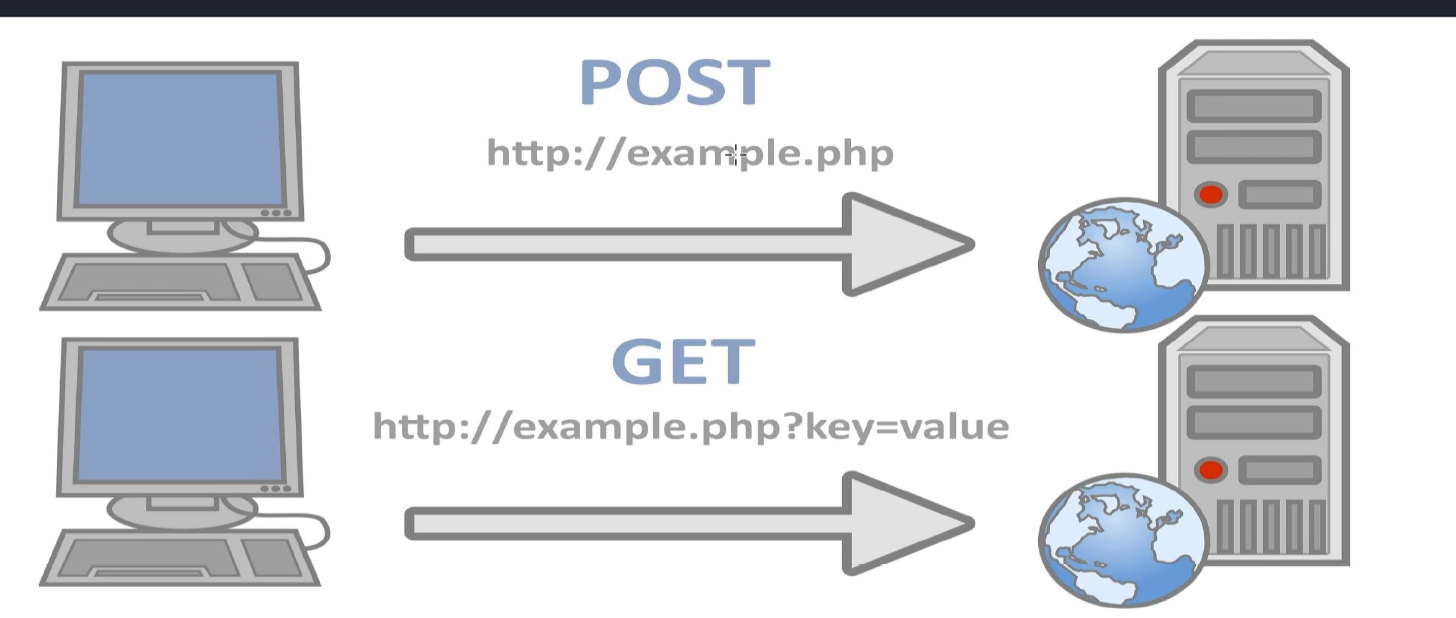
|  |
| --- |
| ***Doğru metod ve kod kullanımı*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| Doğru HTTP metod kullanımı ve Command Injection,SQL Injection,XSS açıklarını önleyecek kod eklentilerine birlikte bakacağız. |

