Web应用靶场建设方案研究

Research on Construction Scheme of Web Application Shooting Range

刘　安,徐　雷,郭新海,王　戈,蓝鑫冲(中国联通研究院,北京 100048)
Liu An,Xu Lei,Guo Xinhai,Wang Ge,Lan Xinchong(China Unicom Research Institute,Beijing 100048,China)

摘　要:
随着数字化进程的推进,Web应用软件在各行各业中得到了广泛应用,其安全性也越发重要。网络靶场是支撑网络安全战略建设的重要基础设施,Web应用靶场建设对Web应用安全有着深远的影响。分析了Web应用安全防护中的痛点以及靶场建设的必要性,提出了具有培训、竞赛、仿真、检测和能力开放等功能的一体化Web应用靶场建设方案。该方案可用于人才培养、人才选拔、漏洞复现、漏洞研究、开放共享共建等Web应用安全场景,有效提高了Web应用的安全性。

关键词:
Web应用;靶场;安全防护
doi:10.12045/j.issn.1007-3043.2025.08.012
文章编号:1007-3043(2025)08-0058-06
中图分类号:TN915
文献标识码:A
开放科学(资源服务)标识码(OSID):

Abstract:
With the advancement of digitalization, Web application softwares are widely used in various industries, and its security is becoming increasingly important. The network shooting range is an important infrastructure supporting the construction of network security strategies, and the construction of Web application shooting ranges has a profound impact on Web application security. It analyzes the pain points in Web application security protection and the necessity of target range construction, proposes an integrated Web application target range construction scheme with functions such as training, competition, simulation, detection, and capability opening, which can be used in Web application security scenarios such as talent cultivation, talent selection, vulnerability replication, leak research, and open sharing co-construction, which effectively improves the security of Web applications.

Keywords:
Web applications;Shooting range;Safety protection

引用格式:刘安,徐雷,郭新海,等. Web应用靶场建设方案研究[J]. 邮电设计技术,2025(8):58-63.

1 背景介绍

随着互联网的发展,Web应用已经成为了各行各业中必不可少的组成部分,商务、社交、教育、金融、政府等领域都离不开Web应用。尤其是Web2.0时代的到来,给人们的生活带来巨大的便利,但也带来了诸多安全风险。每天,大量的Web攻击充斥着整个网络,随之而来的隐私泄露、非法控制、服务中断、恶意软件传播、网络欺诈等安全事件频发[1-2]。核弹级漏洞Log4j、Spring4Shell远程代码执行、ThinkPHP命令执行等影响比较大的漏洞不断爆出,有效解决Web应用安全问题已刻不容缓[1-3]。

网络靶场是支撑网络空间安全技术验证、网络武器装备试验、攻防对抗演练和网络风险评估等的重要基础设施,各国都在加快布局靶场建设,在建设规模、呈现形态和承载力等方面都取得了新的突破[4-6]。Web应用靶场是网络靶场的重要组成部分,它能够从不同维度解决Web应用安全问题,对Web应用安全有

收稿日期:2025-06-26

着深远的影响[7]。从目前网络靶场建设情况来看，Web应用靶场只是作为网络靶场的一小部分存在，尚未建设体系化的Web应用靶场，不能完全满足Web应用安全的需求。随着Web应用安全重要性与日俱增，Web应用安全人员培养、Web应用安全研究、Web应用安全开发、Web应用安全运维等需求日益迫切。因此，建设体系化的Web应用靶场具有十分重要的意义[8-9]。

2 Web应用安全防护中的痛点

Web应用面向众多用户提供不同功能的服务，而且功能越多的应用被用户访问到的Web应用接口也就越多，这些都导致了风险暴露面增加。同时，供应链安全、开源组件安全、框架安全等问题都使得Web应用成为网络攻击的重灾区。Web应用安全防护中的痛点主要有以下几种。

a）开发人员知识欠缺。Web应用的开发人员一般缺乏安全知识，以功能实现为导向的开发模式容易让他们忽略安全因素。在互联网功能快速迭代的今天，开发人员无暇顾及代码的安全性，会从源头处引入缺陷代码，这些缺陷代码在后期的安全测试以及安全防护中，往往很难被发现或者被拦截，从而造成比较严重的安全事件。

