

看雪.纽盾 KCTF 2019 Q2 | 第五题点评及解题思路

KCTF 看雪学院 6月30日

各位朋友周末快乐！昨日我们公布了本次Q2的比赛成绩，戳：【英雄榜单】看雪.纽盾 KCTF 晋级赛Q2 排行榜出炉！恭喜获奖的选手们！

目前我们正在对赛题进行逐一讲解，比赛期间没有做出来的小伙伴们也不要灰心，请持续关注我们，或许点评与解析会让你茅塞顿开哦！🤔

今天我们将继续对第五题《丛林的秘密》进行题目点评与解析。

题目简介

题目背景：

郁郁葱葱都树林之后，是一只只光亮的眼睛。

外星人的活力集中在亚欧大陆上，位于南美洲的亚马逊森林，此时仿佛是世外桃源。阳光通过高耸的树木，散落下来，洒在满地的落叶上。行走在其中，仿佛进入了一场大型动物博览会，天上飞的、树上爬的、地上走的、水里游的，应有尽有，看的人眼花缭乱。不知不觉走了很远，却仍然困在这个森林中。一不小心，你落入了一个深不见底的深坑中，身体不断的陷入黑暗，下沉、下沉、下沉.....突然一束刺眼的光闪入你的眼睛，那是能量宝石！可是能量宝石在深坑的底部，无论你怎么的向下坠落，似乎都无法到达底部.....

本题共有2057人围观，最终有35支团队攻破成功。

第五题：丛林的秘密

⌛ 已结束



出题战队：F_T

围观人数：2057

开始时间：2019-06-10 12:00:00

攻破人数：35

攻破此题的战队排名一览：

攻破此题的战队				题目名称	第五题：丛林的秘密
排名	战队名	破解时间	获取积分	出题战队	F_T
	 萌新队	8195s	132.17		foyjog
	 GANGE66	19129s	78.66		
	 test2018	32510s	68.95		
4.	 AceHub	32679s	68.88	题目简介	<p>郁郁葱葱都树林之后，是一只只光亮的眼睛。 外星人的活力集中在亚欧大陆上，位于南美洲的亚马逊森林，此时仿佛是世外桃源。阳光通过高耸的树木，散落下来，洒在满地的落叶上。行走其中，仿佛进入了一场大型动物博览会，天上飞的、树上爬的、地上走的、水里游的，应有尽有，看的人眼花缭乱。不知不觉走了很远，却仍然困在这个森林中。一不小心，你落入了一个深不见底的深坑中，身体不断的陷入黑暗，下沉、下沉、下沉.....突然一束刺眼的光闪入你的眼睛，那是能量宝石！可是能量宝石在深坑的底部，无论你如何的向下坠落，似乎都无法到达底部.....</p> <p>注：运行环境为安卓8.1及以上</p> <p>----看雪.纽盾 KCTF晋级赛2019 Q2，看雪CTF竞赛QQ群:8601428，加群请注明论坛用户名。</p>
5.	 pwn_it	43605s	65.42		
6.	 金左手	44174s	65.29		
7.	 SU	89430s	60.12		
8.	 名字都被用啦	94200s	59.86		
9.	 打打酱油	105924s	59.33		
				题目下载	SecretJungle.rar

接下来让我们一起来看看这道题究竟有何玄妙之处吧！

看雪评委crownless点评

这道题的难度初级，主要逻辑在WebAssembly中，只要保存下来用wasm2c反编译成c代码，即可获取flag。

设计思路

本题出题战队 F_T 简介：

F_T

战队信息

战队成员(1)

成员动态



战队名称:

F_T

战队签名:

foyjoig

创建者:

foyjog

战队总分:

900

战队介绍:

foyjog

注册时间:

2018-12-01

加入战队

个人简介: foyog, 付震, 北京邮电大学移动互联网安全技术国家工程实验室研三学生, 曾实习于腾讯移动安全实验室, 主要工作是对安卓内核进行fuzz测试和漏洞分析。现实习于360智能安全研究院,从事自动化漏洞挖掘方向的工作。

