攻防世界-baby_web详解

原创

Mr H 于 2020-08-10 21:35:05 发布 1499 收藏 2

分类专栏： 攻防世界web高手进阶 baby_web 文章标签： 安全

本文链接：https://blog.csdn.net/Mr_helloword/article/details/107922462

攻防世界web高手进阶 同时被 2 个专栏收录

13 篇文章 4 订阅

订阅专栏

baby_web

1 篇文章 0 订阅

订阅专栏

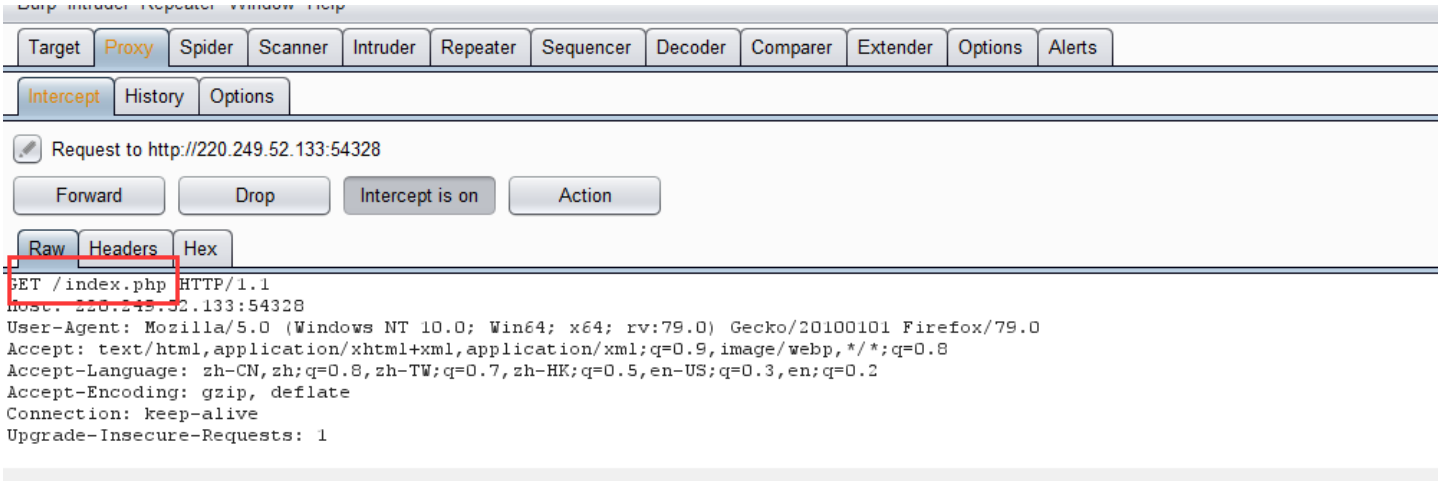
baby_web

题目描述：想想初始页面是哪个

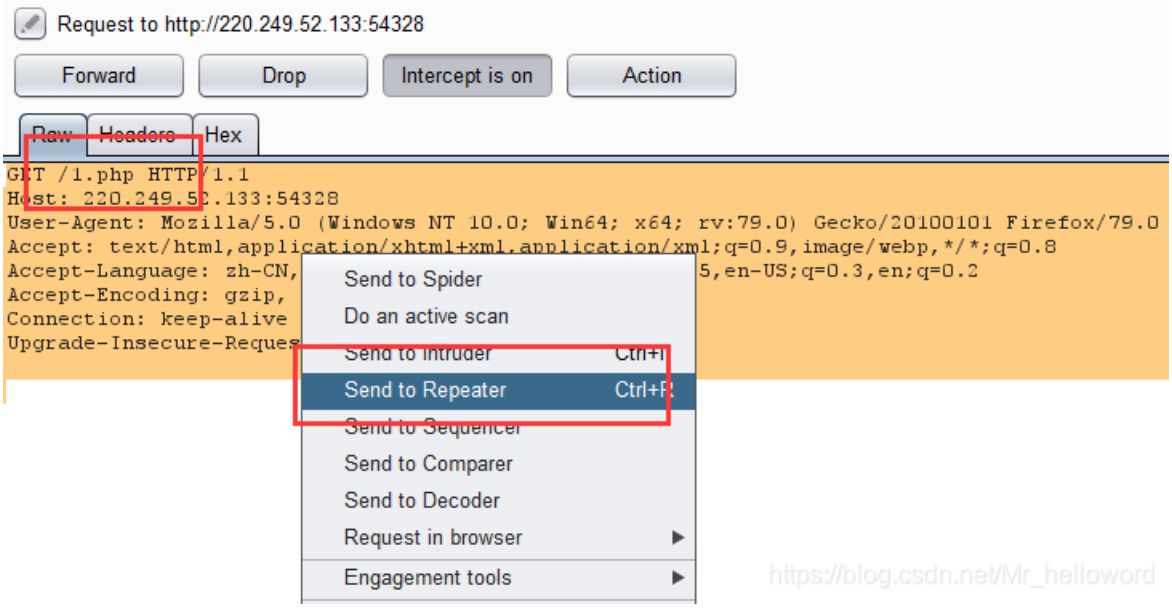
根据提示我们尝试/index.php页面：

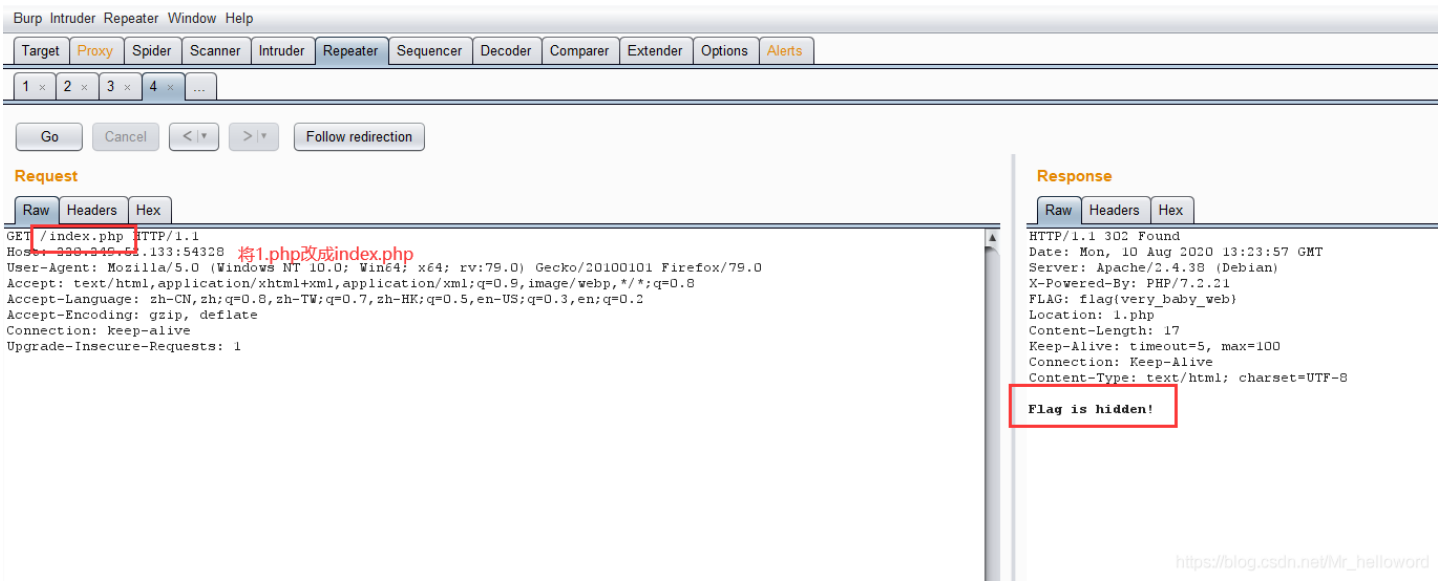
发现网页直接跳转到1.php我们尝试抓包分析

抓包：（index.php）

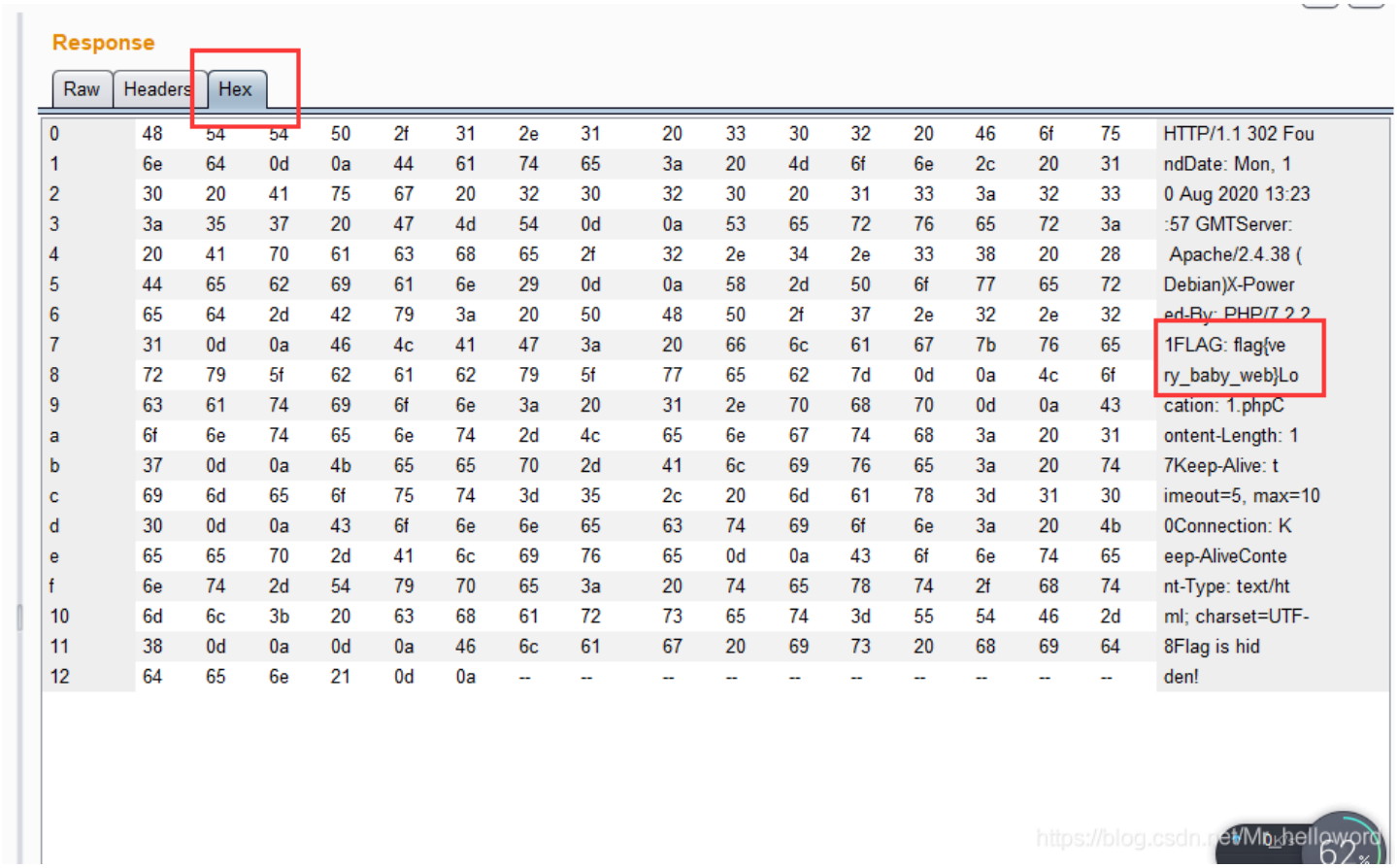


点 Foward放过当跳转到1.php时放到repeater模块





发现flag但是隐藏了



Response

Raw | Headers | Hex

0	48	54	54	50	2f	31	2e	31	20	33	30	32	20	46	6f	75	HTTP/1.1 302 Fou
