# CTFHub Http协议



<u>日月ton光</u> 于 2020-03-08 15:02:22 发布 ○ 2397 ○ 收藏 13 分类专栏: <u>CTF</u> 文章标签: <u>http协议 http请求方式 cookie欺骗</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/sinat\_36711025/article/details/104733085</u> 版权\_\_\_\_\_

<u>CTF 专栏收录该内容</u> 3 篇文章 1 订阅 订阅专栏 1、请求方式

由题目可知,考察的是HTTP请求方法,在Http/1.1协议中定义的八种方法为GET,POST、HEAD、OPTIONS, PUT, DELETE, TRACE 和 CONNECT 方法。



进入题目后,发现提示,HTTP Method 是可以自定义的,并且区分大小写,直接用 CTFHUB 方法请求 index.php 即可拿到 flag。



2、302跳转

302是Http协议的临时重定向状态码。进入页面后发现没有任何消息,按f12进入控制台,点击Give me Flag按钮,发现页面没有任何变化,但其实页面已经发生了跳转,用curl访问新的跳转页面即可得到flag值。

@ CTFHub	× No Flag here!	×	302跳转   CTFI	Hub ×	+				
← → ♂ ŵ	③ challenge-48a97c	4e74c87c48.san	dbox.ctfhub.com	:10080/index.ht	tml	⊌ ☆	Q Search	III\ #P	🗈 🔮 🔺 E
			Ν	lo Flag	g hei	re!			
				Give m	ne Flag				
ি ়ি Inspector ১ Consol	e D Debugger {} Style !	Editor 🕥 Perform	ance 🕼 Memory	↑ Network	Storage	🕇 Accessibility 🌘 H	lackBar 🛛 👜 Adblock Plus		<u>.</u>
🛍 🗑 Filter URLs					HTML CS	S JS XHR Fonts Imag	ges Media WS Other	Persist Logs Disable cache	No throttling 🛊 HAR 🗧
Status Met Domain File		Cause Typ	e Transferred S	ize 0 ms	1.28 s	2.56 s Headers	Cookies Params	Response Timings	
302 GET 🔏 challenge inder	.php	document htm	l 489 B 17	77 B 📕 83 ms		Request URL: h	ttp://challenge-48a97	c4e74c87c48.sandbox.ctfhub	.com:10080
200 GET 🔏 challenge index	.html	document htm	l cached 17	77 B		Request method	: GET		
302 GET challenge favio	on.ico	img htm	l cached 17	77 B		Remote address	: 47.98.148.7:10080		
200 GET 🔏 challenge index	.html	img htm	l cached 17	77 B		Varian HTTD/	<pre>noved remporarily </pre>	nttps:/Wog.csdn.nei/	

### </html>root@kali:~# curl -v http://challenge-48a97c4e74c87c48.sandbox.ctfhub.com:10080/index.php

ctfhub{a39831bab3494820a0320b3ea1ae526cfa1b4757}
\* Connection #0 to host challenge-48a97c4e74c87c48.sandbox.ctfhub.com left intact

#### 3、cookie

访问题目页面发现给的提示是"hello guest, only admin can get flag",我们挂上 BurpSuite 之后重新访问题目页面,在cookie发现admin=0字段,猜测服务器可能是根据此字段来判断浏览者身份。

Filter:	Hiding CSS, image and general	binary co	ntent							
#	Host	Method	URL	Par 🔺	Edited	Status	Length	MIME type	Extension	Т
1	http://challenge-b537a8d5	GET	1			200	360	text		
2	http://challenge-b537a8d5	GET	/			200	360	text		
Req	uest Response									
Raw	Params Headers Hex									
GET /	HTTP/1.1									
Host:	challenge-b537a8d5bc21e9f	b.sandbo	x.ctfhub.com	:10080						
User-1	Agent: Mozilla/5.0 (X11; I	inux x86	_64; rv:68.0	) Gecko/	20100101	Firefox	/68.0			
Accept	t: text/html,application/x	chtml+xml	,application	/xml;q=0	.9,*/*;q	=0.8				
Accept	t-Language: en-US,en;q=0.5	5								
Accept	t-Encoding: gzip, deflate									
Connec	ction: close									
Cookie	e: admin=0									
Upgrad	de-Insecure-Requests: 1									

