|  |
| --- |
| ***bWAPP & Web for Pentester*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Web uygulamaları üzerinde ki zafiyetleri deneyebileceğimiz bir test ortamına ihtiyacımız vardır.Bu ihtiyacı ortadan kaldırmak için bwAPP ve WFP araçlarının kurulum hakkında bilgi vereceğim. |

***bWAPP***

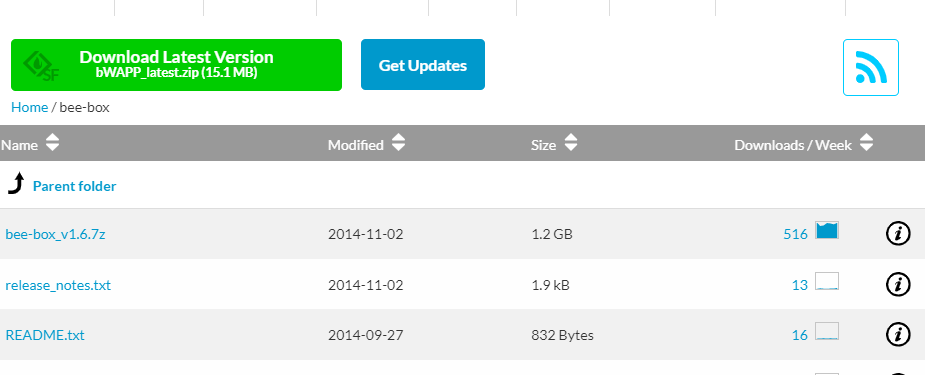
**28.07.2021**

-Açık kaynak kodlu ücretsiz bir web uygulamasıdır.

-Yaklaşık 60 adet güvenlik açığı çeşidi sağlar.

-Sanal makine üzerine kurulum yapılıp basit bir şekilde kullanmaya başlayabiliriz.

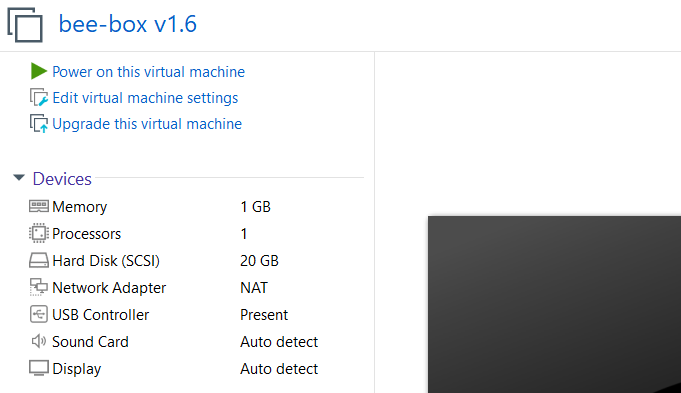
Kurulumuyla başlayalım;



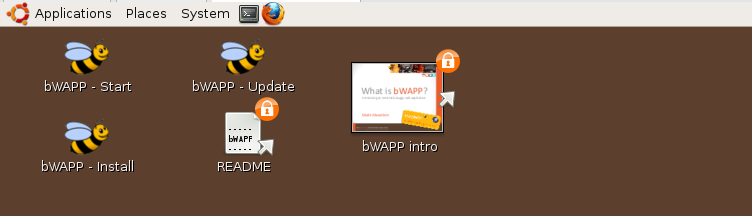
-“ <https://sourceforge.net/projects/bwapp/files/bee-box/>” adresi üzerinden “bee-box\_v1.6.7z” rar dosyasını indiriyoruz.

-İndirdiğimiz .rar dosyasını çıkartıyoruz.Ardından Vmware veya VirtualBox sanallarından birini sanal makine için açıyoruz.Ben VMware üzerinden işlem yapacağım.

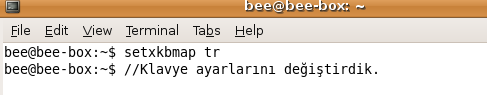
-İndirdiğim dosya kurulum yapılmış haliyle upload edilmiştir.Bu sebeple hiçbir kurulum işlemi yapmadan Vmware üzerinden direk “Open virtual machine” seçeneğini kullanıyorum.İndirmiş olduğum dosyanın içerisindeki “bee-box.vmx” dosyasını açıyorum.



