知道创宇404实验室丨“老坛酸菜鱼”队长Hcamael：我着迷于计算机给我带来的未知

原创

知道创宇KCSC 于 2019-08-26 09:47:23 发布 787 收藏

文章标签： 网络安全 网络安全公司 CTF

在网络安全行业内，知道创宇一直被朋友们赞誉为“网络安全特种兵”。这背后，除了知道创宇拥有众多业内领先的安全技术外，更重要的一个原因是，知道创宇拥有一个业内最强大的技术研究团队——404实验室。

黑哥这样介绍自己的团队：

> “知道创宇404实验室，是国内黑客文化深厚的网络安全公司知道创宇最神秘和最核心的部门……” “404每个成员都很优秀，都是精英。”

黑哥口中的精英是什么样的人？这群人是怎样为404实验室打造出这样耀眼的光环的？

接下来，我们将会用一段时间，走进知道创宇这个最神秘的部门，深度追踪404实验室各个成员身上的闪光点，探寻这群人身上发生的故事，揭开知道创宇404实验室的神秘面纱。

今天故事的主角叫Hcamael，404内部的小伙伴们都称他为队长。

5月下旬，404实验室收到了第二届“强网”拟态防御国际精英挑战赛的邀请，主办方在南京摆下了擂台，请来了位列2019年CTFTIME全球排名第一的乌克兰Dcua战队，2019年CTFTIME全球排名第二的俄罗斯LC↯BC战队，2019年CTFTIME全球排名第八的美国Shellphish战队，以及日本TokyoWesterns战队，波兰p4战队、韩国CyKor战队、伊朗ASIS战队、德国Hxp战队等多支国际顶级CTF战队，堪称国际豪强压境。

国内方面，来自清华、浙大、中科院、北邮、上海交大、电子科技大等高校，以及腾讯、阿里、百度、三六零等企业的强队也将一同赴赛，一场CTF竞赛圈内的诸神之战将在南京打响。

主办方说，有名的战队这次我们都邀请来了，你们知道创宇要不也拉支队伍来“练练”？

不出其然，404实验室一口应了下来，而这个重任也毫无意外的落在了Hcamael的头上。

经过商议，404实验室决定让Hcamael带领另外3名成员（分别是LoRexxar 、w7ay、0x7F）组成“老坛酸菜鱼”战队前往南京迎战。

经历两天的激烈比拼，知道创宇“老坛酸菜鱼”战队不负众望，捧回了第二名的大奖。

再继续讲完这次比赛中发生的跌宕故事前，我们先认识一下Hcamael其人。

喜欢钻研电脑的舅舅在Hcamael心里种下了梦想的种子

比起身边其他在网吧自学成才的朋友们，Hcamael是个幸运的孩子，起码从没有为买台电脑发愁过。小学一年级的时候父母就因为工作需要，就买回家了一台电脑。家里这个新来的事物一下子就引起了Hcamael强烈的兴趣，甚至兴趣程度迅速超过了那台小霸王游戏机。

到二年级的时候，父母工作变得更忙了，在照顾Hcamael这件事情上难免分身乏术，于是父母就把他送回了老家，让姥姥来照顾。

来到姥姥家后，Hcamael没法再像以前一样能天天接触到计算机了。

但是他有一个舅舅在县城里开了一家书店，而且舅舅也对计算机兴趣十足，闲下来的时候自学了很多计算机知识，平时没事儿的时候就自己鼓捣鼓捣计算机，偶尔朋友的电脑出点小状况，一些软硬件方面的小问题都是舅舅帮忙解决的。并且在全家都认为Hcamael要好好学习，怕他沉迷在游戏里的时候，也只有舅舅没有打压他的兴趣，认为适当的娱乐是可以的。

大学之前，Hcamael一直生活在姥姥家，经常一放学就偷偷溜到舅舅的店里，当电脑没在使用时，就能玩会游戏，有时候也在一旁看着舅舅捣鼓电脑，就这样，Hcamael逐渐积累起了一些简单的计算机基础知识。

初中时还曾发生了一个小插曲，Hcamael偶然读到了一本名为《网络骑士》的小说，书里面编织了一个主人公在虚拟的赛博世界中载酒而行，弹三尺青峰快意恩仇，笑看天下群雄的故事。