赛题分析

参赛的题目是一个安卓的程序, 由于安卓webview在4.4后开始使用chrome的内核, 所以经过测试, 安卓8.1及以上的webview版本是可以成功的执行webassembly的。(低版本没有测, 该题目不能保证在低版本下成功运行)。

故使用webassembly作为出题的依据, 由于无法像桌面版的chrome那样直接动态调试webassembly, 解题者需要讲安卓程序上的html网页转移至桌面版即可动态调试。但由于webassembly的字节码不同于x86, 需要解题者对webassembly的字节码进行研究才能解题。

主要算法

首先html网页如下：

安卓程序中将main.wasm直接作为二进制的字符串放在了html中，但是解题流程不变化。

```
1  <!DOCTYPE html>
2  <html>
3  <head>
4    <meta charset="utf-8">
5    <style>
6      body {
7        background-color: rgb(255, 255, 255);
8      }
9    </style>
10 </head>
11 <script>
12
13
14 var instance;
15
16 fetch('../out/main.wasm').then(response =>
17   response.arrayBuffer()
18 ).then(bytes => WebAssembly.instantiate(bytes)).then(results => {
19   instance = results.instance;
20 }).catch(console.error);
21
22
23 function check_flag(){
24   var value = document.getElementById("key_value").value;
25   instance.exports.set_input_flag_len(value.length);
26   for(var ii=0;ii<value.length;ii++){
27     instance.exports.set_input_flag(value[ii].charCodeAt(),ii);
28   }
29   var ret = instance.exports.check_key();
30
31   if (ret == 1){
32     document.getElementById("tips").innerHTML = "Congratulations!"
33   }
34   else{
35     document.getElementById("tips").innerHTML = "Not Correct!"
36   }
37 }
38 </script>
39 <body>
40   <div>Key:<input id="key_value" type="text" name="key" style="width:80%"; value=""><input type="submit" value="check" onclick
41 k="check_flag()"></div>
42   <div> <label id="tips" ></label></div>
43 </body>
44 </html>
```

