

beirry U 于 2021-12-02 15:08:26 发布 O 976 🛠 收藏 分类专栏: 二向箔安全-百日打卡 文章标签: web安全 安全 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/beirry/article/details/121677385</u> 版权



二向箔安全-百日打卡 专栏收录该内容

6篇文章0订阅 订阅专栏

NO.1



伪装者

HELLO, HACKER. 游戏已经正式开始了,这个游戏最刺激的地 方就在于没人会告诉你游戏规则,你所在的 就是一个真实的网页入口, 该怎么做, 发挥

CSDN @beirry

点击提示按钮,可以看到我们需要以admin登录

			
Participant and a second	and <u>登</u> 录		
DEST	present □ present 数认帐号test 密码twosecurity	● 伪装者	
	用户:	HELLO,HACKER. 海咙已经正式开始了一这个游戏最刺激的他	
	确定取消注册	方就在于没人会告诉你游戏规则,你所在的	



此处已经有一个默认账号了,还有一个注册按钮,尝试先登录默认账号。



通过观察,看到cookie中有test字样,将test修改成admin,再刷新。



伪装者

恭喜您目前登录为admin! two{i_like_cookie}



CSDN @beirry

登录成功!

点击小灯泡,显示提示让我们弹个窗,很显然就是告诉我们这个是以xss攻击的靶场。



在URL中可以看到有name的参数值,一般测试xss语句,从标签开始测试,看哪些被过滤了。



大部分情况下<a>, 标签不容易被过滤, <script>易被过滤,所以在尝试xss时,可以先从<a>, 测试。







可以看到这里并没有对用户输入做任何过滤,则可以直接使用弹窗语句



得到flag

NO.3

根据提示可以知道,我们输入值后点击生成链接。应该会有一个<a>标签。



尝试写入 javascript:alert(1),点击后没反应,查看源代码发现在我们输入的值前有一个#



则尝试闭合href,在后面添加onclick来触发。

" onclick="alert(1)



NO.4

登录页面可以从三个方面考虑,第一个是爆破,第二个是万能密码,第三个就是修改cookie值。





HELLO,HACKER. 游戏已经正式开始了,这个游戏最刺激的地 方就在于没人会告诉你游戏规则,你所在的 就是一个真实的网页入口,该怎么做,发挥 你的想象。

CSDN @beirry

尝试先用万能密码,账号输入admin,密码输入 ' or 1#

	登录 用户: admin 密码: or 1# 確定 取消	▶ DESCRIPTION	
			CSDN @beirry

登录成功



又是登录页面



CSDN @beirry

给了一个默认账号,那么可以先考虑修改cookie值的方法

观察cookie值,发现是有32位字符组合而成,那么根据特征猜测可能是md5值



□ 元素 控制台 来源 网络	各性能	内存 应用	安全	Lighthouse	HackBar	01	\$:	×
● ◎ 7 ♀ □ 保留日志 □ 停	用缓存 已停	用节流模式	- <u></u>	<u>+</u>				ф
过滤 🗌 反转 🗌 🖡	隐藏数据网址	全部 Fetch/>	(HR JS CSS	图片 媒体 字	🔆 文档 WS	Wasm 清单	其他	
□ 有已拦截的 Cookie □ 被屏蔽的请求 □	第三方请求							
50 毫秒 100 毫秒 150 毫秒	200 毫秒	250 毫秒	300 毫秒	350 毫秒	400 毫秒	450 毫秒	500 毫利	b
名称	× 标头	预览 响应	启动器	时间 Cookie		1		
home	GET /o	da/home HTTP/	1.1					^
 computer.png 	Host:	rimovni.exeye	.run					
resizeApi.php?id=1215548&size=32	Connect	tion: keep-al	ive					
📓 home	Cache-	Control: max-	age=0					

		sec-ch-ua: "Google Chrome";v="95", "Chromium";v="95", ";Not A Brand";v="99" sec-ch-ua-mobile: ?0 sec-ch-ua-platform: "Windows" Upgrade-Insecure-Requests: 1
伪装者		User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.60 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w ebp_image/apm,*/*ic=0.8,application/signed-exchange;v=b3;q=0.9
欢迎! <u>退出</u>		Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Referer: https://rimovni.exeye.run/oda/index?
	4 个请求 已传输 3.6 kB 230 kB 项资源 注 控制台 搜索 × 问题 新变化	Accept-Encoding: gzip, deflate, br Accept-Language: zh-CN,zh;q=0.9 Cookie: cookie=098f6bcd4621d373cade4e832627b4f6
	Aa .* two{giVe_y0u_giFt}	C O

