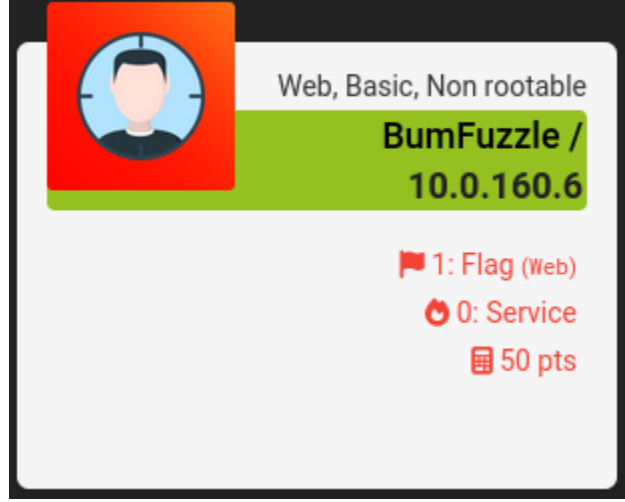




## BUMFUZZLE WRITEUP



Selam arkadaşlar bugün Vulnerday platformu üzerindeki BumFuzzle makinasını inceliyorum.

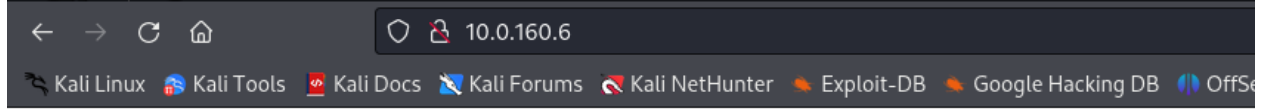
1) Öncelikle makinanın açıklama kısmına bakıyoruz.

“BumFuzzle seni kaybetti ?” bu açıklama pek anlamlı gelmedi bazen şifreli mesajlar olabiliyor ve birçok çıkarımda bulunabiliyoruz.

Makinanın başlığını incelediğimde Web makinası olduğunu seziyoruz ve basit bir makina olduğu dile getirilmiş.

**Onurcan Genc**

2) Ardından makinaya erişim sağlamak için browserdan verilen Ipv4 adresine ilerliyorum.



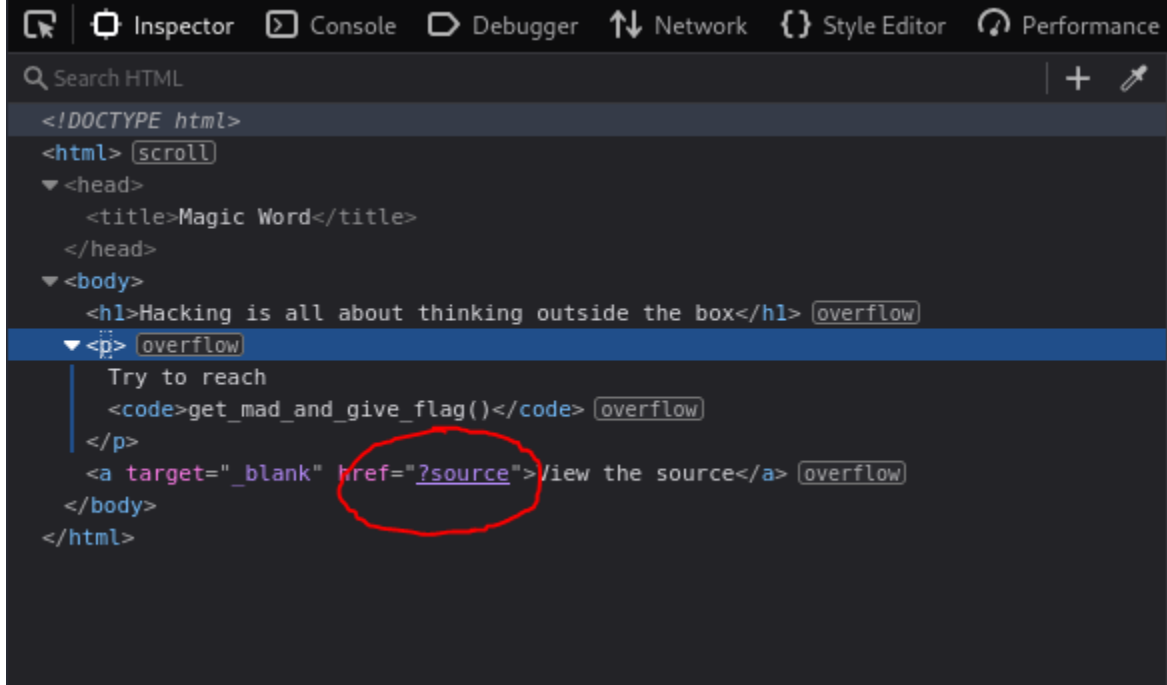
## **Hacking is all about thinking outside the box**

