Vidar——Web 安全启蒙 课后思考、探究题目

> 今天的培训首先为大家介绍了Web应用运作的各个环节，并让大家知道，在每个环节过程中，都可能会出现一些安全问题。同时大家应该也能感受到，各个环节具体的运作方式依然是可以细化的。那么在听课的时候，你有没有考虑过这样几个问题?

1. 在浏览器运作方式的时候，我们提到，浏览器会将返回实体内的 HTML 进行渲染，但是浏览器是如何判断返回的内容实体是HTML、要进行渲染的呢？真的只是看到符合HTML 标签格式的内容就渲染吗？当然不是，那么 浏览器是如何进行判断的呢?
2. 继续说浏览器渲染的问题，我们培训时提到了，浏览器将HTML 渲染为DOM 树，将 CSS 渲染为样式树。那么这个渲染过程究竟是怎样的呢？二者是一起渲染的、还是分开渲染的？页面是等待所有的内容全部渲染完成才显示的，还是边渲染边显示的呢？DOM 树的渲染，又是按照什么顺序进行的呢?
3. 我们说 JavaScript 是负责网页行为的，那么我们是否可以通过在某个网页中插入一段 JS 代码，来控制其他网站的页面行为呢?
4. 除了 JavaScript 之外，还有没有其他的编程语言能够控制页面的行为呢?
5. 来说说服务端，我们提到，服务器会根据请求的文件类型，选择是直接返回文件内容，还是将请求传递给后端程序。也提到了Apache 在遇到 “不认识” 的文件后缀名时，会向前寻找有没有自己 “认识” 的后缀名。那么这个 “认识” 或者 “不认识” 是根据什么决定的呢？不同文件的默认处理方式，又是根据什么决定的呢?
6. 浏览器和服务端通信方面，HTTP 是一种无状态的请求，也就是说，只传递数据，不保持状态。那么“状态”（如登录状态）是通过什么来维持的呢？需要浏览器、服务器、程序 、以及后端的其他软件之间怎样配合呢?
7. 数据合法性校验（如邮箱格式、验证码是否正确等），应该在客户端进行、还是服务端进行呢?
8. xss 是针对客户端的攻击方式，那么客户端（浏览器），通常都有哪些防御、缓解xss 的方式呢?服务端可以提供哪些支持呢

> 以上的问题，所有听了今天培训的同学都可以思考一下，而下面的问题，适合已经开始学习后端相关知识的同学思考

1. 服务器具体是如何处理 HTTP 请求的？（非常笼统的问题，所以答案可以非常具体）
2. 服务端上后端程序运行的默认权限是怎样的呢?
3. 伪静态是什么？如何实现?

上面的问题，大多是有关于 “如何实现” 的，那么听完今天的培训，大家应该知道，我们研究安全，在了解如何实现的基础上，更应该去思考的是：实现的过程中会不会导致安全问题。那么在找到上面的问题的答案之后，你能不能从中学习到一些有关安全的知识呢?