渗透测试工程师技术实战课

常见waf技术的绕过

WAF简介及主要功能介绍

- WAF是Web Application Firewall的简称，也就是WEB应用防护系统，主要有以下功能：
  - 审计
  - WEB应用加固
- 分类
  - 云waf
  - 主机防护软件
  - 硬件ips/ids防护、硬件waf

WAF的过滤机制

- 增强的输入验证
- 白名单&黑名单机制
- 基于规则和基于异常的保护
- 另外还有会话保护、Cookies保护、抗入侵规避技术、响应监视和信息泄露保护等。

WAF绕过方法实战

- WAF身份认证阶段的绕过
  - 伪造搜索引擎
  - 伪造白名单特殊目录
  - 直接攻击源站
  - 请求方式绕过

WAF绕过方法实战

- WAF数据包解析阶段的绕过
  - 编码绕过
  - 请求方式绕过
  - 复参数绕过
- WAF触发规则的绕过
  - 特殊字符替换
  - 注释包含关键字

常见绕过WAF方法总结

- 基本/简单绕过方法
  - 注释符
  - 使用大小写
  - 双写替换
  - 内联注释
- 高级绕过方法
  - 缓冲区溢出/使防火墙崩溃
  - 对字母进行编码
  - 使用其他变量或者命令对注入语句进行替换
  - 利用WAF本身的功能绕过

谢谢观赏