

Shut it d0wn TRACE

Author:- micr0

Contact: micr0security@live.com

Visit: www.garage4hackers.com

This paper is only for the purpose of knowledge and information sharing. Not to teach how to HACK.

Hello everyone,

After webdav I thought to create a paper on the Trace method,

As per the all web vulnerability scanners if TRACE method is enabled then it is vulnerability.

Now lets come to the topic

What is TRACE method?

Well TRACE this is method provided to perform various actions on the web server mainly TRACE method is used for debugging the server for example you can say problem in the network connection.

Now the thing is how can we use these methods for the purpose of hacking?

Basically the thing is this by using TRACE method an attacker can gather the info about the server as well as the this method can cause cross site scripting and cross site tracing (XST) which is nothing but the form of cross site scripting attack.

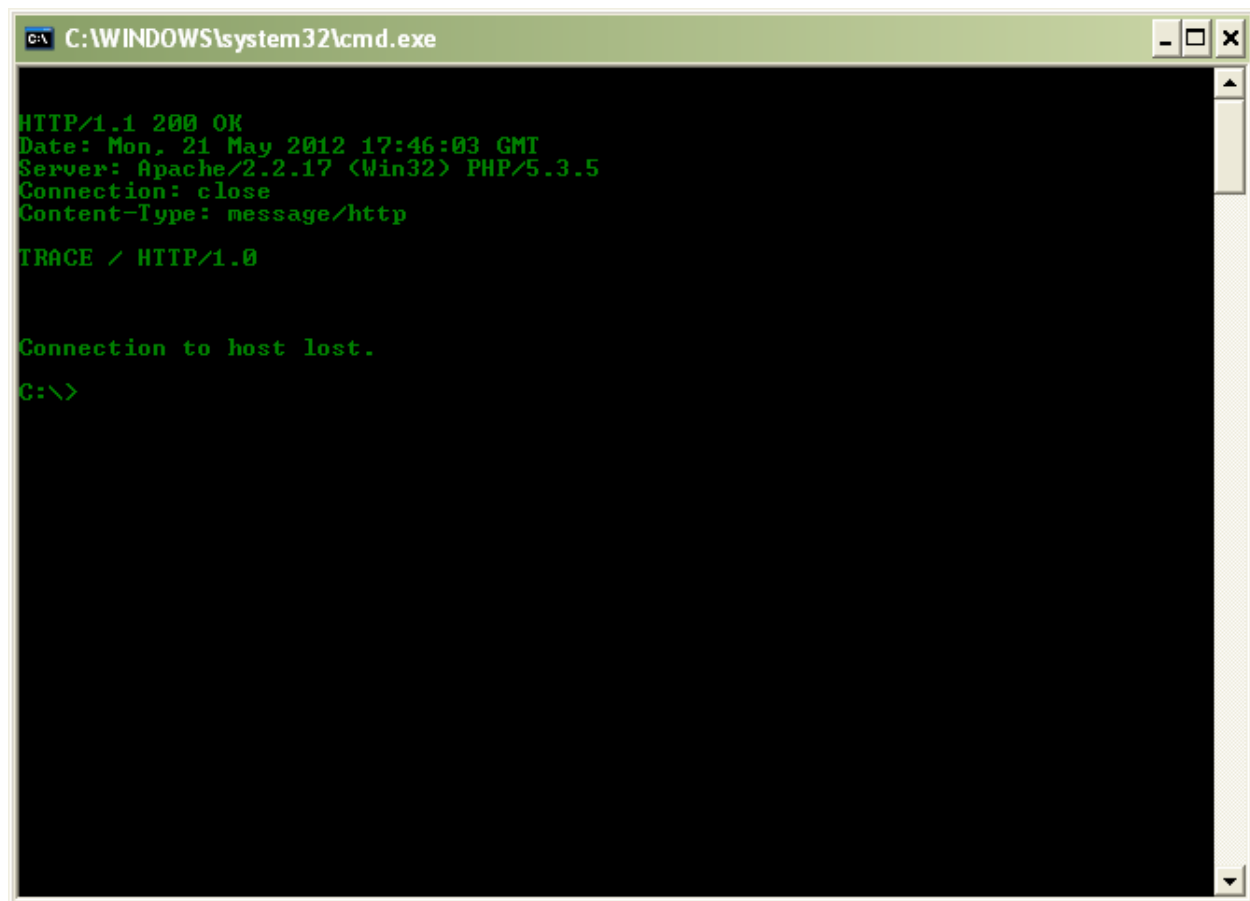
Normally the TRACE method echo back the request sent on the web server by client. So this method can be used to create an attack like cross site scripting.

