Cheatography

JavaScript Cheat Sheet

by binca via cheatography.com/44948/cs/13428/

About

Most common client-side scripting language in use. Originally designed by Netscape in 95 and called LiveScript.

Use for for reading and understanding scripts from the target systems.

Can be used to write attacks against target systems.

In web pages is can be inline with HTML via **<script>** tags, as a part of an HTML item **<img src="link" onload="javascript;">**, or loaded from an external document **<script src=http://evil.agent/bad.js>**

It is an object-oriented language.

Control Statements

while loop	Runs a block of code until a condition is met
for loop	Runs for a set number of times

Variables

Any type of data can be assigned to a variable without concern.

Declaration: **var x;**

Variables can be assigned at declaration or later. **var x="string";** or **x="string";**

If a variable is re-declared after a value is assigned to it, the original value is still assigned.

Global variables are those declared outside of functions and are accessible everywhere.

Instance variables are those declared within a function and are exclusive to the function.

Functions

Functions can be declared anywhere within the page, but it is safest to declare in the <HEAD> to ensure they are loaded before being called.

function name(var1, var2) { some code }

To return data from a function use **return var;** statement within the function.

Call a function using **function_name()**

Events

onload	Page of item is finished loading
onunload	User leaves the page the script is on
onerror	An error occurs loading page or item
onclick	Item is clicked on with mouse
onsubmit	The form is submitted
onfocus	The item receives focus
onblur	The item loses focus
onchange	Content of field changes
onmouseover	The mouse is hovering over item

Every item in a page has a series of associated events. The event calls a function.

Events within Attacks

onload	Change content of page after it loads
onunload	Launch pop-under window to retain control of a zombie browser
onsubmit	Change form values so the transaction is one of the attacker's choosing.
onfocus	Send HTTP request to attacker's web server to reveal which controls the user is selecting.
onerror	Used within web scanners injected via XSS to determine a resource does not exist. Usefule when port scanning a network using JavaScript.
onclick	Change where a link points without the user knowing.
onmouseover	Track the movement of the mouse across a page.
onblur	Send the contents of a form field to an attacker.

JavaScript Cheat Sheet

by binca via cheatography.com/44948/cs/13428/

Document Object Model (DOM)

Provides standard interface tot he document allowing scripts to dynamically access and update content, structure, or style of the page.
Doc referenced is either HTML or XML

DOM provides native objects to access various items of interest:
document.forms[0] refers to 1st form on page
document.write("string") write string to the page
document.write(document.cookie) will write value of the page's cookies to the page

Form object is used to access a specific form
form.action=[URL] sets the forms action to the URL allowing for redirecting the browser to another page
form.submit() will submit form

DOM Nodes

Viewed as a tree the HTML tag is the root and has two children **<HEAD>** and **<BODY>**. Each other them have children and so forth.

Object Methods and Properties

Objects have to be initialized instead of being assigned to a variable;
var string=new String();

Objects have properties, attributes of the object, and methods, which are actions performed on the object.

Devs can create their own objects.

When referring to a property of an object, we use the format **object.property**, such as **document.referrer**.

Calling a method is similar but also requires **( )** with values determined by the method.

Objects and Associated Properties and Methods

Object Type	Method	Property
String	**split()** parses the string	length returns size
Date	**getTime()** returns current time **getMonth()** returns current month	

Objects and Associated Properties and Methods (cont)

Array	**join()** joins the elements in the array **sort()** sorts the array	
Window	**open()** creates a new browser window **alert()** pops up a dialog box	
Document	**write()** writes content to the page **referrer()** returns referring URL	
Location	**reload()** reloads doc	**port()** returns the port of the current page
History	**back()** is the same as the back button	Length returns history item count

Selecting and Changing Content

Scripts can find specific content by walking the DOM.

The script can read the item's attributes and associated items such as text.

The script can then rewrite the item.

```
function counttags(tag) {
count = document.getElementsByTagName(tag).length
return count
}
```

Interacting with Cookies

strCookie=document.cookie returns only the name=value pairs

Parsing the cookie takes a little work.
1. Parse to split each name=value pair. **var arrValues=document.cookie.split(';');**
2. Loop through each pair and split on the **=**. (4:22)

Setting cookies only requires 3-4 parameters: **A cookie name and value pair**
Expiration time for the cookie ad URI path that is able to access it
Data NOT required for session cookies

```
document.cookie="userid=person; expires=Wed, 1-Nov-2017; path=/";
```