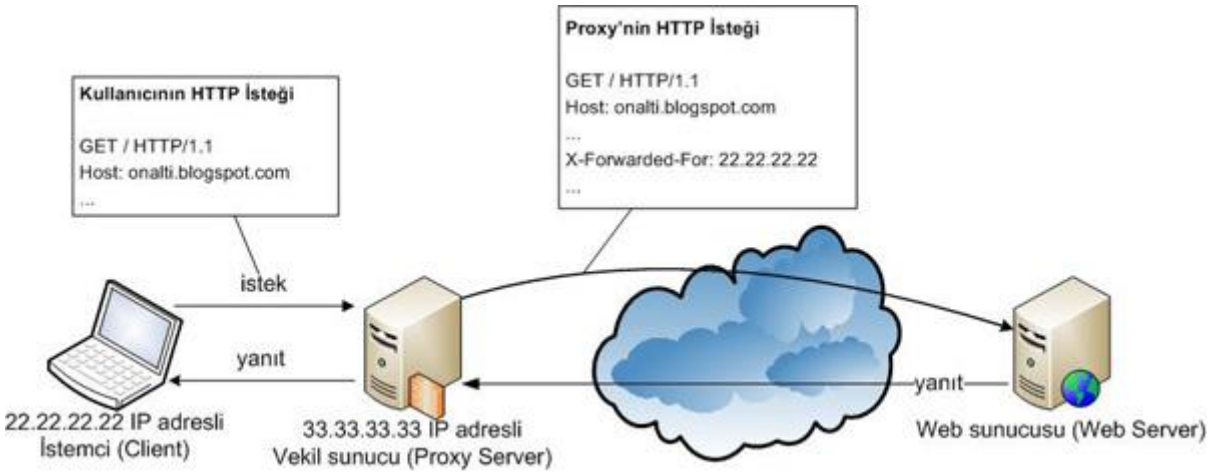
X-Forwarded-For HTTP Başlığının Kötüye Kullanımı

Sertan Kolat, Ekim 2009, WGT E-Dergi 2. Sayı

Internet erişimlerinde bir proxy sunucusu kullanıldığı durumlarda, hedef web sunucusu orjinal isteği yapan kullanıcıya ait gerçek IP adresini göremez. Bunun yerine proxy cihazının IP adresi hedef sisteme bağlanıyor olarak gözükecektir. Aynı durum Internet servis sağlayıcılar tarafından bant genişliği kazanma amaçlı kullanılan transparan proxy cihazları; yük dengeleme, cache vb. amaçlı kullanılan reverse proxy cihazları için de geçerlidir.

Proxy sunucular X-Forwarded-For HTTP başlığını, web isteğini yapan istemciye ait gerçek IP adresinin hedef sunucuya iletmek için kullanmaktadırlar. Bu başlık RFC'lerde geçen bir standart olmamasına rağmen, genel kabul görmüş bir standarttır. İlk olarak Squid proxy geliştiricileri tarafından implemente edilen bu başlık, diğer bir çok proxy cihazında da kullanılmaktadır. X-Forwarded-For HTTP başlığından kısaca XFF olarak da bahsedilmektedir.

Bazı cache ve proxy cihazları ise X-Request-Client-IP, X-Client-IP HTTP başlıklarını kullanmaktadırlar. (Örn. Citrix Application Firewall)



Yukarıdaki şekilde proxy sunucularının istemcilerin yaptığı web isteklerine "X-Forwarded-For: kullanıcının_ip_adresi" şeklinde bir satır eklemesinin detayı görülebilir. Bu sayede şekildeki proxy sunucusu, hedef web sunucusuna bu HTTP isteğini yapan gerçek istemciyi iletmektedir.

X-Forwarded-For nerelerde kullanılır?

