« Practical Homework 1 - HTTP »

استاد: مهندس الوانی

نام و نام‌خانوادگی: نگار کرمی

شماره دانشجویی: ۹۷۲۲۰۳۹

دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

Question 1:

Well, I found two different approaches for achieving what the question wanted.

First one: Using **Loopback Interface**. Loopback is the routing digital data streams back to their source without intentional processing or modification.

Implementations of the Internet protocol suite include a virtual network interface through which network applications can communicate when executing on the same machine. It is implemented entirely within the operating system's networking software and passes no packets to any network interface controller. Any traffic that a computer program sends to a loopback IP address is simply and immediately passed back up the network software stack as if it had been received from another device. Such an interface is assigned an address that can be accessed from management equipment over a network but is not assigned to any of the physical interfaces on the device. The property that makes this virtual interface special is that applications that use it will send or receive traffic using the address assigned to the virtual interface as opposed to the address on the physical interface through which the traffic passes.

Second one: By using **private IP addresses**, we can restrict the access from external public Network. Private (internal) addresses are not routed on the Internet, and no traffic can be sent to them from the Internet; they are only supposed to work within the local network. These addresses are intended for use in closed local area networks, and no one globally controls the allocation of such addresses. Direct access to the Internet from a private IP address is not possible. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments. Both the IPv4 and the IPv6 specifications define private IP address ranges.

Private addresses include IP addresses from the following subnets:

1. Range from 10.0.0.0 to 10.255.255.255 — a 10.0.0.0 network with a 255.0.0.0 or /8 (an 8-bit) mask
2. Range from 172.16.0.0 to 172.31.255.255 — a 172.16.0.0 network with a 255.240.0.0 or /12
3. A 192.168.0.0 to 192.168.255.255 range, which is a 192.168.0.0 network masked by 255.255.0.0 or /16
4. A special range 100.64.0.0 to 100.127.255.255 with a 255.192.0.0 or /10 network mask

Question 2:

Transport Layer Security (TLS) encrypts data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what you transmit which is particularly useful for private and sensitive information such as passwords, credit card numbers, and personal correspondence. TLS protocol provides end-to-end security of data sent between applications

over the Internet but does not secure data on end systems and It is normally implemented on top of TCP in order to encrypt Application Layer protocols.

TLS uses a combination of symmetric and asymmetric cryptography, as this provides a good compromise between performance and security when transmitting data securely.

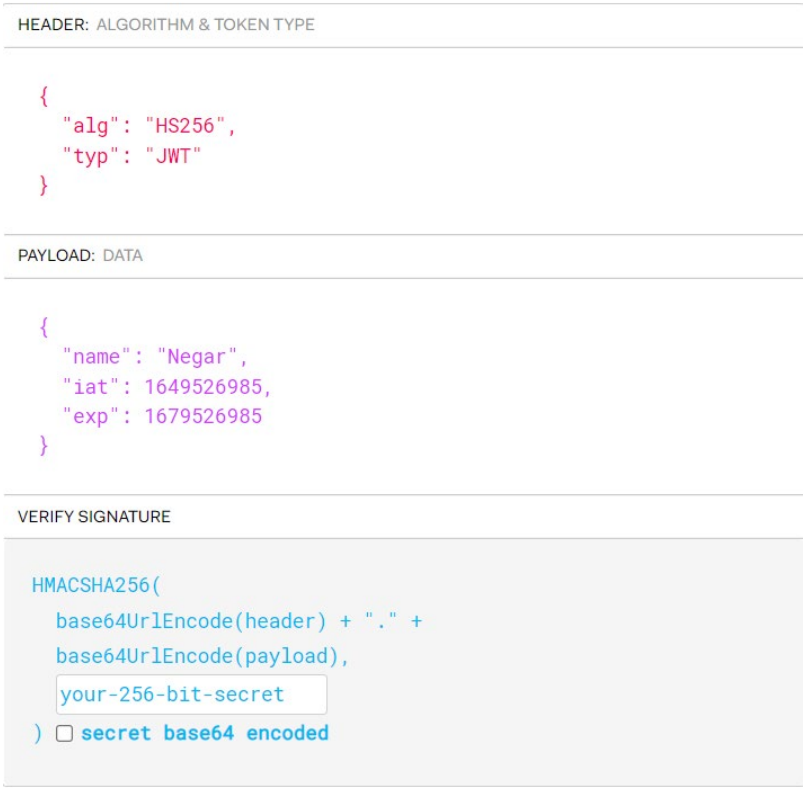
With symmetric cryptography, data is encrypted and decrypted with a secret key known to both sender and recipient. Symmetric cryptography is efficient in terms of computation, but having a common secret key means it needs to be shared in a secure manner.

Asymmetric cryptography uses key pairs – a public key, and a private key. The public key is mathematically related to the private key, but given sufficient key length, it is computationally impractical to derive the private key from the public key. This allows the public key of the recipient to be used by the sender to encrypt the data they wish to send to them, but that data can only be decrypted with the private key of the recipient.

