# 问题详情和风险分析

## 污染源授权#SQL注入

|  |  |
| --- | --- |
| **漏洞名称** | SQL注入 |
| **漏洞URL** | 175.6.46.155:81//BaseDataBaseSite/PSAuthorize/AuthorizeUserList.aspx |
| **漏洞验证** | 漏洞发生页    注入点    注入参数：txtUserName  Payload：  POST /BaseDataBaseSite/PSAuthorize/AuthorizeUserList.aspx HTTP/1.1  Host: 175.6.46.155:81  Content-Length: 5033  Cache-Control: max-age=0  Upgrade-Insecure-Requests: 1  Origin: http://175.6.46.155:81  Content-Type: application/x-www-form-urlencoded  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 Edg/83.0.478.58  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  Referer: http://175.6.46.155:81/BaseDataBaseSite/PSAuthorize/AuthorizeUserList.aspx  Accept-Encoding: gzip, deflate  Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6  Cookie: .ASPXAUTH=; ASP.NET\_SessionId=nbrcj51n20lawrjwg2rttgqg; UserName=csjointsky; StylePath=..%2f..%2fThemes%2fGreen%2fGreen.swf  Connection: close  \_\_VIEWSTATE=%2FwEPDwULLTIwMDMzMzI1OTAPZBYCAgMPZBYEAgcPPCsAEQMADxYEHgtfIURhdGFCb3VuZGceC18hSXRlbUNvdW50AhRkARAWABYAFgAMFCsAABYCZg9kFioCAQ9kFgxmD2QWAmYPFQEIYXBwYWRtaW5kAgEPZBYCZg8VAQ%2FlubPlj7DnrqHnkIblkZhkAgIPZBYCZg8VAQBkAgMPZBYCZg8VARVhcHBhZG1pbkBqb2ludHNreS5jb21kAgQPZBYCZg8VAQBkAgUPZBYCZg8VAghhcHBhZG1pbgZzeXN0ZW1kAgIPZBYMZg9kFgJmDxUBBGhueXhkAgEPZBYCZg8VASTmt7HlnLPlrofmmJ%2Fnp5HmioDlj5HlsZXmnInpmZDlhazlj7hkAgIPZBYCZg8VARI0MjIyMDIxOTg4MDIxMTE4NTRkAgMPZBYCZg8VARAzMzAzOTYxODlAcXEuY29tZAIED2QWAmYPFQELMTg5MDA3MzA4NzlkAgUPZBYCZg8VAgRobnl4BnN5c3RlbWQCAw9kFgxmD2QWAmYPFQEDd3NjZAIBD2QWAmYPFQEk5p2t5bee6IGa5YWJ56eR5oqA5Y%2BR5bGV5pyJ6ZmQ5YWs5Y%2B4ZAICD2QWAmYPFQESNDMwMTgxMTk4NjEwMjMwODE2ZAIDD2QWAmYPFQEZamlheGluZ194aW9uZ0BmcGktaW5jLmNvbWQCBA9kFgJmDxUBCzE4ODA2NTM2MDM3ZAIFD2QWAmYPFQIDd3NjBnN5c3RlbWQCBA9kFgxmD2QWAmYPFQEGemtjd3NjZAIBD2QWAmYPFQEn6ZW%2F5rKZ5Lit56eR5oiQ5rGh5rC05YeA5YyW5pyJ6ZmQ5YWs5Y%2B4ZAICD2QWAmYPFQESNDMwMTAzMTk4NDA2MDIxMDIyZAIDD2QWAmYPFQEVbGl3ZW5qaW5nQGJld2cubmV0LmNuZAIED2QWAmYPFQELMTM4NzU5MjA0NzJkAgUPZBYCZg8VAgZ6a2N3c2MGc3lzdGVtZAIFD2QWDGYPZBYCZg8VAQRobmxoZAIBD2QWAmYPFQEk5rmW5Y2X5Yqb5ZCI56eR5oqA5Y%2BR5bGV5pyJ6ZmQ5YWs5Y%2B4ZAICD2QWAmYPFQESNDMwOTIyMTk4NTEwMzAzODMxZAIDD2QWAmYPFQEQMjU0ODY1NDc3QHFxLmNvbWQCBA9kFgJmDxUBCzEzNjE3MzE2NzM0ZAIFD2QWAmYPFQIEaG5saAZzeXN0ZW1kAgYPZBYMZg9kFgJmDxUBBHh4enhkAgEPZBYCZg8VASfplb%2FmspnluILnjq%2Fkv53lsYDmsaHmn5PmupDnm5HmjqfkuK3lv4NkAgIPZBYCZg8VARI0MzExMjgxOTg3MDUzMDU1MzNkAgMPZBYCZg8VARA0MTQwNTYzNDdAcXEuY29tZAIED2QWAmYPFQELMTg5NzMxNTEzOTFkAgUPZBYCZg8VAgR4eHp4BnN5c3RlbWQCBw9kFgxmD2QWAmYPFQEGZ3poYmtqZAIBD2QWAmYPFQEt6ZW%2F5rKZ5biC5Zu956Wv546v5L%2Bd56eR5oqA5pyJ6ZmQ6LSj5Lu75YWs5Y%2B4ZAICD2QWAmYPFQESNDMwNjIzMTk4MzA1MTIwNTE4ZAIDD2QWAmYPFQEQMzMwODk0NjIwQHFxLmNvbWQCBA9kFgJmDxUBCzE4NjI3NTc2NTEyZAIFD2QWAmYPFQIGZ3poYmtqBnN5c3RlbWQCCA9kFgxmD2QWAmYPFQEFaHF3c2NkAgEPZBYCZg8VAR7plb%2FmspnluILoirHmoaXmsaHmsLTlpITnkIbljoJkAgIPZBYCZg8VARI0MzAxMjIxOTg2MDgxMDAzNjlkAgMPZBYCZg8VAQ96eHEwNDM1QDE2My5jb21kAgQPZBYCZg8VAQsxMzA1NTE5NjgxMGQCBQ9kFgJmDxUCBWhxd3NjBnN5c3RlbWQCCQ9kFgxmD2QWAmYPFQEGeHNid3NjZAIBD2QWAmYPFQEw6ZW%2F5rKZ57uP5rWO5oqA5pyv5byA5Y%2BR5Yy65Z%2BO5YyX5rGh5rC05aSE55CG5Y6CZAICD2QWAmYPFQESNDMwMzgxMTk4MTEyMDQ3MTIwZAIDD2QWAmYPFQEPMTMyMjM0MDNAcXEuY29tZAIED2QWAmYPFQELMTU5NzMxNDkwNjNkAgUPZBYCZg8VAgZ4c2J3c2MGc3lzdGVtZAIKD2QWDGYPZBYCZg8VAQZjc3l3c2NkAgEPZBYCZg8VASHplb%2FmspnluILplb%2FlloTlnrjmsaHmsLTlpITnkIbljoJkAgIPZBYCZg8VAQBkAgMPZBYCZg8VAQBkAgQPZBYCZg8VAQBkAgUPZBYCZg8VAgZjc3l3c2MGc3lzdGVtZAILD2QWDGYPZBYCZg8VAQZueHh3c2NkAgEPZBYCZg8VARjlroHkuaHljr%2FmsaHmsLTlpITnkIbljoJkAgIPZBYCZg8VARI0MzAxMDMxOTc3MDcxNTQ2MTdkAgMPZBYCZg8VARAzOTY1NjgyMDlAcXEuY29tZAIED2QWAmYPFQELMTg1NzAzODc0NzdkAgUPZBYCZg8VAgZueHh3c2MGc3lzdGVtZAIMD2QWDGYPZBYCZg8VAQZ3c2poenhkAgEPZBYCZg8VAS3plb%2Fmspnnu4%2FmtY7mioDmnK%2FlvIDlj5HljLrmsaHmsLTlh4DljJbkuK3lv4NkAgIPZBYCZg8VARIzNjI0MjkxOTc4MTIyOTQxMTNkAgMPZBYCZg8VAQ8xMzIyMzQwM0BxcS5jb21kAgQPZBYCZg8VAQsxMzc1NTAyMDczMmQCBQ9kFgJmDxUCBndzamh6eAZzeXN0ZW1kAg0PZBYMZg9kFgJmDxUBBnhrcHdzY2QCAQ9kFgJmDxUBJ%2BaWsOW8gOmTuuaxoeawtOWkhOeQhuaciemZkOi0o%2