



ob混淆格式化检测存在内存爆破，存在三处内存爆破的地方；

一、定位内存爆破：

□ 第1处内存溢出的位置：

```
var h = function() { h = f ();
var k = new RegExp('\x5cw+\x20*\x5c(\x5c)\x20*(\x5cw+\x20*[\x27|\x22].+[\x27|\x22];?\x20*');
return k['test'](g['removeCookie']()['toString']()); g = {data: {...}, setCookie: f, removeCookie: f, getCookie: f, updateCookie: f}
};
g['updateCookie'] = h; g = {data: {...}, setCookie: f, removeCookie: f, getCookie: f, updateCookie: f}, h = f ()
var i = ''; i = ""
var j = g['updateCookie'](); j = false, g = {data: {...}, setCookie: f, removeCookie: f, getCookie: f, updateCookie: f}
if (!j) {
g['setCookie'](['*'], 'counter', 0x1);
} else if (j) {
i = g['getCookie'](null, 'counter');
} else {
g['removeCookie']();
}
```

```
14      },
15      'setCookie': function(k, l, m, n) { k = ['*'], l = "counter", m = 1, n = {}
16      n = n || {};
17      var o = l + '=' + m;
18      var p = 0x0;
19      for (var q = 0x0, r = k['length']; q < r; q++) {
20          var s = k[q];
21          o += '\x20' + s;
22          var t = k[s];
23          k['push'](t);
24          r = k['length'];
25          if (t !== !![]) {
26              o += '=' + t;
27          }
28      }
29      n['cookie'] = o;
30      },
```

这是一个死循环，会导致页面直接卡死

□ 第2处内存溢出的位置：

```
{function $c(k) { k = undefined
var y = {}; y = {}
y[$b('\x30\x78\x63\x37', '\x21\x46\x77\x37') + '\x69\x74'] = function(Y, Z) {
return Y + Z;
}
;
y[$b('\x30\x78\x64\x30', '\x4e\x41\x33\x5b') + '\x45\x42'] = function(Y, Z) {
return Y & Z;
}
;
y[$b('\x30\x78\x63\x64', '\x67\x23\x6c\x26') + '\x4f\x4b'] = function(Y, Z) {
```

再次进入死循环

```
;
f['prototype']['ZqzWks'] = function(g) {
if (!Boolean(~g)) {
return g;
}
return this['VoeCCy'](this['iZaYAB']);
}
;
f['prototype']['VoeCCy'] = function(g) { g = f (a, b)
for (var h = 0x0, j = this['drtgZu']['length']; h < j; h++) {
this['drtgZu']['push'](Math['round'](Math['random']()));
j = this['drtgZu']['length'];
}
return g(this['drtgZu'][0x0]);
}
;
new f($b)['BXodro']();
$b['SLYmaz'] = !![];
}
```

□ 第3处内存溢出的位置：

```

578         break;
579     }
580 }
581 A[$b('\x30\x78\x38\x65', '\x40\x59\x4b\x68') + '\x50\x44'](setInterval, A['\x77\x4a\x61' + '\x44\x6d'](M), 0x1f4);
582 function N(Y, Z) {
583     Y[A[$b('\x30\x78\x61\x34', '\x29\x31\x59\x32') + '\x53\x7a'](Z, 0x5)] |= A[$b('\x30\x78\x39\x35', '\x23\x32\x69\x6b') + '\x4a\x41'](0x80, A[
584     Y[A[$b('\x30\x78\x31\x30\x39', '\x26\x4a\x36\x4a') + '\x6a\x56'](0xe, A[$b('\x30\x78\x63\x37', '\x68\x79\x69\x30') + '\x4f\x4f'](A['\x77\x6c
585     if (qz) {
586         var a0, a1, a2, a3, a4, a5 = 0x67452301, a6 = -0x10325477, a7 = -0x67452302, a8 = 0x10325476;

function M(Y, Z) {
    var a0 = A['\x46\x68\x59' + '\x77\x45'][$b('\x30\x78\x34\x39', '\x2a\x26\x7a\x50') + '\x69\x74']('\x7c');
    var a1 = 0x0;
    while (![]) {
        switch (a0[a1++]) {
            case '\x30':
                var a2 = A[$b('\x30\x78\x31\x39', '\x29\x35\x72\x25') + '\x6d\x6e'](B, this, function() {
                    var a5 = function() {
                        var a6 = a5[$b('\x30\x78\x61\x39', '\x5e\x73\x72\x71') + '\x73\x74\x72' + $b('\x30\x78\x66\x61', '\x6a\x6b\x69\x4e') + '\x6f\x72']($b(
                        return !a6['\x74\x65\x73' + '\x74']D(a2));
                    };
                    return a4['\x6b\x4f\x48' + '\x59\x71'](a5);
                });
                continue;
            case '\x31':
                A[$b('\x30\x78\x31\x30\x34', '\x4e\x35\x48\x55') + '\x4c\x67'](eval, L(qz));
                continue;
            case '\x32':
                A[$b('\x30\x78\x32\x66', '\x58\x72\x59\x77') + '\x46\x4b'](K);
                continue;
        }
    }
}

```

解决方案：打 script 断点之后 hook RegExp

```

1  RegExp.prototype.test = function(){
2      return true
3  }

```

二、确定加密参数：

抓包工具Fiddler数据重放，发现cookie缺失 m 参数, 请求数据就会失败。

```

1  POST https://www.python-spider.com/api/challenge3 HTTP/1.1
2  Host: www.python-spider.com
3  Content-Type: application/x-www-form-urlencoded; charset=UTF-8
4  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
5  Cookie: sessionid=aq42cy0z4twwx6nd7z5vwpk805dtbkdn;
        m=ef089578918aa25d3a38f3339ea3624d|1699448092000;
6
7  page=1

```

处理方法是hook cookie 的 m 参数, 向上找堆栈找函数入口

```

1  (function () {
2      var cookieVal = '';
3      Object.defineProperty(document, 'cookie', {
4          set: function (val) {
5              if (val.indexOf('m') !== -1) {
6                  debugger;

```

```

7      }
8      console.log('Hook捕获到cookie设置->', val);
9      cookieVal = val;
10     return val;
11   }, get: function () {
12     return cookieVal;
13   },
14   });
15 })());

```

三、找函数入口:

```

}
function W(Y, Z) {
  document[D$b('\x30\x78\x63\x33', '\x36\x4f\x31\x78') + '\x6b\x69\x65'] = A['\x64\x63\x66' + '\x73\x52']D(A[D$b('\x30\x78\x62\x62', '\x32\x52\x59\x40') + '\x5a\x4a']location['\x72\x65\x6c' + $b('\x30\x78\x35\x30', '\x4e\x65\x57\x54')]());
}

```

需要补的环境

```

\x4a\x49']D(M, '\x3d') + A[D$b('\x30\x78\x31\x61', '\x55\x58\x24\x29') + '\x62\x67']D(V, Y) + '\x7c', Y), A[D$b('\x30\x78\x63\x31', '\x40\x41\x77\x64') + '\x41\x4e']];

```

开始抠代码。。。