Telnet & nc ile Http Taleplerinde Bulunma

a. Telnet ile Http Talebi Yapma

> telnet www.includekarabuk.com 80

Output:

```
Trying 46.45.187.221...
Connected to includekarabuk.com.
Escape character is '^]'.
GET / HTTP/1.0                                  // Bu satır girilir
Host:www.includekarabuk.com                     // Bu satır da girilir.

                                                // İki kez enter'lanır.


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
  <head>
        <!-- Tum subPageType'larda olan ortak satirlar... -->
        <title>Anasayfa | #Include &lt;Karabük&#62;</title>
        <link rel="stylesheet" type="text/css" href="kitaplik/css/commonLayout.css">
        <link rel="stylesheet" type="text/css" href="kitaplik/css/rightColumn.css">
        <link rel="stylesheet" type="text/css" href="kitaplik/css/footer.css">
        <link rel="shorcut icon" href="kitaplik/resimler/favicon.ico" type="image/x-icon">
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8"> <!-- iso-8859-9 -->
        <meta name="abstract" content="Karabuk'ten internete bilgi akisi.">
        <meta name="author" content="Hasan Fatih Simsek">
        <meta name="copyright" content="Tum haklari saklidir | 2014">
        <meta name="description" content="İngilizceden gelen teknolojinin Türkçe ile noktası!">
        <meta name="keywords" content="karabuk,webgoat,dvwa,guvenlik,java,data structure">
        <script type="text/javascript" src="kitaplik/jquery/jquery-2.1.1.min.js"></script>

        <!-- ARCHIVE BOX CODE -->
        <script>
```

Görüldüğü üzere http talebinde GET methoduyla bulunduğumuzda dönen cevap header + body şeklinde gelmiştir.

> telnet www.includekarabuk.com 80

Output:

Trying 46.45.187.221...
Connected to includekarabuk.com.
Escape character is '^]'.
HEAD / HTTP/1.0 // İki kere enter'lanır

HTTP/1.1 400 Bad Request
Date: Fri, 09 Jun 2017 07:50:51 GMT
Server: Apache/2.4.25 (Unix) OpenSSL/1.0.1e-fips mod_bwlimited/1.4 PHP/5.5.38
Accept-Ranges: bytes
Connection: close
Content-Type: text/html

Görüldüğü üzere http talebini HEAD methoduyla yaptığımızda dönen yanıt sadece header olarak gelmiştir.

> telnet www.includekarabuk.com 80

Output:

Trying 46.45.187.221...
Connected to includekarabuk.com.
Escape character is '^]'.
OPTIONS / HTTP/1.0 // İki kere enter'lanır

(Hedef sistemde OPTIONS methodu açık olmadığı için yanıtta OPTIONS header'ı gelmemiştir)

b. nc ile http talebi yapma

// Netcat ile http talep gönderimi yaparken paketin ilk satırını yazıp ikinci satırını yazmak
// için bir kere ENTER yaptığımızda http request gönderimini tamamlayamadan ilk satırda
// paket yollanmaktadır. Netcat'te bu satır atlatma olayının iki kere işlemesinden dolayı
// paketler daha ilk satırda sonlanmaktadır. Bazı web sunucular bu şekilde yarım paket
// gönderimine hata dönmezken bazı web sunucular Host header'ı ilavesi de istediğinden
// 400 Bad Request hatası dönmektedir. Eğer netcat ile başarılı bir şekilde http request paket
// gönderimi yapmak istiyorsak string halinde oluşturacağımız http talep paketini input
// olarak netcat'e verebiliriz. Bu şekilde iki satırlık veya daha fazla satırlık http talep paketi
// netcat ile yollayabiliriz.

> echo -e "GET / HTTP/1.1\r\nHost: www.includekarabuk.com\r\n\r\n" | nc includekarabuk.com 80

Not:

echo'nun -e parametresi: Tırnak karakterleri arasındaki escape özelliğindeki backslash'leri yorumlamayı etkinleştirir ve satır atlatma karakterlerini string olarak değil, işlevleri gibi okur.

netcat'in -v parametresi: Verbose çıktı sundurur.

Not 2:

echo ile netcat'e çıktılanan string'te (yani http request pakette) HEAD / HTTP/1.1'den sonra bir adet satır atlatma (\r\n) karakteri yer alır. Host: www.includekarabuk.com'dan sonra iki adet satır atlatma (\r\n\r\n) karakteri yer alır. İkinci satırda iki tane satır atlatma karakteri olması iki kere ENTER anlamındadır. Yani http request paketi sonlandırılmaktadır.

Output:

HTTP/1.1 200 OK
Date: Tue, 04 Jan 2022 11:43:59 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=33be693ccee7bc0457f9a0c3fc9f0aad; path=/
Vary: Accept-Encoding,User-Agent
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
  <head>
    <!-- Tum subPageType'larda olan ortak satirlar... -->
    <title>Anasayfa | #Include <Karabük></title>
    <link rel="stylesheet" type="text/css"
    href="kitaplik/css/commonLayout.css">

<link rel="stylesheet" type="text/css" href="kitaplik/css/rightColumn.css">
...

Görüldüğü üzere http talebinde karşılık gelen http yanıtı header + body şeklinde gelmiştir.

> echo -e "OPTIONS / HTTP/1.1\r\nHost: www.includekarabuk.com\r\n\r\n" | nc includekarabuk.com 80

Output:

(Hedef sistemde OPTIONS methodu açık olmadığı
için yanıtta OPTIONS header'ı gelmemiştir)

Ekstra

Bazen OPTIONS methodu kök dizinde açık değilken farklı dizinlerde açık olarak dönebilmektedir. Dolayısıyla telnet ve nc ile farklı dizinlere http request yapabilmek için / karakteri yerine ilgili path adresi girilebilir. Örneğin;

> telnet www.includekarabuk.com 80

Output:

Trying 46.45.187.221...
Connected to includekarabuk.com.
Escape character is '^]'.
OPTIONS **/kitaplik/** HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 08 Aug 2017 12:57:33 GMT
Server: Apache/2.4.27 (cPanel) OpenSSL/1.0.2k mod_bwlimited/1.4
Allow: GET,POST,OPTIONS,HEAD,TRACE
Content-Length: 0
Connection: close

> echo -e "OPTIONS **/kitaplik/** HTTP/1.1\r\nHost: www.includekarabuk.com\r\n\r\n" | nc includekarabuk.com 80

Output:

```
HTTP/1.1 200 OK
Date: Tue, 04 Jan 2022 12:11:07 GMT
Server: Apache
Allow: GET,POST,OPTIONS,HEAD,TRACE
Vary: User-Agent
Content-Length: 0
Content-Type: httpd/unix-directory
```

Kaynaklar

Tez Raporu / Literatür Taraması / İncelenmiş Makaleler / BGA / Okunmuşlar / Güvenlik Testlerinde Bilgi Toplama (Pdf'in parsellenmiş hali).docx