早已经爱上计算机的Hcamael，恍然间看到了一个新的世界，惩奸除恶，肆意仗剑江湖，这也太酷了吧？舅舅潜移默化的影响和小说中描绘的世界，在Hcamael心里埋下了一颗种子，很快这颗种子会生根发芽，并长成参天大树。

从九又四分之三站出发，一头扎入赛博世界

高中毕业后，Hcamael考入了杭州电子科技大学，学习通信工程专业。

进入大学之后，课程安排不多，有大把的时间可以挥霍。闲下来的Hcamael就跑去问班助，有没有什么黑客技术相关的协会可以报名参加？

Hcamael从班助那里了解到，此时杭州电子科技大学的信息安全专业已经成立了好几个年头，恰好信息安全专业挂在通信工程学院下面（现在已经独立成信息安全学院了），学校信息安全协会也一起挂在了通信工程学院下。院里有兴趣的同学都可以自由参加，协会里平时定期组织一些技术交流活动，他们经常去全国各地打CTF竞赛，甚至还有出国打比赛。但是社团招新要过段日子才会开始，可以等社团招新的时候报名加入。

没过多久，学校社团招新开始了。

在学院社团宣讲会的时候，信息安全协会的会长何少（ID：H·Shao）讲了一句话让站在台下的Hcamael热血沸腾，并且至今还记忆犹新：大学四年，你是想上大学，还是想被大学上？早已对协会万分憧憬的Hcamael没有再犹豫，直接报名加入了协会。

随后两天，在学校组织的大学生国家奖学金评选活动中，Hcamael又一次遇到了会长何少，但这一次他是站在台上参选。前面上去评选的很多学长说的几乎都是大同小异，成绩，奖学金，大学期间在图书馆待了多久，获得过各种校级，市级奖项等等。除了知道他们是学霸外，也没什么别的感觉。

会长何少是倒数第二个出场的，他上来的第一句话就是：“听了前面很多同学都是获过很多校级市级或者是省级奖之类的，这些我都没获得过。我获得的都是全国级和全球级比赛的奖项。”之后一一列举了他获得的比赛奖项，当时Hcamael心想，这也太牛逼了，前面的学长们都是渣渣啊。

最后一位出场的是信息安全协会上一届的会长华哥，他上去宣讲的内容也和别人不一样，“我是去年国家奖学金的获得者，今年也没兴趣来和学弟学妹们再争这个名额，我只是上来给我的学弟何少拉票的”。最后毫无疑问，会长何少获得了国家奖学金一等奖。也正是因为这件事，更加坚定了Hcamael“赖上”协会的决心。

就像哈利波特从九又四分之三站台一头撞进魔法世界中一样，此刻Hcamael也幸运的找到了进入赛博世界的入口。

崭露头角 绽放光芒

大一的时候协会经常会举办一些对新生的培训，协会培训在Hcamael心里是优先级最高的事，每一场协会的培训Hcamael都赶去参加。许多学长的培训至今还影响着Hcamael，一个学长安利了Linux的操作系统，让Hcamael开始接触了除Windows以外的操作系统，至今工作开发都是习惯使用Linux。而另一个学长安利了写blog的好处，也让Hcamael养成了有研究成果就会写blog的习惯。

大一期间Hcamael自学了C语言，计网+CCNA，也学会了装Linux操作系统。也和同届的同学一起组队参加了人数生第一场CTF竞赛——2013年的HCTF，但是Hcamael的第一场CTF竞赛因为连签到题都没做出来，就草草收场了。

真正的快速进阶是在大二的时候，大二后Hcamael在协会中投入了更多的精力和时间，只要有时间就去听学长们的赛题讲解。在协会内部组织的CTF竞赛中，Hcamael开始慢慢的会根据随着题目放出的一些资料学习解题，期间还自学了Python 和Web开发的全家桶（前端html/css/js，后端php，运维），从这里开始进入web安全世界的大门。

大二时，一些实力强的学长们有的毕业了，有的忙着考研，协会二进制选手出现了断层，整个大二协会基本都是打打线上赛，没打进过线下赛。因为协会二进制选手的短缺,大三寒假的时候Hcamael开始自学汇编，从这时起，他才发现二进制才是他真正想学的东西。

