# JavaScript部分面试

1. **JavaScript有哪些输出语句。**

JavaScript 中为我们提供了多种不同的输出语句来向浏览器中输出内容， 主要有一下几个语句：

（1）使用 alert() 函数来弹出提示框；

（2）使用 confirm() 函数来弹出一个对话框；

（3）使用 prompt() 浏览器弹出输入框，用户可以输入；

（4）使用console.log() 在浏览器的控制台输出内容。

（5）使用 document.write() 方法将内容写入到 HTML 文档中；

（6）使用 innerHTML 将内容写入到 HTML 标签中

1. **你了解JavaScript中的BOM和DOM吗？说说他们是什么？**

在JavaScript中，BOM（Browser Object Model，浏览器对象模型）和DOM（Document Object Model，文档对象模型）是两个非常重要的概念，它们分别代表了浏览器和文档（即网页）的不同方面。

**（1）DOM（Document Object Model）**

document：表示文档（表示整个页面）对象。document对象具有页面几乎所有的方法或者属性。例如：

document.title 获取页面的标题。

document.cookie获取页面的cookie。

**DOM 事件**监听：我们计算机在解析我们JS代码的时候，会去看某一些元素身上是否添加了事件。并监听 这些事件有没有被触发，如果触发就立即执行相应的行为。 例如：

onclick 单击

ondblclick 双击

onmouseenter 鼠标进入

**（2）BOM（Browser Object Model）**

BOM提供了与浏览器交互的接口，而不是与页面内容交互。BOM是JavaScript语言的一部分，而不是DOM的一部分。BOM提供了很多对象，用于访问浏览器的功能，如导航、屏幕信息、浏览器历史、本地存储等。

BOM的主要对象包括：

* window：BOM的顶级对象，代表了浏览器的一个实例（通常是浏览器窗口）。它提供了很多属性和方法，用于操作浏览器窗口，如设置定时器、打开和关闭窗口等。例如：window.open() - 打开新窗口
* location：提供了当前窗口加载的文档的URL信息，也可以用来导航到新的URL。例如：history.back() - 与在浏览器点击后退按钮相同
* navigator：提供了有关浏览器的信息，如浏览器名称、版本、操作系统等。例如：navigator.appName - 浏览器名称
* screen：提供了用户屏幕的信息，如分辨率和颜色深度。例如：screen.availWidth - 可用的屏幕宽度
* history：提供了对当前窗口（也就是标签页或浏览器窗口）访问过的URL的历史记录进行访问的接口。例如：location.hostname - 返回 web 主机的域名

1. **假如发现一个前端js加密登录的网站，你会如何做？**

在渗透测试过程中，面对采用前端js加密的登录机制，我首先会系统地收集网站的相关信息，使用网络抓包工具（如BurpSuite）捕获和分析登录请求，分析哪些数据被加密，以及加密的可能类型。接着，利用开发者工具打断点进行调试，找到加密函数和加密逻辑，把js加密代码导出，通过js加密代码编写模拟加密脚本进行验证，最后可以利用模拟加密脚本生成大量的密文字典，并使用自动化工具（如BurpSuite）对网站进行密码爆破尝试。