KCon

智能WEB安全攻击系统

迟程
深信服创新研究院

+1 进阶，
护航未来

KCon

+1

CONTENTS

目录

KCon

+1

讲者简介

Some decorative little English，Some decorative little English

KCon

+1

迟程

博士毕业于中国科学院大学，主要研究方向为AI算法在计算机视觉中的应用，获评中国电子教育学会优秀博士论文。

发表论文10余篇，包括TPAMI、TIP、NeurIPS、ICML、CVPR、AAAI等顶会和顶刊，Google Scholar被引1000余次，并担任AI领域多个顶会和顶刊审稿人。在CVPR 2020曾获Best Paper提名奖，曾获博士后基金面上资助。

目前在深信服带领团队致力于探索AI算法在网络安全中的应用，多个项目获得公司和研发体系的技术大奖。

KCon

+1

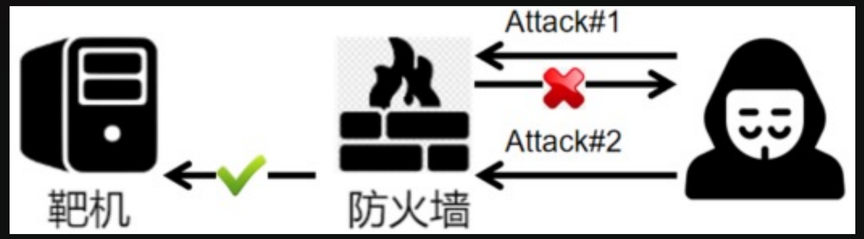
要解决的问题

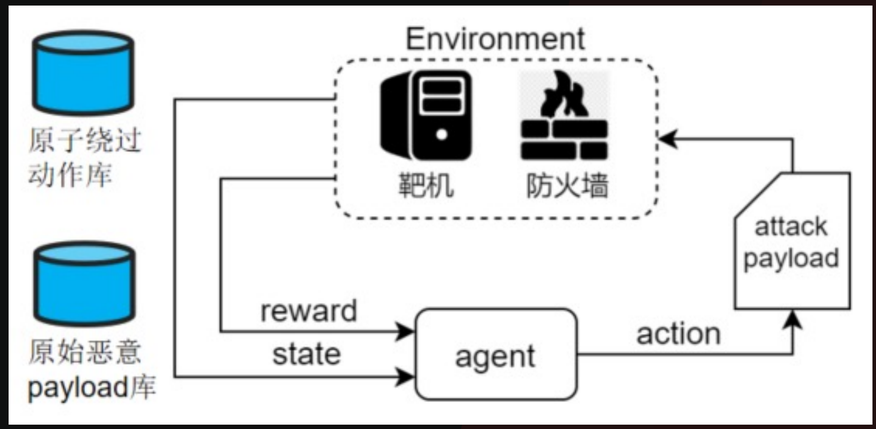
Some decorative little English，Some decorative little English

要解决的问题

渗透测试项目中，攻击队遇到WAF防护时，依赖安全专家经验绕过，并且随着防护技术的迭代，绕过成本越来越高，另一方面渗透专家人数无法随着客户数量线性增加

WAF检测引擎在版本迭代过程中，需要消耗大量人力物力进行安全能力评估

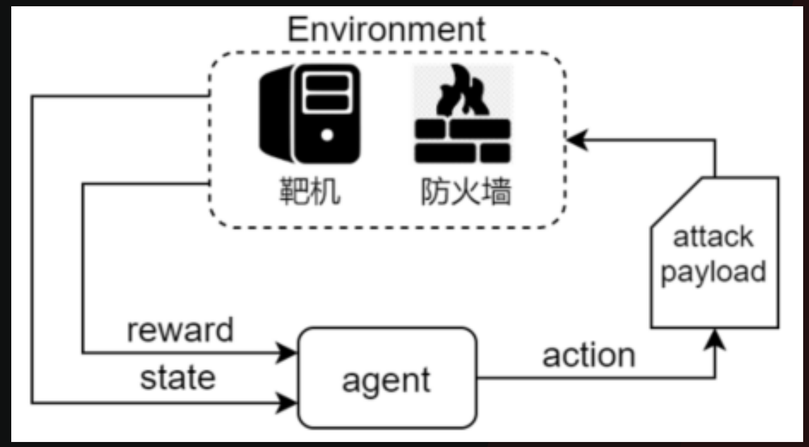




举个例子

①OR FALSE
②OR 替换为 ||
③= 替换为LIKE

1 UNION SELECT 1, version()



1 UNION SELECT 1, version()

1 OR 8916 = 8917 OR 7641 = 7642 UNION SELECT 1, version()

1 || 8916 = 8917 || 7641 = 7642 UNION SELECT 1, version()