当问起为什么下定决心学习二进制时，Hcamael回答到：“大三的时候我已经不是对黑客一无所知的菜鸟了，大众所知的黑客基本都是来源于小说获电影，各种神奇的操作靠的更多是社会工程学，大一的时候看完《欺骗的艺术》和《入侵的艺术》后，反而大大降低了我对黑客的热情，发现这并不是我心目中期待的黑客，并且我对社工的热情也不是很大。

之后搞web安全，也发现做题入侵到了服务器中后，只在第一次的时候有成就感，再往后也觉得十分无趣。现在想起来，其实从小能给我带来心理上满足的是求知的过程，我着迷于计算机给我带来的未知，我想知道计算机每个部分是怎么运作的，从头到尾的了解清楚。

学了汇编后，汇编向我揭开了二进制世界的一角，越学下去心中的疑问越多，也更加的渴望了解它，这也是我长久以来的学习动力。所以大三寒假，马上要开始找实习的时间，我决定从Web狗转到了二进制。这也是为什么我之后找工作一直都是安全研究而不是渗透测试。”

随着Hcamael实力一天天强大起来，协会也有了一些实力很强的新人加入，协会的整体实力再次壮大了。到大四时，协会的HDUISA战队又能偶尔打进线下赛了， Hcamael也在赛场上释放出了他的光芒，他强大的实力被其他战队看在了眼里，这其中就包括Hcamael的下一个战队：Nu1L多校联合战队。

偶然收获Nu1L抛来的橄榄枝

大四的时候，在一次比赛交流中，Hcamael被国内十分有名气的Nu1L多校联合战队看中，前来询问是否愿意加入Nu1L战队。

正巧，Hcamael也有此意向，因为临近毕业，Hcamael自己觉得不适合再以协会的名义出去打比赛了，因为要留给学弟们锻炼的机会，这样协会才能代代相传，生生不息，但是Hcamael并不想完全离开CTF赛场。

当时的Nu1L多校联合战队正处于扩张期，队员已经从最早期的4名初创成员壮大到了接近20名队员，并且Nu1L不归属于任何企业、高校和个人，没有严格的管理制度和章程，每一名成员都拥有自己的专长，凭借对技术的热诚凝聚到一起。

这样一支战队简直正中Hcamael下怀，Hcamael当即同意了加入Nu1L的大家庭。

代表Nu1L出战的最知名的一场比赛，就是去年的2018 BCTF。在两天的比赛里，Hcamael和团队里其他的二进制选手默契配合，为战队拿下了大量比分，力压群雄，和Nu1L的队友一起捧回了冠军的奖杯和31万元的大奖。

接下来我们再回到开头的那个故事里。

在第二届“强网”拟态防御国际精英挑战赛中，主办方创新性的将拟态防御理论融入竞赛模式中，竞赛中选手们需要对拟态路由器、拟态域名服务器、拟态web服务器、拟态防火墙、拟态文件存储服务、借鉴拟态思想的web虚拟主机六款拟态产品构建的真实网络环境中进行渗透测试。赛制上则是采取“黑盒与白盒对比测试、外部突破与注入先后挑战”的规则，为拟态防御进行全方位、高强度的“众测”安全检验。

这样比赛一共分为：拟态黑盒赛，拟态白盒赛和白盒排位赛，白盒排位赛可以看成是一般CTF线上赛的解题模式。

“拟态白盒”挑战赛，其实是主办方将提供特定拟态防御设备的API接口或后门利用途径，参赛战队可以通过API接口或后门获得某一执行体的控制权，用于协助战队突破拟态设备。

而“拟态黑盒”挑战赛，顾名思义，主办方不给出任何提示或限制条件，参赛选手要在短暂的比赛时间内自己寻找产品漏洞，并破解得分。通常条件下，在CTF竞赛中“黑盒”意味着不可能完成的挑战，仅可远观而不可亵玩焉。

另外，本次竞赛还高度模拟真实的关键信息基础设施网络环境，这里隐藏了一条没有充分说明的规则：即在答题过程中，只要干扰服务的正常进行，造成服务的紊乱即为得分。

这条隐藏规则，成了老坛酸菜鱼战队最终错失冠军的罪魁祸首。

老坛酸菜鱼战队有一个成员LoRexxar有去年参加拟态赛的经验，根据去年经验来讲，拟态黑盒的题目基本是无解的，或者说，在有限的时间内（两天）是无解的。所以他们采用的策略是主攻白盒排位赛，拟态白盒赛第一个选个最难的，当弃子了（一不小心还选到了第一轮第一组）。直到我们第一轮的拟态白盒赛结束，才知道扰动得分这个规则，并不需要做出来，只要影响一个执行体正常运行就能得分。

