Apache Fingerprinting Engelleme Ayarı

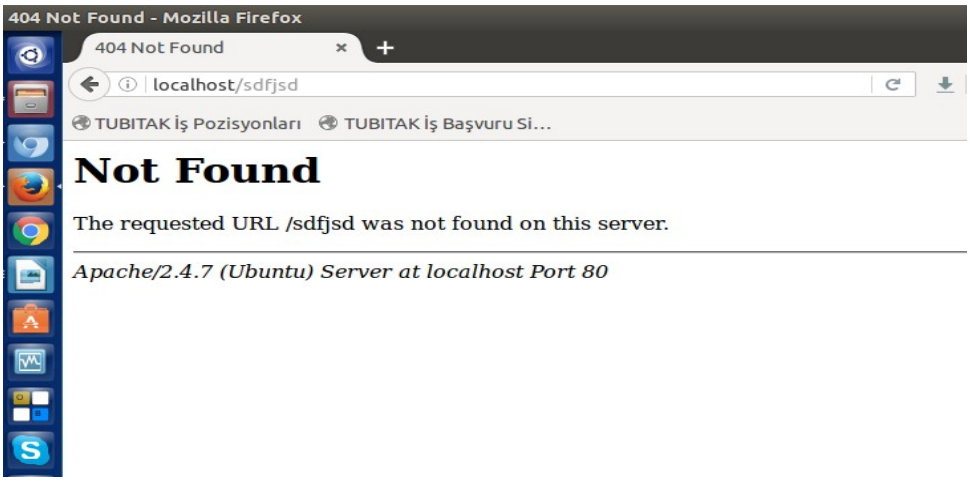
(+) Denendi ve başarıyla uygulandı.

Apache yazılımı kullanan bir web sitesinin olmayan bir dizinine bağlanmaya çalıştığımızda normal koşullarda 404 Not Found hatası alırız. Ancak bazen bu hatanın yanında bir de web sunucuda çalışan web server yazılımının bilgisini, hatta web sunucuda çalışan işletim sisteminin bilgisini alabiliriz. Veyahut siteye bağlandığımızda karşılığında aldığımız HTTP Response paketinin header'ında da aynı bilgileri alabiliriz. Peki bunları nasıl engelleyebiliriz? Bu yazı bunu konu edinmektedir.

a. Hata Sayfalarındaki Bilgi İfşasını Durdurma

Olayı simule etmek için apache kullanan yerel sunucumuzu ele alalım. Örneğin localhost'umuzda olmayan bir dizine aşağıdaki gibi bağlanmaya çalışalım:

http://localhost/sdfjsd



Görüldüğü üzere olmayan bir dizine bağlanmaya çalıştığımızda 404 hatası aldık. Aynı zamanda 404 hatasının aşağısına bakacak olursanız Apache/2.4.7 ve Ubuntu bilgilendirmelerini de aldık. Yani yerel web sunucumuz apache, kendi ismini ve versiyonunu bildirdiği gibi bir de üzerinde koştuğu işletim sisteminin ismini de bildirmiş. Eğer piyasadaki bir web sunucusunda çalışan apache yazılımı bu bilgileri bizde olduğu gibi verirse saldırganlar aldıkları bu veriler ışığında piyasada spesifik exploit aramalarında bulunabilir ve sunucuya sızabilirler. Dolayısıyla bu bilgi ifşasının sonlandırılması için apache'nin *security.conf* dosyasında ufak bir değişiklik yapmamız gerekmektedir. Bunun için aşağıdaki kodlamaları terminale girelim.

```
> sudo su
> gedit /etc/apache2/conf-enabled/security.conf
```

Açılan not belgesindeki

```
#ServerSignature Off
ServerSignature On
```

kısmını aşağıdaki gibi yapalım.

