

IIS Sunucularda Server Header'ını Farklı Bir Değerle Doldurma

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

Windows Server 2008 R2 Sanal Makinası
URLRewrite

Bu yazıda IIS sunucularda Server header'ını modifiye etme ve bu yolla saldırganlar için hedef şaşırtmanın nasıl yapılabileceği gösterilecektir. Bu işlem için IIS sunuculara UrlRewrite tool'unun yüklenmesi ve sistemin restart'lanması gerekmektedir.

Öncelikle hedef IIS sunucusuna bir Http HEAD talebi yapalım ve sunucudan dönen yanıtta Server başlığına bir bakalım.

```
> telnet 172.16.3.92 80
```

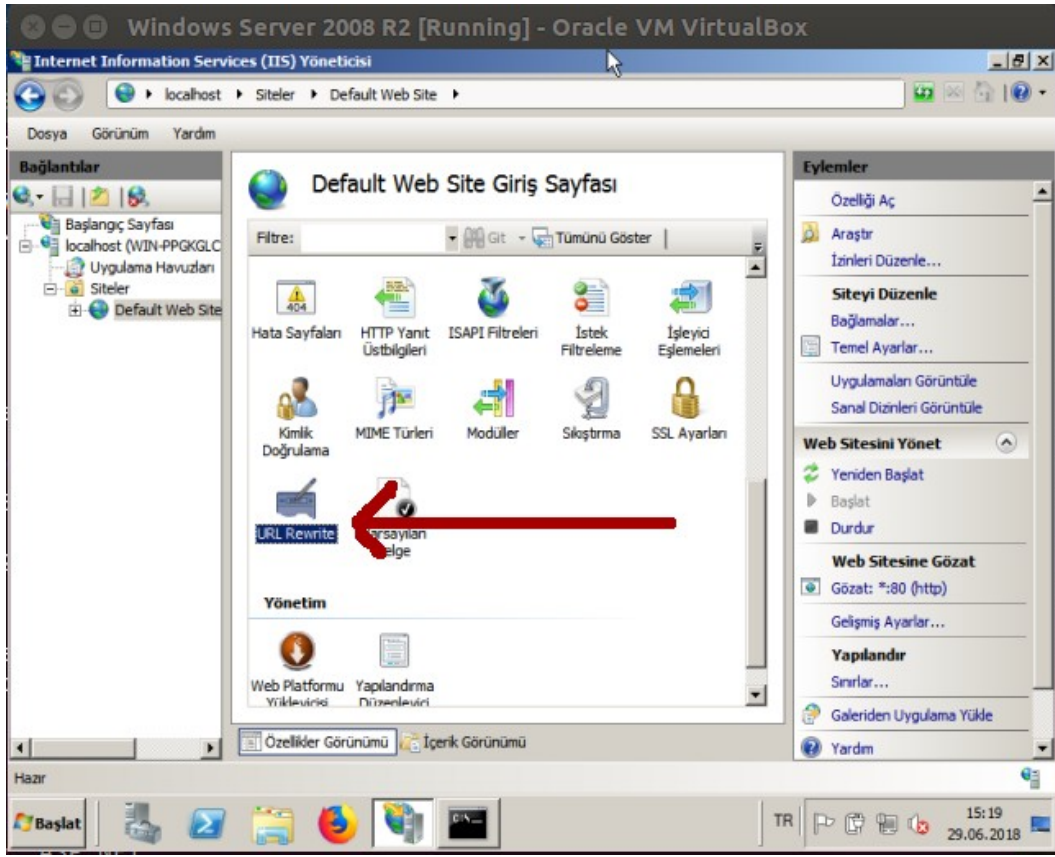
```
// Windows Server 2008 R2 IP'si
```

```
hefese@hefese-HP-EliteBook-8440p: ~
hefese@hefese-HP-EliteBook-8440p:~$ telnet 172.16.3.107 80
Trying 172.16.3.107...
Connected to 172.16.3.107.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Fri, 16 Feb 2018 13:23:58 GMT
Accept-Ranges: bytes
ETag: "175fbb6629a7d31:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Fri, 29 Jun 2018 12:01:54 GMT
Connection: close

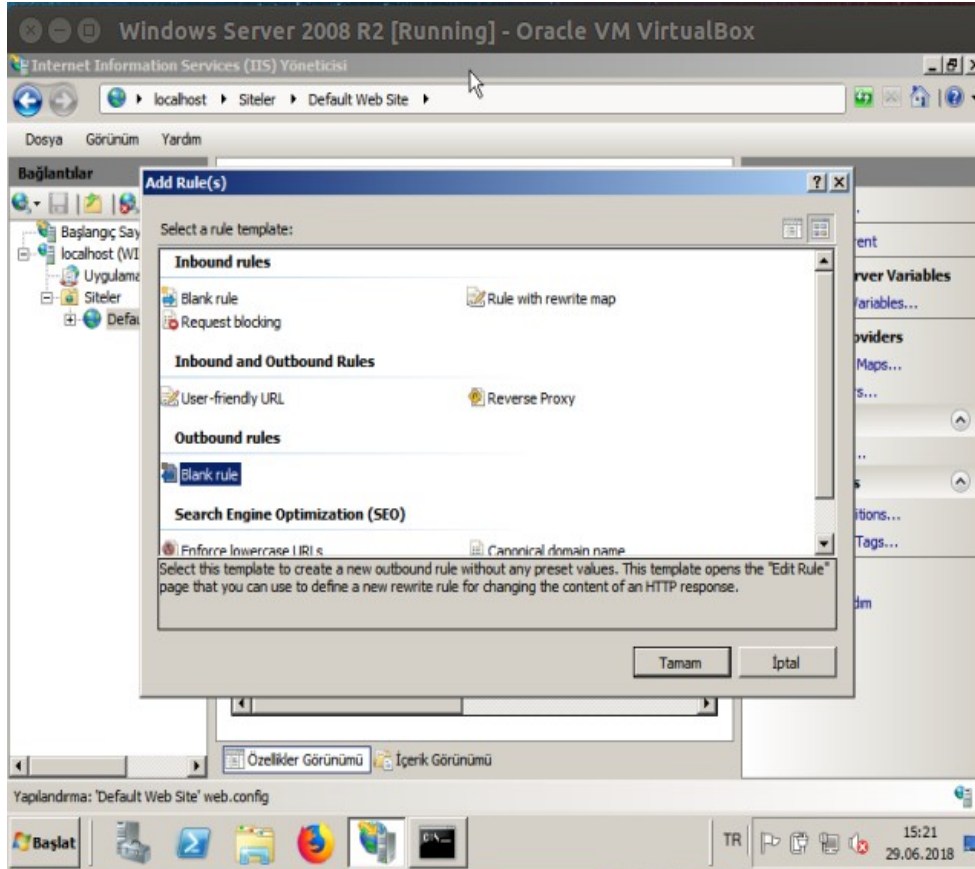
Connection closed by foreign host.
hefese@hefese-HP-EliteBook-8440p:~$
```

