Re：ゼロから始める新世界の渗透勉強

前言

感觉……果然我适合渗透吗……除了社工其它做得还算顺利……

除了内核，渗透也没人问我问题了。果然鹦没人爱啊。

outset

CNSS{Hello_w0rld}

还用说吗……进去之后直接F12，注释里就是flag。

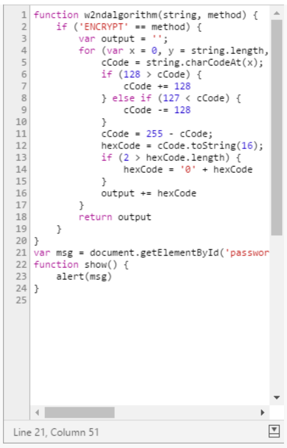
algorithm

CNSS{f1st_st3p_0f_js}

在body的script里发现一段混淆过的js，然而一切混淆在Chrome自带的反混淆面前都是苍白无力的。很简单，新建一个标签，开console粘贴运行一下，因为无法get到ElementById，所以会报错，然后生成这玩意儿。

然后戳一下报错那行VM开头的带下划线的内容，Chrome直接就会生成反混淆后的代码。

当然，如果能小小地format一下就完美了。戳一下左下角那对大括号。



```JavaScript
function w2ndalgorithm(string, method) {
    if ('ENCRYPT' == method) {
        var output = '';
        for (var x = 0, y = string.length, cCode, hexCode; x < y; ++x) {
            cCode = string.charCodeAt(x);
            if (128 > cCode) {
                cCode += 128
            } else if (127 < cCode) {
                cCode -= 128
            }
            cCode = 255 - cCode;
            hexCode = cCode.toString(16);
            if (2 > hexCode.length) {
                hexCode = '0' + hexCode
            }
            output += hexCode
        }
        return output
    }
}
document.getElementById('password').value = w2ndalgorithm(
    '3c312c2c04194e0d0c0b200c0b4c0f204f1920150c02',
    'DECRYPT'
);
```

看看注释，大意是说，w2ndalgorithm第二个method参数只能接受两种字符串，`'ENCRYPT'`和`'DECRYPT'`，不过显然代码中没有`'DECRYPT'`的实现，需要我们将那串长长的字符串逆着来一遍`'ENCRYPT'`，很简单，不详细叙述了。答案算出来就是flag。

UPDATE：后来试了一下，EDGE自带相对Chrome弱一点的反混淆器，但是这段代码是可以反混淆的。

Boss

见果然本弱鶸鰯嶍箣到最后还是没有做出来Boss写个Writeup骗点分.pdf

find

CNSS{ENC0DE_WARS}

一进去就是乱码，然而写过爬虫的我身经百战见识多了（大雾）。页面是utf-8，于是我用python爬了一下，gbk decode了一下，就得到了正常的字符串：“文件名为“扶她奶茶”的URL编码（不要双引号）”。

然而这描述很不详细……我完全不知道文件在哪个目录下，不知道文件名包含不包含后缀，我甚至对这几个字文法分析了半天。

关于二次编码的事情，那是我在某日吃饭的时候突然就想到了，文件名是URL编码，如果我直接发送扶她奶茶的URL编码，服务器那边接收到的还是“扶她奶茶”，所以显然的，需要二次编码，也就是把%也编码了才行。

然后我就懵逼了，那时候大概试过很多后缀名，无后缀、php、html、js、jpg、bmp等等，试过各种前缀，根目录、find、file、filename什么的，以及大小写的url编码我都试过，甚至还去掉过%试过，然而不知道是倒霉还是怎么的，就是没试出来正确答案。

然后有天突然更新了一下提示，说是后缀名是php，小写的url编码……我瞬间就找到了……马上，被重定向至了index.php，然而这又有什么软用呢？我有curl，不执行js。

获取了源代码，答案就出来了。

access

CNSS{HTTP_HEADER_IS_VERY_IMPORTANT}

妈呀这题真的好简单……除了被Cookie坑了好久之外其它的都是秒出……讲真写过爬虫我一点儿也不虚。

看到Only Android and iOS can Access（然后后来改成了WP，害得我又去改了一下UA，还好Chrome内置一堆UA）（结果做完之后发现好像只要UA里有Windows Phone就可以了），我立刻就知道要改UA。第二层是你从哪儿来，于是Referer，乱搞搞出的http://45.78.50.9/access/index.php，算运气好吧。然后提示必须要本地访问……这个我去查了HTTP头，看到了X-Forwarded-For就知道是这个了，不过问题是本地是什么……试了一下45.78.50.9、local然后联想到localhost和127.0.0.1，试了一下过关。

下一关是只允许admin进入……第一直觉POST……好了就不行了。大概POST过username、user、usr、password、passwd之类的组合，没有任何用处。搞着搞着搞了半天注意到了access的题目标签……http header……然后查了一下，先是改了From，设为admin、admin@45.78.50.9，组合POST各种玩，失败。最后抱着试一试的心态去填了Cookie，试过'username=admin;'、'username = admin;'、'user = admin;'和'user=admin;'，突然出现flag的时候……兴奋了好久。