X-Forwarded-For (XFF) HTTP başlığı genelde log'lama amacıyla kullanılmaktadır. Bu şekilde siteyi ziyaret eden gerçek kullanıcının IP adresi log kayıtlarına aktarılmaya çalışılır. Bu kayıtlar, oluşan bir olay sonrası inceleme amaçlı kullanılabildiği gibi, web erişim log'larını analiz eden yazılımlar tarafından da kullanılabilir.

Bazı web uygulamaları ise XFF başlığını aşağıdaki şekillerde kullanabilir;

- Belirli istekleri web sunucusu log'larından bağımsız olarak kaydetmek,
- Kullanıcıya gerçek IP adresini göstermek (Örn. http://checkip.dyndns.org),
- Kullanıcının IP adres bilgisine dayanarak Internet üzerinden kullanıcıya doğru hangi port'ların açık olup olmadığını kontrol etmek
  (Örn. http://www.dyndns.com/support/tools/openport.html).

Nadiren de olsa, XFF başlığının IP bazlı erişim kısıtlamalarında kullanıldığı görülebilmektedir.

X-Forwarded-For'un kötüye kullanımı

HTTP başlıklarını log'layabilen web sunucularına ait kayıt mekanizmalarının, kullanıcı tarafından gönderilen X-Forwarded-For başlığını işleyememesi durumlarında hafıza taşması, web sunucusu haklarıyla komut çalıştırma, log dosyalarına bozuk veri girilerek dosyanın veya formatının bozulması vb. güvenlik problemlerinden etkilenebilir.

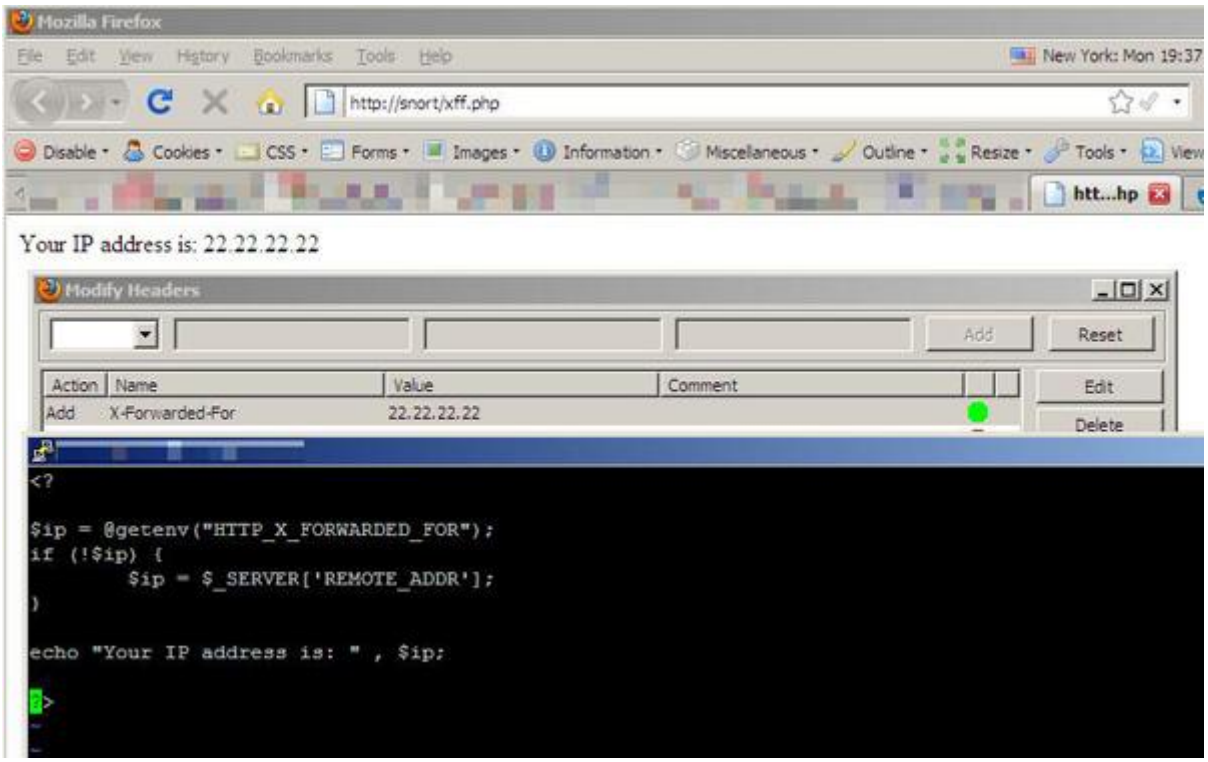
Microsoft IIS web sunucusuna X-Forwarded-For başlığı log'lama özelliği kazandıran ISAPI eklentileri, kullanıcı tarafından gönderilen XFF başlığını işleyemeyerek yukarıda bahsedilen problemlerden etkilenebilirler.