将这串字符用md5解码,解出来可以看到是test,也就是我们默认账号

	密文: 098f6bcd 类型: 自动	4621d373cade4e8326	627b4f6 ✔ [帮助]	
		查询	加蜜	
查询结果: test				

那么我们将admin用md5编码

		当页 解密范围 批量解密 ▶ 会员 ▶ World
<mark>2⁸ gg──键登录</mark>		
	Pass: admin UTE8 \$[HEX Salt: Hex Hash: 49ba59abbe56e057 Hex	
Re ba m m m m m m m n t sh sh sh sh	sult: se64: YWRtaW4= df <u>2123/29757a574389400e4a801fc3</u> d5_middle: 7a57a574389400e4a801fc3 d5_middle: 7a57a574389400e4a801fc3 d5(md5(spass)): 72e2e4cc9b4041200e31dc57db8829 d5(md5(spass)): 72e2e4cc9b4041200e31dc57db8829 d5(md5(spass)): 72e2e4cc9b4041200e31dc57db8829 d5(base64): ISMvKXpXpadDiUcoSoAfww== ysc1: 43e9a4ab75570f5b ysc1: 4acf2302a5ff5c4f67896fc58aab1d615029441 Im: 2090c174da490caeb422/3fa5a7ae634 a1: d033e22ae348aeb5660fc2140aec35850c4da997 a1(sha1(spss)): 7b2e9f54c4ff415dce01f330af6896c3cd7e6cd a1(md5(spss)): 9b09aa7e2580c4ff46e990b78a9fc5ebd6cecad d5(sha1(\$psss)): 90b9aa7e2580c4ff46e990b78a9fc5ebd6cecad d5(sha1(\$psss)): 90b9aa7e2580c4ff64e990b78a9fc5ebd6cecad d5(sha1(\$psss)): 90b9aa7e2580c4ff64e990b78a9fc5ebd6cecad d5(sha1(\$psss)): 90b9aa7e2580c4ff64e990b78a9fc5ebd6cecad d5(sha1(\$psss)): 90b540b4de5570f38322df087f0a9bb225cc257e32eb4ac580c98ef5b3173ac a256: mc675pa02655534c145bde90bd4decE15dfb167a9c873fc4bb8a81f6f2ab448a918 a256(md5(\$pssp)): 90c5504215bde90bd4decE15dfb167a9c873fc4bb8a81f6f2ab448a918 a256(md5(\$pss)): 90c5504215bde90bd4dfs6fb46f5730f5bb278a765b3173ac a256: mc67504025504215bde90bd4decE15dfb167a9c873fc4bb8a81f6f2ab448a918 a256(md5(\$pss)): 90c5504215bde90bd4dfs6fb46f5730f5b27a267a3bb225cc257a43eb4ac580c98ef5b3173ac a256(md5(\$pss)): 90c5504215bde90bd4dfs6fb4fb6730f5b27ab27a42b4ac580c98ef5b3173ac a256(md5(\$pss)): 90c5504215bde90bd4fs6fb4fb6730f5b27a57a43eb4ac580c98ef5b3173ac a256(md5(\$pss)): 90c5504215bde90bd4fs6fb4fb6730fb6730fb675b27ab27a43b4ac580c98ef5b3173ac a256(md5(\$pss)): 90c5504215bde90bd4fs6fb4fb6730fb67557ab20a428d41956b573ba20a248d41956m56fb573ac a256(md5(\$pss)): 90c5504215bd4f5f5b404f5f5b40f555ba20a248d4041956m56f55ba20a2478fb5575ba20a2478fb555ba20a2478fb55575ba20a2478fb5555ba20a2478fb5555ba20a2478fb5555ba20a2478fb5555ba20a2478fb5555ba20a2478fb5555ba20a2478fb5555ba20a2478fb5555ba20a2478fb555ba20a2478fb5555ba20a2478fb5555ba20a2478fb5555ba20a2478fb555ba20a2478fb5555ba20a2478fb555ba20a2478fb5555ba20a2478fb5555ba20a2478fb555ba20a2478fb5555ba20a2478fb5555	
m sh c7 m m m m	addr. zub/stabilization/12/2017/22/2017/22/2017/2017/2017/2017/	7ec

将这串字符覆盖到cookie上,刷新页面





伪装者

欢迎 admin! two{cookie_md5_hahaha}

名称	× 标头 预览 响应 启动器 时间 Cookie
home	GET /oda/home HTTP/1.1
 computer.png 	Host: rimovni.exeye.run
resizeApi.php?id=1215548&size=32	Connection: keep-alive
Le home	<pre>Cache-Control: max-age=0 sec-ch-ua: "Google Chromer;v="95", "Chromium";v="95", ";Not A Brand";v="99" sec-ch-ua-mobile: ?0 sec-ch-ua-platform: "Windows" Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/95.0.4638.69 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/ ebp,image/apmg,"/r;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: same-origin Sec-Fetch-Dest: document Referer: https://rimovni.exeye.run/oda/index? Accept-Incoding: g1p, deflate, br Accept-Incoding: g1p, deflate, br Accept-Incoding: g1p, deflate, br</pre>
4 个请求 已传输 3.6 kB 230 kB 项资源	Cookie: cookie=21232f297a57a5a743894a0e4a801fc3
:	
* TTROTT TROPY OF THE WINCHD	