1 || 8916 LIKE 8917 || 7641 LIKE 7642 UNION SELECT 1, version()

MySQL

Oracle

通过简单原子绕过动作组合，发现复杂绕过模式（MySQL和Oracle语法差异）

KCon

+1

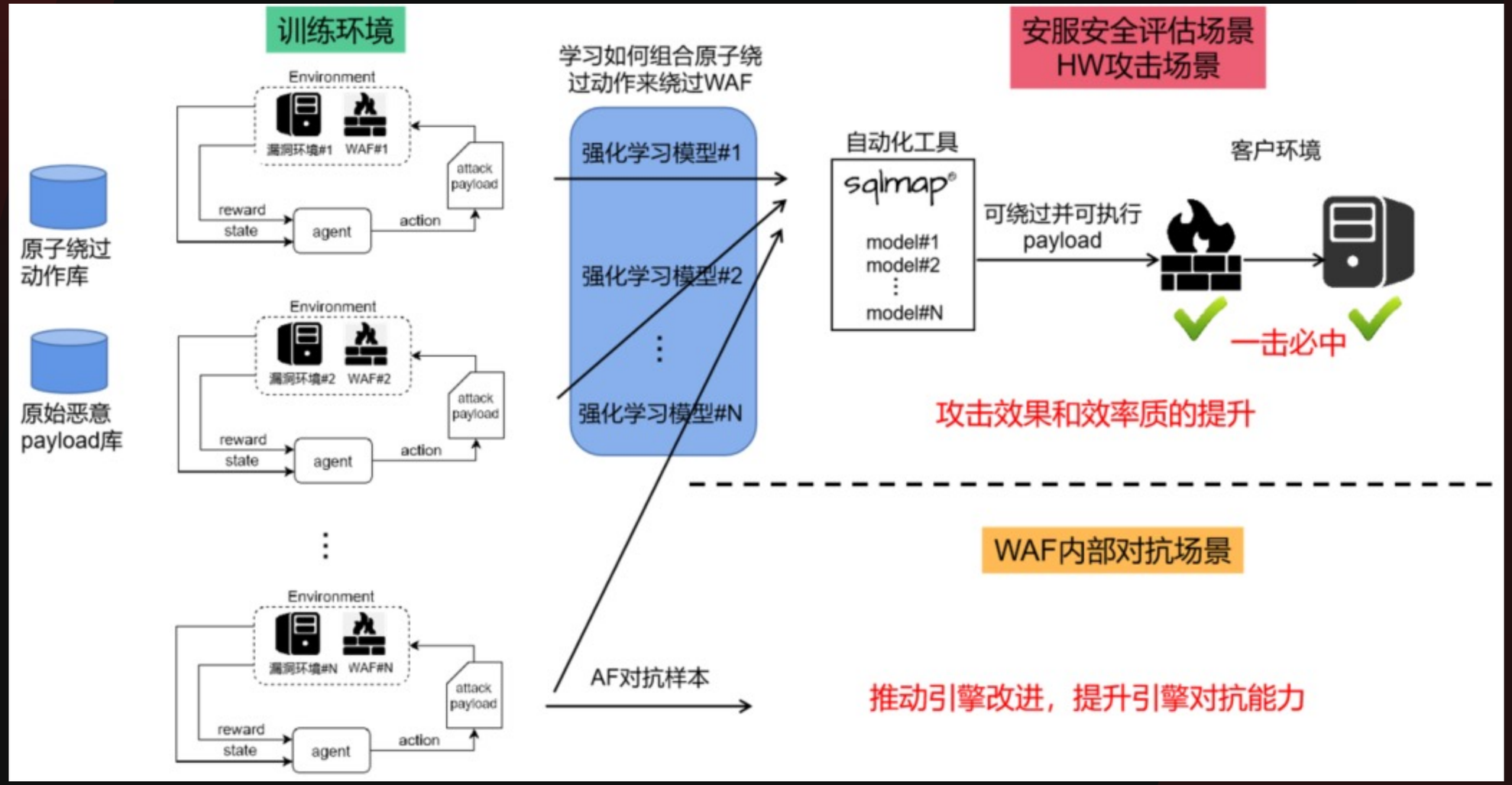
项目难点

Some decorative little English，Some decorative little English

KCon

+1

① 如何在实战场景中应用？



KCon

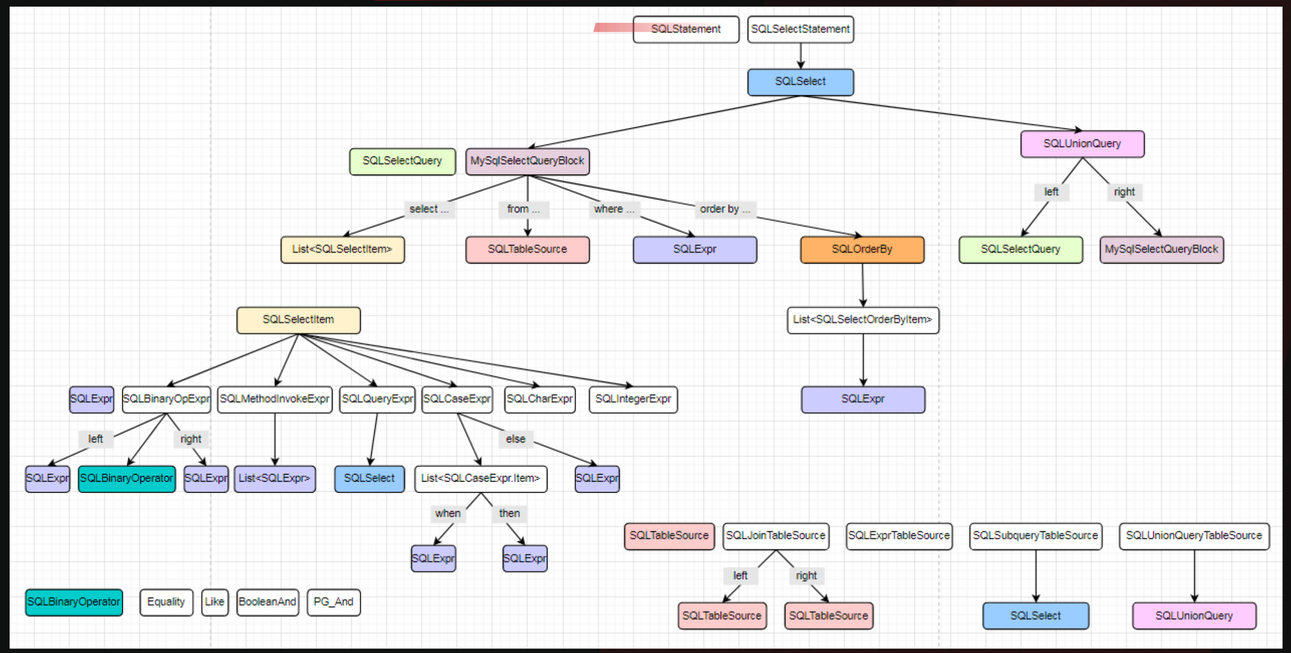
+1

② 如何保证攻击成功率？

传统web fuzz方法会改变payload语义，会导致**变异后payload可以绕过WAF，但不能执行攻击**

我们提出**基于语法和词法解析的变异方法**，首先把payload解析成词法token序列和语法树，在token序列和语法树上进行变异，保持payload的**语义不变性**

我们在**reward设计**上既考虑是否可以绕过WAF，同时也考虑了变异后payload能否在靶机上正确执行攻击



KCon

+1

实验结果

Some decorative little English，Some decorative little English

KCon

+1

内部对抗

黑盒对抗

生成2W+可绕过并能执行的对抗样本，其中提取绕过模式14种，推动完成检测引擎的修复

白盒对抗

利用WISE引擎更多的反馈信息，驱使强化学习智能体发现更多的绕过模式，共发现绕过模式18种

KCon

+1

渗透测试

友商（长亭、FortiWeb、腾讯）绕过成功率100%，功能集成到SQLmap工具中，已在数十家客户验证一键注入效果，并获得客户感谢信

KCon

+1

感谢您的观看

THANK YOU FOR YOUR WATCHING

KCon 2022 黑客大会