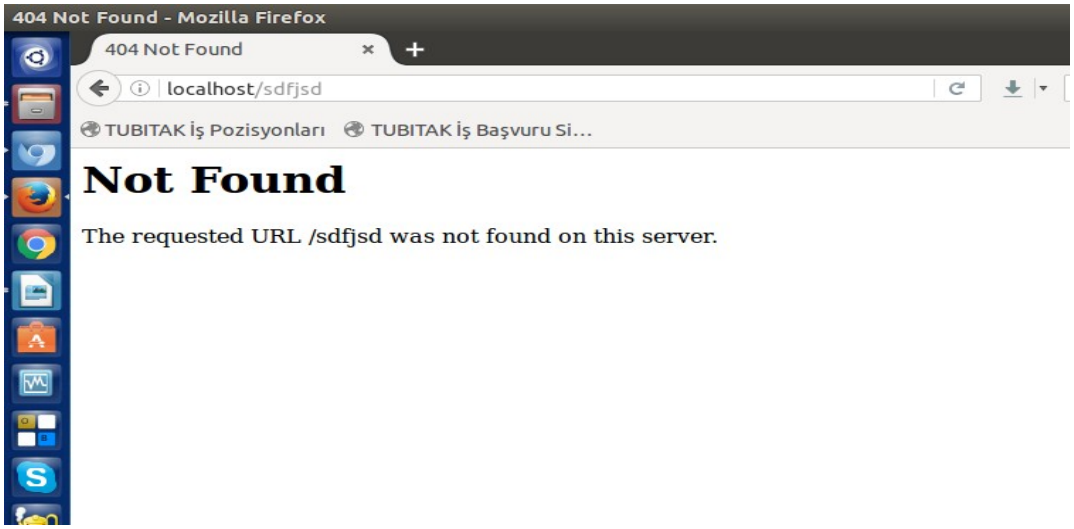
```
ServerSignature Off
#ServerSignature On
```

Ardından apache'yi restart'layalım.

```
> service apache2 restart
```

Böylece sunucu imzasını ifşa etme olayını kapatmış olduk. Yani sunucunun vereceği 404 gibi hata sayfalarında sunucuda koşan yazılım bilgilerinin verilmesine son vermiş olduk. Şimdi tekrar localhost'umuzdaki olmayan bir dizine bağlanmaya çalışalım ve farkı görelim:

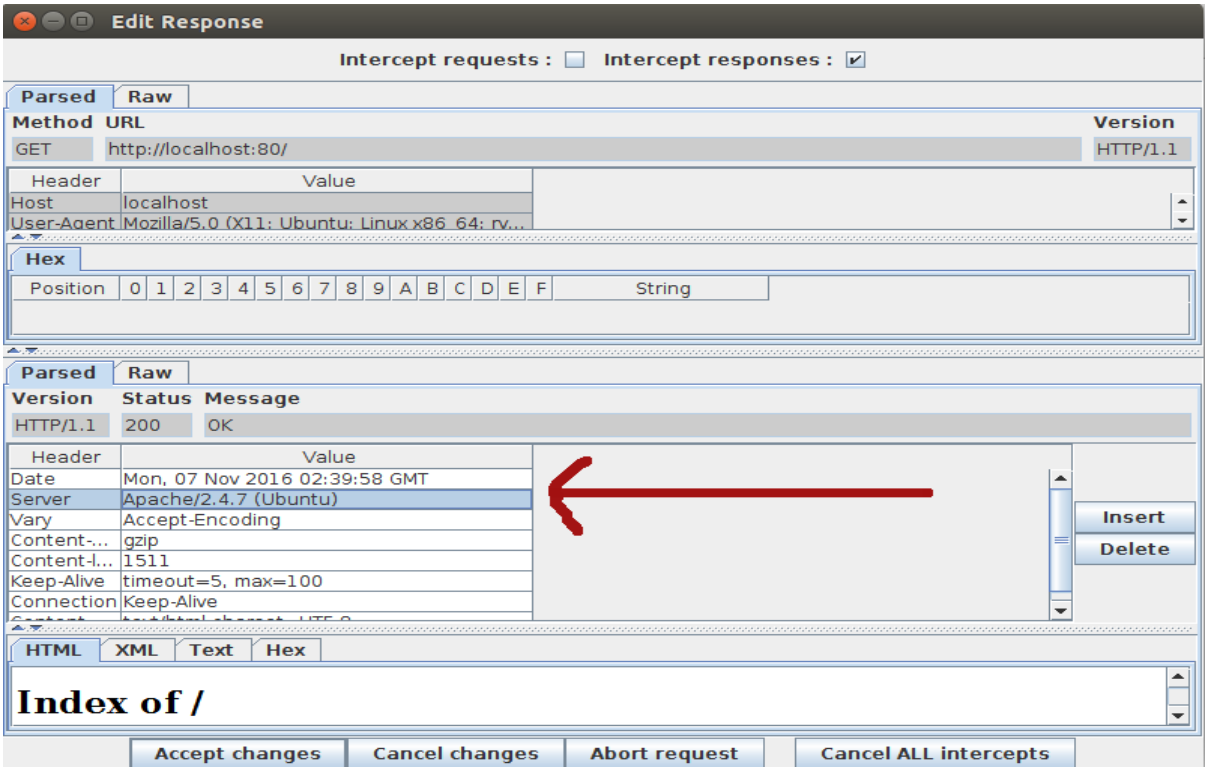
```
http://localhost/sdfjsd
```



Görüldüğü üzere alt taraftaki web sunucu ismi ve işletim sistemi ismi ifşası ortadan kalkmış durumdadır.

b. HTTP Response Header'ındaki Bilgi İfşasını Durdurma // “Server” adlı headerı durdurma

Bir diğer bilgi sızdırdığımız nokta Http Response header'larıdır. Örneğin localhost'umuza bağlanmaya çalıştığımızda Webscarab ile Http Response'un önünü kesersek



Server header'ının Apache/2.4.7 (Ubuntu) ifşasında bulunduğunu görebiliriz. Bu header