Try to reach `get_mad_and_give_flag()`

[View the source](#)

Karşıma böyle bir html sayfası geldi ve hedefe ulaşmam için bir fonksiyonu (invoke) yani uyandırmam çağırmam isteniyor. Bu fonksiyona erişmemiz içinse sayfanın kaynak koduna erişim hakkı tanıyor.

3) Ben yine her zaman olduđu gibi yüzeysel html elementlerini inceleme yoluna gidiyorum.



```
<!DOCTYPE html>
<html>
  <head>
    <title>Magic Word</title>
  </head>
  <body>
    <h1>Hacking is all about thinking outside the box</h1>
    <p>
      Try to reach
      <code>get_mad_and_give_flag()</code>
    </p>
    <a target="_blank" href="?source">view the source</a>
  </body>
</html>
```

Resimden de görüldüğü üzere bir anchor tag yani referans bir element gözüme çarpıyor. Hyperlink yani “href” propertysinin bizi gönderdiği bir kısım var (?source).

- 4) Linkin götürdüğü kısma ulaştığımızda ise bize sayfanın yazıldığı html dışında kasıtlı olarak arka yüz kodları da view edilmiş. Bunu da şuradan anlayabiliriz.

```
<!DOCTYPE HTML>
<?php
    require("flag.php");

    if (isset($_GET['source'])) {
        highlight_file(__FILE__);
        die();
    }
```

isset() fonksiyonu html elementleri içerisinde referans değeri href değerini veyahutta name propertysi ile nitelendirilmiş bir değerin geçtiği yere bakacaktır. Buradan da anladığımız üzere yukarıdaki ?source referans değerindeki ilk “source” kelimesini alıp url tarafında doğrulamasını \$\_GET parametresi ile veriyi tutumuş ve if() conditionı sağladığı için source kelimesi geçtiğinden parametresi 1 olarak dönüyor ve içerisinde highlight\_file() fonksiyonu çağırıyor. Böylelikle \_\_FILE\_\_ isimli dosyayı bastırıyor.

5) Sayfa kaynağındaki PHP kodu iyice incelendiğinde sorunun CTF sorusundan ziyade bir algoritma challengeı olduğu ortaya çıkıyor.

```
<?php
require("flag.php");

if (isset($_GET['source'])) {
    highlight_file(__FILE__);
    die();
}

if (isset($_GET['magic_word'])) {

    $what_he_said = $_GET['magic_word'];
    $what_you_dont_want_to_hear = 'bumfuzzle';
    $what_you_actually_heard = preg_replace(
        "/$what_you_dont_want_to_hear/", '', $what_he_said);

    if ($what_you_actually_heard === $what_you_dont_want_to_hear) {
        get_mad_and_give_flag();
    }
}
?>
```

Lokal makinamda algoritmayı anlamadığım için kendim başta da tanımlanmış `get_mad_and_give_flag()` fonksiyonunu çıkarıp `echo` komutuyla `$what_you_actually_heard` kelimesini bastırmasını söyledim ve `flag.php` bağımlılığını kaldırdım.

6) Böyle olunca ortaya şu görüntü çıkıyor.

```
blank.php > ...
1 <?php
2
3 if (isset($_GET['magic_word'])) {
4
5     $what_he_said = $_GET['magic_word'];
6     $what_you_dont_want_to_hear = 'bumfuzzle';
7     $what_you_actually_heard = preg_replace(
8         | | | "/$what_you_dont_want_to_hear/", '', $what_he_said);
9
10    if ($what_you_actually_heard === $what_you_dont_want_to_hear) {
11        echo $what_you_actually_heard;
12    }
13 }
14 ?>
15
```

Sonra denemeye başladım ve koyduğum hiçbir şey tam sonuç vermedi sonra bir şey farkettim. Pre\_replace() fonksiyonunu anladığımızda aslında ilk değer pattern yani tespit edilecek değeri temsil ediyor ikincisi ise değiştirilecek ifade burada NULL değer konmuş. Sonuncu parametre ise bizim URL üzerinden verdiğimiz inputu temsil ediyor.

