ഒവാസ്പിന്റെ ആദ്യ പത്തു സുരക്ഷാ നിര്‍ദേശങ്ങള്‍ - വിശദമായി

1. ഇഞ്ചക്ഷന്‍ അഥവാ വിനാശകരമായ സ്ക്രിപ്ടുകളുടെ ഉള്‍പ്പെടുത്തലുകള്‍.

കമ്പ്യൂട്ടര്‍ നിര്‍ദേശങ്ങള്‍ വ്യാഖ്യാനിക്കപ്പെടുത്തുന്ന സങ്കേതത്തിലേക്ക് വിശ്വസനീയമല്ലാത്ത ഡാറ്റ അയക്കപ്പെടുംബോഴാണ് എസ്‌ക്യൂ‌എല്‍, ഓ‌എസ്, എല്‍‌ഡി‌എ‌പി മുതലായ സ്ക്രിപ്റ്റ് പിഴവുകളുണ്ടാകുന്നത്. അക്രമി നല്‍കുന്ന കളങ്കിതമായ ഡാറ്റ ഈ സങ്കേതത്തെ കബളിപ്പിച്ചു തെറ്റായ നിര്‍ദേശങ്ങള്‍ നടപ്പിലാക്കുവാനോ അനുവാദമില്ലാതെ ഡാറ്റ കൈകാര്യം ചെയ്യുവാനോ പ്രേരിപ്പിക്കുന്നു.

1. ബ്രോക്കണ്‍ ആതന്‍റിക്കേഷന്‍ ആന്‍ഡ് സെഷന്‍ മാനേജ്മെന്‍റ് അഥവാ പഴുതുകളുള്ള അനുവാദ പ്രക്രിയയും ഉപയോഗ കാലാവധി നിയന്ത്രണവും

പലപ്പോഴും ആപ്പ്ലിക്കേഷനുകളില്‍ അനുവാദ പ്രക്രിയയും ഉപയോഗ കാലാവധി നിയന്ത്രണവും ശരിയായ രീതിയില്‍ നടപ്പാക്കാത്തതുകൊണ്ടു ആക്രമികള്‍ക്ക് പസ്സ്വോര്‍ഡുകളും ഉപയോഗ കാലാവധി നിയന്ത്രണത്തിന് ഉപയോഗിയ്ക്കുന്ന ടോക്കനുകളും മറ്റും മറികടക്കുവാന്‍ സാധിക്കുന്നു. തന്‍മൂലം ആക്രമിക്ക് മറ്റുള്ള ഉപയോക്താക്കളുടെ ഓണ്‍ലൈന്‍ വ്യക്തിത്വം ആര്‍ജിക്കുവാന്‍ സാധിക്കുന്നു.

1. ക്രോസ്സ് സൈറ്റ് സ്ക്രിപ്റ്റിങ് (XSS) അഥവാ വെബ് പേജുകളിന്മേലുള്ള വിനാശകരമായ സ്ക്രിപ്ടുകളുടെ ഉള്‍പ്പെടുത്തലുകള്‍.

ആപ്പ്ലിക്കേഷനുകള്‍ വിശ്വാസയോഗ്യമല്ലാത്ത ഡാറ്റ സ്വീകരിച്ചു ശരിയായ സാധുത പരിശോധന കൂടാതെയോ വേണ്ട ഒഴിവാക്കലുകള്‍ നടത്താതെയോ ബ്രൌസറുകളിലെക്കയക്കുംബോഴാണ് ഈ പിഴവുണ്ടാകുന്നത്. ഈ പിഴവിലൂടെ ഇരയുടെ ബ്രൌസറില്‍ ആക്രമിക്ക് വിനാശകരമായ സ്ക്രിപ്റ്റുകള്‍ പ്രവര്‍ത്തിപ്പിക്കുവാന്‍ സാധിക്കും. ഇതുവഴി ഇരയുടെ ലോഗിന്‍ ചെയ്ത അവസ്ഥ ആക്രമിക്ക് ലഭിക്കാം അല്ലെങ്കില്‍ അദ്ദേഹത്തിന്റെ വെബ് പേജ് മലിനപ്പെടുത്താം അല്ലെങ്കില്‍ അദ്ദേഹത്തെ മോശം സൈറ്റുകളിലേക്ക് വഴിതിരിച്ചു വിടാം.