当老坛酸菜鱼战队突然反应过来时，拟态白盒赛第一轮的分已丢，已经被其他战队拉开了很大的分值差距。所幸，他们在白盒排位赛上拿下了一道Web题和一道Pwn题的三血，有资格参加第二轮的拟态白盒赛。直到一天比赛结束，老坛酸菜鱼战队在白盒排位赛上还剩2道逆向题没做出来，这个时候已经有好几个战队ak了白盒排位赛。在拟态白盒赛上，虽然在下午晚上的轮次中都得分了，但是第一轮丢分的设备已经做出来的人少，是分值最高的。

如果没有什么意外的话，这场比赛老坛酸菜鱼战队是真的很难“咸鱼翻身”了。

这次比赛包括Hcamael在内，老坛酸菜鱼战队一共派出了4名队员，其中Hcamael和0x7F是二进制选手，LoRexxar和w7ay则是web选手。但是在白盒排位赛中，6道赛题中却仅有2道web题，也就意味着web选手做完自己的题后就没有事情做了。

但是拟态白盒挑战赛又是轮流进行的，只能等到自己的轮次才能尝试破解。Hcamael心想，既然拟态“黑盒”是唯一的机会，不如让他们试试研究拟态黑盒题目？

Hcamael当下决定调整思路，自己和另一名二进制选手继续攻克白盒排位赛，缩小和其他人的差距，两名web选手就直接挑战拟态黑盒题目,争取找到逆风翻盘的机会。

到第一天比赛结束，白盒排位赛老坛酸菜鱼战队还剩下2道逆向的题目没做出来。一道是逆向bind9（Linux上的DNS服务端程序）；另一道涉及了Windows内核调试。由于两名二进制选手以前都没搞过windows的内核调试，回到酒店后，他们决定一个人继续逆向bind9，另一个则开始现学windows内核逆向，折腾到第二天天亮，才解决掉这两道题。

逆风翻盘 却又与冠军失之交臂

第二天上午开赛后不久，场内突然爆发出一阵惊呼。原来比赛大屏显示，老坛酸菜鱼战队的队员LoRexxar成功在拟态防火墙设备中通过黑盒测试造成执行体扰动，率先打破黑盒测试赛排行榜零分，无人尝试解题的尴尬局面，一举拿到10500分，排名一下子从十名之外上升至第一名。

所有战队惊呆了，这怎么可能？

实际上，这是一个意外情况，连老坛酸菜鱼战队自己也没想到。

原来，在第一天比赛的夜晚LoRexxar已经对这道题取得了突破性进展，按照大家的规划，第二天继续尝试攻克这道题，但攻克后暂时“捂住”，直到比赛的关键时刻，再抛出这个杀手锏。

但出人预料的是，由于竞赛模式的隐藏规则是，造成执行体扰动，干扰服务的正常进行即可获得比分。而竞赛服务器此时监测到了老坛酸菜鱼战队的行为，并判定为破解成功。

所以， Hcamael跟队员们一起晕掉了。

接下来的结果显然大家可以预料的到。

现场所有战队均瞄准了被老坛酸菜鱼战队得分的拟态黑盒题目，进行“集火”攻击，然而直到中午仍未有队伍再次在黑盒测试中得分。

在所有人都认为老坛酸菜鱼战队将最终夺冠时，在黑盒测试即将结束的13:40分左右，来自福州大学的ROIS战队准确找出了拟态防火墙设备执行体中的同样漏洞进行攻击，并造成裁决器扰动报警，获得黑盒测试得分。ROIS凭借其在拟态白盒赛中的比分优势，超越老坛酸菜鱼战队，位列常规赛排行榜第一名，比赛结束了。

把时间往后倒推至比赛开始之前，如果能早点摸清规则的话，老坛酸菜鱼战队不会在白盒测试的那几个轮次中落后太多；如果老坛酸菜鱼战队晚8分钟再继续尝试黑盒测试的话，无论ROIS实力如何强大，有限的时间内也来不及获得黑盒测试得分。