Görüldüğü üzere hedef sistem IIS/7.5 web sunucu yazılımını kullanıyormuş. Bu bilgiyi manipule edelim ve saldırganlar için hedef şaşırtmaca yapalım. Bu işlem için IIS paneli açılır ve URLRewrite ögesine tıklanır.




Ardından Add Rules linkine tıklanır.

Daha sonra Outbands Rule -> Blank rule seçeneği seçilir ve Tamam denir.



Son olarak gelen sayfaya ařađıdaki deđerler girilir.

 Edit Outbound Rule

Name:
ChangeServerResponseHeaderValue

Precondition:
<None>

Match

Matching scope:
Server Variable

Variable name:
RESPONSE_Server

Variable value:
Matches the Pattern

Using:
Wildcards

Pattern:
*

Ignore case

Conditions

Action

Action type:
Rewrite

Action Properties

Value:
Apache

Replace existing server variable value

Stop processing of subsequent rules

ve Uygula denir. Bylece Server header'ı belirlediđimiz deđerini gsterir duruma gelecektir.

> telnet 172.16.3.92 80

```
hefese@hefese-HP-EliteBook-8440p: ~
hefese@hefese-HP-EliteBook-8440p:~$ telnet 172.16.3.107 80
Trying 172.16.3.107...
Connected to 172.16.3.107.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Fri, 16 Feb 2018 13:23:58 GMT
Accept-Ranges: bytes
ETag: "175fbb6629a7d31:0"
Server: Apache
X-Powered-By: ASP.NET
Date: Fri, 29 Jun 2018 12:07:12 GMT
Connection: close

Connection closed by foreign host.
hefese@hefese-HP-EliteBook-8440p:~$
```

Görüldüğü üzere bir IIS sunucuyu Apache sunucusu gibi gösterdik. Bunun yerine örneğin farklı bir IIS sunucusu bilgisi de girebilirdik veya herhangi alakasız bir string de girebilirdik. Bu tercihe kalan bir şeydir.

Not: URLRewrite tool'u IIS 7 ve sonrasında sorunsuz çalışabilmektedir: IIS 7.0, 7.5, IIS 8, IIS 8.5, IIS 10 (bkz. <https://www.iis.net/downloads/microsoft/url-rewrite>)

Kaynak

<https://blogs.msdn.microsoft.com/benjaminperkins/2012/11/02/change-or-modify-a-response-header-value-using-url-rewrite/>

<https://www.iis.net/downloads/microsoft/url-rewrite>

https://en.wikipedia.org/wiki/Internet_Information_Services