html中调用了wasm中的check_flag函数进行验证。

wasm的源码（由于源码过长，请点击阅读原文在原帖下载）

最根本的算法就是一个32*32的线性方程组，函数为xxx（），而o,oo等八个函数只是简单的做了一个异或运算，迷惑解题者。

线性方程组的A和b为：

1	108, 111, 92, 194, 124, 240, 126, 81, 144, 103, 161, 50, 67, 15, 127, 232, 188, 19, 233, 153, 231, 40, 112, 106, 135, 90, 67,
2	20, 248, 45, 48, 174
3	227, 78, 195, 81, 10, 248, 186, 171, 148, 194, 40, 180, 17, 212, 104, 90, 178, 26, 225, 209, 32, 169, 94, 156, 154, 56, 244,
4	149, 120, 131, 13, 101
5	83, 44, 95, 131, 30, 55, 46, 36, 67, 109, 69, 251, 8, 248, 40, 154, 251, 86, 112, 9, 174, 197, 38, 14, 202, 60, 117, 188, 136,
6	145, 240, 53
7	152, 162, 112, 57, 102, 182, 10, 139, 30, 7, 145, 127, 148, 5, 165, 109, 110, 234, 113, 33, 192, 45, 65, 105, 140, 116, 35, 48,
8	155, 25, 234, 25
9	101, 189, 236, 118, 141, 148, 197, 7, 108, 104, 45, 130, 39, 164, 88, 241, 108, 107, 76, 34, 210, 29, 156, 90, 139, 151, 10,
10	97, 209, 46, 82, 113
11	182, 13, 50, 102, 155, 230, 3, 225, 237, 163, 38, 176, 115, 105, 203, 26, 72, 111, 96, 240, 139, 117, 153, 120, 151, 25, 49, 90,
12	98, 7, 179, 72
13	170, 150, 226, 101, 110, 99, 127, 101, 203, 209, 187, 100, 226, 186, 252, 39, 65, 67, 225, 174, 1, 187, 214, 22, 74, 99, 129,
14	254, 13, 97, 156, 61
15	1, 88, 118, 232, 60, 252, 133, 177, 185, 222, 32, 48, 1, 242, 240, 218, 81, 22, 73, 171, 139, 72, 106, 62, 156, 134, 220, 19,
16	77, 94, 154, 117
17	189, 173, 41, 39, 26, 232, 75, 75, 95, 7, 117, 96, 211, 130, 228, 143, 91, 247, 43, 122, 131, 52, 48, 29, 111, 38, 19, 242,
18	162, 70, 220, 151
19	236, 136, 147, 104, 79, 204, 220, 25, 38, 233, 165, 20, 174, 120, 214, 18, 233, 119, 244, 143, 126, 226, 77, 33, 189, 5, 150,
20	160, 14, 112, 231, 92
21	191, 38, 193, 250, 212, 175, 39, 94, 183, 172, 171, 163, 129, 165, 64, 170, 199, 2, 167, 2, 216, 252, 184, 187, 97, 109, 98,
22	135, 192, 88, 50, 203
23	203, 81, 252, 104, 248, 156, 199, 46, 208, 240, 149, 155, 102, 95, 51, 208, 208, 62, 58, 117, 72, 23, 193, 193, 226, 217, 106,
24	147, 136, 16, 43, 196
25	144, 69, 224, 107, 225, 83, 15, 10, 214, 152, 24, 136, 165, 208, 38, 67, 201, 180, 158, 75, 111, 65, 211, 220, 135, 125, 216,
26	105, 122, 112, 80, 49
27	143, 68, 127, 51, 152, 88, 153, 9, 149, 107, 178, 166, 190, 177, 99, 71, 63, 233, 58, 132, 109, 75, 152, 95, 74, 195, 90, 251,
28	205, 8, 76, 129
29	209, 146, 59, 38, 40, 56, 182, 245, 67, 202, 177, 183, 26, 126, 161, 95, 133, 123, 163, 30, 88, 219, 5, 86, 183, 156, 253, 97,
30	43, 128, 31, 102
31	146, 223, 137, 228, 226, 155, 170, 92, 77, 17, 22, 128, 20, 171, 142, 170, 192, 49, 200, 178, 154, 42, 5, 159, 251, 152, 7,
32	247, 145, 39, 91, 136
	169, 204, 244, 26, 77, 134, 221, 205, 149, 47, 1, 197, 82, 195, 123, 219, 116, 80, 13, 231, 173, 192, 220, 224, 108, 104, 56,
	152, 84, 226, 121, 205
	184, 45, 176, 126, 118, 161, 142, 171, 215, 83, 233, 184, 171, 182, 126, 111, 118, 67, 92, 219, 70, 252, 194, 21, 245, 204, 48,
	150, 39, 85, 73, 95
	48, 224, 164, 138, 92, 3, 191, 94, 19, 50, 34, 167, 75, 72, 238, 15, 111, 216, 84, 40, 145, 112, 140, 204, 154, 195, 175, 250,
	202, 169, 170, 120
	112, 19, 189, 50, 247, 240, 164, 5, 139, 56, 19, 4, 23, 172, 96, 254, 63, 247, 149, 183, 128, 147, 213, 243, 172, 144, 246, 25,
	106, 176, 170, 68
	184, 22, 183, 128, 149, 174, 227, 113, 65, 159, 74, 170, 186, 174, 211, 1, 223, 156, 253, 223, 241, 252, 148, 93, 41, 125, 27,
	136, 78, 248, 41, 31
	155, 237, 242, 10, 145, 99, 239, 105, 3, 43, 46, 155, 208, 75, 140, 181, 197, 140, 10, 170, 142, 212, 186, 27, 105, 118, 198,
	243, 13, 113, 82, 39
	207, 206, 127, 58, 91, 87, 7, 17, 63, 180, 40, 96, 202, 185, 68, 72, 240, 36, 139, 199, 76, 229, 159, 136, 94, 19, 3, 87, 45,
	6, 136, 50
	115, 215, 40, 166, 87, 83, 74, 202, 235, 149, 114, 76, 204, 218, 63, 123, 9, 172, 38, 138, 35, 200, 221, 144, 235, 108, 1, 245,
	153, 184, 90, 12
	123, 190, 55, 180, 84, 231, 81, 116, 61, 3, 94, 85, 190, 187, 142, 62, 225, 240, 179, 150, 77, 85, 196, 12, 144, 122, 28, 224,
	248, 143, 114, 36
	2, 202, 40, 224, 154, 65, 30, 241, 13, 213, 176, 122, 30, 158, 14, 191, 80, 116, 74, 70, 32, 189, 76, 95, 158, 103, 7, 201,
	204, 91, 190, 122
	42, 154, 223, 165, 155, 101, 75, 95, 253, 14, 158, 193, 110, 89, 205, 202, 83, 162, 67, 30, 115, 83, 27, 31, 118, 160, 248, 66,
	88, 44, 5, 176
	34, 168, 72, 160, 243, 41, 146, 29, 62, 235, 185, 180, 10, 150, 208, 140, 125, 114, 35, 34, 38, 123, 163, 208, 5, 29, 207, 111,
	72, 65, 125, 84
	18, 11, 26, 175, 44, 128, 32, 100, 21, 116, 253, 213, 67, 16, 171, 178, 97, 7, 162, 152, 78, 167, 177, 97, 26, 155, 127, 21,
	243, 188, 140, 197
	140, 110, 164, 208, 72, 113, 9, 47, 179, 166, 51, 34, 91, 184, 89, 162, 233, 127, 156, 127, 244, 183, 193, 138, 242, 90, 193,
	7, 252, 113, 152, 7
	133, 105, 75, 146, 173, 27, 97, 142, 164, 15, 10, 177, 239, 141, 189, 67, 153, 108, 206, 210, 171, 252, 84, 249, 7, 168, 100,
	30, 196, 244, 197, 75
	147, 221, 57, 186, 69, 230, 167, 3, 220, 63, 218, 235, 156, 146, 75, 198, 204, 197, 59, 61, 179, 47, 221, 127, 210, 218, 241,
	135, 196, 185, 53, 79