1. ഇന്‍സെക്ക്വര്‍ ഡൈറക്റ്റ് ഒബ്ജക്ട് റെഫറന്‍സ് അഥവാ അതീവ സുരക്ഷിതമായിരിക്കേണ്ട അറിവുകളുടെയോ വസ്തുക്കളുടെയോ നേരിട്ടുള്ള ഉപയോഗം

ഉപയോഗ നിയന്ത്രണ പരിശോധനയോ മറ്റു സുരക്ഷാ പരിശോധനയോ ഇല്ലാതെയുള്ള ഫൈലുകളുടെയോ ഡിറക്ടറികളുടെയോ ഡാറ്റാബേസുകളുടെയോ ഉപയോഗം മൂലം ആക്രമികള്‍ക്ക് ഇവയുടെ മേല്‍ കൃത്രിമം കാണിക്കുവാന്‍ സാധിക്കും.

1. സെക്യൂരിറ്റി മിസ് കോണ്‍ഫിഗുറേഷന്‍ അഥവാ തെറ്റായ സുരക്ഷാ ക്രമീകരണങ്ങള്‍

ശരിയായ സുരക്ഷിതത്വം ലഭിക്കുന്നതിനു വേണ്ടി ആപ്ലിക്കേഷനുകളിലും, ഫ്രെയിംവര്‍ക്കുകളിലും വെബ് സെര്‍വറുകളിലും ഡാറ്റബേസ് സെര്‍വറുകളിലും ശരിയായ സുരക്ഷാ ക്രമീകരണങ്ങള്‍ നിശ്ചയിക്കുകയും അവ വിന്യസിക്കുകയും ചെയ്യേണ്ടതുണ്ട്. ഇവയിലുള്ള തനതായ ക്രമീകരണങ്ങള്‍ പലപ്പോഴും സുരക്ഷിതമല്ലാത്തതാണ്. കൂടാതെ സോഫ്ട്വയറുകള്‍ എല്ലായിപ്പോഴും പുതുക്കി സൂക്ഷിക്കേണ്ടതുണ്ട്.

1. സെന്‍സിറ്റീവ് ഡാറ്റ എക്സ്പോഷര്‍ അഥവാ അതീവ രഹസ്യ സ്വഭാവമുള്ള വിവരങ്ങളുടെ വെളിപ്പെടുത്തലുകള്‍

പല വെബ് ആപ്ലിക്കേഷനുകളും ക്രെഡിറ്റ് കാര്‍ഡ്, പാസ്സ്വേഡ് മുതലായ അതീവ രഹസ്യ സ്വഭാവമുള്ള വിവരങ്ങള്‍ ശരിയായ രീതിയില്‍ സംരക്ഷിക്കുന്നില്ല. ഇതുമൂലം അക്രമികള്‍ ഈ വിവരങ്ങള്‍ മോഷണം ചെയ്തു പലവിധ കുറ്റകരമായ കാര്യങ്ങള്‍ക്കും ഉപയോഗിക്കുന്നു. അതീവ രഹസ്യ സ്വഭാവമുള്ള വിവരങ്ങള്‍ക്കു നിശ്ചലാവസ്ഥയിലോ സഞ്ചാരത്തിലോ എന്‍ക്രിപ്ഷന്‍ മുതലായ സങ്കേതങ്ങള്‍ ഉപയോഗിച്ചുള്ള അധിക സംരക്ഷണം ആവശ്യമാണ്. ഇത്തരത്തിലുള്ള ഡാറ്റാകള്‍ ബ്രൌസര്‍ മുഖാന്തിരം കൈമാറ്റം ചെയ്യപ്പെടുമ്പോള്‍ പ്രത്യേക മുന്‍കരുതലുകള്‍ എടുക്കേണ്ടതുണ്ട്.

1. മിസ്സിംഗ് ഫംഗ്ഷന്‍ ലെവല്‍ ആക്സെസ് കണ്‍ട്രോള്‍ അഥവാ ചുമതലാ തലത്തിലുള്ള ഉപയോഗത്തിനുള്ള നിയന്ത്രണമില്ലായ്മ

മിക്ക വെബ് ആപ്ലിക്കേഷനുകളും അനുമതിയുണ്ടോ എന്നു പരിശോധിച്ചിട്ടെ ബ്രൌസര്‍ തലത്തില്‍ സേവനങ്ങള്‍ പ്രദാനം ചെയ്യാറുള്ളൂ. പക്ഷേ ഈ അനുമതി പരിശോധന സെര്‍വര്‍ തലത്തിലും ചെയ്യേണ്ടതുണ്ട്. ഇപ്രകാരം ചെയ്തില്ലെങ്കില്‍ അക്രമികള്‍ വെബ് സേവങ്ങളിന്മേലുള്ള അപേക്ഷകളില്‍ കൃത്രിമം കാട്ടി അനുമതിയില്ലാതെ അവ ഉപയോഗിക്കും.