b）安全人才缺失。安全人才的培养一直是备受关注的话题，目前许多高校都设立了网络空间安全一级学科，但是未来几年网络安全人才的需求规模仍旧很大[10]。对于众多的互联网企业，专业的Web应用安全人员仍存在缺口，快速培养出理论与实战经验兼备的Web应用安全人才成为难点[11]。

c）安全管理经验不足。网络安全管理人员由于缺乏实战经验、安全技能不足等原因，在Web应用安全运维中往往很难发现管理中的漏洞，或者在Web应用出现安全事件时，缺乏有效的应急响应计划和处理机制，从而引发Web应用安全事件[12]。因此，增加实战经验、提升安全技能、快速响应突发攻击等需求不断增加。

d）安全检测不全面。Web应用安全防护需要从Web应用全生命周期角度考虑安全问题，开发、构建、测试、运行等每个周期节点都要进行安全检测与防护，代码安全、开源组件安全、应用漏洞、框架漏洞、安全运营等方面都需要周全考虑，否则一点击破满盘皆输[13]。目前很多企业很难做到对应用的全生命周期进行全面检测与防护，导致从多个周期节点引入了安全隐患。

e）新的攻击手段隐蔽性强。目前人工智能、大数据等新技术不断发展和应用落地，新的攻击手段层出不穷，传统的安全防护设备很难对这些隐蔽性强的攻击进行检测和防御，需要新的防护手段和工具来应对新的攻击。新的防护手段需要在实验环境下不断改进和创新，且需要多方合作共同完成，所以亟需创建研究平台来进行安全研究与探讨[14]。

3 整体建设方案

以Web应用防护中的痛点为出发点，构建体系化的针对Web应用安全的靶场。该靶场依托于底层基础设施和丰富的网络安全相关资源，形成人才培养、攻防演练、安全检测、漏洞复现和验证、能力开放五大安全能力，满足Web应用安全中不同的需求。在人才培养方面，通过体系化的理论和实践课程进行Web应用安全人才队伍建设；在攻防演练方面，利用竞赛和实战训练增强相关人员的实践经验；在安全检测方面，形成了对应用全生命周期的安全检测与防护能力；在漏洞复现与验证方面，构建了常见的Web应用环境，对快速复现0day和1day漏洞、验证安全防护方法、增加应急响应速度等具有重要意义；在能力开放方面，不仅将靶场能力对外输出，还能够提供Web应用安全研讨和共建共享的平台，汇集业内力量共同提升Web应用安全能力水平。Web应用安全靶场建设方案如图1所示。

4 Web应用靶场主要功能设计

4.1 Web应用安全人才培养

Web应用安全人员需要对Web应用相关知识有深入的理解和认识，能够借助工具发现Web应用中的安全漏洞并解决安全问题，同时要持续学习和巩固所学技能。在构建人才培养体系时，通过理论学习、漏洞复现、教学管理、实战训练为一体的人才培养体系，全方位地培养高质量的Web应用安全人员。

4.1.1 Web应用漏洞实战环境建设方案

以OWASPTOP 10大类漏洞为基础，根据安全经验与频发的漏洞对这些大类漏洞进行了细分类。除此之外，还增加了一些常见的高危漏洞。由于Python、PHP和JAVA是Web应用开发中常用的编程语言，表1根据不同的语言场景设计了不同的漏洞。