XFF başlığını tam olarak kontrol etmeden log'layan mekanizmaların ürettiği log'ları işleyen log analiz yazılımları ve benzeri yazılımlar da komut çalıştırma, Cross Site Scripting vb. problemlerden etkilenebilirler.

Yukarıda bahsedilen güvenlik problemlerinin tespiti, kaynak kodu inceleme ve test ortamlarında yapılacak olan fuzz testing gibi yöntemlerle mümkün olabilir.

XFF'in kötüye kullanılmasının daha kolay olduğu durumlar, uygulama geliştiriciler tarafından XFF başlığının web uygulamaları içerisinde kullanıldığı durumlardır.

Kullanıcı IP adresinin filtrelenmeden kullanıcıya tekrar gösterilmesi durumunda oluşabilecek bir Cross Site Scripting açığını inceleyelim.



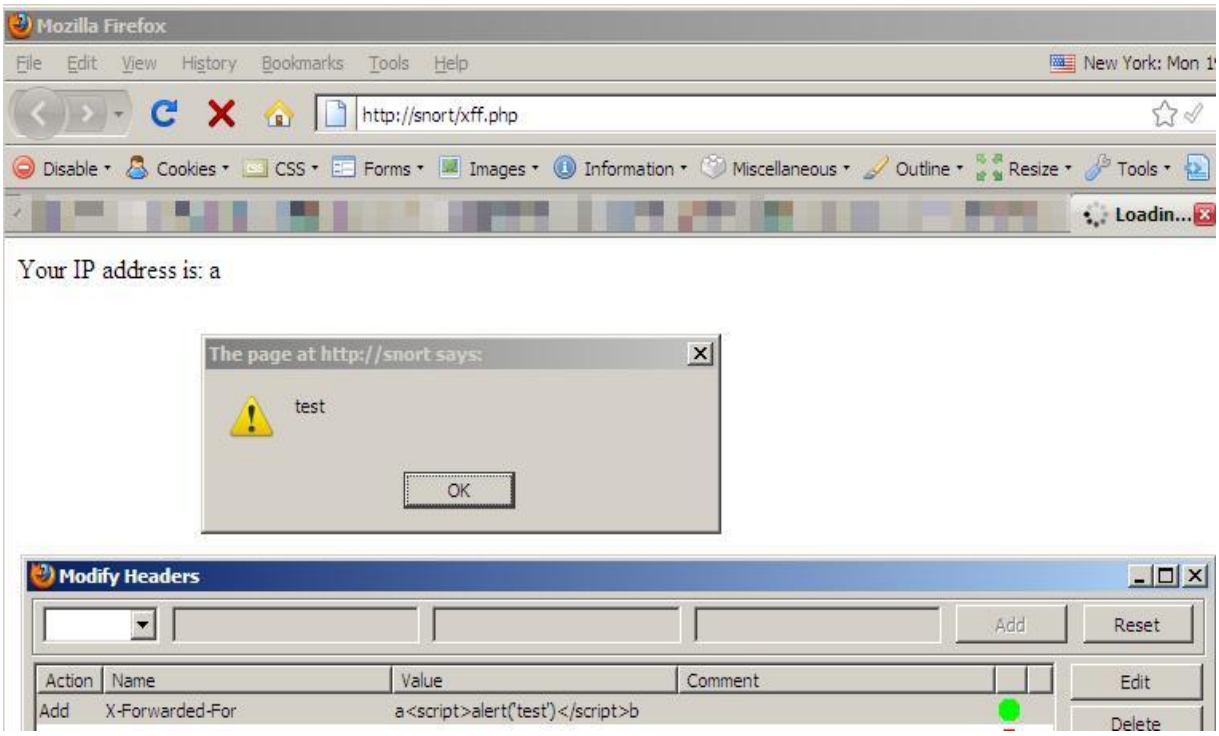
Yukarıdaki ekran görüntüsünün en altında, xff.php dosyasının kaynak kodunu göstermektedir. Kaynak kodunun ilk satırında istemci tarafından gönderilen X-Forwarded-For HTTP başlığı "ip" değişkenine atanarak filtrelenmeden kullanılmaktadır. Eğer yapılan web isteğinde XFF başlığı yoksa, isteği yapan IP adresi ekrana yazılmaktadır (if döngüsü). Bu kodu http://checkip.dyndns.org sayfasındaki kod gibi düşünebiliriz.

