|  |
| --- |
| ***Web Bypass*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Sensitive Data Exposure  -ShellShock Zafiyeti  -Server Side Inclusion Zafiyeti  -PHP Injection Zafiyeti |

**09.08.2021**

***Sensitive Data Exposure***

- Gizli kalması gereken Admin veya Config değerlerinin başka kişiler tarafından görüntülenip ifşa edilebilmesinden kaynaklanan zafiyettir.

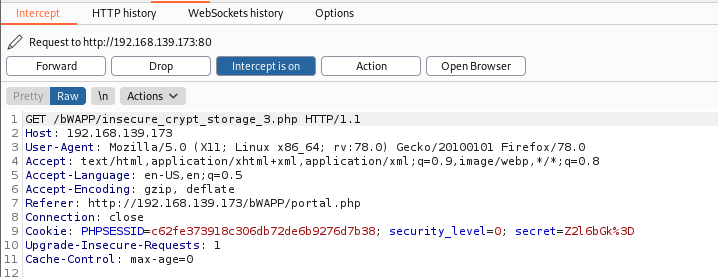
-Kodlama hatası veya Basit Encode tekniklerini kullanılmasından kaynaklı da ortaya çıkabiliyor.

-Bu zafiyet için daha önceden kurulumundan bahsettiğim bWAPP laboratuvarını kullanacağım.

-bWAPP üzerinden Base64 Encoding zafiyetini “Low” düzeyinde başlatıyorum.

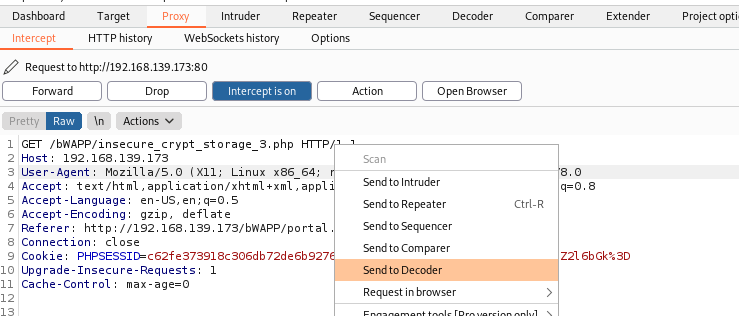


-Zafiyetli sitenin görüntüsü bu şekildedir.

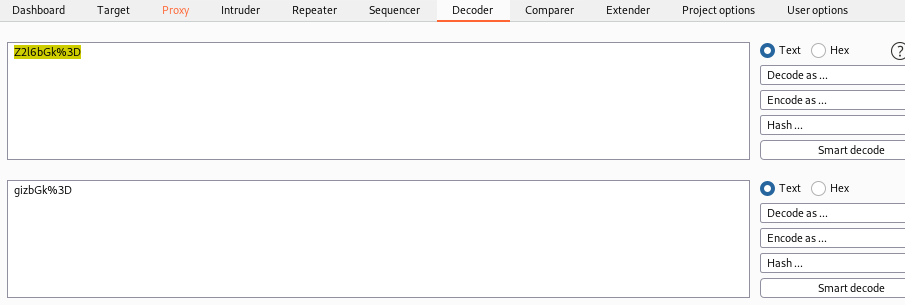


-Arkadan Burpsuite aracımı çalıştırıyorum ve gerekli bilgileri oraya çekiyorum.

-Burada Secret değerleriyle karşılaşıyorum.Bu secret kısmı Base64'e benzediğini düşünüyorum bu sebeple Encoder üzerinden işlemlerime devam edeceğim.



-Sağ tıklayıp "Send to Decoder" ile gönderim yapıyorum.



-Burada işlem gerçekleştirdiğimde çok anlaşılır bir değer elde edemedim.

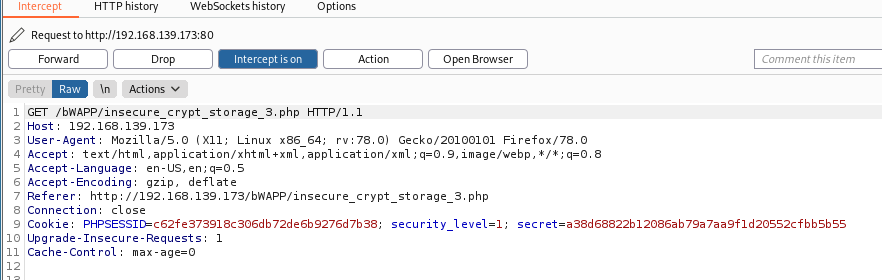
-Bu sebeple tarayıcı üzerinden bir decode işlemi gerçekleştireceğim.

