Cheatography

HTTP Request Methods Cheat Sheet

by binca via cheatography.com/44948/cs/13298/

Request Methods

GET	OPTIONS
POST	CONNECT
HEAD	PUT
TRACE	DELETE

Some other web apps and/or servers add other methods.

GET Method

Used to obtain a web resource from the server by passing parameters via URL

Easily manipulated by attackers

Could be dangerous for authentication-related and session tracking parameters

Easier to script against an app using GET

Enables an attacker to test requests without waiting for payload

POST Method

Requests a web resource but passes parameters via the HTTP payload

Can still be manipulated

Can be changed to a GET for simpler scripting if the app supports **Method Interchange** and **register_globals** is how this happens in PHP

Parameters will not get logged

TRACE Method

Will echo the request as seen by the server back at the client

It is for diagnostic purposes

Enables the attacker to see any changes made by proxies (inbound or outbound)

OPTIONS Method

Asks the server to return the list of request methods supports

Enables an attacker to determine methods for attacks

PUT Method

Uploads data tot he location specified by the URL

Data upload is the HTTP payload

Should not be supported on public internet-facing servers.

DELETE Method

Removes the resource specified by the URL

Could lead to DoS

Can be used to change configurations, such as deleting .htaccess file

Should not be supported on public internet-facing servers.

Attacker's Perspective of HTTP

Look for methods that should **NOT** be supported: **PUT, DELETE, CONNECT**

TRACE can help map network architecture

Check for method interchange, which can ease XSS attacks and scripting because parameters can be passed in the URL

Websocket

Designed to establish connection to a back-end server allowing for long-term communciation

Supports bidirectional communication over a single TCP socket

Designed to handle blocked ports/network restrictions

Depends on the server and the client support for JavaScript and HTML5

Handshake over HTTP(S):
ws :// Protocol handler initiates the request
wss :// for sercure is more widely used

Websocket Tools

Many tools do not handle Websocket to capture, intercept, or fuzz

Wireshark can capture raw network traffic but cannot parse

ZAP was one of the first to support interception and fuzzing of Websocket connections

Use Netcrat to Determine HTTP Methods

```
#! /bin/bash
for method in GET POST PUT TRACE CONNECT OPTIONS;
do
  printf "$method / HTTP/1.1\r\nHost:domain\r\n\r\n" |
nc domain 80
done
```

Can manually type HTTP commands into Netcat or use a bash script like the one above.

By **binca**
cheatography.com/binca/

Not published yet.
Last updated 9th November, 2017.