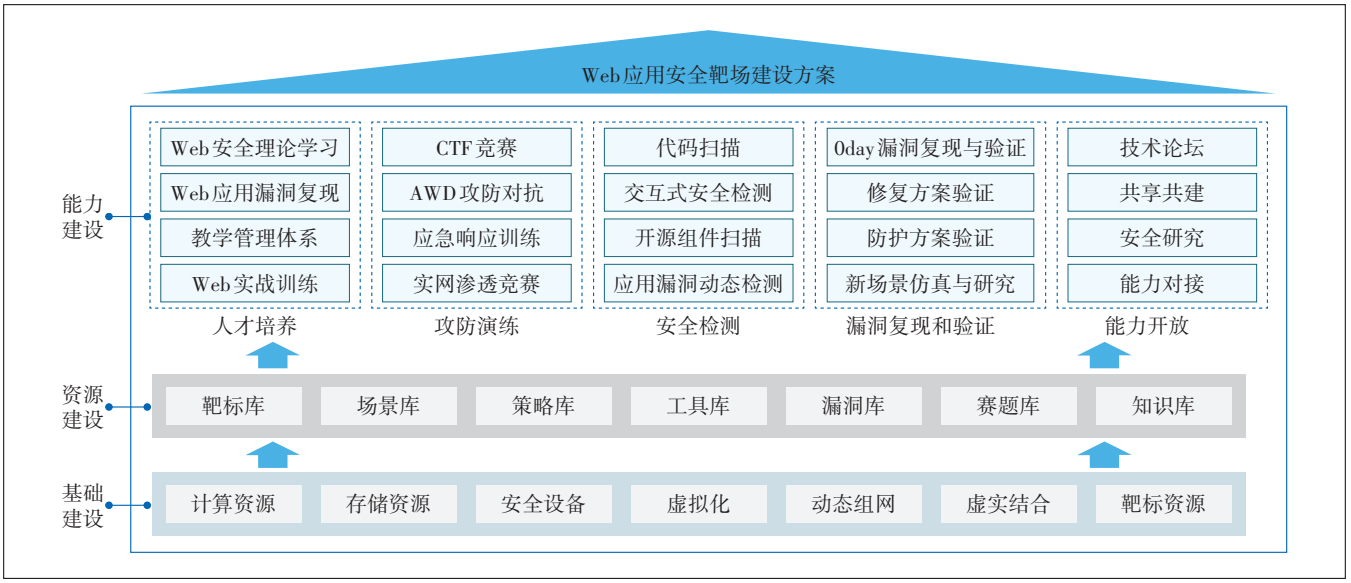

图1　Web应用安全靶场建设方案

表1　Python、PHP和JAVA语言下Web应用漏洞

漏洞类别		JAVA	PYTHON	PHP
OWASP TOP10	失效的访问控制	访问控制不当、授权机制不恰当、控制密钥绕过授权机制		
	加密失败	根目录下敏感数据、加密问题、敏感数据明文存储、不充分的加密强度、侵犯隐私、硬编码、弱口令		
	注入	SQL注入、OS注入、表达式注入、模板注入、NoSQL注入、HQL注入、LDAP注入、邮件注入(SMTP)、XPATH注入、XML外部实体(XXE)		
	不安全设计	不安全设计		
	安全配置错误	Tomcat任意文件写入	Django CSRF	Nginx配置错误
		Tomcat AJP文件包含	Flask SSRF	PHP信息泄露
		Spring Boot远程命令执行	–	–
	使用含有已知漏洞的组件	Weblogic组件	PyYAML	WordPress
		富文本编辑器	Jinja2	Joomla
		FastJson	Requests	PHPMailer
		log4j	–	–
	失效的身份认证	认证机制不恰当、会话固定、跨站请求伪造CSRF		
	不安全的反序列化	Apache Commons Collections反序列化漏洞	pickle反序列化漏洞	不安全反序列化
		FastJson反序列化漏洞	PyYAML反序列化漏洞	–
	不足的日志和监控	CRLF日志注入		
		未记录可审计性事件		
	服务端请求伪造	服务端请求伪造		
其他	跨站脚本攻击	反射型XSS、存储型XSS、DOM型XSS		
	文件操作	任意文件上传、路径遍历、文件包含漏洞		
	条件竞争	条件竞争		
	资源管理错误	前端配置不当、不受控的资源消耗、HTTPS会话中的敏感cookie没有设置安全属性、拒绝服务攻击		
	处理逻辑错误	异常处理		
		–	–	NULL指针引用
	输入确定不当	未检查的输入作为循环条件、URL访问控制不严格、URL跳转		
	Web后门	Web后门		
	点击劫持漏洞	点击劫持漏洞		
	HTTP参数污染	HTTP参数污染		

4.1.2 教学培训方案

首先根据学员的不同基础创建不同的学习计划，让学员通过教学视频进行循序渐进的学习。同时，增加实践环节，引导学员通过使用常见渗透工具对Web应用漏洞环境中的漏洞进行挖掘，然后通过植入木马、注入攻击命令等手段进行漏洞利用。最后是漏洞修复环节，学员可以根据所学知识进行代码修复，也可以调用安全函数库SDK以及参照安全编码规范进行漏洞修复，之后对修复效果进行验证。整个过程如图2所示。