bilgisinin istemcilere minimum bilgi vermesini sağlamak için tekrar security.conf dosyasına dönmemiz gerekir.

> sudo su
> gedit /etc/apache2/conf-enabled/security.conf

Açılan metin belgesindeki

#ServerTokens Minimal
ServerTokens OS
#ServerTokens Full

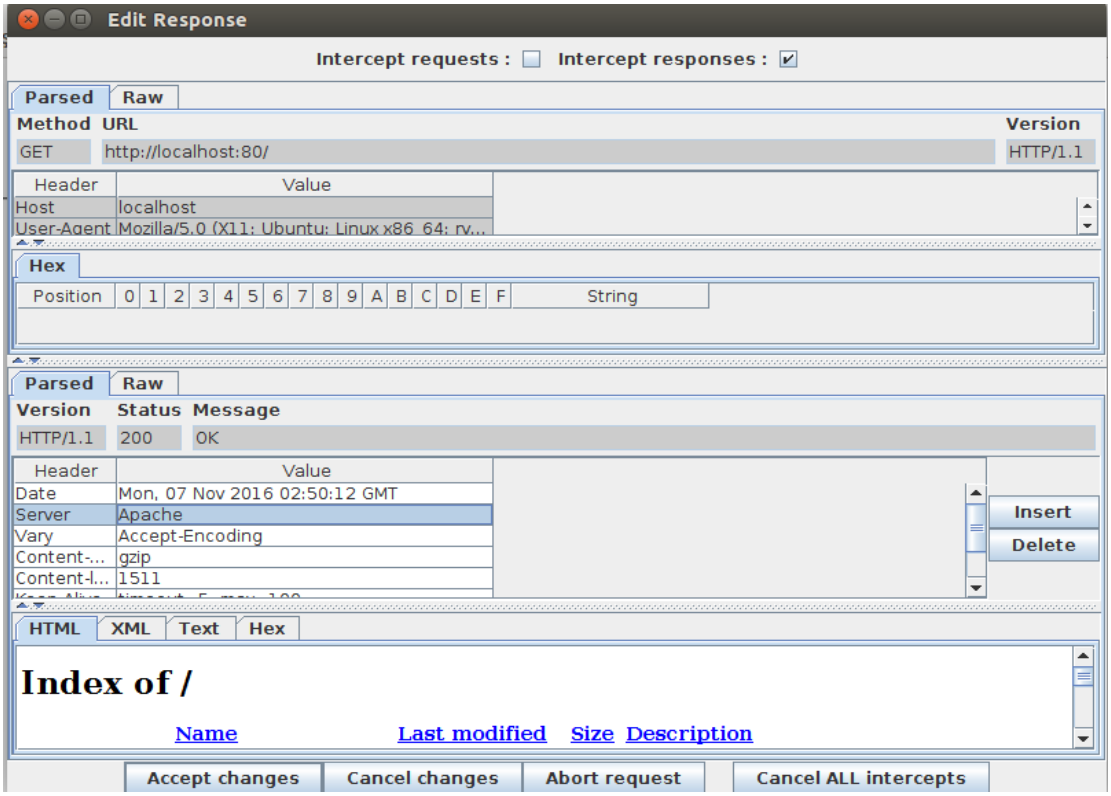
kısmına dikkat edelim. Seçenek olarak Minimal, OS ve Full verilmiş. Ancak bu kısmın yukarısındaki yorum satırlarında en düşük düzeyde bilgi ifşası veren mod için Prod keyword'ü verilmiş. Dolayısıyla biz aşağıdaki gibi yapalım.