我们把这个请求放入"repeater"中修改Cookie: admin=0为Cookie: admin=1后发送,发现在响应页面里包含 Flag。



在HTTP中,基本认证(英语: Basic access authentication) 是允许http用户代理(如: 网页浏览器)在请求时,提供用户和密码的一种方式。详情请查看 https://zh.wikipedia.org/wiki/HTTP基本认证。

原理	[编辑]
文字过	
这一个舅	典型的HTTP客户端和HTTP服务器的对话,服务器安装在同一台计算机上(localhost),包含以下步骤:
1. 4 i	客户端请求一个需要身份认证的页面,但是没有提供用户名和密码。这通常是用户在地址栏输入一个URL,或是打开了一个指向 该页面的链接。
2. /	服务端响应一个401应答码 <sup>[4]</sup> ,并提供一个认证域(英语:Access Authentication) <sup>[5]</sup> ,头部字段为: WWW-Authenticate,
i	该字段为要求客户端提供适配的资源。 <sup>[6]</sup> WWW-Authenticate: Basic realm="Secure Area" 该例子, Basic 为验证 的模式, realm="Secure Area" 为保护域,用于与其他请求URI作区别。
3. 1	接到应答后,客户端显示该认证域给用户并提示输入用户名和密码。此时用户可以选择确定或取消。
4. J	用户输入了用户名和密码后,客户端软件将对其进行处理,并在原先的请求上增加认证消息头(英语:Authorization)然后重新 发送再次尝试。过程如下:
	1. 将用户名和密码拼接为 用户:密码 形式的字符串。
	2. 如果服务器 www-Authenticate 字段有指定编码,则将字符串编译成对应的编码(如:UTF-8)。
	3. 将字符串编码为base64。
	4. 拼接 Basic , 放入 Authorization 头字段, 就像这样: Authorization Basic 字符串 。 示例: 用户名:
	Aladdin , 密码: OpenSesame , 拼接后为 Aladdin:OpenSesame , 编码后 QWxhZGRpbjpPcGVuU2VzYW11 , 在HTTP头部里会是这样: Authorization: Basic QWxhZGRpbjpPcGVuU2VzYW11 。 Base64编码并非加密算法, 其无法保证安全与隐私. 仅用于将用户名和密码中的不兼容的字符转换为均与HTTP协议兼容的字符集。
5. ł	在本例中,服务器接受了该认证屏幕并返回了页面。如果用户凭据非法或无效,服务器可能再次返回401应答码,客户端可以再 次提示用户输入密码。
注意:客	户端有可能不需要用户交互,在第一次请求中就发送认证消息头。

#### 进入题目页面,发现点击click会出现认证页面,

$\leftrightarrow$ $\rightarrow$ X $\hat{\omega}$	<ol> <li>challenge-ca482880fdl</li> </ol>	o7fae9.sandbox. <b>ctfhub.com</b> :10080	••• 🛛 🔂 🔍 Search	$\overline{\mathbf{h}}$
CTFHub 基础	出认证			
Here is your flag: <u>click</u>				
	_			
		Authentication Re	equired	×
	P	http://challenge-ca482880fdb7fae9.sandbox.cti password. The site says: "Do u know admin ?"	fhub.com:10080 is requesting your usernam	ne and
	User Name:			
	Password:			
			Cancel	ок
			https://blog.csd	1n.net/sinat_36711025

挂上 BurpSuite 的代理,随便输个账号密码(比如:账号aaa 密码 bbb)访问,查看 HTTP 响应报文:

Filter: Hiding CSS, image and general binary content         #       Host       Method       URL       Params       Edited       Status       Length       MIME type       Extension         44       http://challenge-2fb9bdbe2       GET       /flag.html       404       1468       HTML       html         43       bttp://dotoctportal firefore       CET       /success bt       200       370       tout       btt         Request Response
#     Host     Method     URL     Params     Edited     Status     Length     MIME type     Extension       44     http://challenge-2fb9bdbe2     GET     /flag.html     404     1468     HTML     html       42     btts://detoctportal firefer     CET     /ourseese bt     200     270     tout     bt       Request Response
44     http://challenge-2fb9bdbe2     GET     /flag.html     404     1468     HTML     html       42     http://datastreated.firefex.s     CET     /ousseene.ht     200     270     text     btt       Request     Response
Request Response
Request Response
Request Response
Raw Headers Hex
GET /flag.html HTTP/1.1
Host: challenge-2fb9bdbe29db055e.sandbox.ctfhub.com:10080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://challenge-21D9Ddde29dD055e.sandbox.ctinub.com:10080/
Connection: close
Authorization: Basic YWFh0mJiVg== https://blog.csdp.pet/sipat_36711025
https://opensional.col/ride
Request Response
Raw Headers Hex HTML Render
HTTP/1.1 401 Unauthorized
Server: openresty/1.15.8.2

得到提示 do u konw admin ?,于是猜测账号是 admin,那么接下来就只需要爆破密码了。注意看到 HTTP 请求 头部的 Authorization 字段,后面的YWFhOmjiYg==用base64 解码后是 aaa:bbb,也就是我们之前输入的账号: 密码。

使用 BurpSuite 进行基础认证爆破

WWW-Authenticate: Basic realm="Do u know admin ?"

Content-Length: 179 Connection: close

(1) 将报文发送到 Intruder, 将 Basic后面 base64部分添加为payload position

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: Sniper	•	
<pre>GET /flag.html HTTP/1.1 Host: challenge?fb9bdbe29db055e.sandbox.ctfhub.com:10080 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 Accept: text/html.application/xhtml+xml.application/xhtg=0.9,*/*;q=0.8 Accept:Language: en-US,en;q=0.5 Accept:Encoding: gzip, deflate Referer: http://challenge-2fb9bdbe29db055e.sandbox.ctfhub.com:10080/ Connection: close Upgrade-Insecure:Requests: 1 Authorization: Basic SYMPHOmJIYg==5</pre>	4	Add § Clear § Auto § Refresh
https://blo	g.csdn.net/s	inat_36711025

(2)在 Payloads选项卡下,选择 Payload Type为SimpleList,然后在 Payload Options 中点击 load 加载密码字 典

#### Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	123456	*
	password	
Load	line	
	12345678	
Remove	qwerty	• • • • • • • • • • • • • • • • • • •
	123456789	
Clear	12345	
	1234	-
	111111	T
Add	Entor a new item	
Add	Enter a new item	
Add from list .	[Pro version only]	T
		https://blog.csdn.net/sinat_3671102

(3) Payload Processing -> Add-> Add Prefix(添加前缀) -> 输入 admin:

Payload Processing -> Add-> Encode(添加一个编码方式) -> 选择 Base64 Encode

?	Payload Proc	essing		
	You can define	e rules to pe	rform various processing tasks on each payload b	efore it i
	Add	Enabled	Rule	
		•	Add Prefix: admin:	
	Edit		Base64-encode	
	Remove			Þ
	Up			
	Down		https://blog.csdn.net/sinat_3671	1025

(4) Payload Encode 取消勾选的 URL-encode, 不然你会看到base64之后的=会被转成%3d, 你就算爆破到 天荒地老也不会出来

?	Payload Encoding	
	This setting can be used to URL-en	code selected characters within the final payload, for safe transmission within HTTP requests.
	URL-encode these characters:	\=<>?+&*;:"{} ~

