Access admin account

SQL Injection

Impersonate

E-skimming

Install malware

XSS

Access server

Access customer account

**Steal customer data**

Session Hijacking

Data / Password Sniffing

Brute force password

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Threat | D | R | E | A | DI | Average | Risk (P x I) |
| SQL Injection | 3 | 3 | 2 | 3 | 2 | 2.6(High) | 42 |
| XSS | 3 | 3 | 3 | 3 | 3 | 3(High) | 54 |
| Session Hijacking | 2 | 2 | 2 | 1 | 3 | 2(Medium) | 21 |
| Brute Forcing | 2 | 1 | 1 | 3 | 2 | 1.8(Medium) | 20 |
| Data / Password Sniffing | 2 | 2 | 2 | 2 | 2 | 2(Medium) | 24 |
| Impersonation | 2 | 2 | 3 | 2 | 2 | 2.2(High) | 28 |

**Control measures**

Looking at the average and risk ranking, designer will need to consider XSS as first to mitigate than SQL injection than Impersonation as the average is high. After addressing the high threat which is session Hijacking an Data sniffing which have the same average score but since password sniffing risk ranking is higher, the designer will mitigate Data sniffing first than session hijacking and lastly brute forcing.