Apache'de Http Options Methodunu Kapatma

Http Options methodu sunucuda izinli http methodları bilgisinin http yanıtlarıyla kullanıcılara gitmesini sağlayan bir http methodudur. Eğer bir sunucuda http options methodu açık olursa web geliştiricisi dalgınlıkla PUT ya da DELETE gibi http methodlarını sunucuda açık bıraktığında saldırganın bundan haberi olacaktır. Saldırgan bu bilgiden yola çıkarak hedef web sunucusuna dosya yükleyebileceğini ya da hedef web sunucusundan dosya silebileceğini anlayacaktır ve saldırısını gerçekleştirecektir.

Sunucularda izinli http methodları bilgisinin http response başlığında gitmesini önlemek için http options methodu kapatılmalıdır. Bu işlem apache sunucularda apache2.conf dosyasını yapılandırarak gerçekleşir.

a) Yöntem I

Önce localhost'umuza bir options talebinde bulunalım.

```
> telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
OPTIONS / HTTP/1.0                          // OPTIONS talebi yapılır.

HTTP/1.1 200 OK
Date: Tue, 15 Aug 2017 13:12:02 GMT
Server: Apache/2.4.7 (Ubuntu)
Allow: GET,HEAD,POST,OPTIONS                // İzinli http methodları bilgisi gelir.
Content-Length: 0
Connection: close
Content-Type: httpd/unix-directory

Connection closed by foreign host.
```

Görüldüğü üzere localhost'umuzda izinli http methodları bilgisi yanıt olarak gelmiştir. Şimdi apache sunucumuzu yapılandıralım ve options methodunu kapatalım. Bunun için apache2.conf dosyasını açalım.

```
> sudo gedit /etc/apache2/apache2.conf
```

Ardından açılan dosyanın en altına aşağıdaki kod bloğunu ekleyelim.

```
<Location />                                // Slash kök dizini ifade eder.
  <LimitExcept HEAD GET POST>
    order deny,allow
    deny from all
  </LimitExcept>
</Location>
```

Not: Yukarıdaki kod HEAD, GET ve POST dışındaki tüm http methodlarını kapatır.

Ardından dosyayı kaydedelim ve apache servisini restart'layalım.

```
> service apache2 restart
```

Böylece OPTIONS methodu kapatılmış olacaktır. Şimdi tekrar localhost'umuza Options talebi yapacak olursak izinli http methodları bilgisinin gelmediğini görebiliriz.

```
> telnet localhost 80

Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
OPTIONS / HTTP/1.0                          // Options talebi yapılır.

HTTP/1.1 403 Forbidden
Date: Tue, 15 Aug 2017 13:20:09 GMT
Server: Apache/2.4.7 (Ubuntu)               // İzinli http methodları bilgisi gelmedi.
Content-Length: 276
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

b) Yöntem II

Önceki yöntemde apache2.conf dosyasına eklenen kodları sildiğimizi varsayalım. İkinci yöntem için localhost'umuza bir options talebinde bulunalım.

```
> telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
OPTIONS / HTTP/1.0                          // OPTIONS talebi yapılır.

HTTP/1.1 200 OK
Date: Tue, 15 Aug 2017 13:12:02 GMT
Server: Apache/2.4.7 (Ubuntu)
Allow: GET,HEAD,POST,OPTIONS                // İzinli http methodları bilgisi gelir.
Content-Length: 0
Connection: close
Content-Type: httpd/unix-directory

Connection closed by foreign host.
```

Görüldüğü üzere localhost'umuzda izinli http methodları bilgisi yanıt olarak gelmiştir. Şimdi apache sunucumuzu yapılandıralım ve options methodunu kapatalım. Bunun için apache2.conf dosyasını açalım.

> sudo gedit /etc/apache2/apache2.conf

Ardından açılan dosyanın <Directory /var/www/> … </Directory> tag'ları arasına aşağıdaki satırı ekleyelim.

deny from all

Görünüm şu şekilde olacaktır:

apache.conf:

…

<Directory /var/www/>
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
deny from all
</Directory>

…

Ardından dosyayı kaydedelim ve apache servisini restart'layalım.

> service apache2 restart

Böylece OPTIONS methodu kapatılmış olacaktır. Şimdi tekrar localhost'umuza Options talebi yapacak olursak izinli http methodları bilgisinin gelmediğini görebiliriz.

> telnet localhost 80

Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
OPTIONS / HTTP/1.0 // Options talebi yapılır.

HTTP/1.1 403 Forbidden
Date: Mon, 26 Feb 2018 14:03:01 GMT
Server: Apache/2.4.7 (Ubuntu) // İzinli http methodları bilgisi gelmedi.
Content-Length: 276
Connection: close
Content-Type: text/html; charset=iso-8859-1

Böylece apache sunucuda http options methodunu kapamış olduk.

Kaynaklar

https://www.acunetix.com/vulnerabilities/web/options-method-is-enabled

https://sureshk37.wordpress.com/2014/10/01/how-to-disable-apache-http-options-method/

https://www.maketecheasier.com/securing-apache-ubuntu-2/