**Zack Pelka**

**HTTP TRACK and TRACE verbs**

|  |  |
| --- | --- |
| Prepared By: | Zachary Pelka |
| Document Version: | 1 |
| Last Updated On: | 2MAY2021 |
| Document Classification: | Public Domain |

The information in the document may contain proprietary and confidential information that is intended for the employees of ZP Enterprises only. If you are not an employee of ZP Enterprises, you are hereby notified that any disclosure, copying, distribution, retention or use of the contents of this information is prohibited in an altered form. This is for public use without modification.

## **Purpose**

# HTTP TRACK and TRACE verbs

TRACK is an HTTP verb that tells IIS to return the full request back to the client. It is Microsoft’s implementation and it is similar to TRACE verb which is RFC complaint.

Vulnerability scan tools may raise a flag if HTTP TRACK and TRACE verbs are enabled in your server. The reason behind is that attackers  capture client cookies by asking web servers to return full requests.

An example text from a vulnerability scan tool in regards to the usage of this verb:

The HTTP TRACK method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLDOM to cause a client to issue a TRACK request and capture the client’s cookies. This effectively results in a Cross-Site Scripting attack.

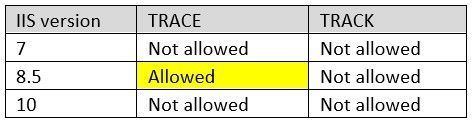
[Source](https://forums.iis.net/t/1210791.aspx)

### 

### **IIS and TRACE/TRACK verbs**

HTTP TRACK is disabled in IIS 6 and newer versions. However, you may see the TRACE verb enabled which may cause your security scan tool to raise a vulnerability flag.

I performed tests by using IIS 7, 8.5, and 10 to see if TRACK and TRACE verbs are enabled or disabled by default:



As you see in the table, TRACK is not allowed by default after IIS 7. However, TRACE is allowed by default in IIS 8.5.

Please note that security scan tools may point out TRACK verb usage but they may actually test for TRACE method.

### 

### **How to disable TRACK and TRACE verbs**

1. Open IIS Manager
2. Select the website
3. Double click “**Request Filtering**” (If you don’t see Request Filtering icon, [install it](https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/requestfiltering/))
4. Go to “**HTTP Verbs**”
5. Click “**Deny Verb**”. Type “**TRACE**”. Click “**OK**”
6. Click “**Deny Verb**”. Type “**TRACK**”. Click “**OK**”

### 

### 

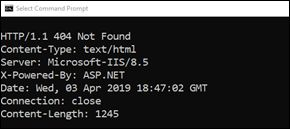
### **Testing**

Try sending a TRACE request to IIS via telnet. If it fails with 404 code, it means this request is not allowed.

Steps to test:

1. Open Command Prompt in your client machine
2. Run telnet <server-ip-address> 80
3. Run the text below line by line. Continue to enter characters even though the window won’t show anything
   * TRACE / HTTP/1.1
   * Host: websitedomain.com
   * HostA: Hello
4. Hit Enter twice

If you see HTTP/1.1 404 Not Found, the setting is working. TRACE is disabled:



If you see HTTP/1.1 200 OK, the setting is not working. TRACE is allowed:

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **By** | **Changes** |
| **1.0** | 2MAY2021 | Zachary Pelka | Initial Draft |
|  |  |  |  |
|  |  |  |  |