

TURVALLINEN OHJELMOINTI, TIE-30600

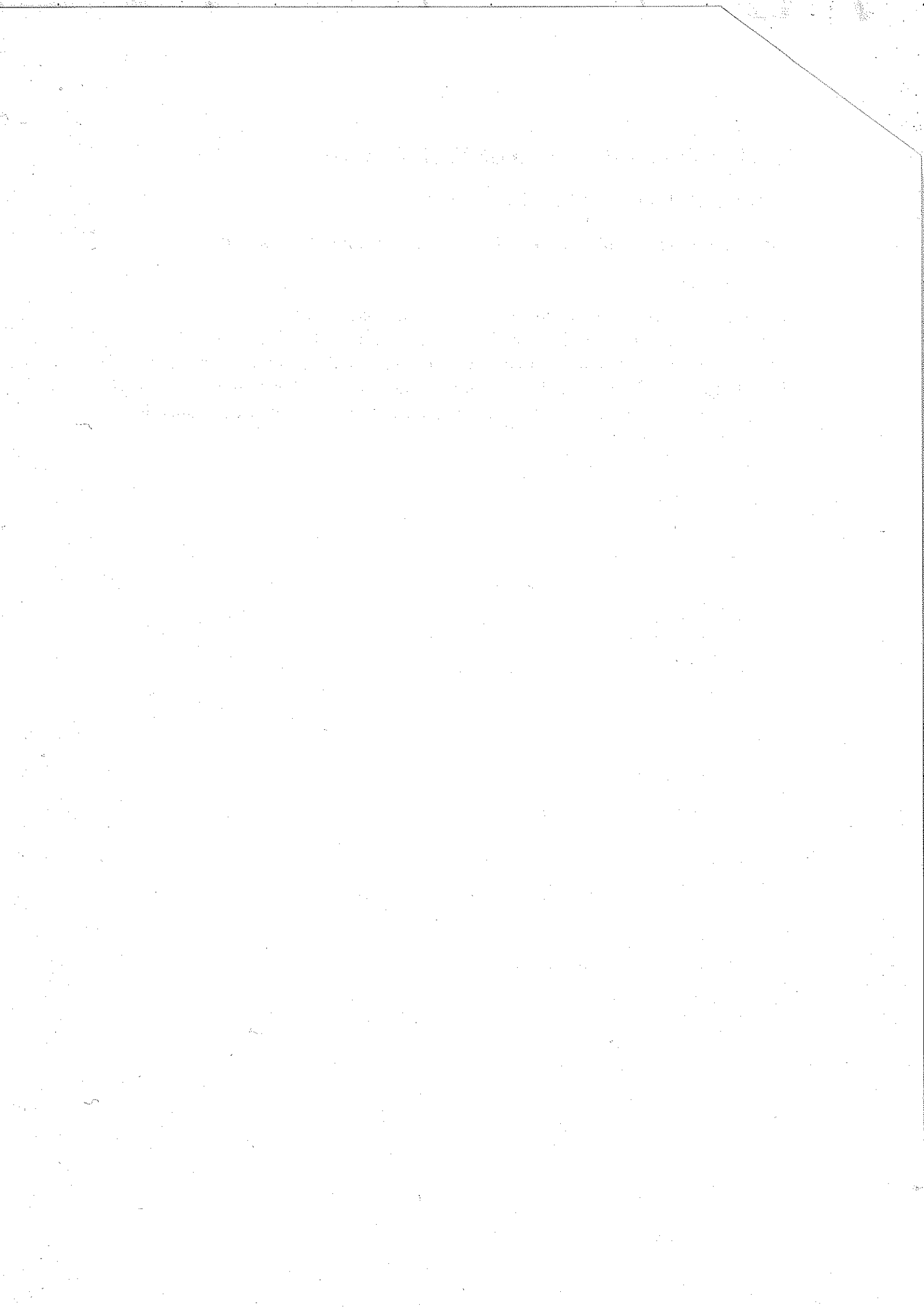
TENTTI 2.12.2014 Marko Helenius

Tentissä ei saa käyttää laskinta eikä oheismateriaalia. Vastaa selkeästi.