>>>>>



-“Base64 Decoder” ile dönüştürdüğümde gizli şeklinde bir bilgiyle karşılaştım.

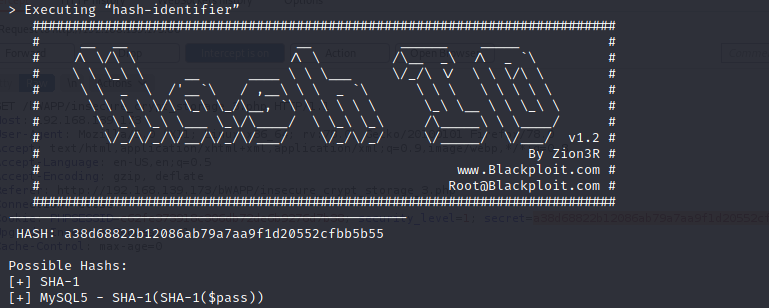
-Low değerini bu şekilde çözdükten sonra “Medium” seviyesi ile devam ediyorum.



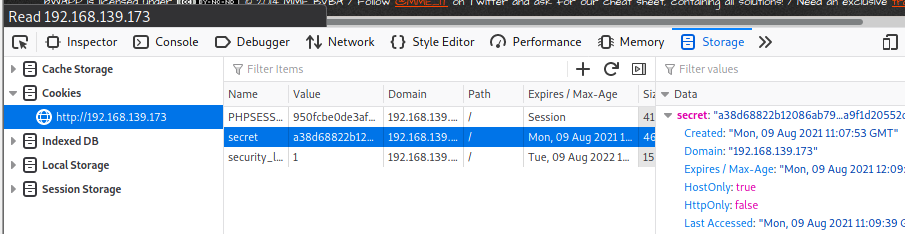
-Önce herzaman ki gibi bilgileri Burpsuite üzerine çekiyorum.Secret bölümünü kopyalıyorum.

-Bu bölüm bana hash değeri gibi geldiği için “hash identifier” aracı kullanacağım.

-Linux üzerinde hazır olarak bulunan "hash-identifier" aracı ile işlemlerime devam edeceğim.

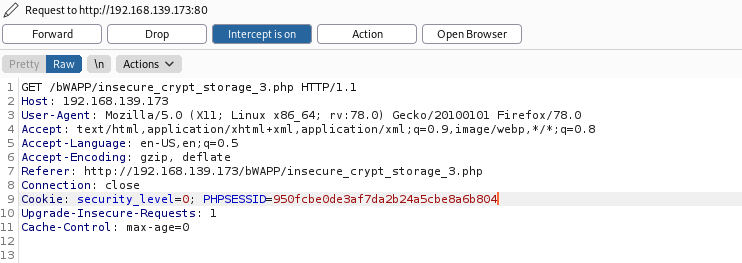


-İşlemi gerçekleştirdiğimde bunun “SHA1” ile şifrelendiğini görüntülüyorum.

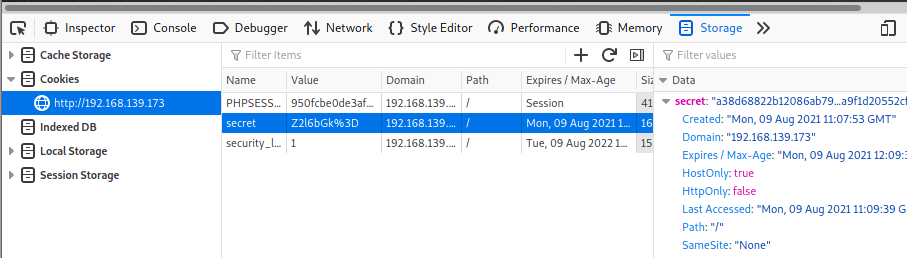


-Sağ tıklayıp "Inspect Element" ile kaynak kodlarını görüntülüyorum.Burada secret değerine baktığımda “SHA1” değeriyle aynı değer olduğunu görüntülüyorum.

