Web_sec

Web güvenliği üzerine oluşturulmuş içirisinde çeşitli zaafiyetlerin bulunduğu bir sistemdir.

Bu proje siber güvenlik alanında lise öğrencilerinin ilgisini çekmek, bu alana yönlendirmek ve farkındalık oluşturmak için en basit haliyle oluşturulmuş bir sitedir.

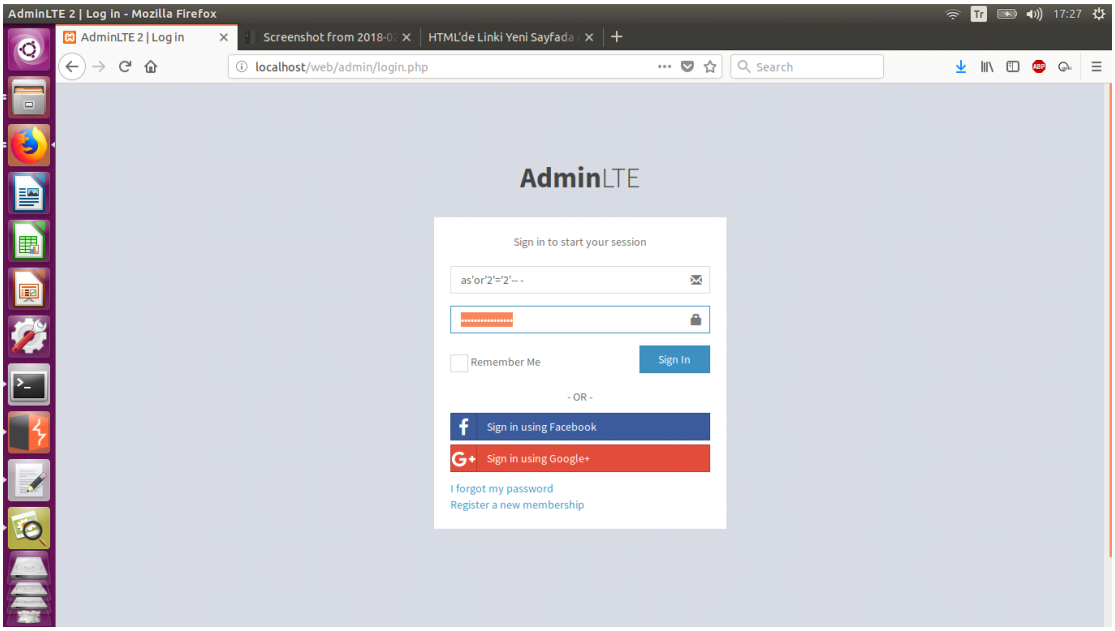
İçerisinde

1. Sql injection
2. Broken Authentication
3. XSS(Cross-Site Scripting)
4. RCE(Remote Command Execution)
5. File Upload
(zaman içerisinde fırsat buldukça ekleme yapmaya çalışacağım)

bulunmaktadır.

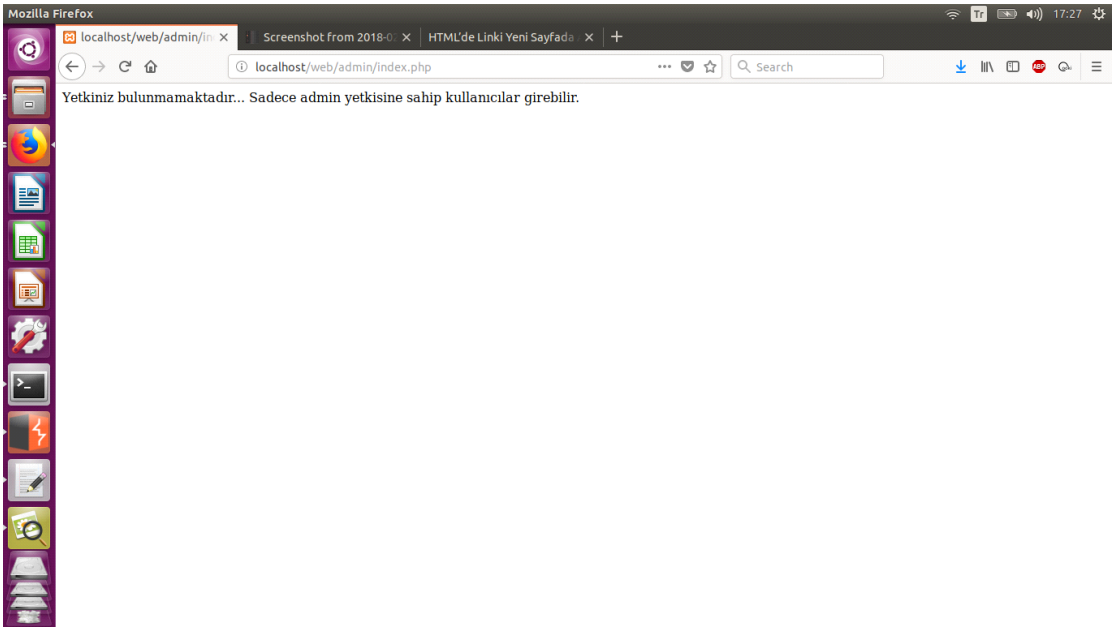
1.Sql injection

Giriş paneli üzerinden kullanıcı adı veya password inputu ile zafiyet exploit edilir.

