Universidade de Aveiro

Departamento de Electrónica, Telecomunicações e Informática

Análise e Exploração de Vulnerabilidades - 2021-2022

Teste 1 **Nome:** _____

Data: 26 de Novembro de 2021 **MEC:** _____

Duração: 90 minutos

```python
def log(req):
    with open(f'{LOGDIR}/{req.headers["X-Forwarded-For"]}.log', 'w') as f: # Open <IP>.log to record access
        f.write(f'{time.time()} - {req.method} {req.url}')          # Write information

def get_user(cookie):
    session = pickle.loads(cookie.get('session', None))    # Load session data with Pickle
    user = dict(name='guest', id=-1)                       # Default user

    if session is not None:
        if os.path.exists(session['id']):                  # Is session exists in storage
            data = open(f'{SESSDIR}/session["id"]', 'r').read()    # Load session data from storage
            user = json.loads(data)                        # Unserialize json data from session

    return user

def get_products(req, q):
    log(req.headers)                           # Log request

    msg = ''                                   # Default values
    data = pics = {}
    user = get_user(req.headers['Cookie'])

    try:
        db = db.connect(user='root', password='root',          # Connect o database using IP
                        host='62.34.19.123', database='store')
        cursor = cnx.cursor()                                  # Create cursor and run query to find products
        cursor.execute(f'SELECT * FROM products WHERE name LIKE "%{q}%"')

        pics = dict()
        for row in cursor:                                     # Iterate over all results
            pic = open(f'{PICDIR}/{row[5]}', 'rb').read()      # Load product picture from storage
            pics[row[0]] = base64_encode(pic)                  # Encode for inline display in HTML

        data = cursor                                          # Returns DB data
    except mysql.connector.Error as err:
        msg = err.msg                                          # Save error to help debug

    return render_template('products.html',                    # Render page with correct data
                           data=data, pics=pics, user=user, msg=msg)
```

1) [2½ pts] Considere o excerto de código anterior e responde às questões seguintes:

(a) Enumere e descreva as vulnerabilidades existentes, explique como podem ser exploradas e descreva qual o impacto da sua exploração.
Assuma que existe uma página HTML (`products.html`) que é usada como template e irá apresentar a informação aqui recolhida com um processamento mínimo.

(b) Para **duas** das vulnerabilidades, identifique os dados de entrada que permitem a sua exploração.

(c) Para **uma** das vulnerabilidades, explique as alterações necessárias no código para a mitigar. Use código real ou pseudocódigo, desde que com o detalhe suficiente para compreender as ações a tomar.

2) [1 pt] Considere que acabou de avaliar o risco de uma vulnerabilidade reportada numa aplicação que gere:

(a) O passo seguinte consistirá na correção do erro de programação? Justifique.

(b) Qual a importância da fase de verificação?

3) [1 pt] Considerando as técnicas de `Fingerprinting` de sistemas operativos e serviços:

(a) Descreva porque é possível utilizar estas técnicas e qual o impacto?

(b) Descreva como um administrador de um sistema pode restringir esta capacidade.