**02.11.2021**

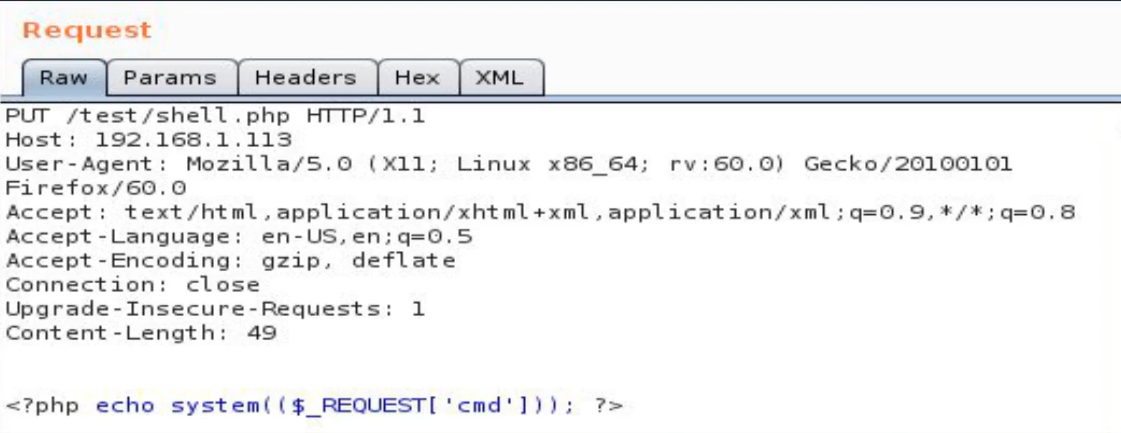
HTTP METODLARI

-Wireshark üzerinden işlem yaptığımızda Get-Post gibi metodlar kullanılmaktadır.



-Bir şema üzerinde göstermek gerekirse bu şekilde gösterebiliriz.

-Post metodu Get metoduna göre bilgiler URL üzerinde gizli tutulduğu için daha güvenlidir.



-PUT metod Servis sağlayıcı üzerindeki bir kaynağı güncelleyebilmemize olanak sağlar.

-Hedef sunucuda ki bir dosyanın içeriğine erişim gerçekleştirip değişime uygulatabiliriz.

-Delete Metodu - > Sunucuda ki herhangi bir veriyi silebiliriz.

-Options -> Belli bir kaynak için kullanılabilecek HTTP metodlarını sunucudan sorgulamak için kullanılır.

-Trace -> Sunucu bu metodla gelen istek mesajının içeriğini aynen yanıt gövdesinde geri göndermelidr.

-Eğer bir vekil sunucu var ise yaptığı değişiklerin tespiti mümkün olabilir.

HTTP Request



-Farklı bir sayfaya geçiş yapmaya çalıştığımızda Request göndeririz.Sayfada ki her değişiklik requesttir.

Request Değerleri

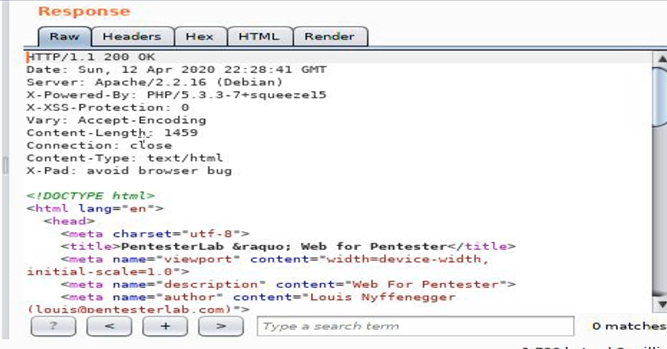
-Accept-HTTP Header => İstemci ne tür dosyaları işleyebileceğini sunucuya bildirir.Sunucu elinde bu türden kaynak varsa gönderir.

-Sunucu veriyi gönderirken Content-Type alanını doldurur.

-Content-Length = > Alıcıya gönderilen ondalık sekizli sayı cinsinden varlık gövdesinin boyutunu belirtri.

-User-Agent => İşletim sistemi bilgisi,kullanılan tarayıcı bilgilerini verir.

-Cookie => Daha önce sunucu tarafından başlık ile gönderilen depolanan HTTP tanımlama bilgilerini içerir.