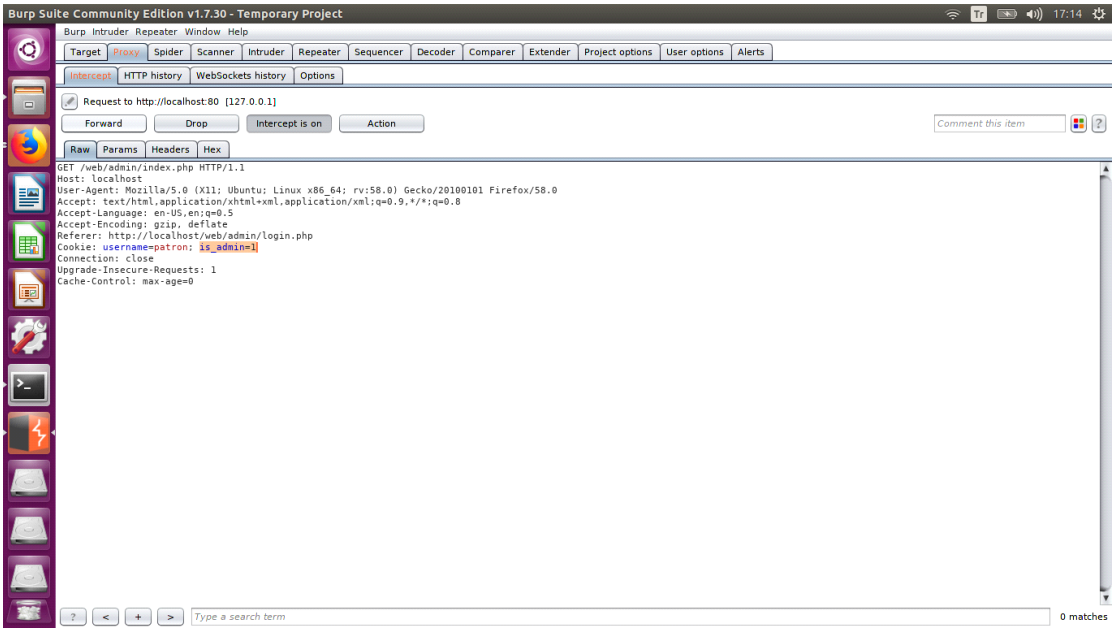


2.Broken Authentication

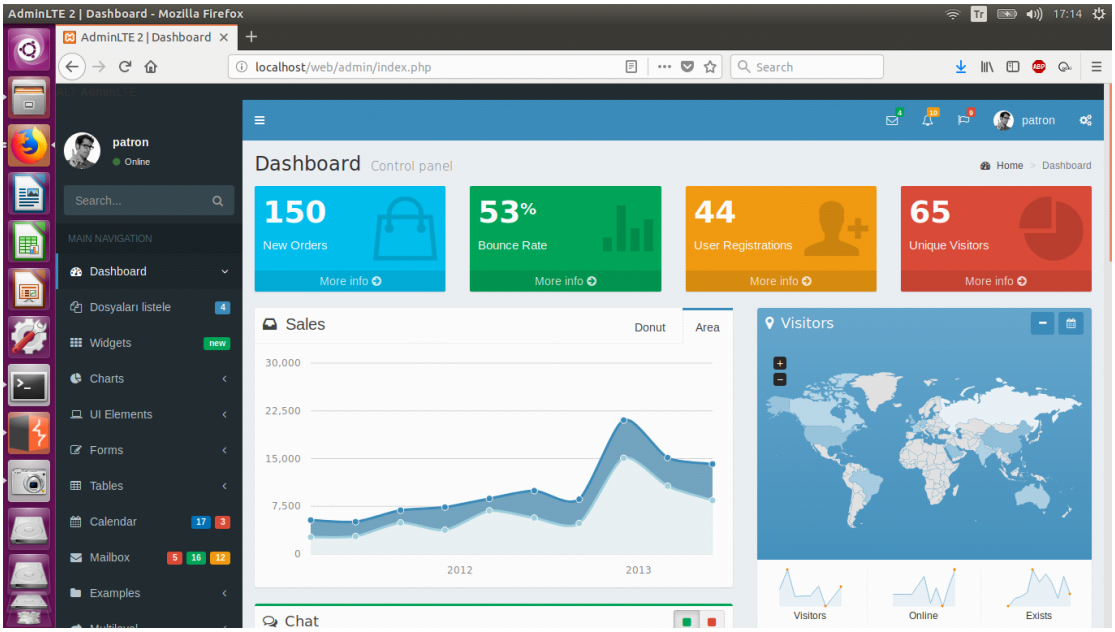
sistem üzerinde hem admin hemde user haklarına sahip kullanıcılar vardır.Sql injection ile girildiğinde normal kullanıcı olarak girmekte.Admin paneline girmemize yetkimiz olmadığı için oturum kapatılmakta.Burada kendimizi admin olarak göstermemiz gerekmekte.



