XCTF攻防世界-Web-WriteUp



(本篇博客作为自己的学习记录,含有部分前辈大佬的码字,但是在操作上有更新之处,并且步骤较 为详细,工具简单,介绍更为具体,特此记录以备回顾之需,也供其他学者借鉴,互相交流学习。)

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】

方法一: 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。



方法二: F12键直接查看网址源代码



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?

- get_post 18 最佳writeup由神秘人 • 孔雀翎提供	WP	🌔 🔮 建议
难度系数: ◆★1.0		
题目来源: Cyberpeace-n3k0		
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?		
题目场景: 点击获取在线场景		
题目附件: 暂无		
愛日已答对		
https://blog.csd	In.net/ <mark>wei칹ih</mark>	38912654

【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】

推荐火狐浏览器 渗透版

【分析过程】

在url后添加/? a=1即可发送get请求。

勾选post data即可发起POST请求

	∃▼ ≜ Co	okies▼	CSS-	2表甲▼ 🚾 🖻	3片▼ 🕕 🕅	则灾信息▼	具他切開	皆• 🥖 称	id• 🥖	缩放▼	※ 1首	• 22	看源代码	▼□选	贝▼					
INT	~	- •	SQL BASIC	S+ UNION	BASED+	ERROR/DC	OUBLE QU	ERY+ TO	DOLS+	WAF B	YPASS-	ENC	ODING+	HTML+	ENCRY	PTION-	OTHER+ X	SS+ LFI+		
G I	.o <u>a</u> d URL																			
8 9	<u>S</u> plit URL																			
۲	E <u>x</u> ecute																			
		\checkmark	Post data	Referrer	— 0 x	(HEX 🗩		%URL 🔰		E BA	ASE64		Insert s	tring to i	replace	Insert rep	placing strir	g 🗹 Repla	ace All	
Post	data																			
Лет	CRAFT .	Servi	ces*																	

操作

文件(E)编辑(E) 查看(V) 历史(S) 书签(B) 工具(I) 帮助(H)
POST&GET × +
(♦ ① 111.198.29.45:37462/?a=1
②禁用▼ ▲Cookies▼ /CSS▼ □表単▼ ■图片▼ ③ 网页信息▼ ■其他功能▼ /标记▼ /缩放▼ ※工具▼ ■查看源代码▼ □.选项▼
INT SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-
load URL http://111.198.29.45:37462/?a=1
8 Split URL
• Execute
🗹 Post data 🗌 Referrer 🥌 0xHEX 🌦 📹 %URL 🌦 📹 BASE64 🌦 🛛 Insert string to replace Insert replacing string 🗹 Replace All 🅭 🗵
Post data (b=2)
Since: New Site Rank: 10383 Site Report 🔤 [CN] China Unicom Beijing province network

请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量

cyberpeace{74b902b1438e81f4dc063b0e09a42fcf}

https://blog.csdn.net/weixin_38912654

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。

robots	1 23 最佳Writeup由MOLLMY提供	📕 WP	建议
难度系数:	★★1.0		
题目米源:	Cyberpeace-n3k0		
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。		
题目场景:			
	倒计时: 03:59:53 延时		
550%///	新工		
巡日期1十.			
	₩ 100 100 100 100 100 100 100 100 100 10		
	·//	J-mp/iide	

【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。

【工具】

不需要

【分析过程】

标签栏提示: robots,可以直接想到robots.txt,扫目录也可以扫到:

直接在地址栏输入http://111.198.29.45:50246/robots.txt



Disallow: flag_ls_h3re.php

HTML访问robots.txt发现f1ag_1s_h3re.php

访问f1ag_1s_h3re.php得到flag

文件(E) 编辑(E)	查看(V) 历史(S) 书签(B) 工具(I) 帮助(H)						
http://111.19	g_1s_h3re.php \times +						
(111.198.29.45:50246/f1ag_1s_h3re.php							
<mark>⊘</mark> 禁用▼ 上 Coo INT ∨	kies▼ /CSS▼ 🗋表单▼ 🔤图片▼ 🗊 网页信息▼ 📄 其他功能▼ /标记▼ /缩放▼ ※工具▼ 🔳 查看源代码▼ 🗓 ■ ♦ SQL BASICS+ UNION BASED+ ERROR/DOUBLE QUERY+ TOOLS+ WAF BYPASS+ ENCODING+ HTM						
lo <u>a</u> d URL ∦ Split URL	http://111.198.29.45:37462/?a=1						
) E <u>x</u> ecute							
HETCRAFT -	Post data Referrer 0xHEX %URL BASE64 Insert string Services* RiskRating Since: New Site Rank: 10383 Site Report [CN] China Unicom Beijing province network						

cyberpeace{836480c6838bfa114fefc7f5ce94f010}

https://blog.csdn.net/weixin_38912654

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!

backup ▲12 最佳Writeup由话求 • 楼宁提供 雅度系数: ◆★1.0 题目来源: Cyberpeace-n3k0 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! 题目场景: ● http://111.198.29.45:37037 ● 御鈴杨泉 ● 倒计时: 03:59:15 延时
推度系数: ◆★ 1.0 题目来源: Cyberpeace-n3k0 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! 题目场景: ■ http://111.198.29.45:37037
难度系数: ◆★1.0 题目来源: Cyberpeace-n3k0 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! 题目场景: ■ http://111.198.29.45:37037
題目来源: Cyberpeace-n3k0 題目描述: 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! 题目场景: L http://111.198.29.45:37037
题目来源: Cyberpeace-n3k0 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! 题目场景: ↓ http://111.198.29.45:37037 删除场景 倒计时: 03:59:15 延时
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,—起来帮小宁同学吧! 题目场景: ■ http://111.198.29.45:37037 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
题目场景:
题目场景:http://111.198.29.45:37037
▲白吻景: 量 110,711,130,29,45,51037 ● 删除场景 ● 倒计时: 03:59:15 延时
图计时: 03:59:15 延时
倒计时: 03:59:15 延时
题目附件: 暂无
flag
提交
https://blog.csdn.net/weixin_38912654

【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】

不需要

【分析过程】

问你知道index.php的备份文件名吗?可以手动猜测,直接把常用的备份文件后缀加上去 http://111.198.29.45:37037/index.php.bak,试出来了;

也可以使用扫目录脚本或软件(我觉得这个麻烦)。

文件(E) 编辑(E) 查看(V) 历史(S)	书签(B) 工具(T) 帮助(H)	
备份文件	× +	
€ 3 111.198.29.45:37037/	/index.php.bak	
②禁用▼ ▲Cookies▼ /CSS▼ [] INT ∨ = ● SQL BASICS	表单▼ 🔤 图片▼ 🚯 网页信息▼ 📄 其他功能▼ 🥒 标记▼ 🥒 缩放▼ 淤 工具 ;• UNION BASED+ ERROR/DOUBLE QUERY+ TOOLS+ WAF BYPASS•	▼ ■查看源代码▼选项 ▼ ・ ENCODING• HTML• ENCRYPTION•
isode URL		
Post data [Referrer < 0xHEX 🗩 < %URL 🍉 🥌 BASE64 🕽	Insert string to replace Insert re eijing province network
	正在打开 index.php.bak 您选择了打开:	×
	☐ index.php.bak 文件举型: bak File (500 字节)	

index.php.bak	
文件类型: bak File (500 字节) 来源: http://111.198.29.45:37037	
您想要 Firefox 如何处理此文件?	
○ 打开, 通过(<u>O</u>) 浏览(<u>B</u>)	
④ 保存文件(S)	
□ 以后自动采用相同的动作处理此类文件	• (<u>A</u>)
	确定取消
	https://blocheselminlet/weixin_38912654