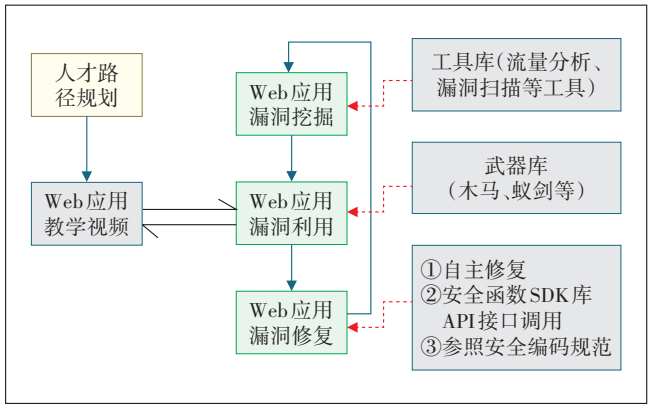

图2　教学培训方案

4.2 Web应用环境仿真

通过虚拟化和云技术，对大规模复杂网络进行仿真，实现对主机、网络、安全设备、应用、场景等的仿真以及Web应用实物接入。可以自定义网络拓扑结构，利用虚实结合的方式模拟实际业务环境全要素[15]，有机整合各元素，构建多类型、多场景的攻防模式。选手可以登录操作机进行内网渗透，穿过网络设备和安全防护设备，发现Web应用系统中的漏洞。能够举办CTF夺旗赛、AWD对抗赛以及内网渗透赛和领地赛等多模式的比赛，从不同维度考察选手的Web应用安全相关技能。也可以根据防护方案搭建模拟环境，验证防护方案的有效性，对实体Web应用进行包围测试、新工具检验等。仿真环境建设方案如图3所示。

4.3 Web应用安全漏洞复现与修复

不同语言开发的Web应用，其开发和运行环境也不相同，开发工具、应用框架、前端环境、应用代理、数据库等一整套环境的搭建会耗费大量的时间，因此，基础环境的准备是Web应用靶场搭建过程中的重要环节，需要搭建的Web应用环境如表2所示。

0day漏洞的出现往往会使所有基于既有经验的安全防护设备失效。当漏洞爆出后，基于靶场基础环境，能够快速复现漏洞并进行漏洞修复，漏洞修复既可以是代码级的修复，也可以是增加防护策略，并及时验证修复方案的有效性，尽可能减少漏洞带来的损失。对于1day和nday的漏洞复现和修复也具有重要的现实意义。整个过程如图4所示。