Burpsuite veya benzeri bir araç ile araya girdiğimizde is_admin parametresi ile 0 göndermekte.Admin ve user yetkisini cookie üzerinden yaptığından bu parametre değiştirilerek (is_admin=1) admin olabiliriz.



İstegi forward ettiğimizde bizi direk admin paneline yönlendirmektedir.



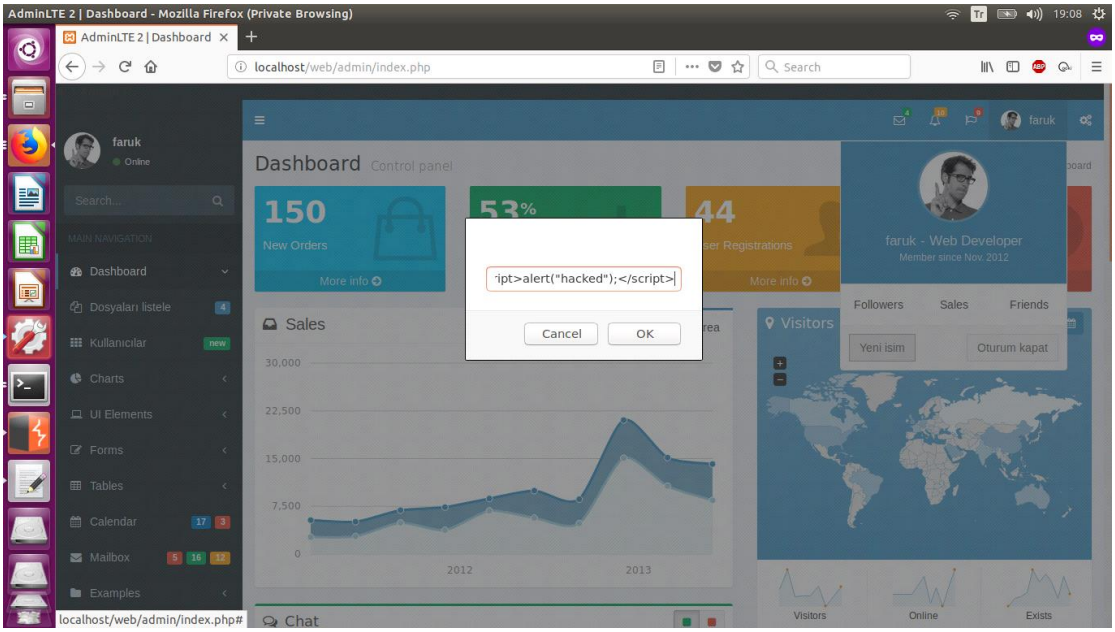
parolayı bilmediğimiz halde sistem üzerinde admin olarak oturum elde etmiş olduk.

3.XSS(Cross-Site Scripting)

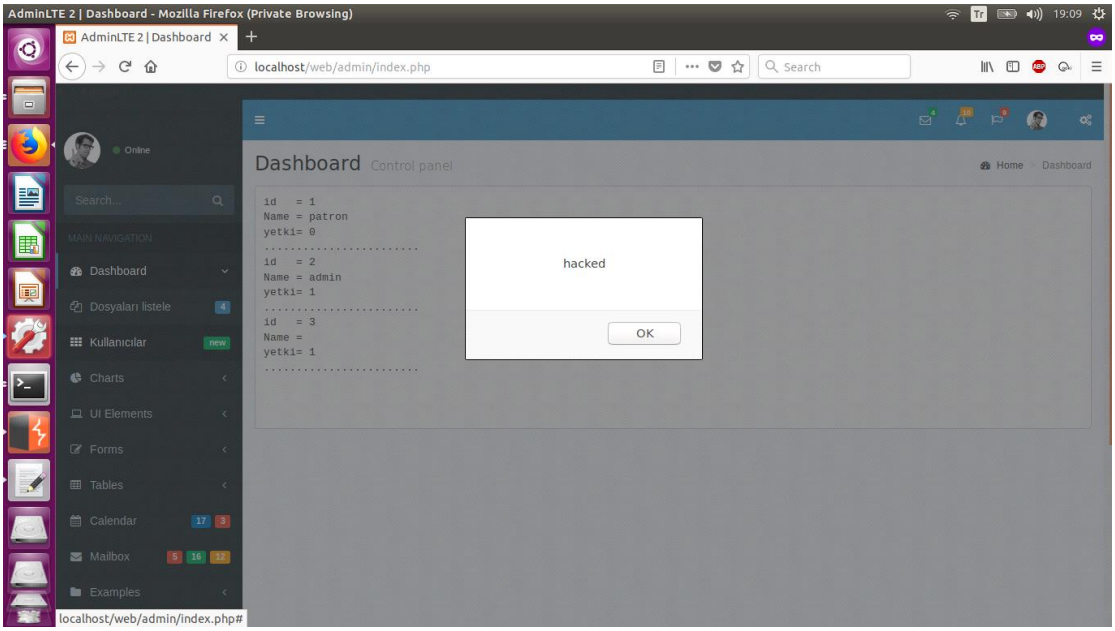
Xss, web sayfalarında javascript kodu enjekte edilerek çalıştırılmasıdır.Xss ile kullanıcı bilgileri çalınabilinir, phishing saldırıları yapılabilinir, site içerisine kod enjekte edilerek farklı sitelere yönlendirme yapılabilinir.Site içerisine keylogger atılabilinir.Var olan bir Xss açığı ile bir çok şey yapılır tamamen bu açığı bulan kişiye ve hayal gücüne bağlıdır.