BS7u%2BWFrOWPuGQCAg9kFgJmDxUBEjQ2MDEwMzE5ODgxMDExMTUyN2QCAw9kFgJmDxUBEDI1ODUwMjAwOEBxcS5jb21kAgQPZBYCZg8VAQsxNTg3NDI2OTk0OWQCBQ9kFgJmDxUCBnhrcHdzYwZzeXN0ZW1kAg4PZBYMZg9kFgJmDxUBBHh5c3dkAgEPZBYCZg8VAR7muZbljZfpkavov5zmsLTliqHmnInpmZDlhazlj7hkAgIPZBYCZg8VARI0MzA2ODExOTgyMDQyMDAwMTBkAgMPZBYCZg8VAQ85Mzc0NTE2NUBxcS5jb21kAgQPZBYCZg8VAQsxMzc4NzIzNTM4MWQCBQ9kFgJmDxUCBHh5c3cGc3lzdGVtZAIPD2QWDGYPZBYCZg8VAQV5bHdzY2QCAQ9kFgJmDxUBHumVv%2BaymeW4guWys%2Bm6k%2BaxoeawtOWkhOeQhuWOgmQCAg9kFgJmDxUBEjQzMDEwNTE5ODUwNTMxMjUxNGQCAw9kFgJmDxUBEDE1ODIzNjU2NEBRUS5jb21kAgQPZBYCZg8VAQsxNzc4ODk2NjY2NGQCBQ9kFgJmDxUCBXlsd3NjBnN5c3RlbWQCEA9kFgxmD2QWAmYPFQEGeHNud3NjZAIBD2QWAmYPFQEw6ZW%2F5rKZ57uP5rWO5oqA5pyv5byA5Y%2BR5Yy65Z%2BO5Y2X5rGh5rC05aSE55CG5Y6CZAICD2QWAmYPFQESMzUwMzIyMTk3OTEwMDgxMDU0ZAIDD2QWAmYPFQEPMTMyMjM0MDNAcXEuY29tZAIED2QWAmYPFQELMTU5NzMxNDkwNjNkAgUPZBYCZg8VAgZ4c253c2MGc3lzdGVtZAIRD2QWDGYPZBYCZg8VAQRmZGh5ZAIBD2QWAmYPFQEt5rWP6Ziz5biC6I%2By6L6%2B5a6P5a6H546v5aKD5Y%2BR5bGV5pyJ6ZmQ5YWs5Y%2B4ZAICD2QWAmYPFQEAZAIDD2QWAmYPFQEAZAIED2QWAmYPFQEAZAIFD2QWAmYPFQIEZmRoeQZzeXN0ZW1kAhIPZBYMZg9kFgJmDxUBBXdjd3NjZAIBD2QWAmYPFQEV5pyb5Z%2BO5rGh5rC05aSE55CG5Y6CZAICD2QWAmYPFQEAZAIDD2QWAmYPFQEAZAIED2QWAmYPFQEAZAIFD2QWAmYPFQIFd2N3c2MGc3lzdGVtZAITD2QWDGYPZBYCZg8VAQVzd3l5eWQCAQ9kFgJmDxUBLea1j%2BmYs%2Be7j%2BW8gOWMuuaxoeawtOWkhOeQhuW3peeoi%2BaciemZkOWFrOWPuGQCAg9kFgJmDxUBEjQzMDUyNTE5NzcxMDE4MjUyMGQCAw9kFgJmDxUBDnhsMjgyOUAxMjYuY29tZAIED2QWAmYPFQELMTM1NzQxNTk1MDRkAgUPZBYCZg8VAgVzd3l5eQZzeXN0ZW1kAhQPZBYMZg9kFgJmDxUBBWNzanljZAIBD2QWAmYPFQEP6ZW%2F5rKZ5Y2354Of5Y6CZAICD2QWAmYPFQEAZAIDD2QWAmYPFQEAZAIED2QWAmYPFQEAZAIFD2QWAmYPFQIFY3NqeWMGc3lzdGVtZAIVDw8WAh4HVmlzaWJsZWhkZAIJDw8WAh4LUmVjb3JkY291bnQCc2RkGAEFFGd2QXV0aG9pcnNpelVzZXJsaXN0DzwrAAwBCAIBZN75RaI7t47LE11nG5ZFPFPCdeCev0DFJRy3%2Fj2ly52l&\_\_VIEWSTATEGENERATOR=C2BFA90C&\_\_EVENTTARGET=&\_\_EVENTARGUMENT=&\_\_EVENTVALIDATION=%2FwEdAARsJnviiZjsCeNu7fd8id2qVmNv1R9DYgS4MUZ%2FZb0l42N6ZYJNGAQHn0c9zMgZU3DoD1J50NTVsO6vk7Zy3iszgdWoJ7uNRdjSi%2F1Ymal0Rki%2FVLIp2bPW0ulzMPlfY5s%3D&txtTrunName=&txtUserName=c11&btnQuery=%E6%9F%A5%E8%AF%A2  结果：    数据库系统：MSSQL 2012  IIS：8.5  数据库库名：  ExchangeDB  JointCloud31  …… |
