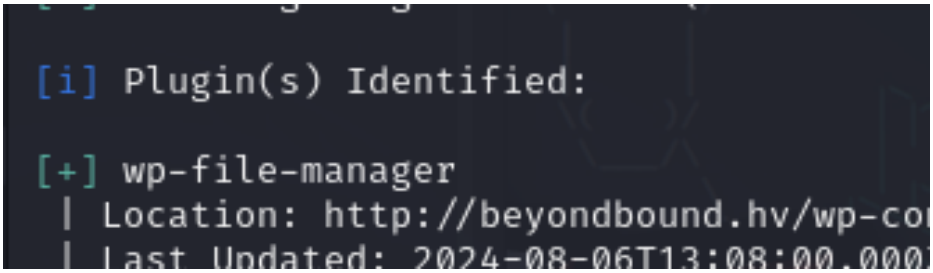
Wordpress'de açık bulmak için **wpscan** toolunu kullanırız.

SORU 4: Hedef websitesinde hangi eklenti kullanılıyor?

Wpscan aracı ile tarama yaptım. Plugins(eklentilerin olduğu kısım) sonucu bir türlü vermedi. Daha sonra uzun araştırmalar sonucu(plugins passive olduğu için vermedi.)

"wpscan --enumerate p --url 172.20.15.46 --plugins-detection aggressive" komutunu buldum.

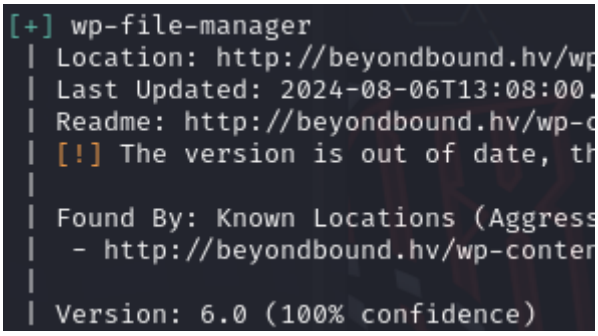
(passive olan kısmı aggressive'ye çevirdik.) Biraz bekledikten sonra sonucu aldık.



Cevap: **wp-file-manager**

SORU 5: Kullanılan eklentinin versiyonu nedir?

Yine aynı çıktı sonucunda:

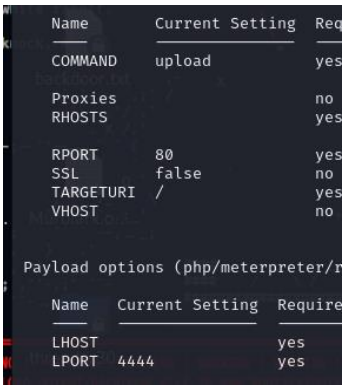


Cevap: **6.0**

SORU 6: Durumu bilinmeyen uydunun adı nedir?

Bu sorunun cevabı için bir önceki sorudaki cevabı biraz Google üzerinde araştırma yaptım. Ve bu klasör ile ilgili açık bulunmuş zamanında. Biz de bu açığı sömürmek için Metasploitable kullanacağız.

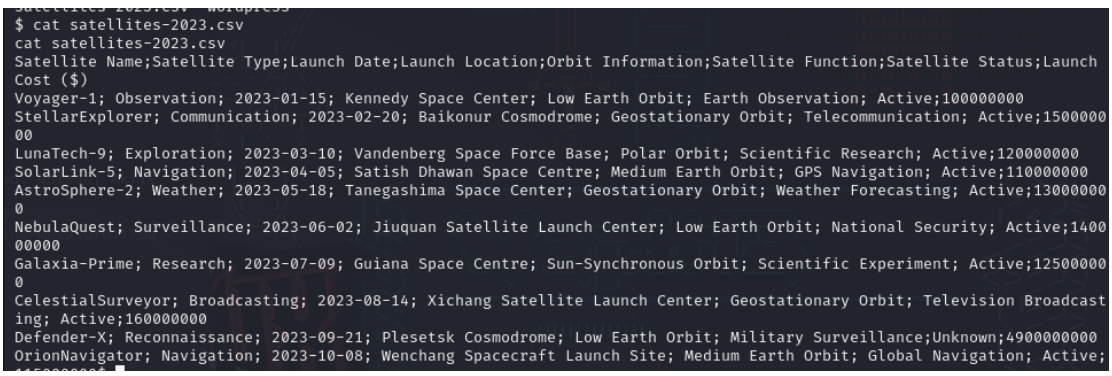
use 0 ile seçelim.



RHOSTS ve LHOST eklemesini yapalım.

Run diyerek çalıştıralım. Shell aldık. Şimdi dosyalar arasında dolaşalım.

Var/www/html dosyası içerisinde satellite-2023.csv adlı dosya buldum.



Burada durumu bilinmeyen(unknown) **DEFENDER-X** olduğunu bulduk.