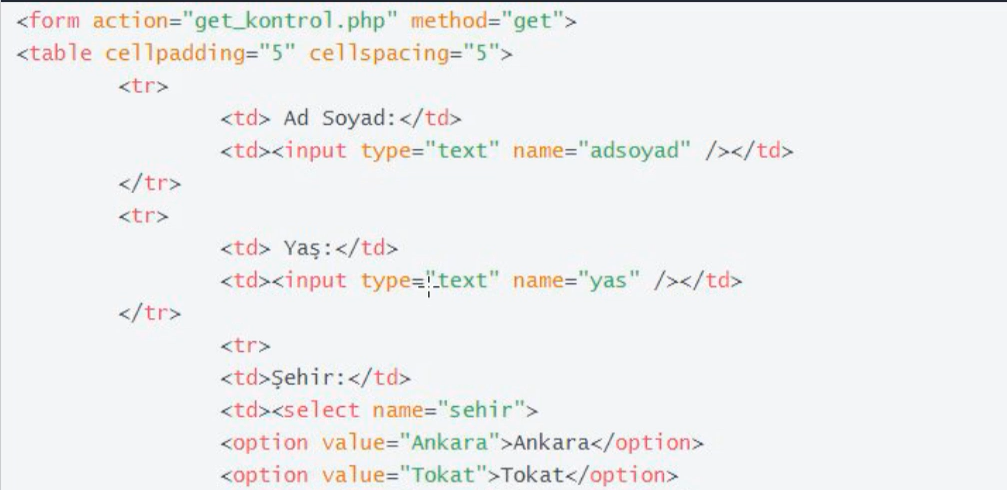
Her request'in bir response'u vardır.

-Burada 200'lü kod dönmesi olumlu olduğunu anlamına gelir.

Response değerleri

Server => Hedef sunucuda kullanılan işletim sistemi ve sürüm bilgisini verir.

X-Powered-by => Hangi yazılım dilinin kullanıldığı ve yazılım dilinin sürüm numarasını verir.



-GET ile gönderilen veriler

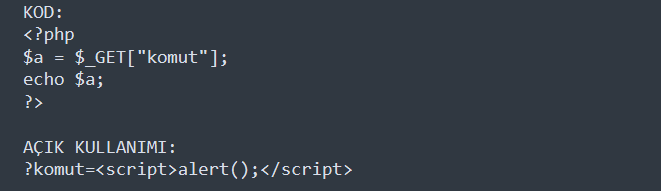


-POST ile gönderilen veriler

-Verileri POST üzerinden göndermek çok daha güvenilirdir.

Basic Kaynak Kod Analizi

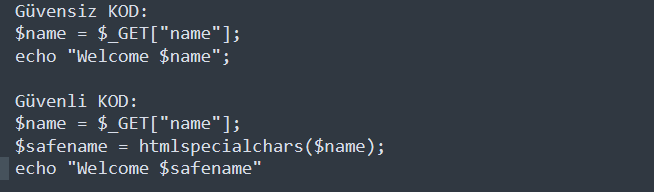
XSS



-Burada $\_GET[] ile alınan değer kontrol edilmeden alınmış.Yukarıda index.php?komut=selam yazılırsa ekranda selam yazısı çıkar

-Yazdığımız scriptte Alert içerisinde session,cookie bilgilerine erişebilir ve kullanıcı bilgilerini çalabiliriz.

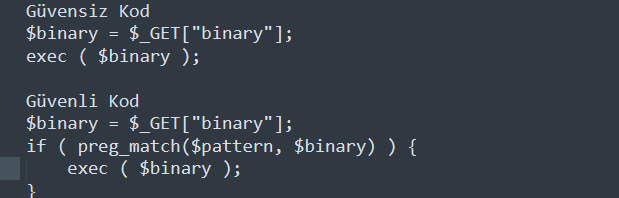
-Bu açığı kapatmanın yolu ise çok kolay.Ekrana yazarken "htmlspecialchars" ile yazarsak,HTML ifadelerine karşı koruyucu önlem almış oluruz.



-Örnek üzerinde göstermek gerekir ise kod yazımı bu şekilde olursa bu açık kapatılabilir.

COMMAND INJECTİON

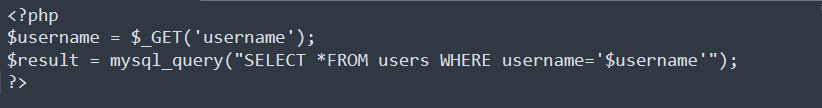
-Kodlarda bulunan açık sayesinde sisteme yüklediğimiz bağlantılar üzerinden elde ettiğimiz zafiyettir.



-Örnekte gösterdiğim gibi basit bir şekilde bu açık kapatılabilir.

SQL INJECTİON

-Bir uygulamanın bir kullanıcıdan girdi aldığı ve kullanıcının ek olarak girdiye sql komutlarını dahil edebilmesi sonucu elde edilen zafiyettir.



-Doğru kod yazımı