-Bunu Burpsuite üzerinden değiştirip Forward ile değiştirmeyi deneyeceğim.



-Forward işlemini 5-6 kere gerçekleştiriyorum.



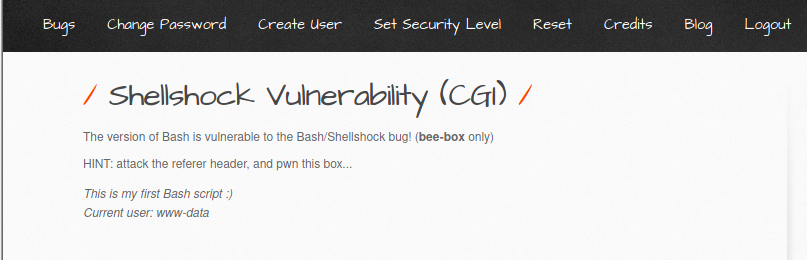
-Daha sonrasında siteye geçiş yaptığımda Kaynak kodlarını görüntülediğimde burada Önceki uygulamada Encode ettiğim Karakter olduğunu görüntülüyorum.

-Burada gizlenmiş zafiyeti görüntüleyebiliyorum.

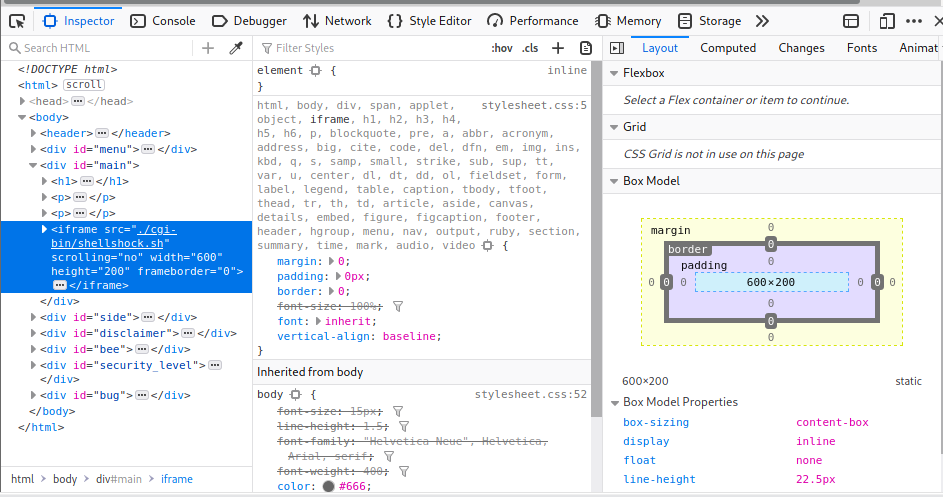
***ShellShock***

-Bu zafiyet sayesinde web sitesinde bash kodu kullanılabiliyor.

-Bu zafiyet içinde daha önceden kurulumunu yaptığımız bWAPP laboratuvarını kullanacağız.

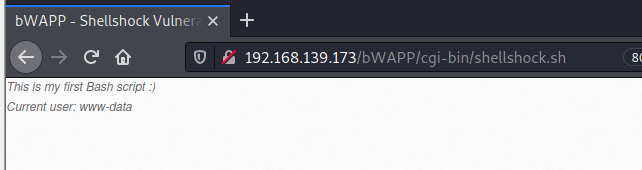


-Zafiyetimin bulunduğu sayfayı bu şekilde görüntüleyebiliyorum.



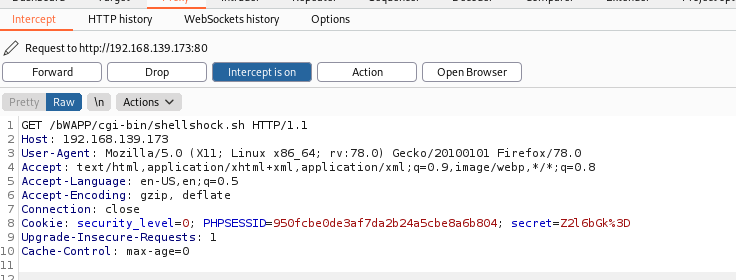
-Sağ tıklayıp “İnspect Element” ile kaynak kodunu görüntülüyorum.Burada bir dizin görüntülüyorum.