1. ക്രോസ്സ് സൈറ്റ് റിക്വെസ്റ്റ് ഫോര്‍ജറി (CSRF) അഥവാ വെബ് സേവനങ്ങളുടെ ആവശ്യപ്പെടലുകളില്‍ കൃത്രിമം നടത്തുക.

ഈ ആക്രമണത്തിലൂടെ ലോഗിന്‍ ചെയ്ത ഇരയുടെ ബ്രൌസറിനെ ബലം പ്രയോഗിച്ച് ആക്രമിയുടെ നിയന്ത്രണത്തിലുള്ള വെബ് ആപ്ലിക്കേഷനിലേക്ക് ഇരയുടെ ഉപയോഗ കാലാവധി നിയന്ത്രണ ഡാറ്റയും മറ്റു അനുവാദ വിവരങ്ങളും ചോര്‍ത്തി കൊടുക്കുന്നു. ഇപ്രകാരം ആക്രമിക്ക് ഇരയുടെ ബ്രൌസറില്‍ നിന്നു തെറ്റായ വെബ് സേവന അപേക്ഷകള്‍ സാധാരണ എന്ന പോലെ സെര്‍വേറിലേക്ക് അയക്കുവാന്‍ സാധിക്കുന്നു.

1. യൂസിംഗ് കോംപോണേന്റ്സ് വിത്ത് നോണ്‍ വള്‍നറബിലിറ്റീസ് അഥവാ അറിയപ്പെടുന്ന സുരക്ഷാ വീഴ്ചകളുള്ള ഘടകങ്ങളുടെയൊ സേവനങ്ങളുടെയോ ഉപയോഗം

ലൈബ്രറികള്‍, ഫ്രെയിംവര്‍ക്കുകള്‍ മുതലായ സോഫ്റ്റ്വെയര്‍ ഘടകങ്ങള്‍ പലപ്പോഴും പരിപൂര്‍ണ അനുവാദത്തോടെയാണ് ആപ്ലിക്കേഷനുകളില്‍ ഉപയോഗിക്കുന്നത്. ഇപ്രകാരമുള്ള ഘടകങ്ങളിലെ പിഴവുകള്‍ അക്രമികള്‍ ചൂഷണം ചെയ്യുന്നതുമൂലം കടുത്ത ഡാറ്റാ നഷ്ടങ്ങളോ സെര്‍വറുകളിന്മേലുള്ള നിയന്ത്രണ നഷ്ടമോ സംഭവിക്കാം. സുരക്ഷാ പിഴവുകളുള്ള സോഫ്റ്റ്വെയര്‍ ഘടകങ്ങളുടെ ഉപയോഗം മൂലം ആപ്ലിക്കേഷനുകളുടെ സുരക്ഷാ പ്രതിരോധം ദുര്‍ബലമായി പലവിധ ആക്രമങ്ങള്‍ക്കും ആഘാതങ്ങള്‍ക്കും പാത്രീഭവിക്കും.

1. അണ്‍വാലിഡേറ്റെഡ് റീഡൈറെക്ട്സ് ആന്‍ഡ് ഫോര്‍വേര്‍ഡ്സ് അഥവാ പരിശോധനകൂടാതെയുള്ള തിരിച്ചയക്കലോ തിരിച്ചുവിടലുകളോ

വെബ് ആപ്ലിക്കേഷനുകള്‍ പലപ്പോഴും ഉപയോക്താക്കളുടെ സേവന അപേക്ഷകള്‍ മറ്റു വെബ് പേജുകളിലേക്കോ സൈറ്റുകളിലേക്കൊ അന്ധമായി വിശ്വസിച്ച് തിരിച്ചു വിടാറുണ്ട്. ശരിയായ ഉറപ്പുവരുത്തലുകളില്ലാതെ തിരിച്ചയക്കലോ തിരിച്ചുവിടലുകളോ ചെയ്യുന്നത് ചൂഷണം ചെയ്തു അക്രമികള്‍ ഉപയോക്താക്കളെ മോശമായതും ആപല്‍ക്കരവുമായ സൈറ്റുകളിലേക്ക് വഴി തിരിച്ചു വീടുകയോ അനുവാദമില്ലാത്ത വെബ് പേജുകള്‍ ഉപയോഗിക്കുവാന്‍ നിര്‍ബന്ധിക്കുകയോ ചെയ്യുന്നു.