但是这世上从来都没有如果，没有假如也没有早知道。我们只是又一次错失冠军而已，但是我相信，下一次，冠军一定是我们，Hcamael肯定的说。

除了是一名强大的CTF选手，Hcamael还有另外一面

除了攻防技术方面的研究外，在404实验室中Hcamael还主要负责二进制方面的技术研究，以及Web、IoT、智能合约等领域内的安全研究。在KCon 2018黑客大会上，Hcamael还登上演讲台，为参会者们分享了自己的研究成果《从OPCODE看以太坊智能合约安全》，获得了各界的关注。

每次全球范围内重大安全事件、高危漏洞爆发时，每次快速的组织起漏洞跟踪研究，Hcamael也在其中扮演着重要角色，做出了突出贡献。

而404实验室也正是将这些年轻人集聚到一起，将他们的安全能力形成一股合力，为保护国家和民众的网络安全奉献着力量。

下面是一些有趣的问答彩蛋分享给大家：

1、你在CTF圈子里面大概是什么段位？

属于中游水平吧，因为见过很多厉害的大佬，协会也接触了很多厉害的学长，所以有自知之明，并不觉得自己很厉害。

或者这么想，比你厉害的人里还有：比你聪明跟你一样努力的，比你聪明还比你努力的，比你聪明还比你努力还有女朋友的，还可以加上学的比你久的，这么一想，顿时觉得自己菜爆了。

而这些并不是我YY出来的，在曾经的HCTF线下赛的时候，就有一个大佬一个人带着女朋友来比赛，然后拿了第一。还有我作为主办方的2014HCTF线下赛，浙大和复旦的两人联队，吊打其他四人队伍。听说去年第一届“强网”线下赛的时候也有一个大神，自己一个人吊打全场，最后关头才被浙大eee反超，相当于一战封神了。

比起他们来比起他们我还只是一个小学生，还有太多太多的技能需要点亮。这是从仰望大佬的角度来看，从自身的角度呢，自己的TODOLIST有一堆需要学习的知识点，并且做题的速度是一个非常大的短板，打了这么久的比赛，基本没抢到过一血。

2、平时还有带大家出去打什么比赛吗？

个人的话可能有时候Nu1L队里缺人手的时候去凑个热闹，404实验室的小伙伴的话，还是很少一起出去打比赛的。很多比赛现在都是线上预选赛加线下赛的模式，会比较耗费时间和精力，所以除了邀请参加线下赛外，基本上很少一起参赛。

还有一个很重要的原因嘛，现在很多比赛都是在周末，搬了一星期砖，好不容易周末了，不在家睡觉还去打什么比赛啊。

3、你还想当那个在网络世界中肆意翱翔的黑客吗？

当黑客只是年少轻狂时候的幻想，当了解这个行业以后，我发现我还是更喜欢当一个安全研究员，去学习了解让我着迷的计算机。

4、怎么看待CTF竞赛和工作的关系？

辩证的看吧。很多人觉得CTF跟工作没关系，我觉得只是他们没想到联系。CTF中和工作中关联最大的要属逆向题吧，考的都是自身的基本功，你做逆向的题目牛逼，平常在工作中逆向分析漏洞也一样牛逼。还有CTF的各种做题工具也能在分析漏洞中用到。就算是没联系，但是很有趣的赛题，碰到一些自己没接触过的知识点，也能算是知识扫盲了。而且做CTF题的过程就想以前做数学题一样，每一次解出难题的那种感觉，会让人着迷，也能够得到极大的放松，在某些程度上也会缓解工作上的压力。

5、需要个人出去参赛的时候，黑哥和隋刚会放人吗？

黑哥平时不怎么限制大家，会给大家充分的自由。刚哥人也很好的，从来不干涉我自己出去打比赛的安排，不过本身我已经很少出去打比赛了，只是队里缺人的时候去参加。

其实在工作中刚哥也特别照顾大家的情绪，我们每个人都有自己擅长的领域嘛，在工作的时候他很尊重我们的个人意愿给我分配一些二进制方面的研究工作，就会感觉在这里得到了极大的自由，有充分的空间让我们自由发挥，这也是我选择404实验室的原因。

欢迎关注我和专栏，我将定期搬运技术文章～

也欢迎访问我们：知道创宇云安全 https://www.yunaq.com/?from=CSDN90826

如果你想与我成为朋友，欢迎加微信kcsc818~~