7) Peki tamam da URL üzerinden nasıl php ye input sağlayacağız ?

```
blank.php > ...  
1 <?php  
2  
3 if (isset($_GET['magic_word'])) {  
4  
5     $what_he_said = $_GET['magic_word'];  
6     $what_you_dont_want_to_hear = 'bumfuzzle';  
7     $what_you_actually_heard = preg_replace(  
8         | | | "/$what_you_dont_want_to_hear/", '', $what_he_said);  
9  
10    if ($what_you_actually_heard === $what_you_dont_want_to_hear) {  
11        echo $what_you_actually_heard;  
12    }  
13 }  
14 ?>  
15
```

Bu kısımda PHP arka yüz dilinin bilgisi ölçülüyor ve aslında biz parametrelerle nasıl iletişime geçiyoruz ve form elementlerini işliyoruz ortaya çıkıyor. \$\_GET \$\_POST yaygın kullandığımız global php variablelları ve bu değişkenler kullanıcılardan veriyi çekmeyi ve veriyi işlemeye yarıyorlar. Fazla detaya inmeden gerekli bilgiye bakalım.

8) Sorumuzda inputu vermemiz için istenen \$\_GET parametresi “magic\_word” kelimesi. Tamam da nasıl oluyorda bir veriyi tarayıcı üzerinden php kullanarak çekeceğiz.

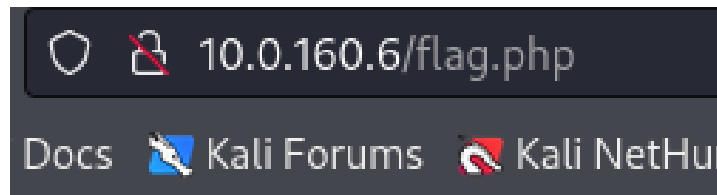
Bu php nin built in kuralı aslında çözümü şu şekilde

[http://10.0.160.6/?\\$\\_GET](http://10.0.160.6/?$_GET) parametremizin değeri

sorudaki parametre ise “magic\_word”. Buraya kadar bilgi kısmını size verdim. Şimdi ise Baştaki php kodunun zorunlu tuttuğu php dizinine bir bakalım.

```
<?php  
require("flag.php");
```

9) Sorumuzun başında belirtilen require() fonksiyonu elimizdeki arka yüz komutunu çalıştırmamıza olanak sağlayan kodun yazıldığı dosyayı belirtiyor. Bu dosyaya erişmek için çok ufak bir dizin hareketiyle ilerliyorum.





- 10) Sayfa bizi bembeyaz bir ekranla karşıladı peki neden zorunlu tuttuğu dosyaya rağmen halen bu noktadayız sorumuzun cevabı php içerisinde aslında.

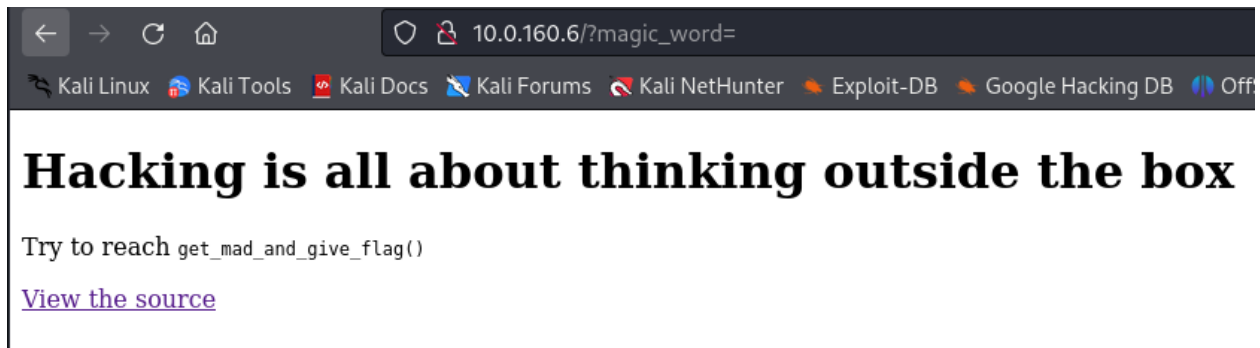
```
if (isset($_GET['magic_word'])) {  
    $what_he_said = $_GET['magic_word'];  
    $what_you_dont_want_to_hear = 'bumfuzzle';  
    $what_you_actually_heard = preg_replace(  
        "/$what_you_dont_want_to_hear/", '', $what_he_said);  
  
    if ($what_you_actually_heard === $what_you_dont_want_to_hear) {  
        get_mad_and_give_flag();  
    }  
}  
?>
```

