# XCTF攻防世界Web12道简单题

转载

高野02 于 2020-11-30 20:34:28 发布 198 收藏 1

分类专栏： CTF 安全

原文链接：https://www.lagou.com/lgeduarticle/38567.html




CTF 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏


安全

8 篇文章 0 订阅

订阅专栏

0x00 准备

【内容】

在xctf官网注册账号，即可食用。

【目录】

目录



0x01 view-source

【题目描述】

X老师让小宁同学查看一个网页的源代码，但小宁同学发现鼠标右键好像不管用了。

【目标】

学会查看源代码

【工具】

firefox浏览器

【分析过程】

可以通过view-source:的方法来访问源码：html view-source:http://10.10.10.175:32796

在url中提交后便可访问页面源码，在源码中可找到flag。

【参考网址】

https://blog.csdn.net/weixin_43605586/article/details/90020256

【温故知新】

view-source:命令 等价于 右键网页，查看网页源代码

这是一个大多数人都会的操作，只是不知道这个操作其实就是一个简单的命令而已。

当然这个题说的是右键不管用了，那么就只能输入这个命令来查看源代码了，道理都是一个样。

0x02 get post

【题目描述】

X老师告诉小宁同学HTTP通常使用两种请求方法，你知道是哪两种吗？

【目标】

了解http请求方法，此处考察get和post两个最常用的请求方法。

HTTP协议中共定义了八种方法或者叫“动作”来表明对Request-URI指定的资源的不同操作方式，具体介绍如下：

·GET：向特定的资源发出请求。

·POST：向指定资源提交数据进行处理请求（例如提交表单或者上传文件）。数据被包含在请求体中。POST请求可能会导致新的资源的创建和/或已有资源的修改。

·OPTIONS：返回服务器针对特定资源所支持的HTTP请求方法。也可以利用向Web服务器发送'*'的请求来测试服务器的功能性。

·HEAD：向服务器索要与GET请求相一致的响应，只不过响应体将不会被返回。这一方法可以在不必传输整个响应内容的情况下，就可以获取包含在响应消息头中的元信息。

·PUT：向指定资源位置上传其最新内容。

·DELETE：请求服务器删除Request-URI所标识的资源。

·TRACE：回显服务器收到的请求，主要用于测试或诊断。

·CONNECT：HTTP/1.1协议中预留给能够将连接改为管道方式的代理服务器。

【工具】

火狐浏览器插件hackbar（license随便乱写，然后save，重启即可食用）

【分析过程】

在url后添加/？a=1即可发送get请求。

F12，使用hackbar插件，复制get的url，选择postdata，填入b=2，选择execute。即可发送POST请求。

【有待提高】

这里只了解了GET和POST请求，但对于其他的6个请求知之甚少，仍需要大量的相关题型才能有一个全面的了解。所以，有待提高！

0x03 robots

【题目描述】

X老师上课讲了Robots协议，小宁同学却上课打了瞌睡，赶紧来教教小宁Robots协议是什么吧。

【目标】

掌握robots协议的知识

robots.txt是搜索引擎中访问网站的时候要查看的第一个文件。当一个搜索蜘蛛访问一个站点时，它会首先检查该站点根目录下是否存在robots.txt，如果存在，搜索机器人就会按照该文件中的内容来确定访问的范围；如果该文件不存在，所有的搜索蜘蛛将能够访问网站上所有没有被口令保护的页面。

【环境】

无

【工具】

扫目录脚本dirsearch(项目地址：https://github.com/maurosoria/dirsearch)

【分析过程】

提示robots,可以直接想到robots.txt,扫目录也可以扫到:

python python3 dirsearch.py -u http://10.10.10.175:32793/ -e *

这里我们将下载好的dirsearch脚本解压后，打开dirsearch.py文件，运行一下，提示需要输入命令：-u http://10.10.10.175:32793/ -e *。（跑程序相对较慢，稍作等待）

在.reports111.198.29.45目录下找到刚输出的文件：

打开即可看到扫出的目录和文件。即可看到存在robots.txt文件。

HTML访问robots.txt发现f1ag_1s_h3re.php

访问robots.txt发现f1ag_1s_h3re.php

【有待提高】

扫目录的脚本的原理一脸懵逼！

【知识扩展】

利用robots.txt快速抓取网站的小窍门

0x04 backup

【题目描述】

X老师忘记删除备份文件，他派小宁同学去把备份文件找出来,一起来帮小宁同学吧！

【目标】

掌握有关备份文件的知识

常见的备份文件后缀名有: .git .svn .swp  .~ .bak .bash_history（共6种）

【工具】

火狐浏览器插件hack bar

扫目录脚本dirsearch(项目地址：https://github.com/maurosoria/dirsearch)