Burada ki dizini kopyalıyorum.



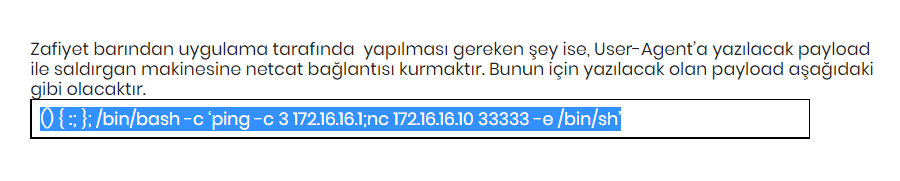
-Dizini görüntülediğimde burada zafiyetli bir sayfa olduğunu görüntülüyorum.

-Burada ki bilgileri gerekli ayarlar sonucunda “Burpsuite” aracıma çekiyorum.

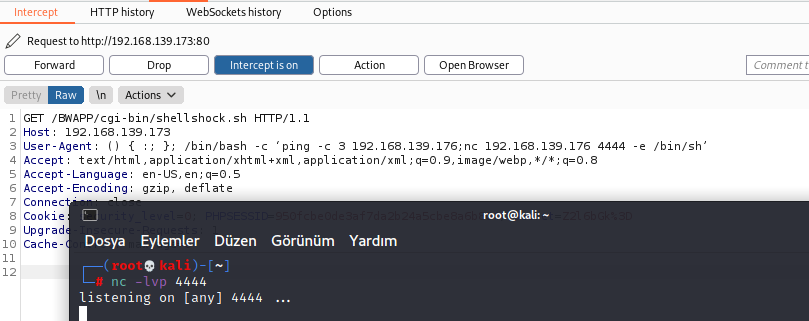


-“Burpsuite” aracında görüntülediğimde bilgiler bu şekildedir.

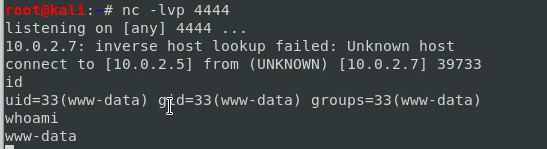
-User-agent üzerinden işlem gerçekleştireceğim.



-Bu işlem için tarayıcı üzerinden bir payload buluyorum ve” User agent” sekmesine ekleyeceğim.



-Netcat üzerinden dinleme işlemini başlatıyorum.Payload üzerinden kendi IP adresimi eklediğim sayfayı Forward ediyorum ve işlemi başlatıyorum.



-Netcat üzerinden dinlemeye aldığım kısım üzerinden erişimi başarılı bir şekilde sağlayıp konsol erişimi elde ettim.

-Artık burada istediğim komutu kullanabilirim.

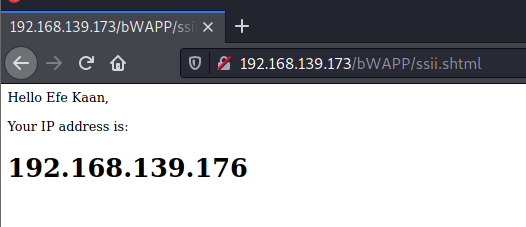
***Server Side İnclusion***

-SSI olarak bilindiği gibi “WWW “ üzerinde çok sık kullanılan bir dildir.

- Bu zafiyet içinde daha önceden kurulumunu yaptığımız bWAPP laboratuvarını kullanacağız.

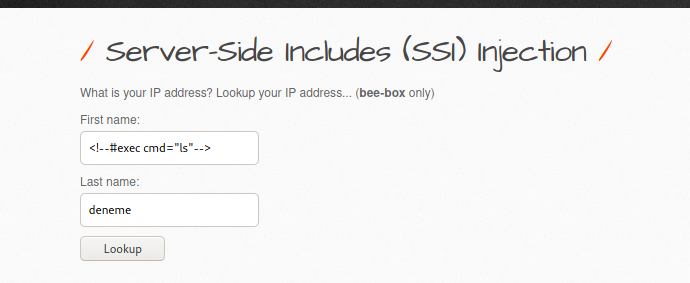


-Zafiyetimin ekranı bu şekildedir.