Bizim sistemimizde kullanıcı adı değiştirdiğinde her hangibir önlem alınmadan yeni isim direk alınmaktadır ve alınan isim ekrana direk yazılacağından xss zafiyeti oluşur.

İlk resimde saldırgan yeni isim kısmına zararlı kod yazmakta

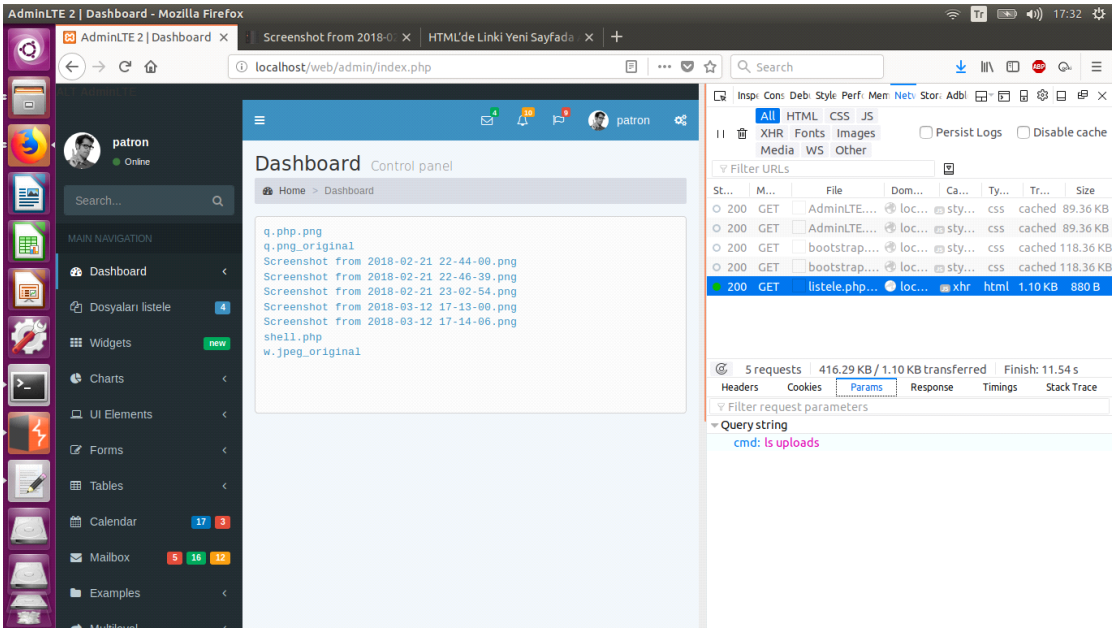


ikinci resimde başka bir tarayıcıda admin oturum açmış durumda.Kullanıcıları listeleme kısmında kullanıcı adı yerine yazılan script çalışacaktır.

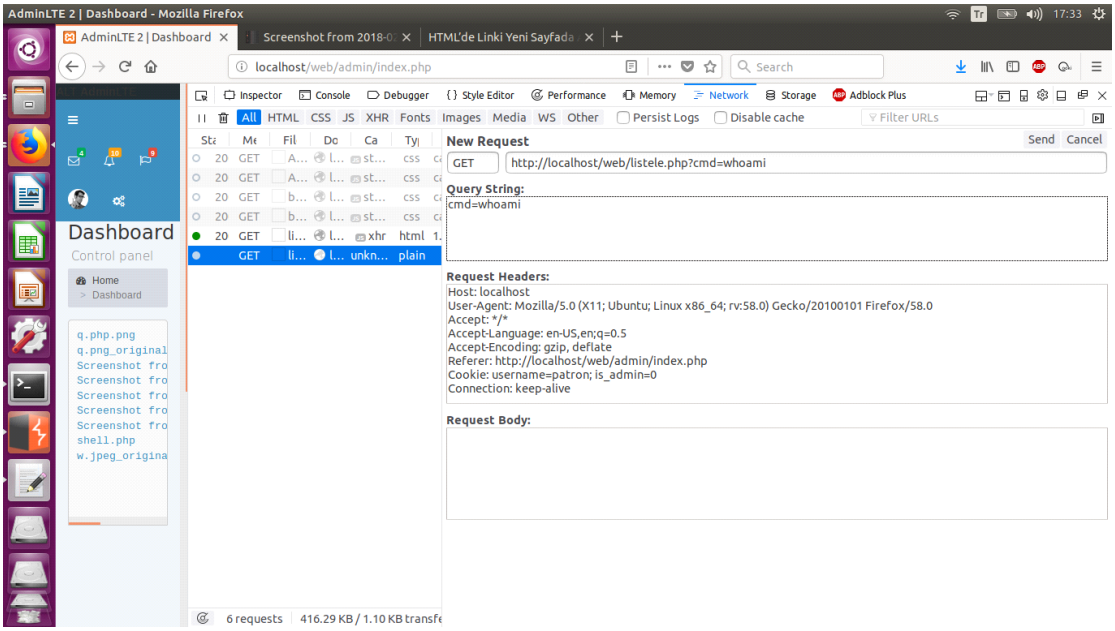


4.RCE(Remote Command Execution)