1. (6 pistettä)

Tarkastele oheista ohjelman osaa. Vasemmassa reunassa on ohjelmaan viittaamisen helpottamiseksi rivinumerot. Missä kohdassa ohjelmaa on haavoittuvuuksia, mitä nämä haavoittuvuudet ovat, mitä niistä voi seurata ja miksi? Miten korjaisit haavoittuvuudet? Haavoittuvuudeksi tulee tehtävässä laskea myös sellaiset virheet, jotka johtavat viittaukseen virheelliselle muistialueelle tai jumittavat ohjelman.

```
1: const int OLETUS_KOKO = 256;
2:
3: class Merkkijono
4: {
5: private:
6:     float* puskuri;
7:     int koko;
8:
9: public:
10:     Merkkijono();
11:     Merkkijono(int pituus);
12:     ~Merkkijono();
13:     bool Aseta(int indeksi, float luku);
14:     void Tulosta();
15:     float Summa();
16:     void Poista();
17: };
18:
19: Merkkijono::Merkkijono()
20: {
21:     Merkkijono(OLETUS_KOKO);
22: }
23:
24: Merkkijono::Merkkijono(int pituus)
25: {
26:     puskuri = new float[pituus]; // varataan muisti
27:     koko = pituus;
28: }
29:
30: bool Merkkijono::Aseta(int i, float luku)
31: {
32:     puskuri[i] = luku;
33:     return true;
34: }
35:
36: void Merkkijono::Tulosta()
37: {
38:     for (int i=0; i<koko; i++)
39:         cout << puskuri[i];
40: }
```



```
41: float Merkkijono::Summa()
42: {
43:     float summa = 0;
44:     for (int i=0; i<koko; i++)
45:         summa += puskuri[i];
46:     return summa;
47: }
48:
49: Merkkijono::~Merkkijono()
50: {
51:     delete puskuri;
52: }
```

2. OWASP Top 10 –listassa ovat oheiset kohdat. Kuvaa jokaisesta kohdasta muutamalla virkkeellä, mitä kukin kohta tarkoittaa.

A1-Injection

A2-Broken Authentication and Session Management

A3-Cross-Site Scripting (XSS)