Hala PHP'ye istediği değişkeni ve değişken değerini göndermedik. Bunu yapmak için ise:



Parametremizi değişken olarak gittiğini tanımlamak için \$\_GET değişkenine soru işareti koyarak gönderiyoruz. Tamam ama halen bir dönüt alamıyorum çünkü değişkene istediği değeri koymadık.(Sonradan farkettim ki hali hazırda PHP flag.php dosyasını zaten import etmiş)

Ardından bu şekilde bir boş sorguda sitenin vereceği tepkiyi merak ettim.



Evet site bizi boş bir panelden ziyade başa döndürdü böylelikle zaten istenilen flag.php dizininin varlığının boş olduğunu farkettim. Bu şekilde denemeye devam ediyorum.

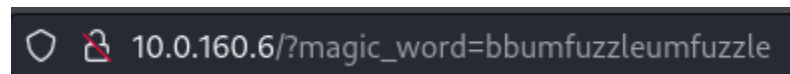
12 ) Değişkenimize istenen değeri koymak için tekrar algoritma analizine başlıyorum.

```
$what_he_said = $_GET['magic_word'];
$what_you_dont_want_to_hear = 'bumfuzzle';
$what_you_actually_heard = preg_replace(
    "/$what_you_dont_want_to_hear/", '', $what_he_said);

if ($what_you_actually_heard === $what_you_dont_want_to_hear) {
    get_mad_and_give_flag();
}
}
```

Buradan anlayacağımız şu olmalıdır. PHP gördüğü ilk bumfuzzle kelimesini harf harf inceleyerek yok ediyor. Aklımda şu geldi peki ya PHP'ye iç içe yazılmış bir string verir sonunu aynen devam ettirsek ne olur dedim.

13) Sonradan dedim ki eğer içeriye şöyle bir parametre sıkıştırırsak ne olur “bbumfuzzleumfuzzle”



Sonuca ulaştık ama dikkat edilmesi gereken nokta şu:

Fonksiyon string yok etme işlemini yaparken şu şekilde bir yol izliyor haydi beraber bir trace edelim.

Önce ilk b harfini alıyor ardından bulabildiği ilk u yu alıyor ardından ise ilk m yi ve bu şekilde gidiyor eğer ki bunların hepsini çıkarırsak şöyle bir sonuç ortaya çıkıyor.



Kırmızıyla belirttiğim harfleri tek tek çıkarınca arada yaklaşık 8 karakterlik bir boşluk kalıyor. Peki ya öyleyse sonuç şu şekilde olmalı “b\*\*\*\*\*umfuzzle”. Hayır, PHP bu işlemi bitirince ardından string concatenation yapıyor ve bir string halinde değişkeni topluyor.

Şimdi vereceğimiz input ile atanmış stringi karşılaştırarak bir if() condition yaratılmış. Bizim verdiğimiz input \$what\_you\_actually\_heard içerisinden çıkıyor. Yani sonuç olarak “bumfuzzle” kelimesini elde ediyoruz. If burada iki stringin eşit olup olmadığını kontrol ettikten sonra get\_mad\_and\_give\_flag() fonksiyonu invoke oluyor.

```
if ($what_you_actually_heard === $what_you_dont_want_to_hear) {  
    get_mad_and_give_flag();  
}
```

Sorumuzun cevabı “bumfuzzle” olarak ortaya çıkıyor. Verdiğimiz input ise herhangi aradaki bir string olabilir “bbumfuzzleumfuzzle” veya “bubumfuzzleumfuzzle” şeklinde.

What did you just say to me?!? ~~What did you just say to me?!?~~