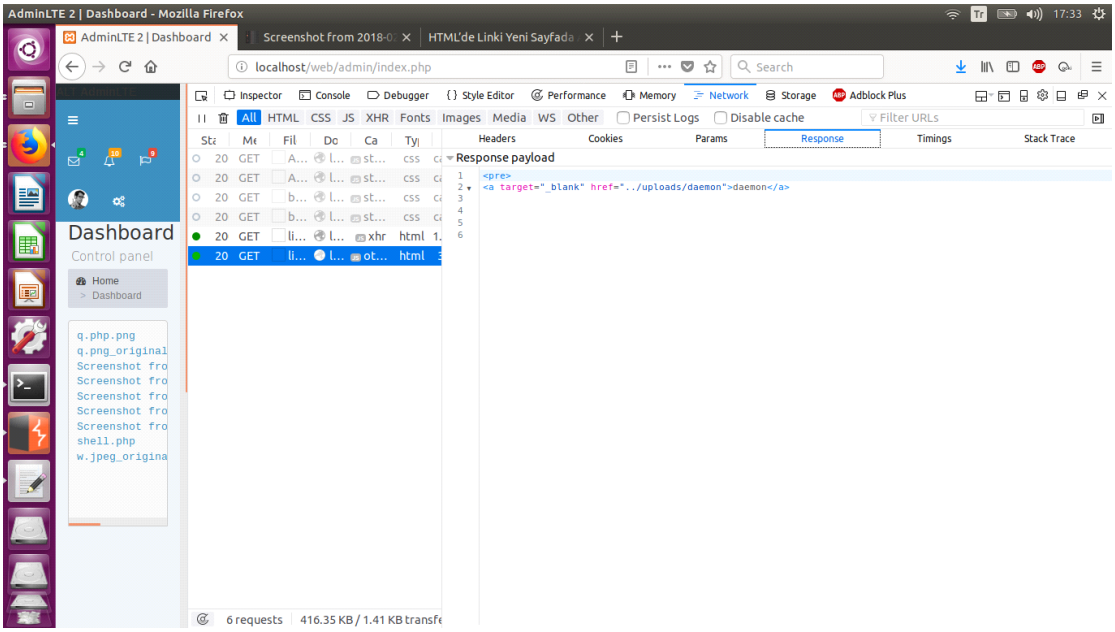
Sunucu üzerinde işletim sistemi kodu çalıştırabilme zafiyetidir.En tehlikeli açıklardandır.Sitede Dosyaları listele dediğimiz sekmede "ls uploads" komutunu çalıştırarak sunucu üzerindeki dosyaları listelemektedir.Sayfa isteklerinin arasına girerek komutu değiştirdirerek istediğimiz komutu çalıştıracağız



F12 ye basıp network sekmesini seçerek yapılan isteklerden GET ile gönderilen "ls uploads" değerini değiştiriyoruz.



Dönen değer

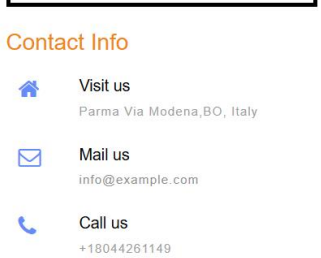


whoami komutu ile komutu çalıştıran kullanıcın ismini vermektedir.
Bu sistemede biz daemon olarak oturum açmış bulunmaktayız.whoami yerine yazacağımız komutlar ile sisteme reverse veya bind bağlantısı yaparak bağlantı sağlayıp daha fazla sisteme sızabiliriz.

