攻防世界XCTF—web入门题知识点、进阶提高题Writeup

原创

带你看宇宙 于 2020-08-21 00:19:58 发布 264 收藏 3

分类专栏： CTF 文章标签： 信息安全 python web php

本文链接：https://blog.csdn.net/ZHANGJIALIh/article/details/108135309

WriteUp

- XCTF-Web
  - 新手入门区
    - view_source
    - get_post
    - robots
    - backup
    - cookie
    - disabled button
    - simple js
    - xff referer
    - weak auth
    - webshell
    - command execution
    - simple_php
  - 高手进阶区

XCTF-Web

> 2016 年全国大学生信息安全竞赛开始设立创新实践技能赛，采取的就是传统的 CTF 赛制。在《2016年全国大学生信息安全竞赛参赛指南》中主办方给出的竞赛内容相对全面，值得参考。
>
> 系统安全。 涉及操作系统和 Web 系统安全，包括 Web 网站多种语言源代码审计分析（特别是 PHP）、数据库管理和 SQL 操作、Web漏洞挖掘和利用（如 SQL 注入和 XSS）、服务器提权、编写代码补丁并修复网站漏洞等安全技能。

攻防世界: 传送门.

新手入门区

view_source

知识点：查看源代码

> **Description：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。**

查看源代码的方法：

1. 功能键+F12打开开发者工具查看
2. 在url中通过view-source:的方法来访问源码，在url中提交view-source:http://
3. 通过Burpsuite抓包查看源代码
4. 通过python的requests.get()获取网页源码

get_post

知识点：通过url使用get传递参数和学会使用hackbar

> **Description：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？**

GET方式想要传递参数的格式：在网址后面拼接上参数名和参数值就可以，**地址?参数名1=参数值&参数名2=参数值**

POST方式需要以表单形式提交参数，使用火狐浏览器**Hackbar**插件提交参数名=参数值

robots

知识点：robots协议（爬虫需要遵守这个规定）

robots协议别名爬虫协议、机器人协议，通过robots协议告诉搜索引擎哪些页面可以抓取、哪些不能抓取，用于防治搜索引擎抓取敏感信息，维持网站和搜索引擎之间的平衡。一般来说，网站是通过robots.txt来实现robots协议。

文件用法

例1. 禁止所有搜索引擎访问网站的任何部分

User-agent: *

Disallow: /

实例分析：淘宝网的 Robots.txt文件

User-agent: Baiduspider

Disallow: /

User-agent: baiduspider

Disallow: /

很显然淘宝不允许百度的机器人访问其网站下其所有的目录。

例2. 允许所有的robot访问 (或者也可以建一个空文件 "/robots.txt" file)

User-agent: *

Allow: /

例3. 禁止某个搜索引擎的访问

User-agent: BadBot

Disallow: /

例4. 允许某个搜索引擎的访问

User-agent: Baiduspider

allow:/

> **Description: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。**

先找robots.txt文件，在网页的url后面加/robots.txt就可以转到该页面，得到 flag_1s_h3re.php ，直接访问这个php即可拿到flag。

backup

知识点：常见的备份文件后缀名有: .git .svn .swp .svn .~ .bak .bash_history

> **Description：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！**

题目提示为index.php的备份文件，网站备份压缩文件有 .rar .zip .7z .tar.gz .bak .swp .txt .html 等格式，挨个尝试，.bak访问成功下载index.php的备份文件，使用文本编辑器打开即可拿到flag。

也可以用目录扫描工具dirsearch扫出index.php.bak文件，然后构造链接。

cookie

知识点：cookie，指某些网站为了辨别用户身份、进行 session 跟踪而储存在用户本地终端上的数据（通常经过加密）。

> **Description：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？**

第一种方法，在控制台输入javascript脚本显示出cookie；alert(document.cookie)

也可使用另一种方法，使用Burpsuite工具抓包查看http请求头的Cookie值，访问后提示查看response，在响应头里找到flag。

disabled button

知识点：标签属性

> **Description：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？**

使用浏览器开发者工具查看源代码，发现 < input >标签存在属性disabled 使按钮无法交互，删去 disabled 属性即可点击按钮拿到flag 。

simple js

知识点：url编码，一种浏览器用来打包表单输入的格式。

URL编码遵循下列规则： 每对name/value由&；符分开；每对来自表单的name/value由=符分开。如果用户没有输入值给这个name，那么这个name还是出现，只是无值。

任何特殊的字符将以百分符%用十六进制编码，当然也包括 =,&；，和 % 这些特殊的字符。简单来说，url编码就是一个字符ascii码的十六进制。不过需要在前面加上“%”。

