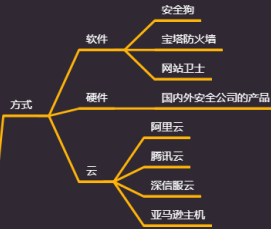


WAF 攻防-菜刀&冰蝎&哥斯拉&流量通讯&特征绕过&检测反制&感知

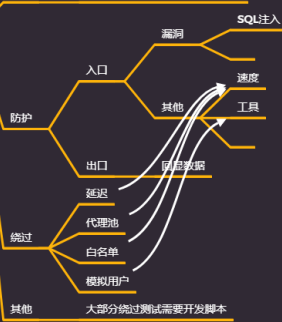


② 基本概念

Web Application Firewall (web应用防火墙), 一种公认的说法是“web应用防火墙通过执行一系列针对HTTP/HTTPS的安全策略来专门为web应用提供保护的一款产品。”



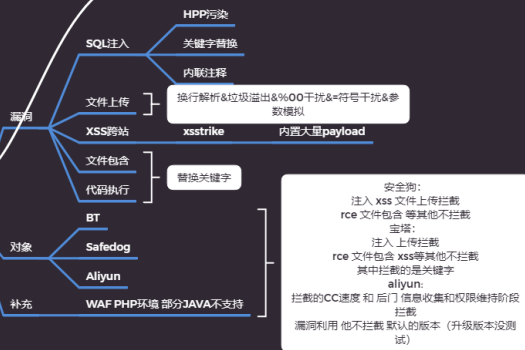
① 信息收集



② 漏洞发现



③ 漏洞利用



④ 权限维持



加密流程：

AntSword：

requests	response
base64等方式	明文

冰蝎2.0：

requests	response
开启Openssl扩展-动态密钥aes加密	aes加密+base64
未开启Openssl扩展-异或	异或+base64

冰蝎3.0：

requests	response
开启Openssl扩展-静态密钥aes加密	aes加密+base64
未开启Openssl扩展-异或	异或+base64

哥斯拉：

requests	response
php的为base64+异或+base64	异或+base64+脏字符
jsp的为Base64+AES	aes+base64+脏字符

#知识点:

- 1、菜刀-流量&通讯&检测&绕过
- 2、冰蝎-流量&通讯&检测&绕过
- 3、哥斯拉-流量&通讯&检测&绕过

代码块&传参数据&工具指纹等(表面&行为)

- 1、代码表面层免杀-ASP&PHP&JSP&ASPX 等
- 2、工具行为层免杀-菜刀&蚁剑&冰蝎&哥斯拉等

#章节点:

WAF 绕过主要集中在信息收集, 漏洞发现, 漏洞利用, 权限控制四个阶段。

#补充点:

- 1、什么是 WAF?

Web Application Firewall (web 应用防火墙), 一种公认的说法是“web 应用防火墙通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 web 应用提供保护的一款产品。

基本可以分为以下 4 种

软件型 WAF

以软件的形式安装在服务器上面, 可以接触到服务器上的文件, 因此就可以检测服务器上是否有 webserv, 是否有文件被创建等。

硬件型 WAF

以硬件形式部署在链路中, 支持多种部署方式。当串联到链路上时可以拦截恶意流量, 在旁路监听模式时只记录攻击但是不进行拦截。

云 WAF

一般以反向代理的形式工作, 通过配置后, 使对网站的请求数据优先经过 WAF 主机, 在 WAF 主机对数据进行过滤后再传给服务器

网站内置的 WAF

就是来自网站内部的过滤, 直接出现在网站代码中, 比如说对输入的参数强制类转换啊, 对输入的参数进行敏感词检测啊什么的

- 2、如何判断 WAF?

Wafw00f, 看图识别, 其他项目脚本平台

https://mp.weixin.qq.com/s/3uUZKryCufQ_HcuMc8ZgQQ

- 3、常见 WAF 拓扑&防护?

网上图流量走向, 常见漏洞

演示案例：

- 菜刀-流量&绕过&特征&检测
 - 冰蝎-流量&绕过&特征&检测
 - 哥斯拉-流量&绕过&特征&检测
-
-

#菜刀-流量&绕过&特征&检测

1、版本

2014 \$_POST=\$_REQUEST 2016 可以

2、特征:

数据包流量特征:

1, 请求包中: ua 头为百度爬虫

2, 请求体中存在 eval, base64 等特征字符

3, 请求体中传递的 payload 为 base64 编码, 并且存在固定的

```
QGLuaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwuMCIpO0BzZXRfdGltZV9saW1pdCgwK
TtpZihQSFBfVkvSU0lPTjwnNS4zLjAnKXtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW
1lKDAP0307ZWNoBygiWEBZIik7J
```

#冰蝎-流量&绕过&特征&检测

0、介绍

冰蝎利用了服务器端的脚本语言加密功能, 通讯的过程中,

消息体内容采用 AES 加密, 基于特征值检测的安全产品无法查出。

1、通讯

以代码 Key 为密钥的 AES 加密解密过程

2、

特征:

0、User-agent: 代码中定义

1、Pragma: no-cache

2、Content-Type: application/x-www-form-urlencoded

3、Accept:

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
```

4、Accept-Encoding: gzip, deflate, br

5、Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7

#哥斯拉-流量&绕过&特征&检测

1、通讯加密见图

2、特征:

1、User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0)
Gecko/20100101 Firefox/84.0

2、Accept:

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
*/*;q=0.8
```

3、Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](#)