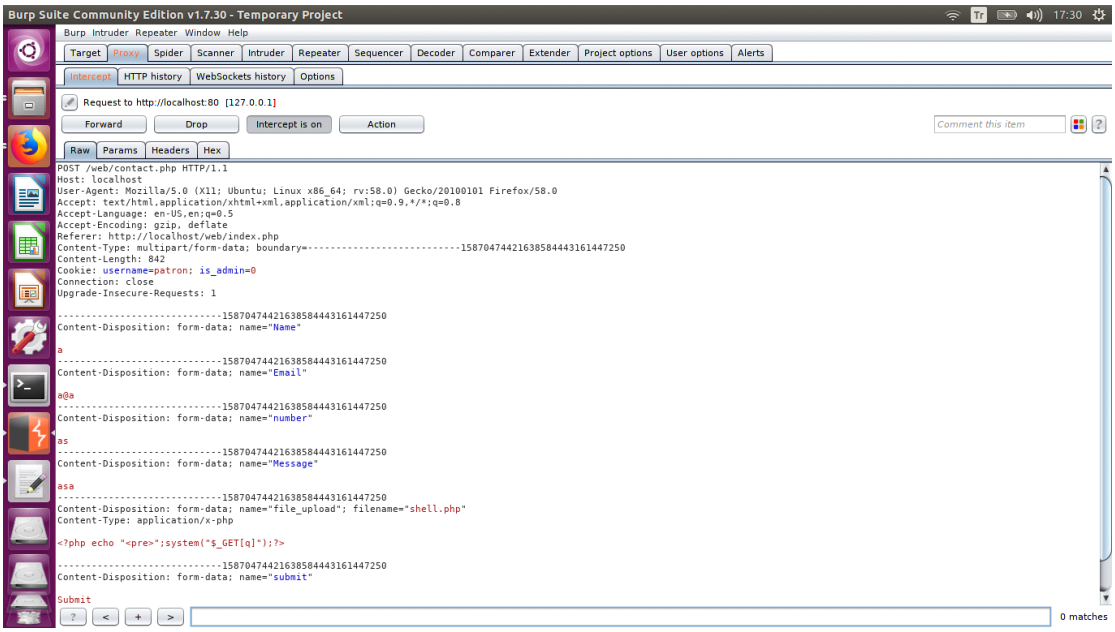
5. File Upload

File upload zafiyeti normalde sistem bize kendi istediği dosyaları yükleyebilmemiz için dosya yükleme sayfası oluşturmuştur.Biz bu sayfa üzerinden sunucudaki güvenlik önemlerini atlatarak kendi istediğimiz shell dosyalarını sunucuya yükleyeceğiz.

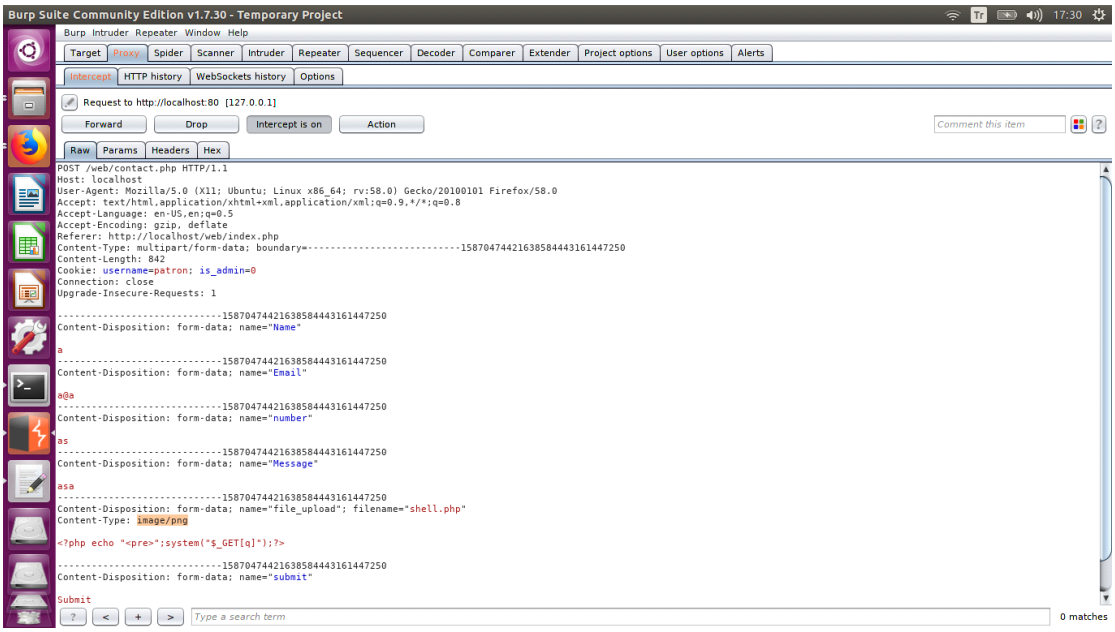
Normal resim dosyası yüklendiğinde sıkıntı yok direk yükleniyor ama php dosyası yüklemeye çalıştığımızda yüklenmemektedir.