b:

```
1 359512
2 387514
3 301487
4 296549
5 344514
6 346892
7 386678
8 348667
9 316884
10 372620
11 413102
12 428661
13 371484
14 350848
15 334408
16 382822
17 420160
18 402263
19 366968
20 384909
21 425203
22 372162
23 297509
24 372215
25 370337
26 314564
27 325974
28 307088
29 322340
30 380716
31 393331
32 430295
```

解题者需要利用脚本文件去读取这些参数并求解。解为：

S0m3time_l1tt1e_c0de_1s_us3ful33

而由于o、oo等八个函数只是做异或运算，可以得到flag为：

K9nXu3_2o1q2_w3bassembly_r3vers3

安卓程序

只有一个activity，其中最主要的是一个webview，通过loadurl(127.0.0.1:8000)来解析html。

但是程序中还写了一个textview，一个button和一个edittext来迷惑解题者。

主要代码：

```
1  @Override
2  protected void onCreate(Bundle savedInstanceState) {
3      super.onCreate(savedInstanceState);
4      setContentView(R.layout.activity_main);
5      editText1 = findViewById(R.id.editText);
6      textView1 = findViewById(R.id.textView);
7      ((WebView) findViewById(R.id.text1View)).loadUrl(u);
8      ((WebView) findViewById(R.id.text1View)).getSettings().setJavaScriptEnabled(true);
9      button1 = findViewById(R.id.button);
10     button1.setOnClickListener(new View.OnClickListener() {
11         @Override
12         public void onClick(View v) {
13             String key = editText1.getText().toString();
14             int ret = check_key(key);
15             if(ret == 1){
16                 textView1.setText("Congratulations!");
17             }
18             else{
19                 textView1.setText("Not Correct!");
20             }
21         }
22     });
23 }
24
25 }
```