【分析过程】

可以手动猜测,也可以使用扫目录脚本或软件,扫一下,这里使用的是github上的脚本dirsearch,命令行下: py python3 dirsearch.py -u http://111.198.29.45:47591 -e *

看到存在备份文件index.php.bak访问 http://10.10.10.175:32770/index.php.bak

下载到本地打开，即可看到flag

0x05 Cookie

【题目描述】

X老师告诉小宁他在cookie里放了些东西，小宁疑惑地想：‘这是夹心饼干的意思吗？’

【目标】

掌握有关cookie的知识

Cookie 可以翻译为“小甜品，小饼干”，Cookie 在网络系统中几乎无处不在，当我们浏览以前访问过的网站时，网页中可能会出现 ：你好 XXX，这会让我们感觉很亲切，就好像吃了一个小甜品一样。这其实是通过访问主机中的一个文件来实现的，这个文件就是 Cookie。在 Internet 中，Cookie 实际上是指小量信息，是由Web服务器创建的，将信息存储在用户计算机上的文件。一般网络用户习惯用其复数形式 Cookies，指某些网站为了辨别用户身份、进行Session 跟踪而存储在用户本地终端上的数据，而这些数据通常会经过加密处理。

【工具】

浏览器开发者工具

【分析过程】

F12-存储-Cookie-look here-look here：cookie.php

发送cookie.php请求，提示看http响应。在响应头里发现flag。

【有待提高】

Cookie怎么存储，存储的原理，传输的原理尚未可知！

0x06 disabled button

【题目描述】

X老师今天上课讲了前端知识，然后给了大家一个不能按的按钮，小宁惊奇地发现这个按钮按不下去，到底怎么才能按下去呢？

【目标】

初步了解前端知识

对于HTML的基本语法知识需要一定的了解，对于每个标签，有一些不可用属性，如：disabled，借助开发者工具可以删除这些属性，从而让其变得可用！

【工具】

开发者工具

【分析过程】

F12，将标签input中的disabled（不可用）属性删除，x掉调试框，点击按钮，即可得到flag。

也可以手动POST相关数据，以下为部分源代码：

于是构造POST请求：auth=flag

0x07 simple js

【题目描述】

小宁发现了一个网页，但却一直输不对密码。(Flag格式为 Cyberpeace{xxxxxxxx} )

【目标】

掌握有关js的知识

【工具】

开发者工具

【分析过程】

F12查看网页源代码，找到index文件，仔细阅读js代码。（或者view-source:命令）

会发现dechiffre返回值与参数pass_enc没有任何关联，返回值是固定的，即不论输入什么都是一样得输出。所以猜测密码在string这一行里。

利用python代码来求出flag：先将16进制数输出，再将数字（ascii码）转换为对应的字符。

0x08 XFF Referer

【题目描述】

X老师告诉小宁其实xff和referer是可以伪造的。

【目标】

掌握有关X-Forwarded-For和Referer的知识

X-Forwarded-For:简称XFF头，它代表客户端，也就是HTTP的请求端真实的IP，只有在通过了HTTP 代理或者负载均衡服务器时才会添加该项。

HTTP Referer是header的一部分，当浏览器向web服务器发送请求的时候，一般会带上Referer，告诉服务器我是从哪个页面链接过来的，服务器基此可以获得一些信息用于处理。

xff 是http的拓展头部，作用是使Web服务器获取访问用户的IP真实地址（可伪造）。由于很多用户通过代理服务器进行访问，服务器只能获取代理服务器的IP地址，而xff的作用在于记录用户的真实IP，以及代理服务器的IP。

格式为：X-Forwarded-For: 本机IP, 代理1IP, 代理2IP, 代理2IP

referer 是http的拓展头部，作用是记录当前请求页面的来源页面的地址。服务器使用referer确认访问来源，如果referer内容不符合要求，服务器可以拦截或者重定向请求。

【环境】

firefox选项-常规-网络设置-手动代理配置（与burp suite代理地址相同）-不使用代理服务器-确定

https的取得看https://baijiahao.baidu.com/s?id=1608443655431062847&wfr=spider&for=pc

【工具】

火狐浏览器插件hackbar

火狐浏览器插件modify headers（不要下载mini版本的）

或burp suite然间

【分析过程】

在Proxy的History里找到目标网页，右键选择发送到repeater。

在repeater里查看目标地址内容，添加：

X-Forwarded-For:123.123.123.123（这一步是伪造XFF，go一下，收到提示）

Referer:https://www.google.com（这一步是伪造Referer）

0x09 weak auth（弱口令密码）

【题目描述】

小宁写了一个登陆验证页面，随手就设了一个密码。

【目标】

掌握有关密码爆破的知识

Intruder是一个定制的高度可配置工具，可以对Web应用程序进行自动化攻击。

原理：Intruder在原始请求数据的基础上，通过修改各种请求参数获取不同的请求应答。在每一次请求中，Intruder通常会携带一个或多个有效攻击载荷（Payload），在不同的位置进行攻击重放，通过应答数据的比对分析获得需要的特征数据。

