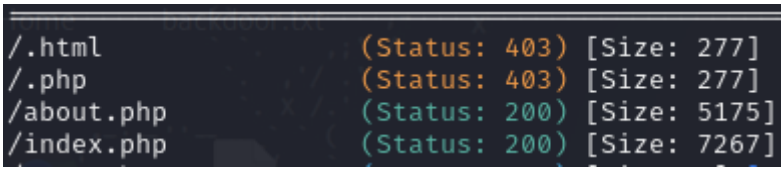
ALOHOMORA WRİTE-UP

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

SORU 1: Blog yazarının e-posta adresi nedir?

Bu sorunun cevabını bulmak için gobuster ile dizin taraması yaptım.

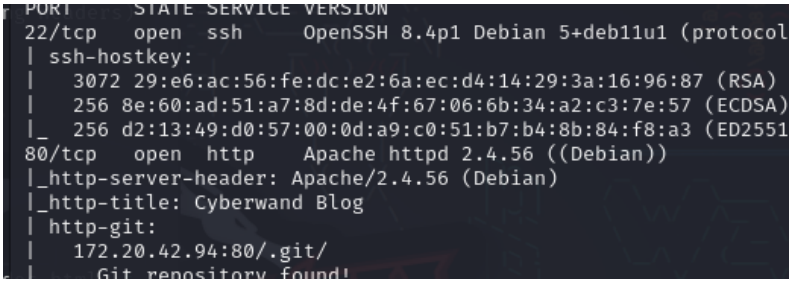


Daha sonra about.php sayfasına gittim.

Cevap: tommy@cyberwand-blog.com

SORU 2: Dizin keşfinde bulunan ve içinde git ile ilgili dosyalar bulunan dizinin adı nedir?

Bu noktada bilgi toplamak için Nmap taraması atalım.



Cevap: **.git**

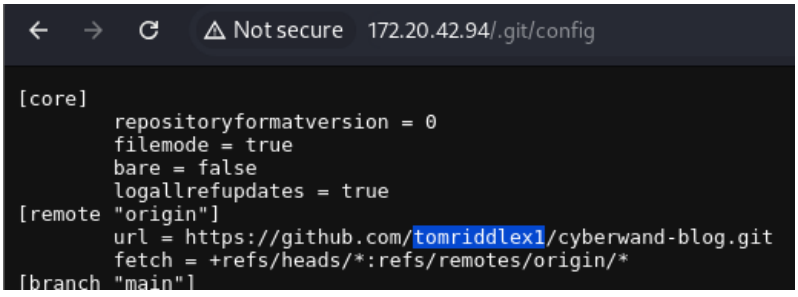
(Nmap taraması sonucunun en alt kısmında bu dizini bize gösteriyor.)

Ayrıca dirsearch aracını kullanalım.

Yine cevabı bulduk.

SORU 3: Geliştiricinin kullanıcı adı nedir?

Bu sorunun cevabı için bir önceki soruda bulduğumuz .git dizinine gidiyoruz. Burada config.php var.



İçine bakınca cevaba ulaşıyoruz. Cevap: **tomriddlex1**

SORU 4: Hangi branch aktif?

Bir önceki fotoğrafta en alt kısımda “**main**” branch’ının aktif olduğunu görüyoruz.

SORU 5: Commitleri gösteren git komutu nedir?

Commitleri gösteren git komutu “**git log**” komutudur.

SORU 6: Branch i değiştiren git komutu nedir?

Bir önceki soru bu soru da Google üzerinde araştırma yaparak bulunacak sorulardan birisidir.

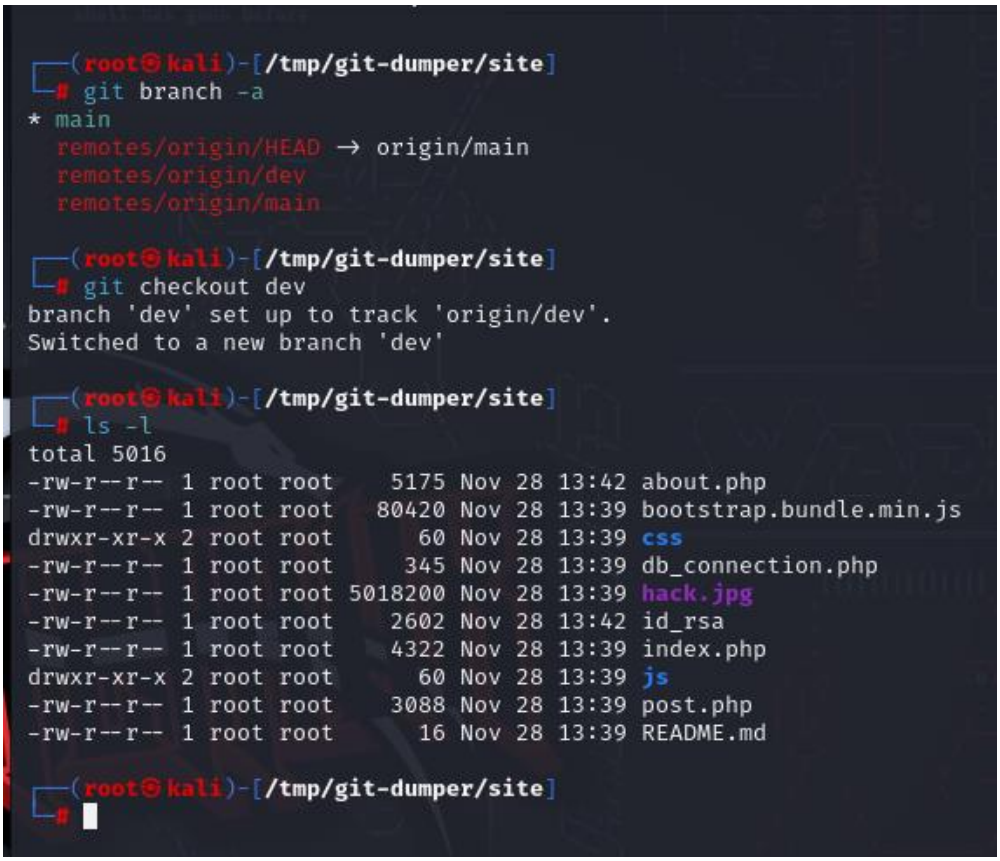
Cevap: **checkout**

SORU 7: Dev branchinde unutulan dosyanın adı nedir?

Şimdi .git dosyası için “git-dumper” aracı ile bu verileri çekelim.

Diyerek site klasörü içine atalım.

Elimizde dosyalar var.



Git branch –a komutu ile branch’ları görüntüledik.

“Git chechkout dev” diyerek dev branchına geçiş yaptık. Ls –l ile içindeki dosyaları görüntüledik.

Burada “**id_rsa**” dosyası bulduk.

SORU 8: hackviser kullanıcısının parola hashi nedir?
Önceki görevde bulduğumuz id_rsa dosyası ile ilgili Google üzerinde araştırma yaptığımızda SSH'a bağlanmak için kullanılan bir anahtar dosyası olduğunu anlıyoruz.

İlk başta ssh ile bağlanmayı denedim hata aldım. Daha sonra id_rsa dosyasına chmod +x ile yetki verdim. Tekrar denedim.

Başarılı bir şekilde bağlantı kurduk. Şimdi hash bulmak için /etc/shadow dosyasını görüntülemeyi deneyelim.

CEVAP: **yj9T$FOWx5qCAorpq72xggPErc0$zkgSTMnKfdrb/jH1zRKBvHCIsNCtmPElDaM4TjhNE7B**