-Vmware üzerinden bu şekilde bir pencere beni karşılayacak,burada yapacağım tek ayar ise “Network Adapter” kısmını Bridged konumuna getirmek olacaktır.Eğer bu ayar yapılmazsa Sanal makinalar arasında bağlantı sağlanamaz.



-bWAPP açıldığında bu ekran beni karşılar.Öncelikle yapacağım işlem konsol kısmına geçip klavye ayarlarımı Türkçeye çevirmek olacak.



“setxkbmap tr” komutu ile aynı Linux platformunda ki komut ile klavyemi Türkçe ayarlara çevirdim.

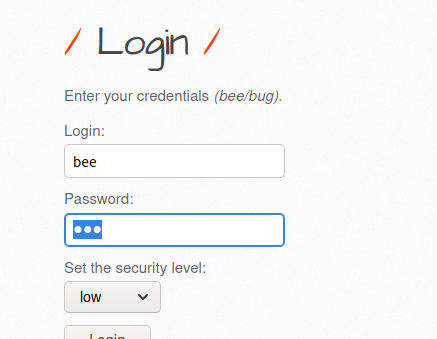


-Ardından diğer sanal makinem üzerinden bağlantı sağlayacağım IP adresini “ifconfig” komutu ile öğreniyorum.

-bWAPP üzerinde yapacağım işlemler sona erdi.Sadece çalışma yaptığım sürece arka plan üzerinde çalışması gerekmektedir.



-Kali Linux makinama geçiş yapıyorum ve ifconfig üzerinden görüntülediğim Ip adresini tarayıcı üzerinden açıyorum.Ardından açılan sayfa üzerinden bWAPP butonuna basıyorum.



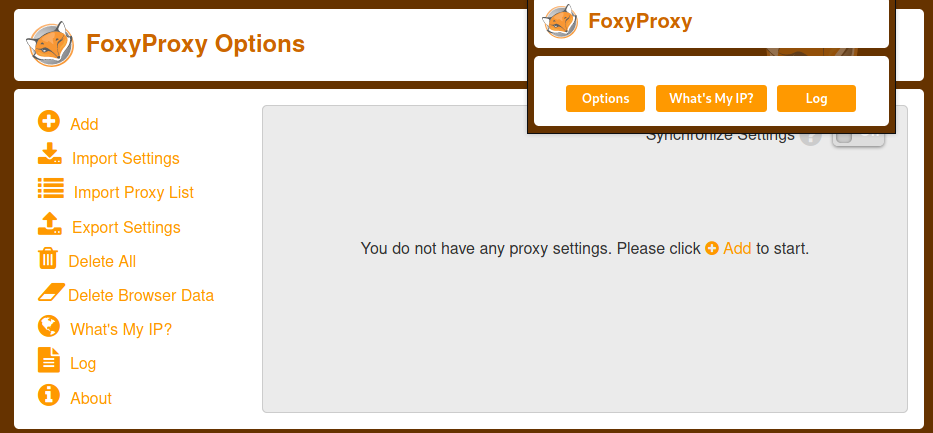
-bWAPP uygulamasını başarılı bir şekilde çalıştırdım.Sıra sisteme giriş yapmakta Default olarak Kullanıcı adı/şifre = bee/bug şeklinde ayarlanmıştır.Sisteme kullanıcı adı ve şifre ile giriş yapıyorum.

-Kurulumum ve ayarlamalarım başarılı bir şekilde ayarlandı artık istediğim zafiyet işlemini gerçekleştirebilirim.

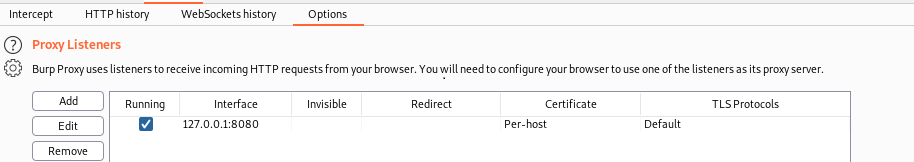


-bWAPP üzerinde çalışma yaparken BurpSuite uygulamasın çok fazla kullanacağız sürekli proxy ayarı değiştirmek yerine Firefox üzerine “FoxyProxy” eklentisini ekliyorum.

