

TENTTI 17.10.2017 TURVALLINEN OHJELMOINTI, TIE-30600

Marko Helenius

Tentissä ei saa käyttää oheismateriaalia eikä laskinta. Vastaa selkeästi.

Vastaa seuraaviin kohtiin turvallisen ohjelmoinnin periaatteiden mukaisesti (6 pistettä/tehtävä):

1. Tarkastele oheisia ohjelmien osia. Mitä haavoittuvuuksia tai ongelmia niissä on, mitä niistä voi seurata ja miksi? Miten korjaisit? (2 pistettä/kohta)

a)

```
TAG_RE = re.compile(r'<(.*?)(&#x27;>|&#x22;>|&#x2F;>|&#x3E;|&#x0A;|&#x0D;|&#x09;|&#x00;|&#x01;|&#x02;|&#x03;|&#x04;|&#x05;|&#x06;|&#x07;|&#x08;|&#x09;|&#x0A;|&#x0B;|&#x0C;|&#x0D;|&#x0E;|&#x0F;|&#x10;|&#x11;|&#x12;|&#x13;|&#x14;|&#x15;|&#x16;|&#x17;|&#x18;|&#x19;|&#x1A;|&#x1B;|&#x1C;|&#x1D;|&#x1E;|&#x1F;|&#x20;|&#x21;|&#x22;|&#x23;|&#x24;|&#x25;|&#x26;|&#x27;|&#x28;|&#x29;|&#x2A;|&#x2B;|&#x2C;|&#x2D;|&#x2E;|&#x2F;|&#x30;|&#x31;|&#x32;|&#x33;|&#x34;|&#x35;|&#x36;|&#x37;|&#x38;|&#x39;|&#x3A;|&#x3B;|&#x3C;|&#x3D;|&#x3E;|&#x3F;|&#x40;|&#x41;|&#x42;|&#x43;|&#x44;|&#x45;|&#x46;|&#x47;|&#x48;|&#x49;|&#x4A;|&#x4B;|&#x4C;|&#x4D;|&#x4E;|&#x4F;|&#x50;|&#x51;|&#x52;|&#x53;|&#x54;|&#x55;|&#x56;|&#x57;|&#x58;|&#x59;|&#x5A;|&#x5B;|&#x5C;|&#x5D;|&#x5E;|&#x5F;|&#x60;|&#x61;|&#x62;|&#x63;|&#x64;|&#x65;|&#x66;|&#x67;|&#x68;|&#x69;|&#x6A;|&#x6B;|&#x6C;|&#x6D;|&#x6E;|&#x6F;|&#x70;|&#x71;|&#x72;|&#x73;|&#x74;|&#x75;|&#x76;|&#x77;|&#x78;|&#x79;|&#x7A;|&#x7B;|&#x7C;|&#x7D;|&#x7E;|&#x7F;|&#x80;|&#x81;|&#x82;|&#x83;|&#x84;|&#x85;|&#x86;|&#x87;|&#x88;|&#x89;|&#x8A;|&#x8B;|&#x8C;|&#x8D;|&#x8E;|&#x8F;|&#x90;|&#x91;|&#x92;|&#x93;|&#x94;|&#x95;|&#x96;|&#x97;|&#x98;|&#x99;|&#x9A;|&#x9B;|&#x9C;|&#x9D;|&#x9E;|&#x9F;|&#xA0;|&#xA1;|&#xA2;|&#xA3;|&#xA4;|&#xA5;|&#xA6;|&#xA7;|&#xA8;|&#xA9;|&#xAA;|&#xAB;|&#xAC;|&#xAD;|&#xAE;|&#xAF;|&#xB0;|&#xB1;|&#xB2;|&#xB3;|&#xB4;|&#xB5;|&#xB6;|&#xB7;|&#xB8;|&#xB9;|&#xBA;|&#xBB;|&#xBC;|&#xBD;|&#xBE;|&#xBF;|&#xC0;|&#xC1;|&#xC2;|&#xC3;|&#xC4;|&#xC5;|&#xC6;|&#xC7;|&#xC8;|&#xC9;|&#xCA;|&#xCB;|&#xCC;|&#xCD;|&#xCE;|&#xCF;|&#xD0;|&#xD1;|&#xD2;|&#xD3;|&#xD4;|&#xD5;|&#xD6;|&#xD7;|&#xD8;|&#xD9;|&#xDA;|&#xDB;|&#xDC;|&#xDD;|&#xDE;|&#xDF;|&#xE0;|&#xE1;|&#xE2;|&#xE3;|&#xE4;|&#xE5;|&#xE6;|&#xE7;|&#xE8;|&#xE9;|&#xEA;|&#xEB;|&#xEC;|&#xED;|&#xEE;|&#xEF;|&#xF0;|&#xF1;|&#xF2;|&#xF3;|&#xF4;|&#xF5;|&#xF6;|&#xF7;|&#xF8;|&#xF9;|&#xFA;|&#xFB;|&#xFC;|&#xFD;|&#xFE;|&#xFF;') # matches the start of an html tag

def _SanitizeTag(t):
    """Sanitizes a single html tag.

    This does both a 'whitelist' for
    the allowed tags and a 'blacklist' for the disallowed attributes.

    Args:
        t: a tag to sanitize.

    Returns:
        a safe tag.
    """
    allowed_tags = [
        'a', 'b', 'big', 'br', 'center', 'code', 'em', 'h1', 'h2', 'h3',
        'h4', 'h5', 'h6', 'hr', 'i', 'img', 'li', 'ol', 'p', 's', 'small',
        'span', 'strong', 'table', 'td', 'tr', 'u', 'ul',
    ]
    disallowed_attributes = [
        'onblur', 'onchange', 'onclick', 'ondblclick', 'onfocus',
        'onkeydown', 'onkeypress', 'onkeyup', 'onload', 'onmousedown',
        'onmousemove', 'onmouseout', 'onmouseover', 'onreset',
        'onselect', 'onsubmit', 'onunload', 'onmouseover'
    ]

    # Extract the tag name and make sure it's allowed.
    if t.startswith('</'):
        return t
    m = TAG_RE.match(t)
    if m is None:
        return t
    tag_name = m.group(1)
    if tag_name not in allowed_tags:
        t = t[:m.start(1)] + 'blocked' + t[m.end(1):]

    # This is a bit heavy handed but we want to be sure we don't
    # allow any to get through.
    for a in disallowed_attributes:
        t = t.replace(a, 'blocked')
    return t
```



The first part of the document discusses the importance of maintaining accurate records of all transactions. It emphasizes that every entry should be supported by a valid receipt or invoice. This ensures transparency and allows for easy verification of the data.

Additionally, it is noted that regular audits are essential to identify any discrepancies or errors early on. This proactive approach helps in maintaining the integrity of the financial statements and prevents any potential issues from escalating.

The second section focuses on the role of technology in modern accounting. It highlights how software solutions have revolutionized the way businesses manage their finances. From automated data entry to real-time reporting, these tools significantly reduce the risk of human error and improve efficiency.

However, it is also stressed that while technology is a powerful asset, it should not replace the expertise of a professional accountant. The human element is crucial for interpreting the data, understanding the underlying business context, and providing strategic advice to management.

In conclusion, the document underscores the need for a balanced approach that combines robust internal controls, the use of advanced technology, and the oversight of skilled professionals to ensure the most accurate and reliable financial reporting.