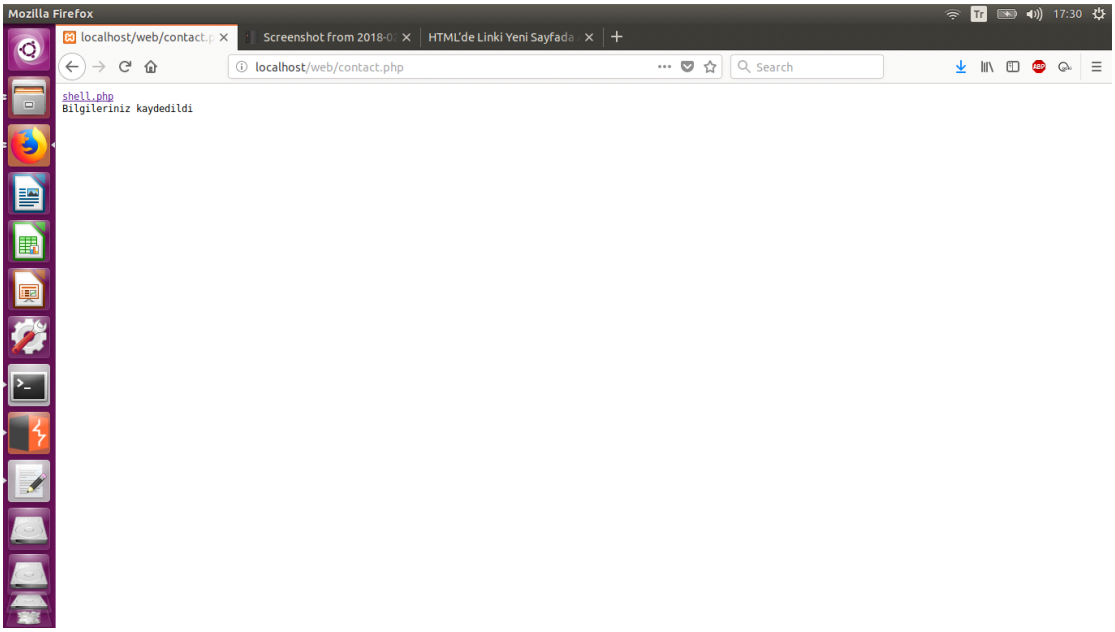
Burp ile araya girip bilgileri kontrol ediyoruz.



Content-type kısmı dosyanın türünü belirtir.

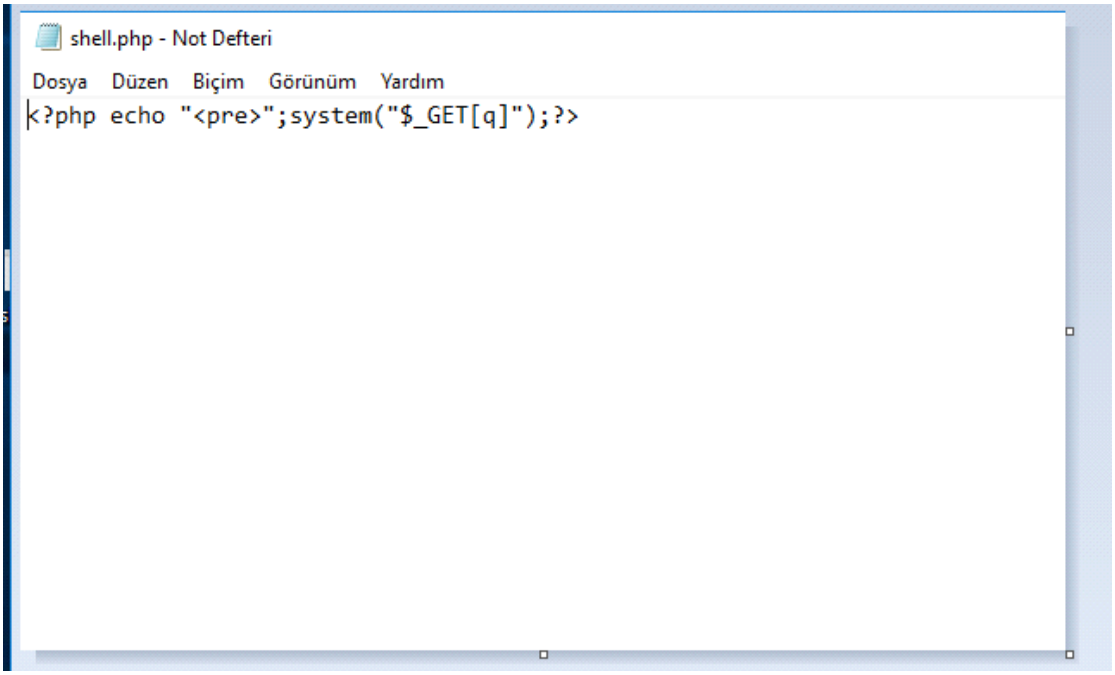


application/x-php olan kısmı image/png yaparak php dosyasının resim dosyası olduğunu söylüyoruz.