native的函数主要工作为，实现一个简单的http服务器，内容为上面的wasm代码。

代码请见文末左下角阅读原文。

解题思路

本题解题思路由看雪论坛 **风间仁** 提供：


发消息

风间仁

专家 ★★★

精华数：19

RANK：1150

雪币：16309

商城

浏览人数：591

在线时长：🌞🌙🌟🌟🌟

注册时间：2006-02-24

最近活跃：3小时前



这个是Web页面，url: <http://127.0.0.1:8000>。

```
public class MainActivity extends AppCompatActivity {
    private Button button1;
    private EditText editText1;
```

```

private TextView txView1;
public String url;

static {
    System.loadLibrary("gogogo");
}

public MainActivity() {
    this.url = gogogoJNI.sayHello();
}

protected void onCreate(Bundle arg3) {
    ...
    this.findViewById(2131165318).loadUrl(this.url);
    this.findViewById(2131165318).getSettings().setJavaScriptEnabled(true);
    ...
}

jstring __fastcall Java_com_example_assemgogogo_gogogoJNI_sayHello(JNIEnv *a1)
{
    // http://127.0.0.1:8000
    for ( i = 0; i != 21; ++i )
        url[i] = byte_2D28[i] ^ 0x66;
    url[21] = 0;
    return (*v2)->NewStringUTF(v2, url);
}

```

在JNI_OnLoad中监听8000端口，发送html页面。

.text:00000D1A	ADD	R1, PC ; "8
...		
.text:00000D26	BLX	getaddrinfo
...		
.text:00000C50	ADD	R0, PC ; "H
...		
.text:00000C60	BLX	accept
...		
.text:00000CA6	BLX	send

html页面：


```

<html>
<script>
var instance;

WebAssembly.compile(new Uint8Array(`
...
`.trim().split(/\s\r\n]+/g).map(str => parseInt(str, 16))
)).then(module => {
  new WebAssembly.instantiate(module).then(results => {
    instance = results;
  }).catch(console.error);})
function check_flag() {
  var value = document.getElementById("key_value").value;
  if(value.length != 32)
  {
    document.getElementById("tips").innerHTML = "Not Correct!";
    return;
  }
  instance.exports.set_input_flag_len(value.length);
  for(var ii=0;ii<value.length;ii++){
    instance.exports.set_input_flag(value[ii].charCodeAt(),ii);
  }
  var ret = instance.exports.check_key();

  if (ret == 1){
    document.getElementById("tips").innerHTML = "Congratulations!"
  }
  else{
    document.getElementById("tips").innerHTML = "Not Correct!"
  }
}
</script>
<body>
  <div>Key: <input id="key_value" type="text" name="key" style="width:60%" ;="" val

</body></html>

```

主要逻辑在WebAssembly中，保存下来用wasm2c反编译成c代码：

<https://github.com/WebAssembly/wabt>

```
./wasm2c test.wasm -o test.c
```

将代码抠出来，z3解得sn：K9nXu3_2o1q2_w3bassembly_r3vers3。



[1、看雪.纽盾 KCTF 2019 Q2 | 第一题点评及解题思路](#)

[2、看雪.纽盾 KCTF 2019 Q2 | 第三题点评及解题思路](#)

[3、看雪.纽盾 KCTF 2019 Q2 | 第二题点评及解题思路](#)

[4、看雪.纽盾 KCTF 2019 Q2 | 第四题点评及解题思路](#)

[5、【英雄榜单】看雪.纽盾 KCTF 晋级赛Q2 排行榜出炉！](#)

主办方



看雪学院 (www.kanxue.com) 是一个专注于PC、移动、智能设备安全研究及逆向工程的开发者社区！创建于2000年，历经19年的发展，受到业内的广泛认同，在行业中树立了令人尊敬的专业形象。平台为会员提供安全知识的在线课程教学，同时为企业提供智能设备安全相关产品和服务。

合作伙伴



上海纽盾科技股份有限公司 (www.newdon.net) 成立于2009年，是一家以“网络安全”为主轴，以“科技源自生活，纽盾服务社会”为核心经营理念，以网络安全产品的研发、生产、销售、售后服务与相关安全服务为一体的专业安全公司，致力于为数字化时代背景下的用户提供安全产品、安全服务以及等级保护等安全解决方案。




👉 小手一戳，了解更多



公众号ID: ikanxue

官方微博: 看雪安全

商务合作: wsc@kanxue.com

 戳原文，查看更多精彩writeup!

阅读原文