(5) Start Attack, 然后按 Length 排序, 并看到状态码出现200的, 即爆破成功

Request	Payload	Status	Error	Timeout	Length	Comment
22	YWRtaW46cXdlcnR5dWlvcA==	200			394	
0		401			404	
1	YWRtaW46MTIzNDU2	401			404	
2	YWRtaW46cGFzc3dvcmQ=	401			404	
3	YWRtaW46bGluZQ==	401			404	
4	YWRtaW46MTIzNDU2Nzg=	401			404	
5	YWRtaW46cXdlcnR5	401			404	
6	YWRtaW46MTIzNDU2Nzg5	401			404	
7	YWRtaW46MTIzNDU=	401			404	
-	CALIFOR COLORED FOR ALL	4.6.1				

4	I WRITE WHOLD	12C3UVCIIQ- 401		
3	YWRtaW46	Converted back		
4	YWRtaW46	Converted text	^	
5	YWRtaW4(			
6	YWRtaW4(			
7	YWRtaW4(	Copy to clipboard	Close	
8	YWRtaW4(			
9	YWRtaW4(	admin:qwertyuiop		
10	YWRtaW4(			
11	YWRtaW4(			
L12	VM/D+-34/44			
Beguaat	Baapapa		T I	
Request	Respons			
Raw Hea	aders H		0 matches	
Host: chall	lenge-2fł			
User-Agent:	Mozilla/5	.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0		
Accept: tex	ct/html,app:	lication/xhtml+xml,application/xml;q=0.9,*/*;q=0.8		
Accept-Lang	guage: en-US	S,en;q=0.5		
Accept-Enco	oding: gzip,	, deflate		
Copposition	close	enge-zib9bdbez9db055e.sandbox.clinub.com:10080/		
Upgrade - Ing	secure-Recur	ests: 1		
Authorizati	ion: Basic	YWRtaW46cXdlcnR5dW1vcA==		

## 查看 Response,得到flag

	nespo	inse [		
Raw	Headers	Hex	Render	
ontent	-Type: te	xt/htm	l; chars	et=utf-8
onnect	ion: clos	e		
ast-Mo	dified: S	un, 08	Mar 202	03:35:27 GMT
Tag: W	/"5e6467f	£-31"		
ccess-	Control-A	11ow-0	rigin: *	
	Control-A	llow-H	leaders:	(-Requested-With
Access-		llow-M	lethods:	
Access -	Control-A			
Access Access Content	Control - A - Length:	49		
Access- Access- Content	Control-A -Length: c03267167	49 c9ee01	e06e8e63	010ff6da5125beac}

## 5、响应包源代码

## 题目页面打开后是一个网页版的"贪吃蛇"小游戏

③ 贪吃蛇	
← → C ▲	不安全   challenge-c72d5ecd84ca0244.sandbox.ctfhub.com:10080
	_ • •
	_ = =
	le la constante de la constante
	https://blog.csdn.net/sinat_C1FHUb

根据题目要求是查看响应包源代码,可以使用burpsuite,也可以使用浏览器自带的开发调试工具,按f12进入调试界面,查找flag中的关键字段cfthub,就可以得到结果。

Image: Image	∰ Memory <b>†↓</b> Networ	k 🗄 Storage 📫 Accessibility				
Q, ctfhub	🛛 1 of 1 🕂 🗡	🗑 Filter Styles				
<html> [event] &gt; <heas <="" head="" im=""> &lt; <body &lt; <convas height="700%&lt;/canvas&gt;&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;▶&lt;di≱@&gt;/div&gt;&lt;br&gt;▶&lt;script type=" id="canvas" javascript"@<="" script="" text="" width="1000"> <td></td><td></td></convas></body </heas></html>						
ctfhub{b944dccefb6295b92d7568eeaa781612317a894f} 						