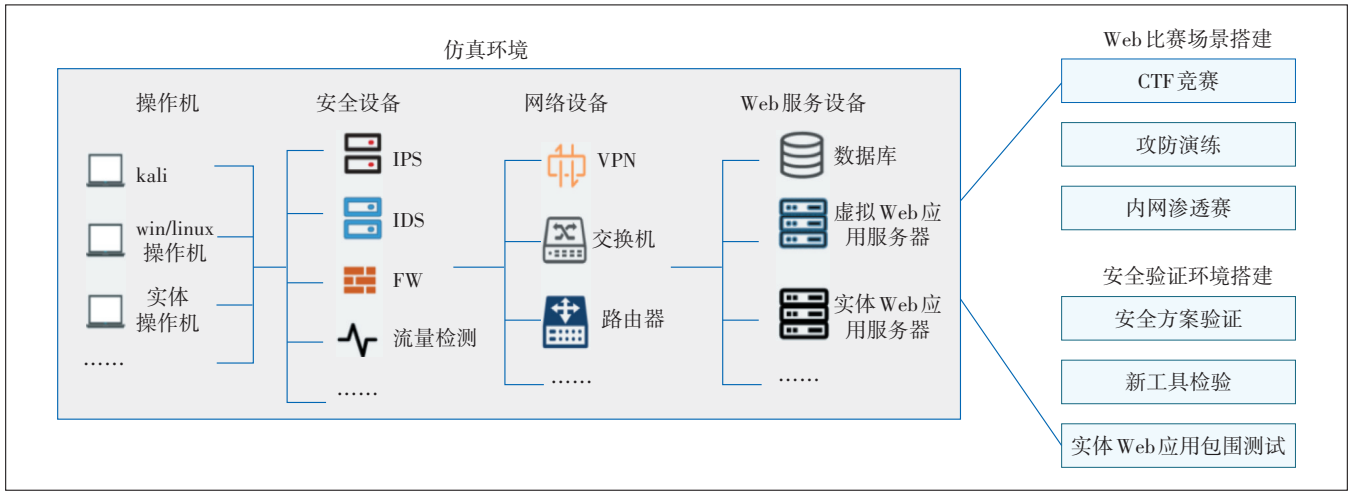

图3　Web应用环境仿真建设方案

4.4 Web应用安全检测

安全检测不仅针对Web应用本身，还需要检测Web应用的安全防护能力。对Web应用自身的安全检测应覆盖Web应用的全生命周期，包括编码、构建、测试、运行等阶段，在不同的阶段，需要建设相应的能力来进行漏洞检测和应用防护，整个Web应用全生命周期的防护方案如图5所示。

表2　Web应用环境搭建配置

程序运行环境	JDK、Python、Go、PHP等
容器/编排工具	Docker、docker-compose等
代码管理	Git、Gitlab、SVN等
数据库	MySQL、MongoDB、Redis等
代理服务器	Nginx等
前端环境	NodeJS等
Web应用服务器	Tomcat、Weblogic、Jboss、Apache、IIS等
Web应用框架	Django、Flask、Laravel、SpringMVC、Spring等
开发工具	VS Code、IDEA、Sublime Text、PhpStorm等

Web应用的安全防护能力建设需要借助入侵与攻击模拟技术来实现。首先，通过扫描网络资产，识别可能存在的漏洞和风险点。然后，根据所识别的风险，制定各种自动化攻击脚本以模拟黑客行为，进而测试系统的防御能力。最后，分析攻击结果，找出防御的薄弱环节并进行改进。整个方案采用以攻促防的理念，从实战攻防角度自动化验证安全措施的有效性，并结合全链路进行评估。在网络边界、终端系统和内网环境等场景中部署攻击靶机，通过攻击探针对不同场景内的靶机发起攻击，以检验Web系统防御的有效性。Web应用安全防护能力检测方案如图6所示。