1	6e	64	0d	0a	44	61	74	65	3a	20	4d	6f	6e	2c	20	31	ndDate: Mon, 1
2	30	20	41	75	67	20	32	30	32	30	20	31	33	3a	32	33	0 Aug 2020 13:23
3	3a	35	37	20	47	4d	54	0d	0a	53	65	72	76	65	72	3a	:57 GMTServer:
4	20	41	70	61	63	68	65	2f	32	2e	34	2e	33	38	20	28	Apache/2.4.38 (
5	44	65	62	69	61	6e	29	0d	0a	58	2d	50	6f	77	65	72	Debian)X-Power
6	65	64	2d	42	79	3a	20	50	48	50	2f	37	2e	32	2e	32	ed-By: PHP/7.2.2
7	31	0d	0a	46	4c	41	47	3a	20	66	6c	61	67	7b	76	65	1FLAG: flag{ve
8	72	79	5f	62	61	62	79	5f	77	65	62	7d	0d	0a	4c	6f	ry_baby_web}Lo
9	63	61	74	69	6f	6e	3a	20	31	2e	70	68	70	0d	0a	43	cation: 1.phpC
a	6f	6e	74	65	6e	74	2d	4c	65	6e	67	74	68	3a	20	31	ontent-Length: 1
b	37	0d	0a	4b	65	65	70	2d	41	6c	69	76	65	3a	20	74	7Keep-Alive: t
c	69	6d	65	6f	75	74	3d	35	2c	20	6d	61	78	3d	31	30	imeout=5, max=10
d	30	0d	0a	43	6f	6e	6e	65	63	74	69	6f	6e	3a	20	4b	0Connection: K
e	65	65	70	2d	41	6c	69	76	65	0d	0a	43	6f	6e	74	65	eep-AliveConte
f	6e	74	2d	54	79	70	65	3a	20	74	65	78	74	2f	68	74	nt-Type: text/ht
10	6d	6c	3b	20	63	68	61	72	73	65	74	3d	55	54	46	2d	ml; charset=UTF-
11	38	0d	0a	0d	0a	46	6c	61	67	20	69	73	20	68	69	64	8Flag is hid
12	64	65	6e	21	0d	0a	--	--	--	--	--	--	--	--	--	--	den!

falg：

flag{very_baby_web}