Translation of <https://www.owasp.org/index.php/Top_10_2013-A1-Injection>

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ആക്രമകാരികള്‍** | **ആയുധങ്ങള്‍** | **സുരക്ഷാ ദൗര്‍ബല്യം** | | **സാങ്കേതിക ആഘാതം** | **വ്യാവസായിക ആഘാതം** |
| **ആപ്ലിക്കേഷാനുസൃതം** | **ബലഹീനത എളുപ്പം** | **സാധ്യത സാധാരണം** | **കണ്ടുപിടിത്തം ശരാശരി** | **ആഘാതം രൂക്ഷം** | **ആപ്ലിക്കേഷന്‍/ വ്യവസായ അനുസൃതം** |
| വിശ്വസനീയമല്ലാത്ത ഡാറ്റ സിസ്റ്റത്തിലേക്ക് അയക്കുവാന്‍ കഴിയുന്ന ആരെ വേണമെങ്കിലും ഇവിടെ പരിഗണിക്കാം. ഉദാഹരണത്തിന് പുറത്തുനിന്നും അകത്തുനിന്നും ഉള്ള ഉപയോക്ത്താക്കള്‍, നിയന്ത്രിക്കുന്നവര്‍. | അക്രമി ലളിതമായ പദങ്ങള്‍ അയച്ച് ലക്ഷ്യത്തിലുള്ള വ്യാഖ്യാന സംവിധാനത്തിന്‍റെ ഘടനയെ ചൂഷണം ചെയ്യുന്നു. ആഭ്യന്തര സ്രോതസ്സുകളുള്‍പ്പെടെ ഏതു ഡാറ്റ സ്രോതസ്സും സ്ക്രിപ്റ്റ് ഉള്‍പ്പെടുത്തലുകള്‍ക്ക് വിധേയമാകാം. | ഉള്‍പ്പെടുത്തലുകള്‍ എന്ന വൈകല്യം ഉണ്ടാകുന്നത് ആപ്പ്ളിക്കേഷനുകള്‍ വിശ്വസനീയമല്ലാത്ത ഡാറ്റ ഒരു വ്യാഖ്യാന സംവിധാനത്തിലേക്ക് അയക്കുംബോഴാണ്. ഈ വൈകല്യം സര്‍വസാധാരണമാണ് പ്രത്യേകിച്ചു പരമ്പരാഗത കോഡുകളില്‍. മിക്കവാറും SQL, LDAP, XPath, NoSQL വാക്യങ്ങളില്‍, OS നിദേശങ്ങളില്‍, XML വ്യാഖ്യാനങ്ങളില്‍, SMTP തലക്കട്ടുകളില്‍, പ്രോഗ്രാമ്മുകള്‍ക്ക് നല്‍കുന്ന വിവരങ്ങളിലും ഇവ കാണപ്പെടുന്നു. കോഡ് വായിക്കുമ്പോള്‍ ഉള്‍പ്പെടുത്തല്‍ വൈകല്യം എളുപ്പം കണ്ടെത്താം എന്നാല്‍ മറ്റ് പരിശോധനകളില്‍ ഇവ കണ്ടെത്താന്‍ വളരെ പ്രയാസമാണ്. സ്കാനറുകളും ഫസ്സറുകളും ഉള്‍പ്പെടുത്തല്‍ വൈകല്യം കണ്ടെത്താന്‍ ആക്രമകാരികളെ സഹായിക്കുന്നു. | | ഉള്‍പ്പെടുത്തലുകള്‍ എന്ന വൈകല്യം നിമിത്തം ഡാറ്റ നഷ്ടപ്പെടുകയോ, വികലമാക്കപ്പെടുകയോ, ഉടമസ്ഥ തര്‍ക്കം വരികയോ, ലഭ്യത തടസ്സപ്പെടുകയോ ചെയ്യാം. ഈ പ്രശ്നം കാരണം ഒരുപക്ഷേ സിസ്റ്റത്തിന്റെ നിയന്ത്രണം മറ്റൊരാള്‍ എടുക്കാന്‍ ഇടവരുത്തും. | ചൂഷണം ചെയ്യപ്പെട്ട ഡാറ്റായുടെയും വ്യാഖ്യാന സംവിധാനം ഓടുന്ന സിസ്റ്റത്തിന്റെയും വ്യവസായിക മൂല്യം കണക്കാക്കുക. എല്ലാ ഡാറ്റയും കവര്‍ച്ച ചെയ്യപ്പെടുകയോ, രൂപാന്തരപ്പെടുത്തുകയോ നശിക്കപ്പെടുകയോ ചെയ്യാം. ഇത് നിങ്ങളുടെ സല്‍പേരിന് കോട്ടം തട്ടാമോ? |

|  |
| --- |
| **എനിക്ക് ഉള്‍പ്പെടുത്തല്‍ ഭീഷണിയുണ്ടോ?** |