#ServerTokens Minimal
#ServerTokens OS
#ServerTokens Full
ServerTokens Prod

Ardından apache'yi restart'layalım:

> service apache2 restart

Ve tekrar localhost'a bağlanmaya çalışalım ve Webscarab ile de Http Response'un önünü keselim:



Görüldüğü üzere Server header'ı Apache/2.4.7 (Ubuntu) ifadesinden Apache ifadesine dönüşmüştür. Yani bilgi ifşası minimuma indirgenmiştir.

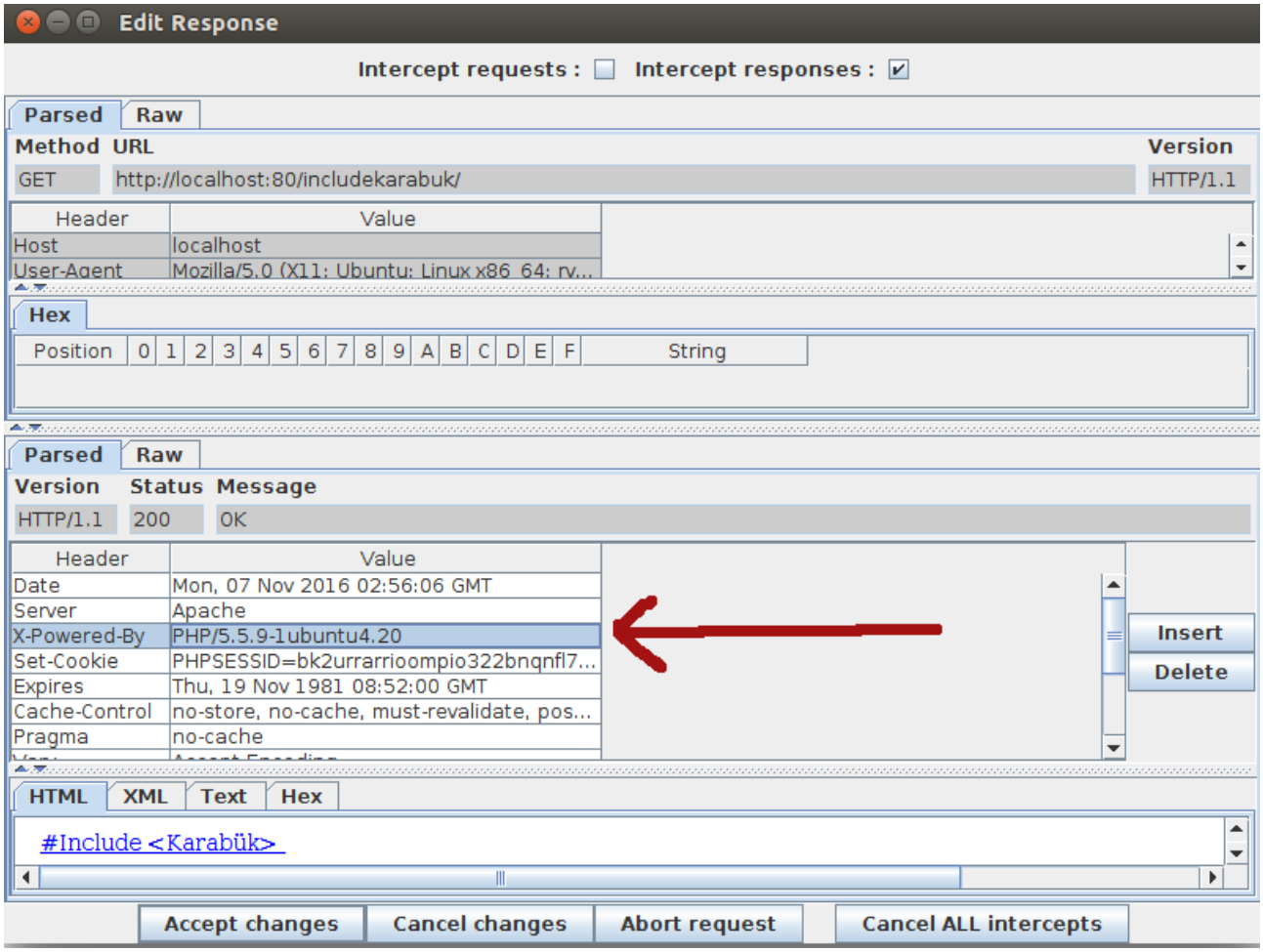
NOT: Peki Apache yazısı yerine “Merhaba” yazıp hacker'ları kızdırmak istersek ne yapabiliriz? Mevcut şartlarda bu mümkün değildir. Ne Server: Apache header'ını kaldırabiliriz ne de yerine başka bir şey yazabiliriz. Bunun nedeni Apache geliştiricilerinin apache kaynak kodunu bu bilginin değiştirilemeyeceği yönünde ayarlamalarından dolayıdır. Minimum bilgi olarak Server: Apache'nin durmasından yanadırlar. Ayrıntılı bilgi için bkz. https://stack overflow .com/questions/35360516/cant-remove-server-apache-header