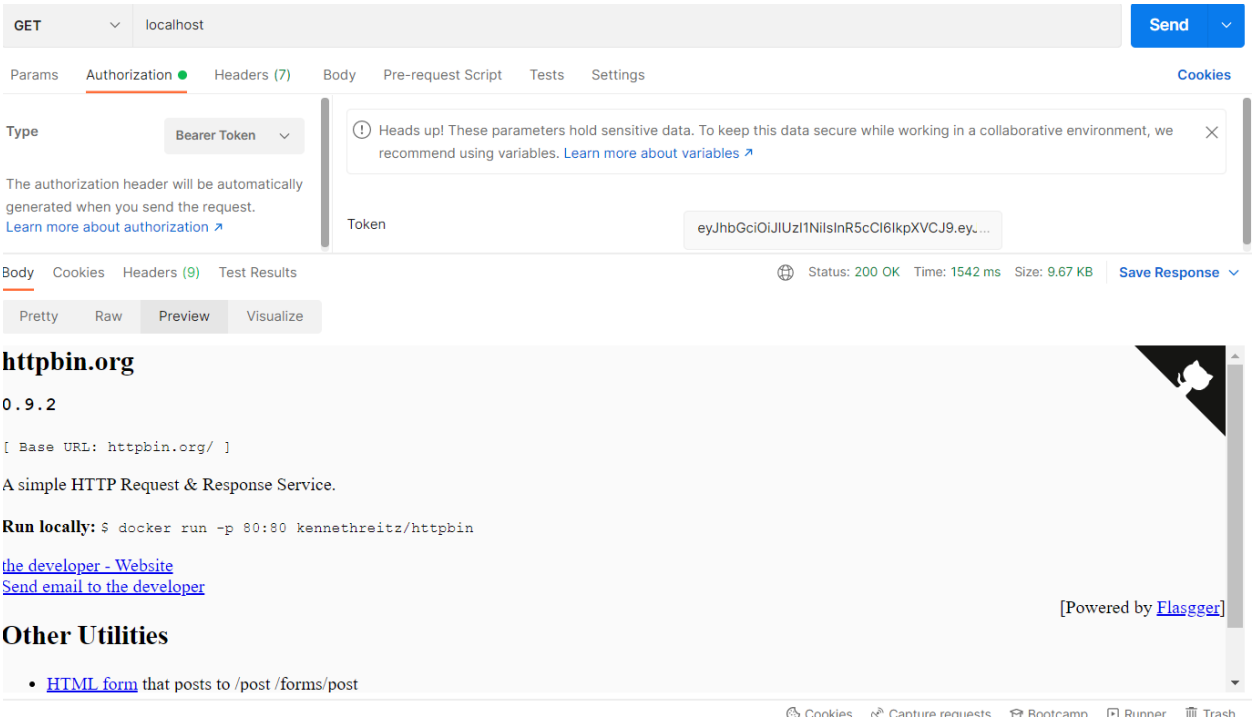
Question 3:

If we send correct token like bellow, we will get this output:

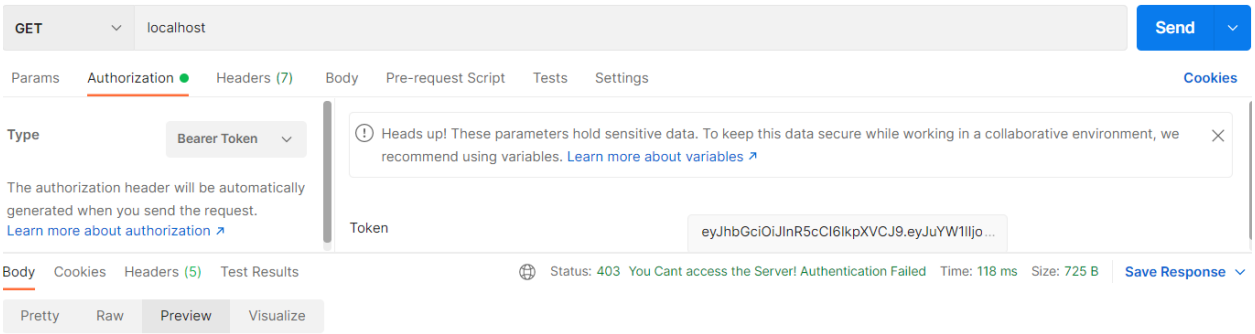
Token =
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoiTmVnYXIiLCJpYXQiOjE2NDk1MjY5ODUsImV4cCI6MTY3OTUyNjk4NX0.1n9Gqa5kKmqNBAHei0vDQHYWE48p7GDblSQcedWxt3c



Output:



But if we send incorrect token or don't send any token at all, we will get this output:



Error response

Error code: 403

Message: You Cant access the Server! Authentication Failed.

Error code explanation: 403 - Request forbidden -- authorization will not help.