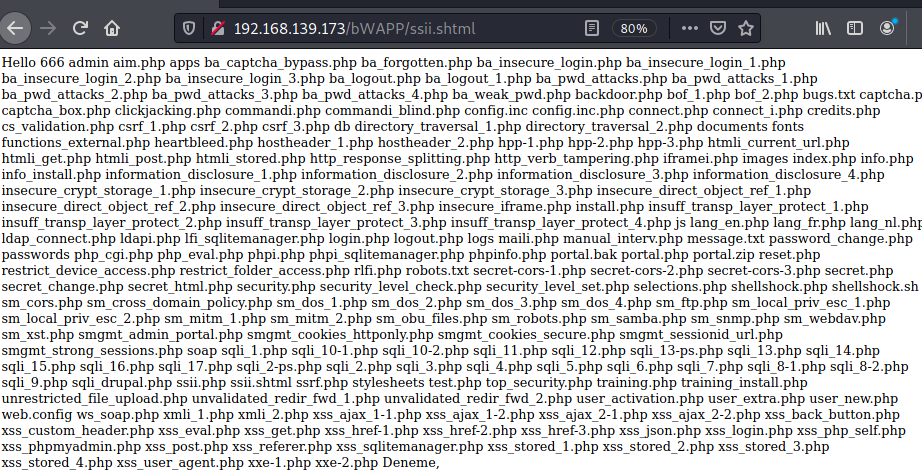


-Bu ekranı doldurup çalıştırdığımda bana böyle bir geri dönüt veriyor.

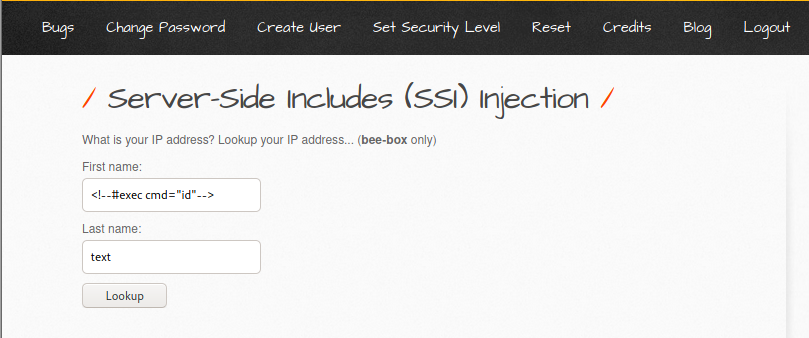
-Eğer burada bir denetleme yok ise burada zafiyet kullanılabilir.



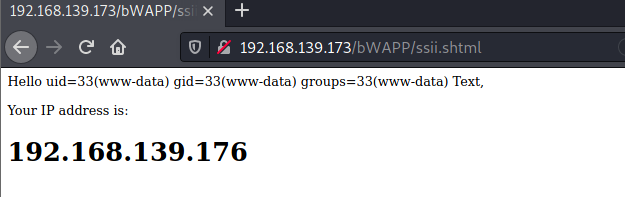
-SSI dili ile yazılmış bir "ls" komutunu deniyorum.



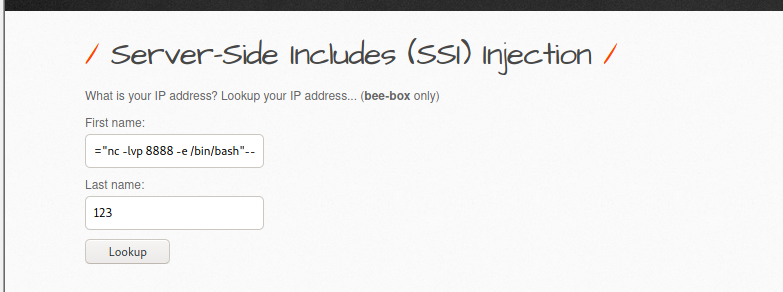
-İçinde bulunan tüm php dosyalarını listeleyebildim.



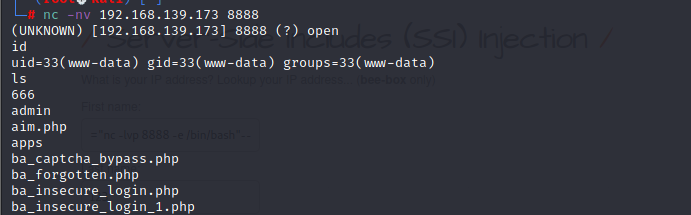
-SSI dili ile yazılmış bir komut ile “ID” komutunu görüntülemeye çalışıyorum.



