1. Web framework developer wants to optimize CSRF token processing by not sending the token from server but calculating it in the client and verifying in the server. Can he do it securely?

2. If a web application framework locks sessions to be usable only by one query at a time, what are the pros and cons of that?

3. Find all potential vulnerabilities in this C function:

```c
void *parse_packet (unsigned char *packet)
{
    unsigned char * p, *data;
    short num, len;
    int size, total;

    num = *(short *)p; // copy 16-bit integer
    p += sizeof(short); // advance 2 bytes
    if (num > 13) return 0;
    len = *(short *)p; // copy 16-bit integer
    p += sizeof(short); // advance 2 bytes
    if (len > 2048) return 0;
    size = len;
    total = size*num; // int to fit result
    data = malloc(total);
    memcpy(data, p, total);

    return data;
}
```

4. Find all potential vulnerabilities in this PHP snippet:

```php
<?php
if (isset($_REQUEST['user']) && isset($_REQUEST['password'])) {
    $sql = "UPDATE users SET password=HASHBYTES('sha1'," .
            $_REQUEST['password'] . ") WHERE username=" .
            $_REQUEST['user'] . " ";
    mysql_query($sql) || die($sql);
    echo "Password of " . $_REQUEST['user'] . " changed."
}
?>
```
5. Find all potential vulnerabilities in this Python function:

```python
def save_data(mymask, mydata):
    thefile = os.popen('echo ' + mymask).readline()
    if not os.path.exists(thefile):
        raise IOError('"%s" does not exist' % thefile)
    if os.access(thefile, os.X_OK)
        raise IOError('"%s" is executable, not writing' % thefile)
    if os.path.islink(thefile):
        raise IOError('"%s" is a symbolic link' % thefile)
    f = open(thefile, 'w')
    f.write(mydata)
    f.close
```

Send response by e-mail to mroos@ut.ee no later than 12.00. You can answer either in English or in Estonian.