First of all we need to check whether the TRACE method is enabled on the server or not.

For this test we can use telnet or Netcat .

Here I just telnet the target system and given the following command

telnet <target ip> port number (i.e 80)



A screenshot of a Windows command prompt window. The title bar at the top reads "C:\WINDOWS\system32\cmd.exe". The window has standard Windows window controls (minimize, maximize, close) on the right. The command prompt shows the following text in green on a black background:

```
HTTP/1.1 200 OK
Date: Mon, 21 May 2012 17:46:03 GMT
Server: Apache/2.2.17 (Win32) PHP/5.3.5
Connection: close
Content-Type: message/http

TRACE / HTTP/1.0

Connection to host lost.
C:\>
```

Here we got output that is HTTP/1.1 200 OK

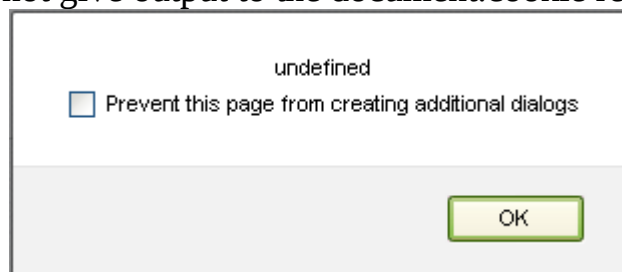
That means TRACE method is enabled.

The web server can be used by an attacker to launch an attack like cross site scripting.

This is the method to check simple http protocol you can check the same thing for https also using openssl client s_client.

Attack details :

In a normal cross site scripting attack an attacker send the malicious link to the victim and try to get the cookies or other valuable data. But now days the httpOnly mechanism is used to avoid this if the httpOnly is enabled then no use of such attack because it do not give output to the document.cookie request.



Here you can see the trace method is not available so the output of the document.cookie is as above

```
C:\WINDOWS\system32\cmd.exe

HTTP/1.1 405 Method Not Allowed
Date: Mon, 21 May 2012 17:44:21 GMT
Server: Apache/2.2.14 (Ubuntu)
Allow:
Vary: Accept-Encoding
Content-Length: 307
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>405 Method
Not Allowed</title>
</head><body>
<h1>Method Not Allowed</h1>
<p>The requested meth
od TRACE is not allowed for the URL /.</p>
<hr>
<address>Apache/2.2.14 (Ubuntu) Se
rver at www.icomplaints.in Port 80</address>
</body></html>

Connection to host lost.
C:\Documents and Settings\Admin>_
```

But there is a possibility to an attacker to overcome on this issue. Even if the httpOnly is used and TRACE method is enabled then an attacker can grab the cookies and some local credential also.

Now if the victim is logged in to the server using his/her credentials then an attacker can check the cookies. Here we have to understand that an attacker can write a malicious script and compromise the credentials of the victim.

Just take a look at the process of an attack.

Attacker → (receives the malicious page from attacker) **victim** → **victim** click on the link provided by the **attacker** → (victim's server reply on the request which is actually done by an **attacker** → **victim** get the echo from the **web server** → now the victim's system send the data to an **attacker**

Here if we see the trace method is enabled so the server is replying back to the victim. If the server is not running TRACE method the attack can avoid.

Prevention from the attack

- 1) Disable TRACE method (if not needed).
 - 2) Use Mozilla Firefox latest version or use latest internet explorer version 7 or 8.
- Stay aware and stay safe 😊 .

References

Obviously god of the blue nowhere:-www.google.com

OWASP