WEB PENTESTING

BY D4RK LEGEND

HTTP BASICS

1. What Is HTTP ?
2. HTTP Request & HTTP Responses.
3. HTTP Methods.
4. HTTP Headers.
5. Status Codes.

WHAT IS HTTP?

HTTP Stands for Hypertext Transfer Protocol. hypertext is chunks of text documents which are linked to each other via hyperlinks and HTTP is the protocol to send hypertext from the web server to web browser.

HTTP (Hypertext Transfer Protocol) is an application protocol and is used to access the world wide web.

HTTP REQUEST & RESPONSES

In a HTTP request the client sends request to the server in order to get the response. An HTTP request consists of one or more headers each on a separate line.

Example of an HTTP Request:-

HTTP RESPONSE

In an HTTP Response, the server sends response to the client of the given request. The HTTP response consist of one or more headers each on a separate line.

Example Of An HTTP Response:-

```
HTTP/1.1 200 OK
Date: Sat, 19 May 2007 13:49:37 GMT
Server: IBM_HTTP_SERVER/1.3.26.2  Apache/1.3.26 (Unix)
Set-Cookie: tracking=tI8rk7joMx44S2Uu85nSWc
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=ISO-8859-1
Content-Language: en-US
Content-Length: 24246

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html lang="en">
<head>
    <meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">
```

HTTP METHODS

HTTP METHODS ARE SUPPLIED IN THE REQUEST LINE AND SPECIFY THE OPERATION THAT THE CLIENT HAS REQUESTED. THE TWO MAIN METHODS IN THIS ARE GET & POST METHODS. ALONG WITH THIS THERE ARE OTHER METHODS WHICH HAVE BEEN CREATED FOR SPECIFIC PURPOSES.

1. GET:- GET IS TYPICALLY USED TO FETCH/RETRIEVE DATA FROM THE SERVER.
2. POST:- POST METHOD IS USED TO SEND THE DATA TO THE SERVER.
3. PUT:- PUT METHOD IS USED TO UPDATE THE CURRENT EXISTING RESOURCES.
4. DELETE:- DELETE METHOD IS USED TO DELETE THE RESOURCE GIVEN BY URL.
5. OPTIONS:- OPTIONS METHOD IS USED TO REPRESENT REQUEST FOR INFORMATION ABOUT THE COMMUNICATION OPTIONS FOR THE TARGET RESOURCE.

HTTP HEADERS

HTTP Headers give information about the request and response of message headers for HTTP. HTTP Headers are the code that transfer data between web server and browser.

There are three types of HTTP message headers:-

1. General Header:- The General Header fields have common applicability for both request and response message.
2. Request Header:- Request Header fields have applicability for only request message.
3. Response Header:- Response Header fields allow the server to pass extra information through the response message.

STATUS CODE

HTTP Response indicate whether a specific HTTP request has been successfully completed or not.

The Status Code is divided into five groups:-

1. 1xx:- This is informational means the request has been received.
2. 2xx:- This means that the server successfully processed the request.
3. 3xx:- This means the user is redirecting to somewhere else.
4. 4xx:- This means that there is an error in the request which prevented the server from being able to process.
5. 5xx:- This means that the client made the right request but the server failed.

UPCOMING..

Hope The Topics are clear to you.

In The upcoming series we will look into the topics:-

1. Networking basics terminology.
2. IP addresses.
3. DNS & PORTS.

Please mail your queries , questions at :- community@sec.army

We look forward to help you and enrich the community.

THANK YOU .

https://community.sec.army