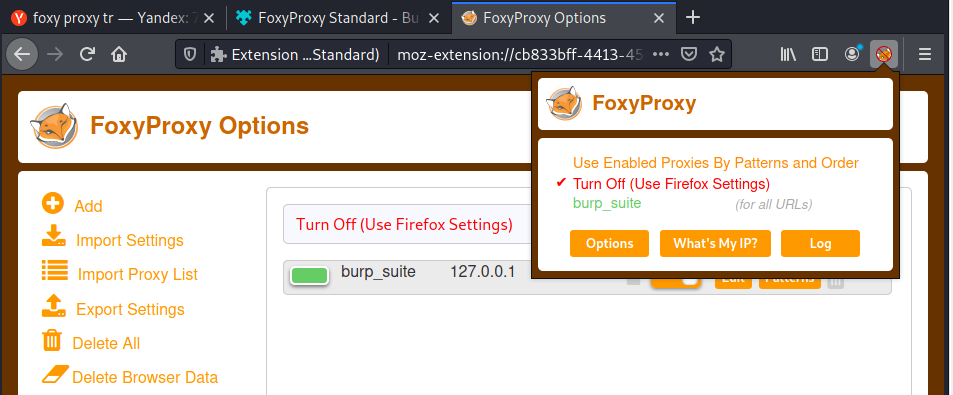
-Bu eklentiye Firefox FoxyProxy araması sonucu erişim sağlayabiliriz.



-Foxyproxy eklentisine geçiş yapıyorum ve Options bölümüne geçiş yapıyorum.



- Burpsuite uygulamasında Proxy bölümünden ayarlamış olduğum IP ve Port numarasını FoxyProxy Options bölümünden ekliyorum ve kaydediyorum.



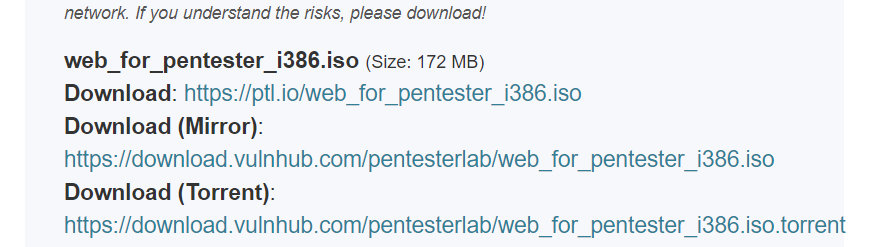
-Artık Burpsuite üzerinden işlem yaparken sürekli proxy değiştirmeme gerek kalmadan,icon üzerine basıp burp\_suite proxysini aktif ederek işlem yapabilirim.

-Detaylı kullanımını yapacağımız injection örneklerinde inceleyeceğiz.

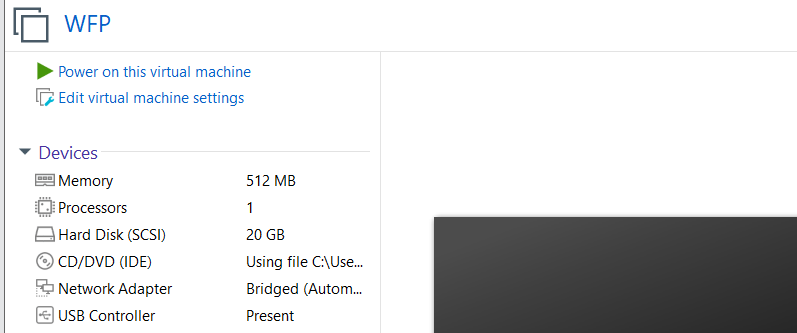
***Web for Pentester***

-Sanal makine üzerinden hiçbir kurulum gerektirmeksizin XSS,SQL,LDAP gibi popüler zafiyetler üzerinden çalışmamızı sağlayan bir web uygulama aracıdır.

