HTTP Methods on the Programmer Perspective

Many different languages are used to design and make a website functional. To be able to perceive the website structure, to give an example from real life, features such as hair color, eye color and height of the appearance help the individual to visually perceive the person. Likewise, HTML and CSS contain externally perceptible visual works of a website. Parts such as a text color and type, image sizes, buttons, and background design are created with the help of HTML and CSS. The brain and nervous system, which perform the processes that help the individual to use his physical features besides his appearance, coincides with languages such as ASP.NET, PHP and JavaScript on websites. Request Methods are used for the websites we create to be seen by others and to interact with people. Request Methods are similar to the questions we encounter daily. Below are both examples from daily life and the appearance of the same questions in terms of web sites.

Request	Purpose	Daily Life Part	Website Part
HEAD	Gather general information.	What's Your Name?	HEAD / HTTP/1.1
TRACE	Testing the connection with the source.	Do You Hear Me?	TRACE / HTTP/1.1
GET	Gather all information about the source.	Talk About Yourself	GET / HTTP/1.1
POST	Change an information owned by the resource.	You Don't Like Cats.	POST / HTTP/1.1
PUT	Imposing new information on the resource.	You have to do what I say.	PUT / HTTP/1.1
DELETE	Deletes the information of the source.	You don't have a name	DELETE / HTTP/1.1

As seen above, some HTTP Methods can cause serious changes. If the owner of the website can only access the specified methods, there is no problem in this part. Generally, HTTP Methods can greatly assist programmers for remote website control. In particular, some applications that are mostly used on websites have to make changes on the site. For example, in order for the website to run faster, a purchased app will have to change some of the website's algorithms over time, and the PUT method will use for it.

HTTP Methods on the Hacker Perspective

The functions of some HTTP Methods are mentioned in the table. Some of the functions mentioned will bring major troubles for the target. In particular, PUT and DELETE requests that are not filtered by programmers can be easily used to control the target website. Using the PUT method, a new page that may be harmful can be added to the website and all information about the target can be easily manipulated. Also, the

DELETE method can be used to make a website unusable. Hackers generally use applications that scan automatically to investigate a website's weaknesses. However, the specified applications are not always able to convey correct information about HTTP Methods. The following examples will show the methods used to search the HTTP Methods for the target website. The OPTIONS method, which is also an HTTP Method, can be used to detect unfiltered HTTP Methods found on a website. The OPTIONS method can reveal the methods allowed by the website. As can be guessed, programmers do not have the chance to deactivate all methods because they need methods such as HEAD, PUT and TRACE in order for browsers to go through their website. The table below contains information about which HTTP Methods can pose problems;

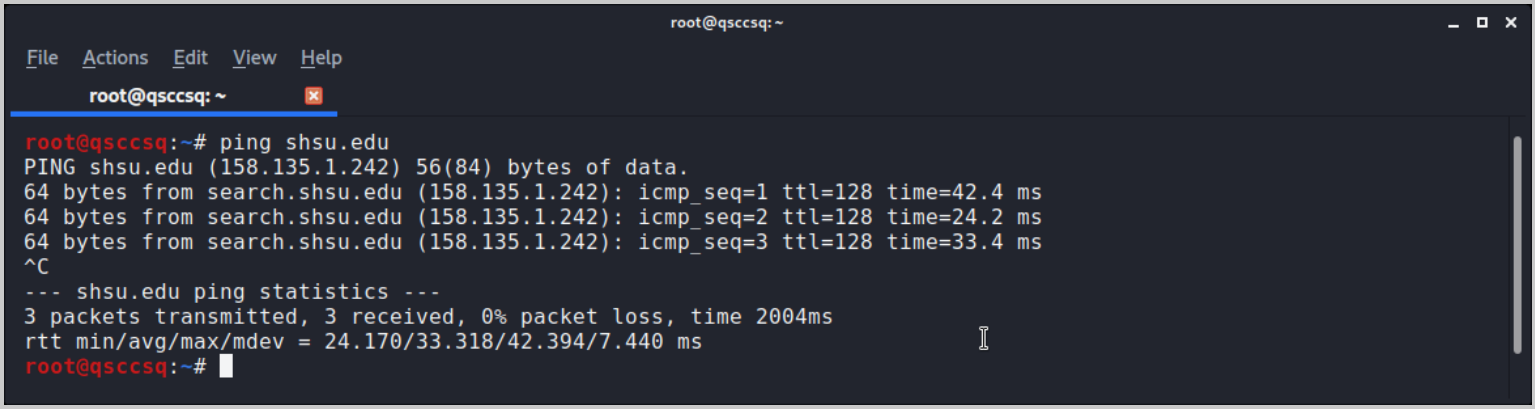
HTTP method	RFC	Request has Body	Response has Body	Safe	Idempotent	Cacheable
GET	RFC 7231	Optional	Yes	Yes	Yes	Yes
HEAD	RFC 7231	Optional	No	Yes	Yes	Yes
POST	RFC 7231	Yes	Yes	No	No	Yes
PUT	RFC 7231	Yes	Yes	No	Yes	No
DELETE	RFC 7231	Optional	Yes	No	Yes	No
CONNECT	RFC 7231	Optional	Yes	No	No	No
OPTIONS	RFC 7231	Optional	Yes	Yes	Yes	No
TRACE	RFC 7231	No	Yes	Yes	Yes	No
PATCH	RFC 5789	Yes	Yes	No	No	No