下载到本地用UE或者记事本打开,即可看到flag



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?'

cookie	最佳Writeup由神	税人 ●孔雀翎提供	📕 WP	🌻 建议
难度系数:	• * 1.0			
题目来源:	Cyberpeace-n3k0			
题目描述:	X老师告诉小宁他在c	ookie里放了些东西,小宁疑惑地想:'这是夹心饼干的意思吗?'		
题目场景:	http://111.19	8.29.45:54897		
	倒计时: 03:56:24	4 延时		
题目附件:	暂无			
		flag		
		提交 提交		
L		https://blog	.csdn.net/weixir	_38912654



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】

火狐渗透版

或者浏览器开发者工具

【分析过程】

查看cookies信息

火狐渗透版

文件(E) 编	文件(E)编辑(E)查看(V)历史(S)书签(B)工具(I)帮助(H)							
Cookie	× @ Cookie 信息 来自 http:// × +							
(O chrome://web-developer/content/generated/view-cookie-information.html							
⊘禁用▼	⑦禁用▼ ▲Cookies▼ 》CSS▼ □表単▼ 回图片▼ ① 网页信息▼ □ 其他功能▼ // 标记▼ // 堆故▼ ※工具▼ ■ 查看源代码▼ Ⅰ 选项▼							
INT	禁用 Cookie(D) >> N BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-							
lo <u>a</u>	添加 Cookie(A)							
🐰 Spli	删除该域名下的Cookie							
● E <u>x</u> e	删除该路径下的Cookie(P)							
	翻绘读会话期的Cookie(S) er 🛫 OxHEX 🗩 🛫 %URL 🌫 🧮 BASE64 🏊 Insert string to replace Insert replacing string 🔽 Replace All 🛬 🚬							
HETCR	查看 Cookie 信息(V)							
Cookie 信息 文档 - Cookies - 全部收起 全部展开								

http://111.198.29.45:54897/

□ 1 cookie

名称	look-here
值	cookie.php
主机域名	111.198.29.45
路径	1
到期	在会话结束时
安全的	否
HttpOnly	否
@ 删除 ✔编辑	

https://blog.csdn.net/weixin_38912654

可以看到有个cookie.php

发送cookie.php请求http://111.198.29.45:54897/cookie.php

浏览器开发者工具

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

可以看到有个cookie.php

发送cookie.php请求http://111.198.29.45:54897/cookie.php

See the http response

https://blog.csdn.net/weixin_38912654

提示看http响应,那就F12进去看响应头信息

文件(E) 编辑(E)	查看(V) 历史(S) 书签(B) 工具(I) 帮助(H)	
Cookie	╳	
€ 0 111.1	98.29.45:54897/cookie.php	
	kies▼ 💋 CSS▼ 📋表单▼ 國際片▼ 🚯 网页信息▼ 🗐 其他功能▼ 🖉 标记▼	
INT Y	SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS-	• WAF BYPASS• ENCODING• HTML• ENCRYPTION• OTHER• XSS• LFI•
E Load URL		
Split URL		
Execute		
L	Post data Referrer CXHEX - WURL	BASE04 Dinsert string to replace Insert replacing string M Replace All
RETCRAFT -	Services Since: <u>New Site</u> Rank: <u>10383</u> <u>Site Report</u> [CN]	China Unicom Beijing province network
	として「「「「「」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」	
前 所有 日	TMI CSS 1S XHR 字体 图像 媒体 Flash WS 其他	b
		· · · · · · · · · · · · · · · · · · ·
200	GET cooliio pho	「おきの人」 「おうの人」 「おうろう人」 「おうろう人」 「おうの人」 「おう人」 「おう人」 「おう人」 「おう人」 「おう人」 「おう人」 「」 「」 「」 「」」 「」 「」」 「」」 「」 「」」 「」」 「」
0 200		请求方法: GET
0 200	GET bootstrap.min.css	远程地址:111.138.29.45:54897
0 200	GET bootstrap.min.css	状态码: ● 200 0K
0 200	GET bootstrap.min.css	版本: HTTP/11
		◎ 辺瀬角思头
		▼ 喇应头 (0.317 KB)
		Content-Encoding: "azip"
		Content-Length: "253"
		Content-Type: "text/html"
		Date: "Tue, 17 Dec 2019 11:34:52 GMT"
		Server: "Apache/2.4.7 (Ubuntu)"
		Vary: "Accept-Encoding"
		X-Powered-By: "PHP/5.5.9-1ubuntu4.26"
		flag: "cyberpeace{e6f9cda39e046cd3bb31631766038813}"
		▼ 请求头 (0.384 KB)
		User-Agent: "Mozilla/5.0 (Windows NT 10.0: WOW64: nr:52.0) Gecko/20100101 Firefox/52.0"
		Accept: "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
		Accept-Language: "zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3"
		Accept-Encoding: "gzip, deflate"
		DNT: "1"
		Connection: "keep-alive"
		Upgrade-Insecure-Requests: "1"