| **风险等级** | 高 |
| **问题影响** | 可进行数据库数据获取。 |
| **加固建议** | 1、参数化查询  2、特殊字符黑名单处理  3、部分参数在系统内多处使用，建议进行全局修复。 |

## 一般工业企业#SQL注入

|  |  |
| --- | --- |
| **漏洞名称** | SQL注入 |
| **漏洞URL** | http://175.6.46.155:81/BaseDataBaseSite/PolluteChargePage/ExemptionManager.aspx?PSCode=&PSClassCode=1&WorkYear=2011&DataType=&UserType=01& |
| **漏洞验证** | 漏洞入口菜单：    发生处：（发生菜单）    数据包：    注入参数：selYear  Payload:  POST /BaseDataBaseSite/PolluteChargePage/ExemptionManager.aspx?PSCode=&PSClassCode=1&WorkYear=2011&DataType=&UserType=01& HTTP/1.1  Host: 175.6.46.155:81  Content-Length: 3912  Cache-Control: max-age=0  Upgrade-Insecure-Requests: 1  Origin: http://175.6.46.155:81  Content-Type: application/x-www-form-urlencoded  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 Edg/83.0.478.58  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  Referer: http://175.6.46.155:81/BaseDataBaseSite/PolluteChargePage/ExemptionManager.aspx?PSCode=&PSClassCode=1&WorkYear=2011&DataType=&UserType=01&  Accept-Encoding: gzip, deflate  Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6  Cookie: .ASPXAUTH=; ASP.NET\_SessionId=nbrcj51n20lawrjwg2rttgqg; UserName=csjointsky; StylePath=..%2f..%2fThemes%2fGreen%2fGreen.swf  Connection: close  \_\_EVENTTARGET=selYear&\_\_EVENTARGUMENT=&\_\_LASTFOCUS=&\_\_VIEWSTATE=%2FwEPDwULLTE4MTM5NDk3OTcPFgYeC1BTQ2xhc3NDb2RlAgEeCERhdGFZZWFyAtsPHghVc2VyTmFtZQUKY3Nqb2ludHNreRYCAgMPZBYIAgEPEGQPFkdmAgECAgIDAgQCBQIGAgcCCAIJAgoCCwIMAg0CDgIPAhACEQISAhMCFAIVAhYCFwIYAhkCGgIbAhwCHQIeAh8CIAIhAiICIwIkAiUCJgInAigCKQIqAisCLAItAi4CLwIwAjECMgIzAjQCNQI2AjcCOAI5AjoCOwI8Aj0CPgI%%2BHHDHiAXQ5O0x%2FqidKWhRPoABtR1FehreL&\_\_VIEWSTATEGENERATOR=3FF33240&\_\_EVENTVALIDATION=%2FwEdAFFl6ZySRDApeWc1ISEpVACA35nI5e5hEdIQ9LtxnYwP%2Fqvour8IViwR09dbBJeYjoFRpT6cOotYxtfPnx9wV3JI0BOtFrJ7eV%2FIiUgOq10dFRPqC1H3PjRK6Ui%2FAwlYSN7E1wzSHpEyo4b8svQPXJ6S4ZsNZRFUagkBDeq5rtgfZcqw6Pr08h1T0NQRav9z5Qv3yKAoXRueil9exa8VKIQijpZdOGm1CcxjQhMd2OC2Pq%2BYVwfz4Fp9B06zA64%2F7dn0AnyakWo4ZpPFLxqZlPEdgLhjxOViYQBUvVnNZr4rIJ0fomLfmUPWt%2Feb8x3a2%2FxmggrHQw3lLnV6GHaCFnMzJOJRM9QLszGsl9NRPdVf5w4WjC3I6f6B9yRhpT7lpcedmMiWH0lMxm7ajtJxviduQhUDPMvT%2FuwTpnOJZzWXf2pQ5pw5raKoRrOc6KWsAb%2F5uiw6AkfrE%2B%2BkB5E3uPQkZAM%2FDpuYJxgjIl%2FC7oDsxfr2VF9TLO5WpKZB%2Fa9CE%2BnRAgvR3Sq1sGnEE3L7cTSoDCBjL7wEOH6QvX5IzkrbikKcgQ0azlOzmVE1zA92X9LI8XeEVkTQNrJIdjiEcOuz4aFKkK0JrzwWnAhP6Gv1a6nmMLIFEtjFh6hDciEkHSgsaeKsR0FnJJRlNVnYldsRYstPTP%2BguqrZG6YAqImoOTeE5R4oxtYevtFh9e7EUsLjDG8S6JOatZLvbCa0MrjzrGGZFOcm3JR8IwHofJpDkz4j6xH6BU1hnI91wgJrVI8qYyGv79i4HeNBaOrLQQrVDqJAmtp89Wy3ksUTdwWVEq0AMy9XCFwyIqaWHLrLMBr2Uz6Epla0QrWgBqLgpLsrH%2B0KwmVum%2Fkl9mdCglxxRB5stfZdVIo%2FHrsqae%2Bh70RniFyrQPe0Mpip4L9DCZbEG46BpTSw%2BYQVBAY54PGjtmpaZ01gJtJU3D731KuRC%2FoIasWvbUuAig39SDy9rjh9eSIAF6nxUvUZM5WtgVjdAwr6oYzzW9y6n3xC9ofRt%2BmTSR%2Fu9ddSjcYvplt2Rnw%2BBw%2B85oCa7zWd820LOJmatjIWn8v1a79T4Ddu3fjjEZyTEyzmMvOtUARdwEWzIIgW7VD6s6WYTDYzxghe%2FokH2%2BuoHdiZcbp1BtfqfZexcBIEliM2QeoRcxDgfq1LvZbik6X6Hf2nq8NUBFlft9%2BDqsBE39yKf6k3c4MNbrPCbANg7McybUALh1LCZP%2F5OQOkvDgpLvMMJLtKbTCaXcwb5cU824G83qCu%2FyMAzNiAbqxIkUZ3EOiQNBn2LKfQyoqmnmdiSqSeW6VkQiRQQYfNFsmJMK8YeVrIFRe%2FQ%2FnvlwoGY2BgQbxROY2FGPMqgEsZ1WVz3qWlvnb15SxlKCxJokYu4hZxNAj%2FnuAKALOB1Qtcj8RwazcZ40nB4licDtB1LaEPpCAhC%2BFxyvDzQ16%2BMJwsv4NOhB%2BhJ3Bv6ktbrWGkCc2DUHuh0oY3VyYnw1M84pL5Ac2x92LhXfuyTILgXiezn%2Fx%2FcRPpb0ucWzPCeu%2FPV3CVhLbcW7V%2BQTo54smCRcfbSqEGXU7%2B3qzo0SRb5hqFDJV3LhmBfdVcoPTjAF343cziRTj%2BrqEpd56dzV5PMBgYLxRC1F7yxfEIh5j3i5ZYgDymPir0Zp4mFYzbkIhXkRFbU1wC%2BuBOEBP%2BpRoWAclvk65gkEWFh0udZaBQIbRJjR%2BgP%2BqvYUB%2FbWEzK%2FxEMefGsDZWsriafdBW%2FwvoAbdE6X5HD6r6rMWPr308wg%3D%3D&selYear=2014&rbList=1&txtApprover=&selPSList=&hidStartYear=1950&hidEndYear=2020 |
| **风险等级** | 高 |
| **问题影响** | 可进行数据库数据获取。 |
| **加固建议** | 1、参数化查询  2、特殊字符黑名单处理  3、部分参数在系统内多处使用，建议进行全局修复。 |