Source: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

Obtaining the IP Address of the Target

Code: ping shsu.edu After 2 sec. Ctrl + C (for stopping)

IP: 158.135.1.242

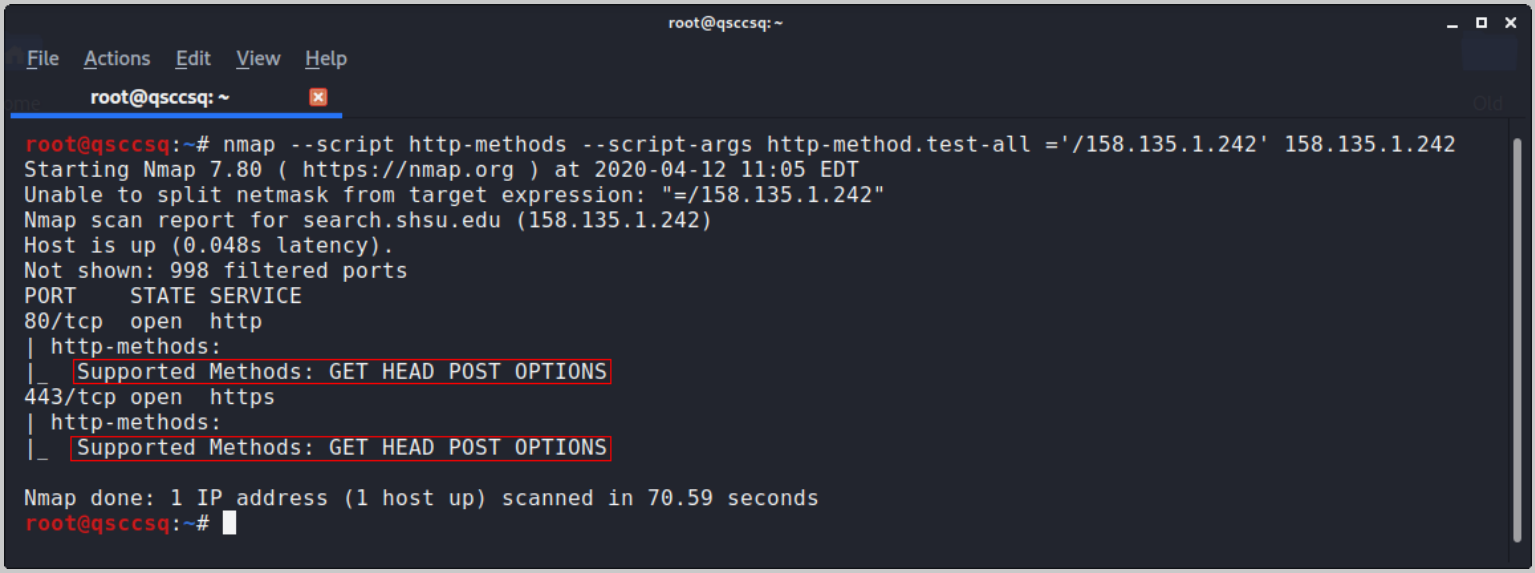


Nmap Usage

We can İdentify the HTTP Options Available on the Target by the help of Nmap;

Code: nmap -Pn --script http-methods --script-args http-method.test-all ='/158.135.1.242' 158.135.1.242

This process may take a while.



NetCat Usage

First Code: nc 158.135.1.242 80

Second Code: OPTIONS http:// 158.135.1.242 / HTTP/1.0

Third Code: host: 158.135.1.242

HTTP/1.0 302 Found = Web Site Does Not Show Methods with NetCat

Homework: Investigate a website for determining HTTP Methods using NMAP and NetCat. Write down difference between results of Nmap and NetCat. Take screenshots each steps and put them with your notes to a word file then send it.