| Risk ID | Risk Name | Vulnerabilities | Threats | assets | Impact | Risk Level |
| --- | --- | --- | --- | --- | --- | --- |
| 001 | Unauthorize application access | [CVE-2018-1002105](https://github.com/kubernetes/kubernetes/issues/71411),9.8,high,remote,not required,critical  [CVE-2018-11988](https://www.cvedetails.com/cve/CVE-2018-11988/),4.6,high,remote,not required,medium | CAPEC-115: Authentication Bypass | Point of sale | high | high(very high,high,high) |
| 002 | Improper input validation | [CVE-2008-2169](https://www.cvedetails.com/cve/CVE-2008-2169/),7.1,high,remote,not required,DoS,High  [CVE-2014-0984](https://www.cvedetails.com/cve/CVE-2014-0984/),4.3,high,remote,not required,DoS,medium | CAPEC-74: Manipulating State | router | high | high(high,high,high) |
| 003 | Cause denial of service | CVE-2015-1574,5.0,medium,remote,not required,DoS,Meidum  CVE-2017-17689, 4.3,medium,remote,not required,DoS,Meidum | CAPEC-227: Sustained Client Engagement | Email Service | medium | medium(medium,medium,medium) |
| 004 | Unauthorized access to critical data of database | [CVE-2017-10261](https://www.cvedetails.com/cve/CVE-2017-10321/),4.0,medium,remote,not required,Info,medium  [CVE-2017-10190](https://www.cvedetails.com/cve/CVE-2017-10190/),4.3,medium,remote,not required,Info,medium | CAPEC-115: Authentication Bypass | Database | medium | medium(medium,high,medium) |
| 005 | Injection of HtML or web script | [CVE-2012-4923](https://www.cvedetails.com/cve/CVE-2012-4923/),4.3,high,remote,not required,xss,medium  [CVE-2008-0494](https://www.cvedetails.com/cve/CVE-2008-0494/),4.3,high,remote,not required,xss,medium | CAPEC-153: Input Data Manipulation | Firewall | high | high(medium,high,high) |
| 006 | Execution of arbitrary code via unspecified protocol operations | [CVE-2013-6035](https://www.cvedetails.com/cve/CVE-2013-6035/),10.0,high,remote,not required,Exec code, critical  [CVE-2013-6034](https://www.cvedetails.com/cve/CVE-2013-6034/),10.0,high,remote,not required,Exec code, critical | CAPEC-175: Code Inclusion | IP | high | high(very high, high, high) |
| 007 | Data gathering | [CVE-2017-7855](https://www.cvedetails.com/cve/CVE-2017-7855/),4.3,medium,remote,not required,xss,medium  [CVE-2011-3825](https://www.cvedetails.com/cve/CVE-2011-3825/),5.0,medium,remote,not required,+info,medium | CAPEC-117: Interception | server | medium | medium(medium,medium,medium) |