-Burada bana “ID” ile ilgili bilgiler döndürdüğünü görüntüleyebiliyorum.



-"ID" yerine bir Netcat komutu yerleştirip dinleme işlemi gerçekleştiriyorum.

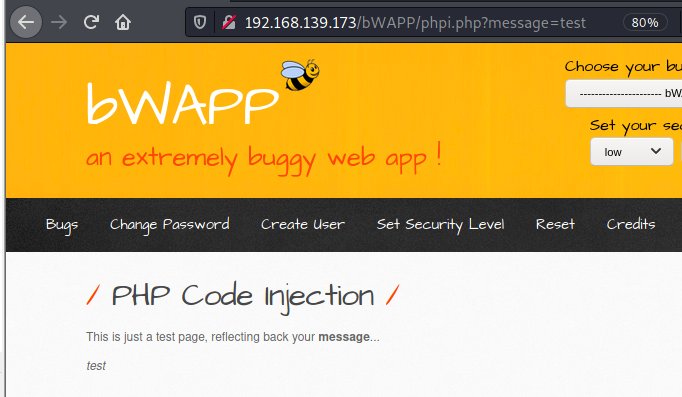


-Ardından Linux makineme geçiş yapıyorum ve burada da “nc“ komutu çalıştıracağım.

-Çalıştırma işleminin ardından hedef sistemi ele geçirebildim.

***PHP Injection***

-Bu zafiyet içinde daha önceden kurulumunu yaptığımız bWAPP laboratuvarını kullanacağız.

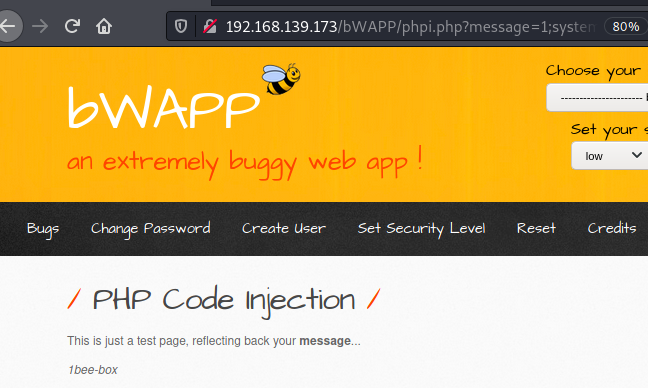


-Bwap üzerinden zafiyetimi başlatıyorum.Zafiyet ekranı bu şekildedir.

- Message bölümüne tıkladığımda zafiyetimin URL kısmı değişmektedir.

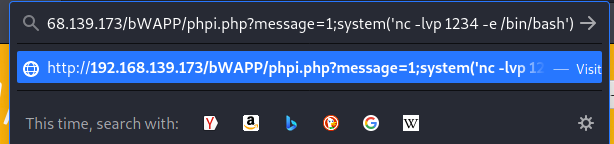


-URL sonuna phpinfo() komutu eklediğimde PHP ile ilgili bilgilere sahip olduğumu görüntülüyorum.

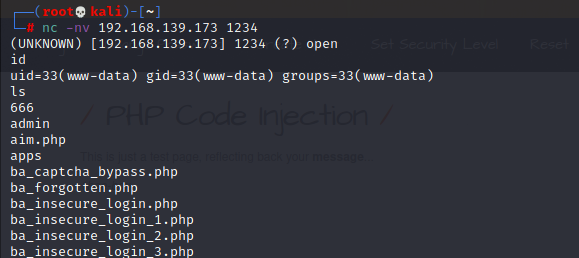


- URL sonuna 1;system('hostname') komutunu ekliyorum ve burada gerekli bilgileri yine döndürebiliyorum.

-Burada “Shell” kullanarak erişim almak istiyorum.



-URL sonuna eklediğim "nc" komutu ile Sunucu üzerinde 1234 portunda bir “Shell” oluşturuyorum.



- Ardından Linux makinesi üzerinden hedef sunucu IP adresi üzerinden “netcat” işlemi ile “Shell” bağlantısı kuruyorum.

-Zafiyetten başarılı bir şekilde yararlandım.Artık istediğim komutu çalıştırabilirim.