在响应头里发现flag。

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?

- disabled_button 11 最佳Writeup由沐-清提供	📕 WP	🌔 建议
难度系数: ◆★1.0		
题目来源: Cyberpeace-n3k0		
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?		
题目场景: http://111.198.29.45:36331		
倒计时: 03:58:12 延时		
题目附件: 暂无		
fiag		
提交		
https://blog.c	sdn.net/weixin	_38912654

【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,然后在出现的调试会话框左上角箭头点击一下然后去点击flag按钮定位代码段,将标签input中的 disabled (不可用)属性删除, x掉调试框。



https://blog.csdn.net/weixin_38912654

点击按钮,即可得到flag。



flag

cyberpeace{41bfc3dae76523be890dbb8cbe3eec02}

https://blog.csdn.net/weixin_38912654

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})

- simple_js 113 最佳Writeup由Venom • IceM提供	📕 WP	🎈 建议
难度系数: ◆★1.0		
题目来源: root-me		
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{xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx		
题目场景: 点击获取在线场景		
题目附件: 暂无		
flag		
提交 ————————————————————————————————————		
https://blo	g.csdn.net/weixir	_38912654

【目标】

掌握有关js的知识

【工具】

开发者工具

【分析过程】

进入环境后Ctrl+U查看代码

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。

先将16进制数输出进制

}	
String["fromCharCode"](dechiffre(\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x2c\x34\x39\x2c\x31\x30

📃 ASCII及进制转换 🕘 😣	📃 ASCII及进制转换 📃 👟
操作 工具 关于	操作 工具 关于
进制转换。字符转换、子网划分辅助	以 <mark>#制装换 字符技换 了码划分排动</mark>
\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c \x31\x31\x35\x2c\x36\x2q\x39\x2c\x31\x31\x34\x2c	55 56 54 79 115 69 114 116 107 49 50
\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c	
18331830	
55,56,54,79,115,69,114,116,107,49,50	7860sErtk12
字符转换	字符转换
Ascii偏移 字符转ASCII	Ascii偏移 字符转ASCII
	ASCINE ASCINE
前置符: 🗽	前置符: 字符串转十六进制
后置符: 十六进制转字符串	后置符:
	编码转换
字符转Base64(Base64转字符) (改变密钥) (恢复密钥)	字符號Base64 Base64號字符 改变密钥 恢复密钥
ntin]千大进制转季将审旧/WeixIn_389126547	转换结果 nun ASCII報学符 chunenweixin _55912654

进制转换工具http://www.xitongzhijia.net/soft/59990.html

得出: 786OsErtk12

此时你是不是觉得就完了?不要太激动,这不是正确flag,请注意审题:

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{xxxxxxxxx}))

(太坑了)

最终flag: Cyberpeace{786OsErtk12}

未完。。。。。。