【工具】

Burp Suite

【分析过程】

查阅了很多资料（书、网页等）

方法同上，设置Firefox的代理，找到目标网址，右键选择发送到Intruder。（也可以选择Raw的文本）

找到Positions，清楚标记Clear，指针指向password=后面，添加标记Add，如下图所示，将密码放在两个$pass$之间。

找到Payloads，加载Load Payload Options，将下载好的字典添加进去。

选择左上角startAttack开始爆破。

结果在Results里，选择length排序，（点两下）与其他不一样长的便是答案（一般说来，有特殊情况）。如图：

【名册解释】

Payload 载荷

Grep 匹配

Case Sensitive match 大小写敏感

Number of retries on network failure 网络故障的重试次数

pause before retry 重试前等待的时间

Throttle between requests 请求之间的等待时间

Recursive grep 递归查找

brute force 暴力破解

【参考书籍】

《Web安全攻防》Intruder模块P60

【参考网页】

BurpSuite之Intruder详解
对Intruder的解释非常详尽，并且配置了生动的图文教程，是目前学习BurpSuite最好的网页。值得推荐！

Github上的爆破字典
这是一个来自Github上的字典，基本涵盖了大多数的常用非复杂密码。你，值得拥有！

0x10 web shell

【题目描述】

小宁百度了php一句话,觉着很有意思,并且把它放在index.php里

【目标】

了解如何使用web shell

【工具】

中国菜刀

蚁剑（还没用过） https://github.com/AntSwordProject/antSword/releases(https://github.com/AntSwordProject/antSword/releases

【分析过程】

打开中国菜刀，右键空白处添加，填入如下内容：

编辑(确定）后，双击添加的url，打开flag.txt。得到flag

【参考网页】

中国菜刀如何使用

0x11 command_execution

【题目描述】

小宁写了个ping功能,但没有写WAF,X老师告诉她这是非常危险的，你知道为什么吗。

【目标】

掌握有关命令执行的知识

windows或linux下:

command1 && command2 先执行command1，如果为真，再执行command2

command1 | command2 只执行command2

command1 & command2 先执行command2后执行command1

command1 || command2 先执行command1，如果为假，再执行command2

命令执行漏洞（| || & && 称为 管道符）

【工具】

无

【分析过程】

一脸懵逼

啥也不知道，为什么大家上来就知道flag藏在当前目录的上三级目录里。

所以命令如下图所示：

flag藏在home里，继续一脸懵逼。

这里是懂了，使用cat命令打开flag

【参考书籍】

《Web安全攻防》命令执行模块P173

0x12 simple php

【题目描述】

小宁听说php是最好的语言,于是她简单学习之后写了几行php代码。

【目标】

掌握php弱类型比较

php中有两种比较符号:

==: 先将字符串类型转化成相同，再比较值

===: 先将字符串类型转化成相同，再比较值

字符串和数字比较使用==时,字符串会先转换为数字类型再比较 php var_dump('a' == 0);//true，这里'a'会被转换数字0 var_dump('123a' == 123);//true，这里'123a'会被转换为123

【工具】

无

【分析过程】

var_dump(‘1234a’ == 1234)结果为true,php的弱类型比较会忽略字母a

所以后半段可以用： html http://10.10.10.175:32779/index.php?a=a&b=1235a

这里我们采用如下图所示的url。

a=字符0，if判断a==0，字符0转换成数字0，所以为真；a为字符，非空，为真。

0xff 附录

【总结】

web新手题12道全部完成，一共用了3-4天时间吧！感觉web题需要的知识点很宽泛，需要平时的积累，其难度大多都是利用某一个点，可能是还没有接触进阶题的缘故，所以题解都很简单，只需要掌握一些简单的工具和一些语言的部分语法即可食用！在这些工具里，最强大最综合的是Burp Suite了，熟练掌握对解题很有帮助！但是有一个工具Nmap至今没有接触过，这个才是网络攻击的最强杀手锏。（不知道是不是还有没有流通出来的完整版Nmap）接下来的计划有两种选择：

从头学习《web安全攻防》，主要涉及搭建自己的本地服务器，并对常见的web漏洞有一个直观的感受和实战操作。为下步打下坚实的基础。但比较枯燥。
继续解题，web的进阶题，趣味性强，知识点宽泛且散度较大。不利于知识点的归纳和总结。