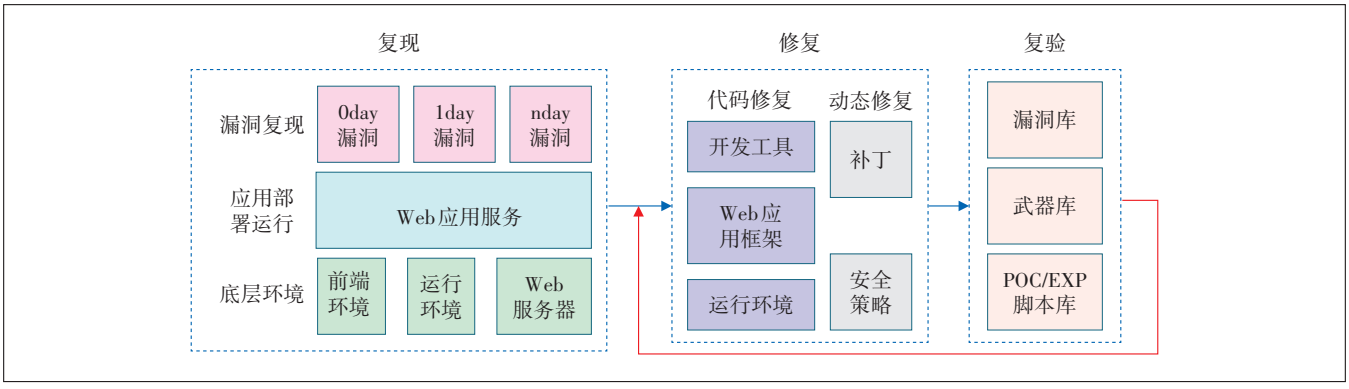

图4　漏洞复现与修复方案

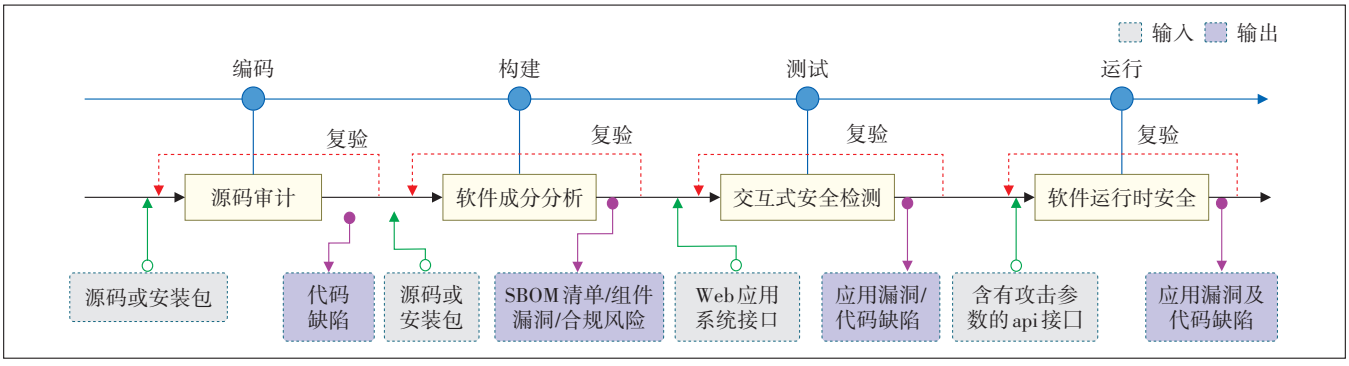

图5　Web应用全生命周期安全检测方案

4.5 Web应用靶场能力开放

Web应用安全防护是一个长期而艰巨的任务，暴露面广、攻击手法多样、供应链复杂等一系列问题需要业界共同研究解决。靶场需要建设开放性平台进行安全研究和开放共享，具体建设方案如图7所示。

5 结束语

没有网络安全就没有国家安全，网络战具有成本低、效果显著、范围广等特点，已成为影响战局走向和大国间博弈的重要因素。Web应用作为网络攻击者的重要入侵对象，需要予以重点关注和防护。网络靶场是网络安全战略建设的重要基础设施，当前各国都在加快推进新型靶场的建设。本文针对Web应用安全防护的痛点问题，提出了具有培训、竞赛、研究、检测和能力开放等功能的体系化Web应用靶场建设方案，填补了目前Web应用靶场体系建设的空白，对