Ekran görüntüsünün ortasında Modify Headers adlı Firefox eklentisi kullanılarak, yapılan HTTP isteklerine "X-Forwarded-For: 22.22.22.22" satırı eklenmektedir. Bu nedenle en üstte hedef web uygulamasına yapılan istek, uygulamanın IP adresimizi 22.22.22.22 olarak bize göstermesini sağlamaktadır.

Sadece bu basit örnek bile, XFF başlıklarının erişim kısıtlamalarında kullanılmaması gerektiğini bize göstermektedir.

Bir sonraki ekran görüntüsünde görüldüğü gibi, önceki sahte IP adresini içeren XFF başlığı yerine, "X-Forwarded-For: a<script>alert('test');</script>b" başlığı yapılan HTTP isteğine yerleştirilmiştir.

Web uygulaması istemci tarafından gönderilen veriyi filtrelemeden tekrar kullanıcıya gösterdiği için, uygulama Cross Site Scripting açığından etkilenmektedir. Herhangi bir saldırgan, oluşturmuş olduğu farklı bir HTML sayfası ile bu sayfada bulunan güvenlik açığını tetikleyebilir (XMLHttpRequest setRequestHeader özelliğini kullanarak).



Yukarıdaki örnek güvenlik problemi, aynı şekilde IP adresimizi filtrelemeden SQL veritabanına yazan bir web uygulamasını SQL'e Sızma (SQL Injection) güvenlik açığına maruz bırakacaktır. Saldırganlar, normal bir değişkeni değiştirir gibi XFF başlığını da kolayca değiştirebilirler.

Bu güvenlik probleminin testi otomatikleştirilerek hedef web uygulamaları, SQL'e Sızma, XSS, Komut Çalıştırma, Kod Çalıştırma, Hafıza Taşması gibi problemlere karşı kontrol edilebilir.

XFF başlıklarının kötüye kullanımı, sisteminizde bulunan açık servislerin uzaktan erişilebilirliğini test eden web servislerini birer port tarama servisine dönüşebilirler. Bu nedenle benzer servis sağlayıcılar, XFF başlığı kullanımına dikkat etmektedirler.

Tıpkı değişkenlerde olduğu gibi, bazı web uygulamalarında kullanıldığına şahit olduğum X-Forwarded-For, X-Client-IP, X-Request-Client-IP gibi HTTP başlıkları, kötü niyetli kullanıma karşı filtrelenmelidir. Web sunucularının bu HTTP başlıklarını kayıt altına alan modülleri, log analiz yazılımları, bu başlığı inceleyen veya işleyen firewall, IDS, web application firewall vb. yazılımlar bu değerin hatalı işlenmesinden kaynaklanabilecek güvenlik problemleri için birer potansiyel oluşturmaktadır.