Kurulumuna geçelim;

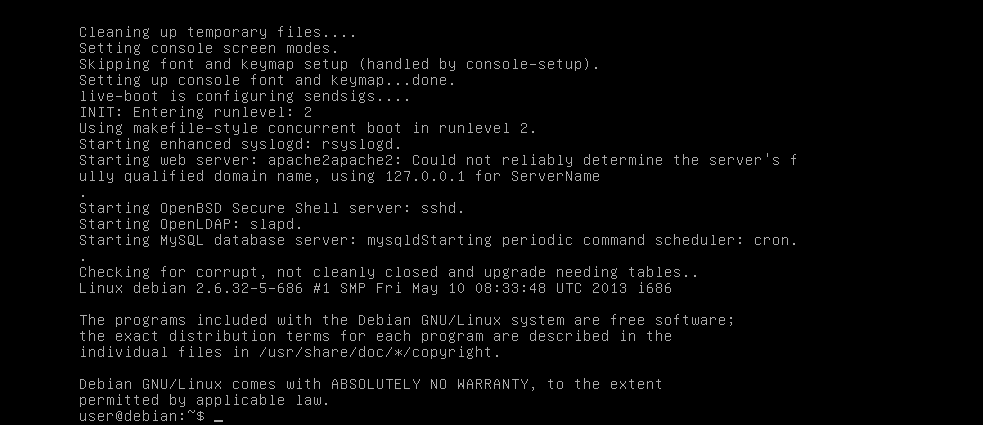


-“https://www.vulnhub.com/entry/pentester-lab-web-for-pentester,71/” bağlantısı üzerinden mirror ve i386 işlemcisiyle kullanılan versiyonunu indiriyoruz.



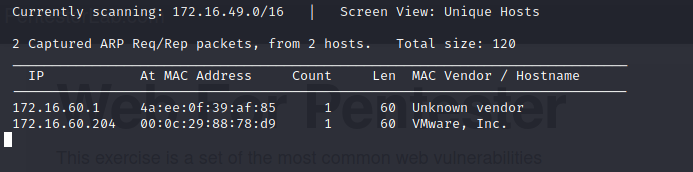
-Ardından Vmware veya VirtualBox üzerinden “New Virtual Machine” diyerek sanal makine kurulumu gerçekleştiriyoruz.

-Vmware üzerinden bu şekilde bir pencere beni karşılayacak,burada yapacağım tek ayar ise “Network Adapter” kısmını Bridged konumuna getirmek olacaktır.Eğer bu ayar yapılmazsa Sanal makinalar arasında bağlantı sağlanamaz.

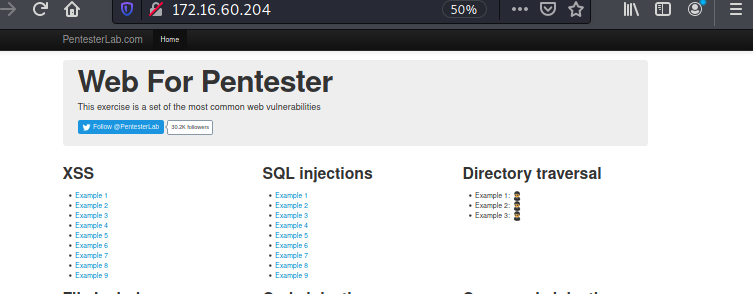


-WFP aracını çalıştırdığımda karşıma böyle bir ekran gelecektir.WFP üzerinde yapacağım işlemler bu kadardır ve çalışma yapacağım sürece arka planda çalışması gerekmektedir.

-Kurulum işlemlerinin ardından Linux makinem üzerinden bağlantı kurma işlemini birlikte yapalım.



-Linux makineme geçiş yapıyorum ve uçbirim üzerinden “Netdiscover” komutunu çalıştırıyorum.Hostname ismi “VMvare,Inc.” olan IP numarası WFP makinesinin numarasıdır.



-Ardından bu IP numarasını tarayıcı üzerinden çalıştırdığımda WFP ile Linux makinem arasında bağlantıyı başarılı bir şekilde sağlamış bulunmaktayım.