c. HTTP Response Header'ındaki Bilgi İfşasını Durdurma 2 // X-Powered-By'ı durdurma

Http Response header'ındaki PHP script'ine dair olan bilgi ifşası ise ayrı bir konudur. Peki onu nasıl önleriz? Diyelim ki localhost'ta yer alan php script'inin kullanıldığı bir projeye bağlanmaya çalıştık.

localhost/includekarabuk

Webscarab ile Http Response'un önünü kesersek Http Response'ta aşağıdaki header bilgileri görülecektir.



X-Powered-By header'ı PHP/5.5.9 ve 1ubuntu4.20 bilgisini ifşa etmiş.

(!) Uyarı:

Bir PHP uygulamasının http response'una bakılmalı. Aksi takdirde X-Powered-By yanıt başlığı hiç görünmez.

Bu ifşayı durdurmak için php.ini dosyasında ufak bir değişiklik yapmamız yeterlidir. Öncelikle php.ini dosyasını açalım:

> sudo su
> gedit /etc/php5/apache2/php.ini

Açılan metin belgesindeki

expose_php = On

kısmını

expose_php = Off

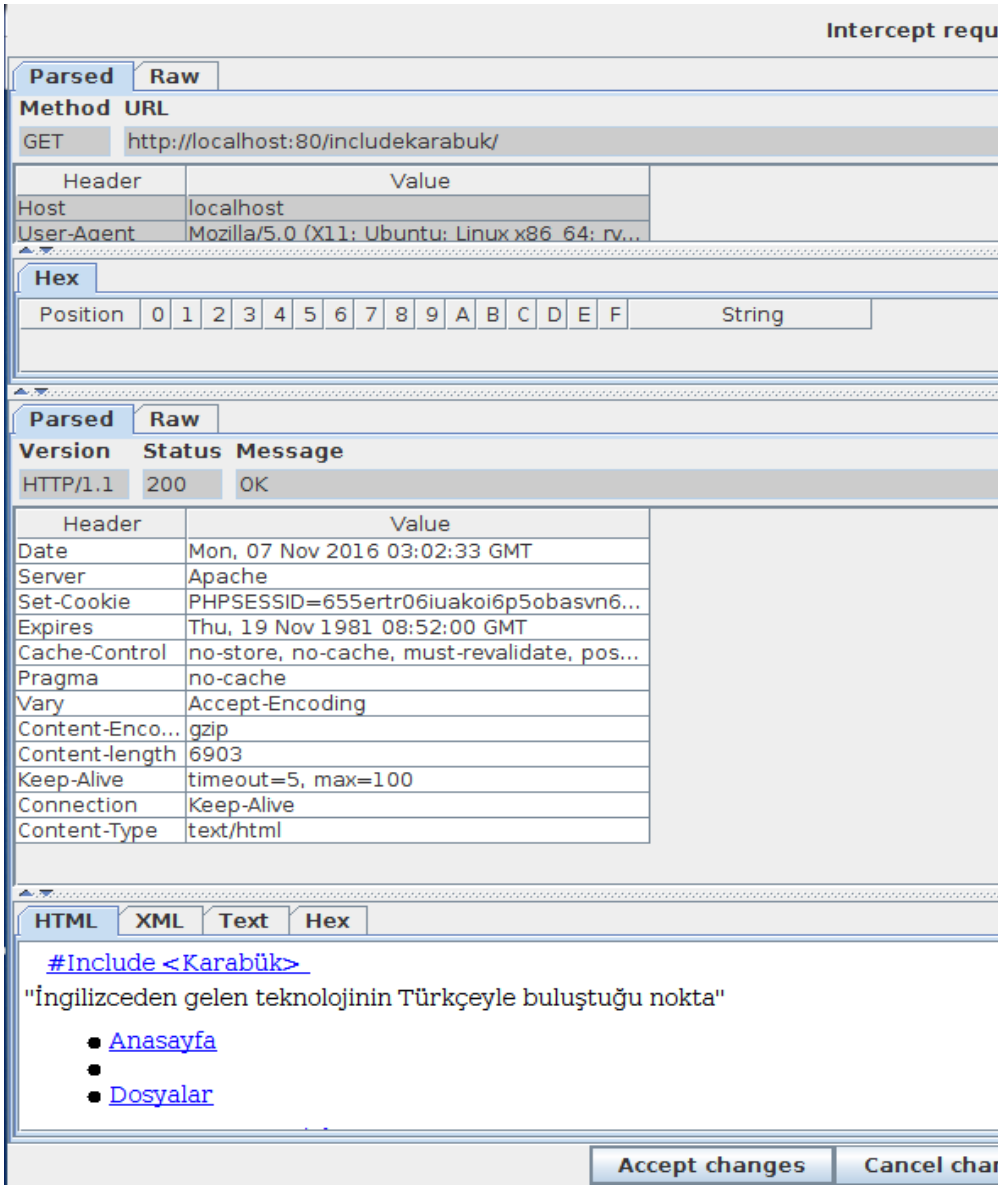
yapalım ve apache'yi restart'layalım:

> service apache2 restart

Tekrar php script'i kullanan projemize bağlanmaya çalışalım:

localhost/includekarabuk

Webscarab ile Http Response'un önünü kestiğimizde X-Powered-By'ın ortadan tamamen kalktığını göreceksiniz:



Böylelikle 404 gibi hata sayfalarında görülen bilgi ifşasını ve http response header'ındaki iki bilgi ifşası kapatmış olduk. Artık saldırganların işi biraz daha güç hale gelmiştir.

Kaynak

> Tez Raporu/Literatür Taraması/İncelenmiş Makaleler/Genel/HTTP-Fingerprinting.docx dökümanını okuduktan sonra aldığım ilhamla bahsedilmeyen security.conf'u ve içerisindeki On ve Off olayını keşfettim ve sırayla deneyerek deneyimlediğim farkı buraya not ettim.
>
> http://ask.xmodulo.com/turn-off-server-signature-apache-web-server.html