HTTP verbs are also called HTTP methods, we can use these methods in some cases to exploit a target.

The most common HTTP methods are GET, POST, HEAD, PUT, DELETE

GET – is used to request a web resources, eg when the client wants to open a web page. A picture containing text

Description automatically generated

An example of the GET method. (note GET must have a host defined)

Guest can also be used to pass arguments (parameters) to the webpage like this: Text

Description automatically generated with medium confidence

POST – Is usedto submit HTML form data. All post parameters reside in the message (request) bodyText

Description automatically generated

HEAD – Very similar to GET, but asks the server to only respond with headers instead of a response bodyDiagram

Description automatically generated with medium confidence

PUT – is designed for uploading files to a server. This method if allowed and misconfigured can lead to major vulnerabilities for the websever, due to the nature of this method. Text

Description automatically generated

Text

Description automatically generated with low confidenceDELETE – Is used to remove a file from the server, this is another method that MUST be properly configured to prevent malicious behavior. Misconfigured DELETE methods can lead to DOS attacks and data loss.

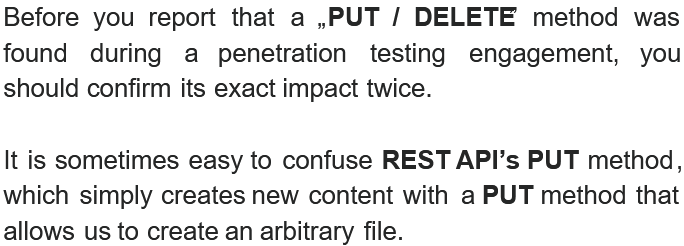
OPTIONS – Is used to query the web server for enabled HTTP Methods (verbs) A picture containing text

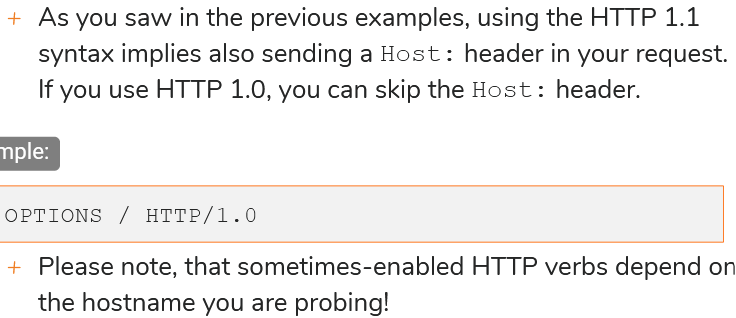
Description automatically generated

**REST API’s:** Representational State Transfer Application Programming Interface

REST API’s are a specific type of web application that heavily relies on almost all HTTP methods. REST API’s are also commonly referred to as web services or simply API’s.

Due to their heavy reliance on HTTP verbs, these verbs often come with subverted functionality.

* Its common for this type of application to use PUT for saving data as opposed to saving files. 
* After you issue a PUT request you should try to look for the existence of the file you created.



**Exploiting Misconfigured HTTP verbs:**

First we need to enumerate which methods are allowed by sending the OPTIONS method in netcat. Text, letter

Description automatically generated

Graphical user interface, text, application, email

Description automatically generatedExploiting DELETE: We could point this at a login page for example, making it impossible for anyone to log into the application.

Exploiting PUT:

Exploiting PUT is more complex as you need to know the size of the file you want to upload to the server. To find this you can use the UNIX utility, wc (word counter) with the -m flag to count how long in bytes the payload is. Ex: wc -m payload.php

Now that we known the size of our payload, we can do the following: Graphical user interface, text, application, email

Description automatically generated

Uploading a PHP shell with PUT:

Diagram, text

Description automatically generatedGraphical user interface, text, application

Description automatically generated

Graphical user interface, text

Description automatically generated

OR could read the file with cat utility. Any Linux utility could work here. We could also cat /etc/passwd

A screenshot of a computer

Description automatically generated with medium confidence