A4-Insecure Direct Object References

A5-Security Misconfiguration

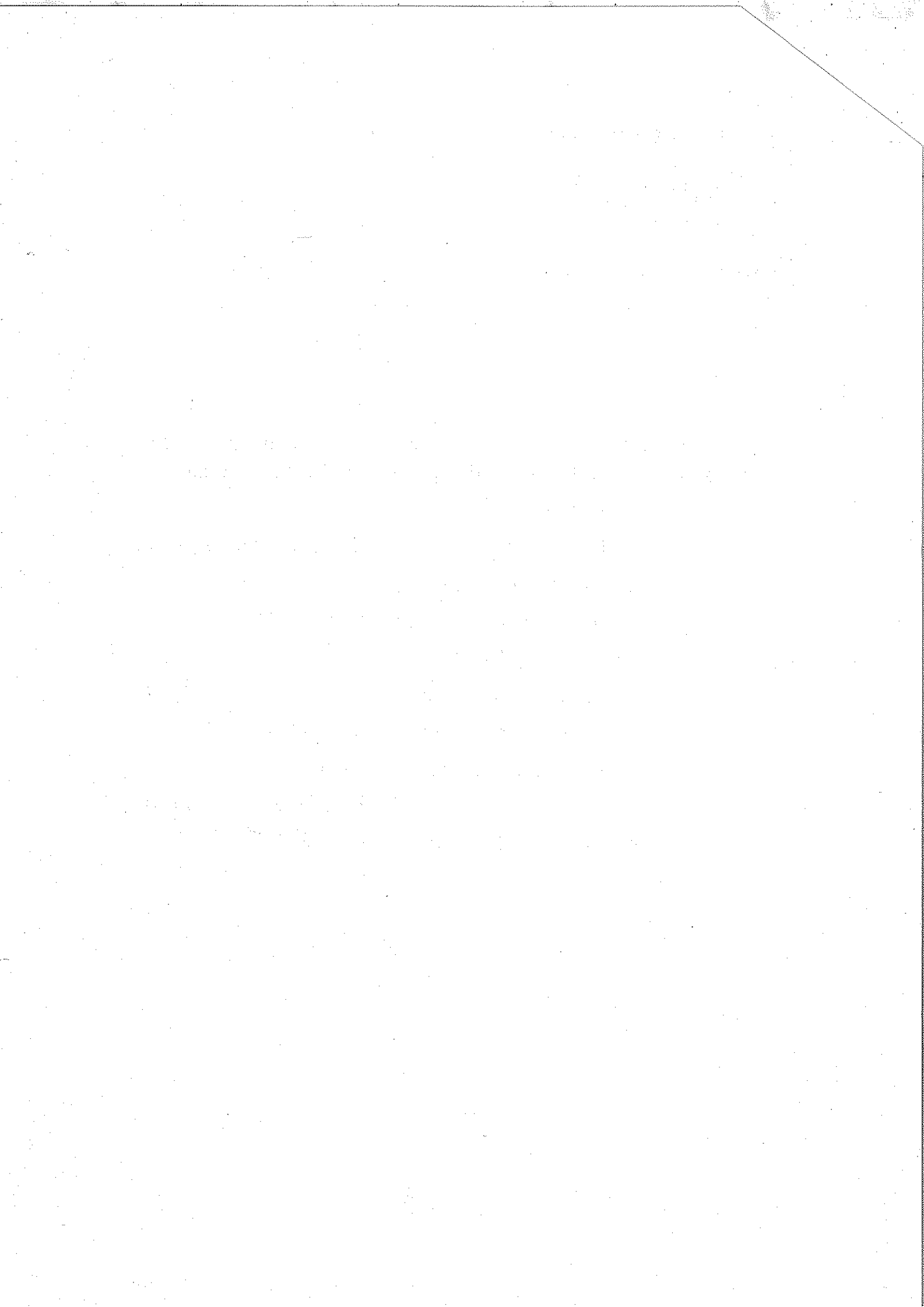
A6-Sensitive Data Exposure

A7-Missing Function Level Access Control

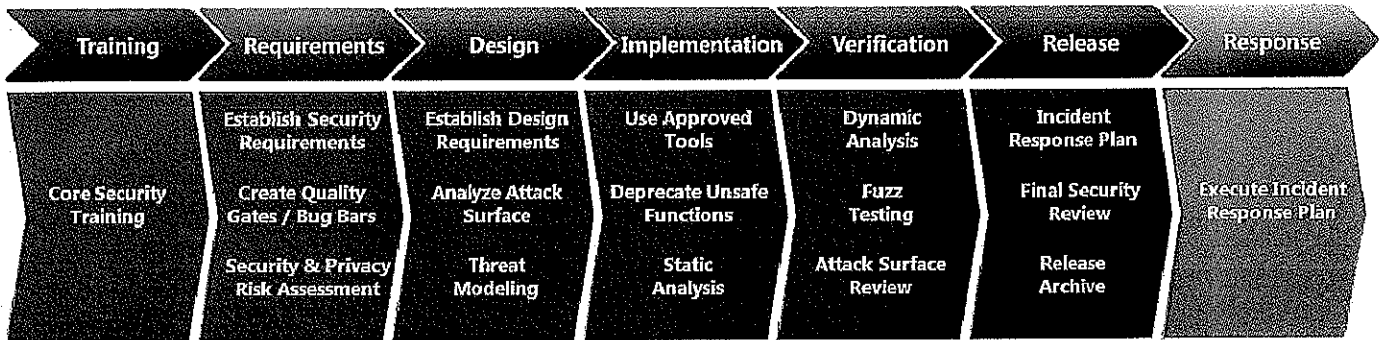
A8-Cross-Site Request Forgery (CSRF)

A9-Using Components with Known Vulnerabilities

A10-Unvalidated Redirects and Forwards



3. Oheisessa kuvassa ovat yksinkertaistetun MSDL:n vaiheet. Mitä kukin vaihe sisältää ja mitä niissä pitää ottaa huomioon?



4. Kirjoita oheisen kuvan perusteella essee. Kuva mitä kullakin käsitteellä tarkoitetaan.