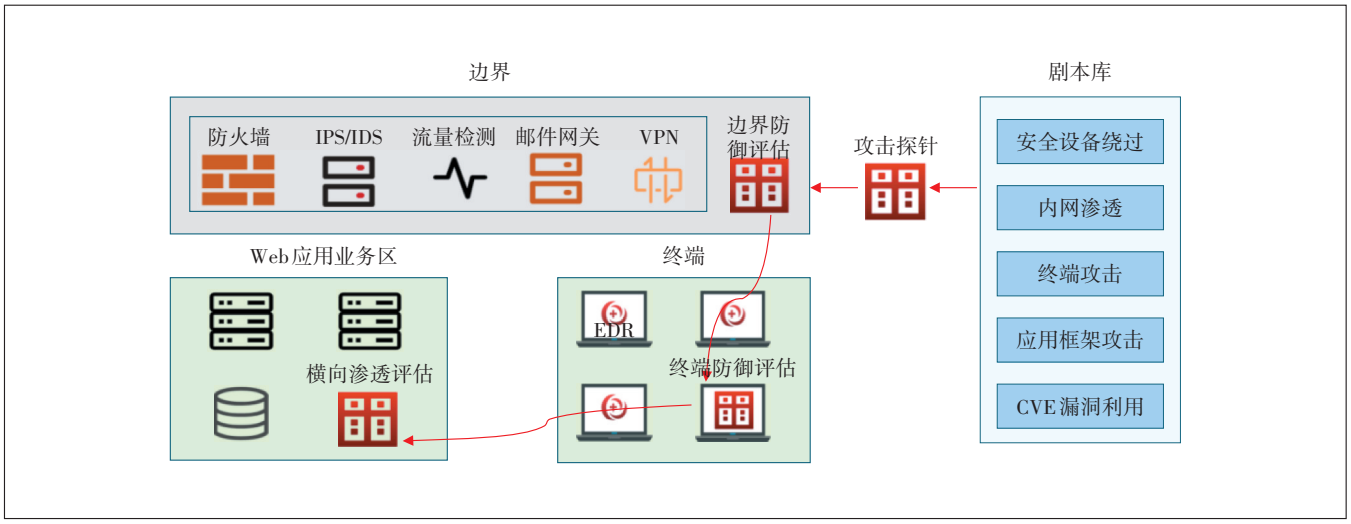

图6　Web应用安全防护能力检测方案

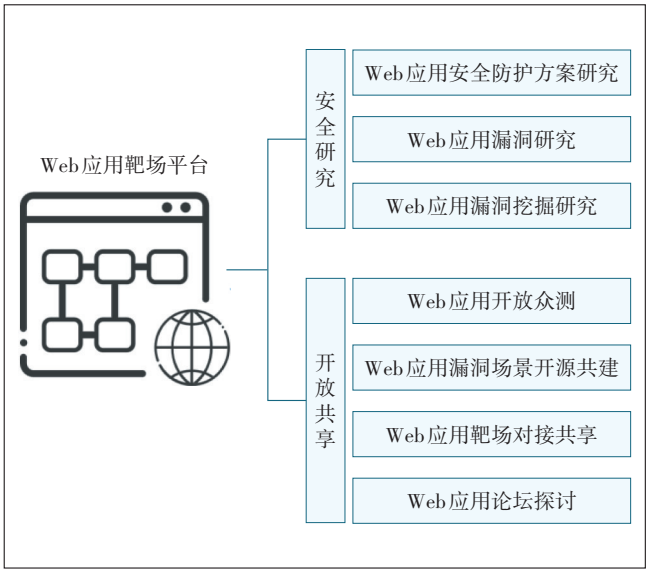

图7　能力开放建设方案

Web应用安全具有重要的现实和长远意义。

参考文献：

[1] 康志辉. Web应用系统文件上传漏洞分析[J]. 信息与电脑(理论版),2023,35(4):32-34.
[2] 李子东,王微微,尤枫,等. Web应用漏洞报告理解及漏洞复现[J]. 计算机系统应用,2023,32(11):62-72.
[3] 王鑫. 网络安全测评中Web应用安全渗透测试方法分析[J]. 无线互联科技,2023,20(4):165-168.
[4] 赵静. 网络空间安全靶场技术研究及系统架构设计[J]. 电脑知识与技术,2020,16(3):51-54.
[5] 赵千,李耀兵,江浩,等. 网络靶场的建设现状、基本特点与发展思路[J]. 中国信息化,2020(6):62-64.
[6] BIESECKER C . TSA To Add Tabletop Exercises As A Requirement In Cybersecurity Directives[J]. Defense Daily,2023.
[7] 宋智英,续焕超,李陆,等. 军工领域建设网络安全攻防靶场平台的思路[J]. 网信军民融合,2020(1):54-56.
[8] 严浩,石西华. 渗透测试在网络安全等保测评中的运用[J]. 电子技术与软件工程,2021(24):240-241.
[9] 许林,孟娜,袁静,等. 基于SDN的网络安全攻防虚拟仿真实战平台设计[J]. 电子设计工程,2022,30(16):139-142,147.
[10] 刘刚. 俄罗斯国家网络靶场体系建设探析[J]. 中国信息安全,2022(6):94-99.
[11] GIDDEON N. ANGAFOR, IRYNA YEVSEYEVA, YING HE. Game-based learning: A review of tabletop exercises for cybersecurity incident response training[J]. IEEE Security & Privacy,2020.
[12] NICHOLS J A,SPAKES K D,WATSON C L,et al. Assembling a Cyber Range to Evaluate Artificial Intelligence / Machine Learning (AI/ML) Security Tools[J].arXiv e-prints,2022.
[13] 王帅,金华敏,邓晓东,等. 网络安全靶场数据监控关键技术方案研究[J]. 广东通信技术,2021,41(12):41-44.
[14] MEIER R, LAVRENOVS A, HEINAARO K, et al. Towards an AI-powered Player in Cyber Defence Exercises[C]//2021 13th International Conference on Cyber Conflict (CyCon).2021.
[15] 方滨兴. 从"人、财、物"视角出发,提升网络空间的安全态势[J]. 中国科学院院刊,2022,37(1):53-59.

作者简介：
刘安,工程师,硕士,主要从事网络与信息安全研究工作;徐雷,高级工程师,博士,主要从事云计算、未来网络、网络与信息安全等新技术研究工作;郭新海,工程师,硕士,主要从事网络与信息安全研究工作;王戈,工程师,硕士,主要从事网络与信息安全研究工作;蓝鑫冲,工程师,硕士,主要从事网络与信息安全研究工作。