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

打开网页可以看到这些js代码，将里面的字符串转换为URL编码
%35%35%2c%35%36%2c%35%34%2c%37%39%2c%31%31%35%2c%36%39%2c%31%31%34%2c%31%31%36%2c%31%30%37%2c%34%39%2c%35%30
转换为URL编码，解码得55,56,54,79,115,69,114,116,107,49,50
输出ascii码对应的字符，得到flag。

xff referer

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

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。

> **Description:X老师告诉小宁其实xff和referer是可以伪造的。**

在请求头里伪造 X-Forwarded-For: 123.123.123.123 ，可以用火狐浏览器插件X-Forwarded-For Header直接修改成123.123.123.123， burpsuite抓包发送到repeater， 添加Referer值为需要的 url 如https://www.google.com，go一下得到flag。

weak auth

知识点：弱口令(weak password)，容易被别人猜测到或被破解工具破解的口令均为弱口令。

> **Description：小宁写了一个登陆验证页面，随手就设了一个密码。**

进入看到一个表单，需要输入账号密码登陆，随便输入得到提示要使用admin账户登陆。使用浏览器开发者工具查看源代码，发现提示：需要一个字典。

题目说随手设置一个密码，极有可能是弱口令；
需要一个字典且登陆不需要验证码；
因此使用暴力破解的方式猜解出密码登陆。

暴力破解可以用burpsuite抓包，发送到intruder，然后添加自己的字典，start attack进行爆破。在爆破结果中看到一个长度不一样的，尝试用这个密码登录，点开response，可以看到flag。

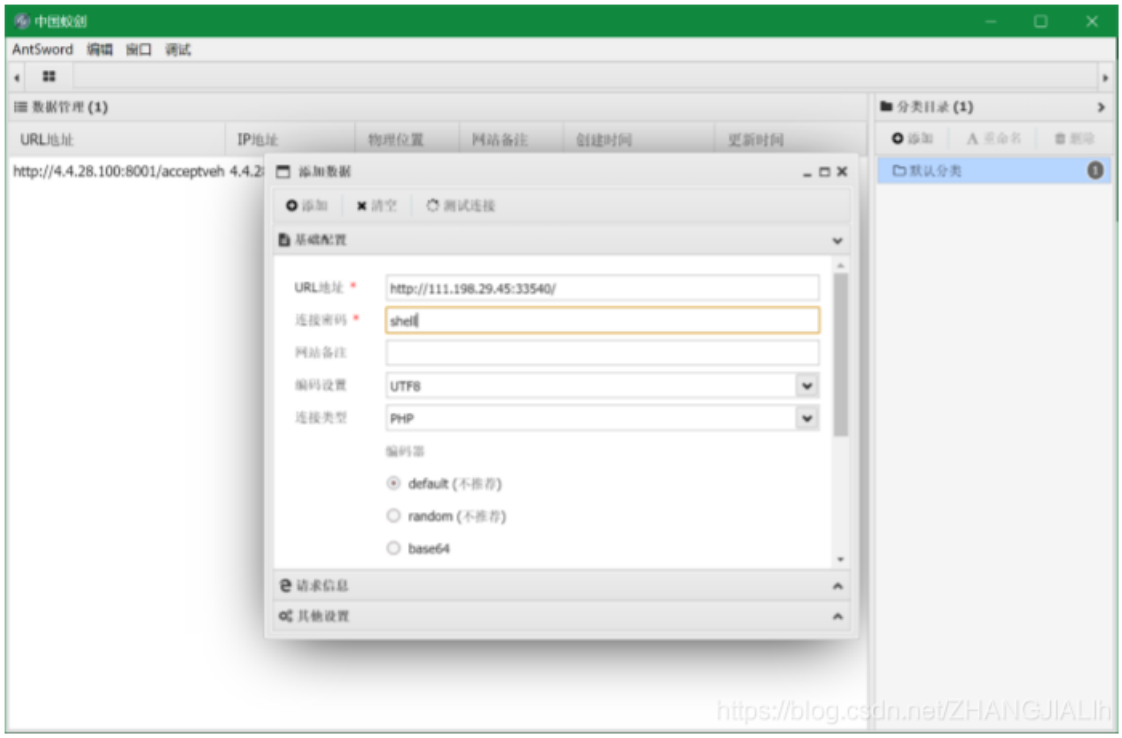
webshell

知识点：一句话木马(简称Webshell)

> **Description：小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。**

根据题目提示，在index.php当中存在一个一句话木马，我们可以使用工具**中国蚁剑**直接连接一句话木马。

拿到网站权限打开网页，一句话木马内容显示出来；传参方式为POST，由题可知蚁剑连接密码为shell，接下来用蚁剑：



添加其URL地址，双击添加的webshell进入网站目录，看到目录下存在文本文件 flag.txt，打开即可得到flag。

command execution

知识点：Web应用防护系统（也称为：网站应用级入侵防御系统，简称： WAF）。WAF对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效防护。

ls命令用于显示指定工作目录下之内容；
cat 命令用于连接文件并打印到标准输出设备上。

> **Description：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。**

打开网页看到这样的界面，题目说没用waf，先看看点完ping按钮，发现执行了linux的ping命令。

linux可以用一些管道符号使命令写在一行并依次执行，这里使用ls命令查看目录下所有文件夹及文件，一般flag文件都在home文件夹里，查看一下发现 flag.txt 文本文件，使用cat命令打开文件拿到flag。

simple_php

知识点：php弱类型，== 作用是将两个变量转换成相同类型再比较，必须是两个变量类型相同值也相同才会返回真。

> **Description：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。**

打开网页看到源码，其中的判断部分使用的是双等号 == ，存在弱类型比较漏洞。

a变量可以使用0a来绕过 a == 0 以及 a的值不为0；
b变量变成数组可以绕过且b不为数字也不为字符串， 以及 b数组里的值大于1234 的要求；

于是构造如下，得到flag。
构造get请求：http://111.198.29.45:54873/?a=0x&b=1235x

高手进阶区

待更