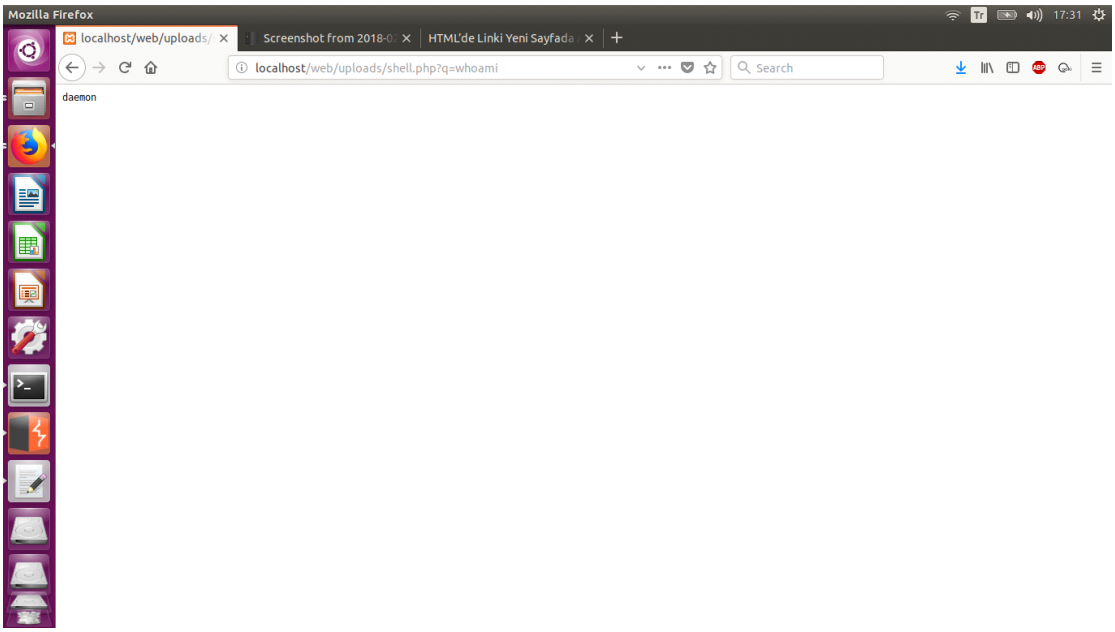


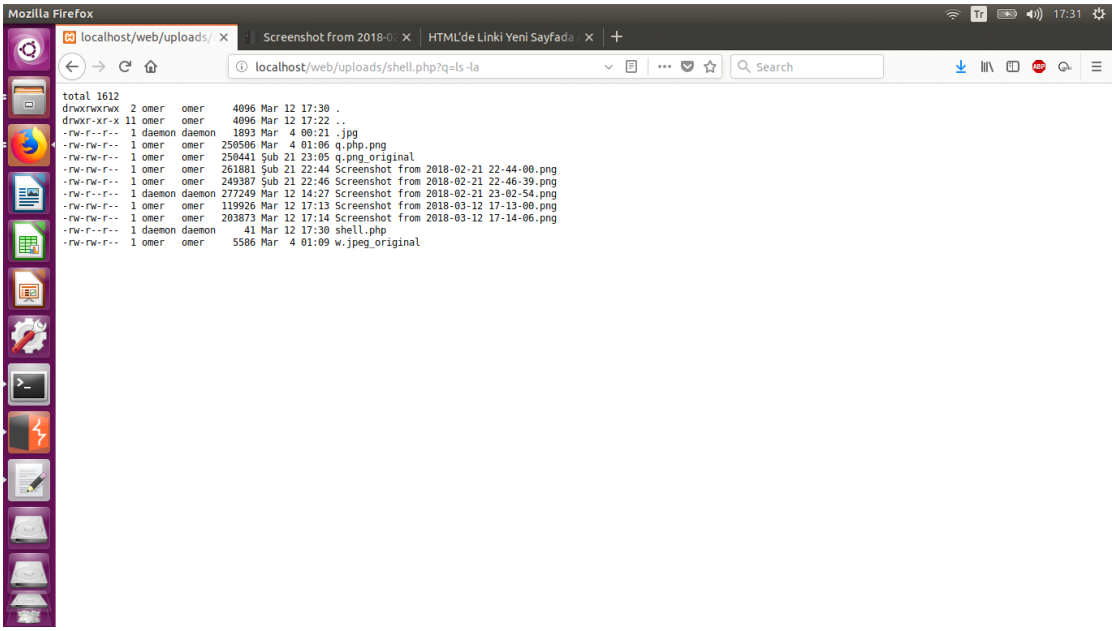
ve dosyamız başarılı bir şekilde yüklendi.

Php dosyasının içeriği en basit hali ile kod çalıştıracak şekilde yazıldı.
$_GET sayfaya GET methodu ile yapılan istekleri almak için kullanılacak.
system() fonksiyonu içerisine yazılan komutu çalıştırıp çıktıını ekrana basar.
<pre> ile çıktıların daha okunaklı şekilde yazılmasını sağlayacaktır.



http://…/shell.php?q= eşittirden sonra yazacağımız her kod sunucuda çalıştırılacak ve çıktısı verilecektir.





Bu zafiyetler dışında robots dosyası üzerinden okuma yapılarak önemli bilgilerde okunabilinir.Dikkatsizlik, dalgınlık yada daha önemli durumların arasında göze çarpmamasından dolayı yedek dosyaları, config dosyaları içerisinde önemli bilgilerin bulunduğu dosyalar sunucular üzerinde kalabiliyor.

Tamamen güvenli, %100 güvenli diye birşey yoktur.Her zaman bir zafiyet olabileceğini hiç bir zaman unutmamalıyız.Bizim işimiz tüm noktaları kapatmak ama hackerların tek bir açık bulması yeterli.

Bu site ufak bir çalışma daha iyisi olabilirdi.Üstüne ekleyip düzelterek daha iyi konuma getirebilecek zaman inşallah olur.

Ömer Faruk GERİŞ

https://twitter.com/OmerFarukGeris