|  |  |
| --- | --- |
| 编 号 | {report\_number} |
| 日 期 | {report\_date} |

**{target\_host}**

**平台API模糊检测报告**

Version 1.2

2020年12月

© 2020 Packer FuzzeR团队

Poc-Sir、KpLi0rn、Liucy、RachesseHS、Lupin-III

* **版权声明**

Packer Fuzzer检测报告（下简称本报告）模板版权归Packer Fuzzer开发团队（下简称本团队）所有，并受法律保护。本团队有对本报告模板的修改和解释权。在修改本报告模板内容时，应保留相应的版权声明。未经本团队授权，不得以任何方式将Packer Fuzzer工具（下简称本工具）用于商业性目的。违反上述声明的个人或企业，本团队将保留进一步追究其法律责任的权利。

* **适用声明**

本报告适用于一切使用本工具检测的目标系统，请妥善保管，未经目标系统所有者允许不得传出。

* **免责声明**

本报告为本工具根据使用者检测结果自动生成的报告，报告内容不代表本团队的立场及观点。由于传播、利用此工具提供的检测功能而造成的任何直接或者间接的后果及损失，均由使用者本人负责，本团队不为此承担任何责任。请在使用本工具时遵循使用者以及目标系统所在国当地的相关法律法规，一切未授权测试均是不被允许的。

* **修订记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **修改日期** | **修改人** | **修改记录** | **批准人** |
| 1.0 | 2020/8/5 | Lupin-III | 无 | Poc-Sir |
| 1.2 | 2020/12/18 | Lupin-III | 新增内容模块 | Poc-Sir |

**一．报告摘要**

**被扫描平台：{target\_host}**

输入参数值：{target\_url}

本次扫描采用{scan\_type}扫描模式，使用{scan\_ip}作为扫描IP，共耗时{scan\_time}秒。

发起扫描时间：{start\_time}

扫描完成时间：{end\_time}

本次扫描共发现{api\_num}个有效API接口。

共发现{js\_num}个相关JS文件，分别是：

{js\_list}

共发现{vuln\_num}个安全漏洞，其中高危{vuln\_h\_num}个、中危{vuln\_m\_num}个、低危{vuln\_l\_num}个。分别是：

{vuln\_list}

附加Cookies信息为：{extra\_cookies}

附加传输头部信息为：{extra\_head}

**经过本工具分析，目标平台的安全风险等级为：{sec\_lv}**

**二．漏洞详情**

{vuln\_deta}

**三．API清单**

{api\_list}

**四．安全建议**

{suggest\_foryou}

**五．额外内容**

{extra\_tree}

**六．附录**

* **漏洞描述**

**CORS漏洞：**跨域资源共享可以放宽浏览器的同源策略，可以通过浏览器让不同的网站和不同的服务器之间通信。假设用户登陆一个含有CORS配置网站vuln.com，同时又访问了攻击者提供的一个链接evil.com。 evil.com的网站向vuln.com这个网站发起请求获取敏感数据，浏览器能否接收信息取决于vuln.com的配置。如果vuln.com配置了Access-Control-Allow-Origin头且为预期，那么允许接收，否则浏览器会因为同源策略而不接收。

**未授权访问漏洞：**接口未授权访问，顾名思义在不进行请求授权的情况下，能够直接对相应的业务逻辑功能进行访问、操作等。通常是由于认证页面存在缺陷或者无认证、安全配置不当等导致的。

**敏感信息泄露漏洞：**信息泄露指在网站页面或JS文件中泄露了敏感信息。通过这些敏感信息，攻击者可进一步入侵服务器。

**水平越权漏洞：**越权漏洞是指应用程序未对当前用户操作的身份权限进行严格校验，导致用户可以操作超出自己管理权限范围的功能，从而操作一些非该用户可以操作的行为。水平越权会导致同一层级间的用户可以互相访问到对方的敏感信息，如姓名、手机号、联系地址、个人资料、订单记录等。同时还可能会以其他平级权限用户的身份来执行某行功能，如删除，添加，修改等。

**SQL注入漏洞：**SQL注入漏洞产生的原因是网站应用程序在编写时未对用户提交至服务器的数据进行合法性校验（类型、长度、业务参数合法性等），同时没有对用户输入数据进行有效地特殊字符过滤，使得用户的输入直接带入数据库执行，超出了SQL语句原来设计的预期结果，导致了SQL注入漏洞。

**弱口令漏洞：**网站管理、运营人员由于安全意识不足，为了方便、避免忘记密码等，使用了非常容易记住的密码，或者是直接采用了系统的默认密码等。攻击者利用此漏洞可直接进入应用系统或者管理系统，从而进行系统、网页、数据的篡改与删除，非法获取系统、用户的数据，甚至可能导致服务器沦陷。

**任意文件上传漏洞：**应用系统在文件上传功能处对用户上传文件类型、格式、内容等做合法性校验，导致攻击者可以上传Webshell（.php、.jsp、asp等）恶意脚本文件或者非期望格式的文件比如：HTML文件、SHTML文件等，同时可利用目录跳转等字符或者控制上传目录，直接上传文件到Web目录或任意目录下，从而可能导致在远程服务器上执行任意恶意脚本文件，从而直接获取应用系统权限。

* **漏洞等级**

本报告内置三个漏洞等级，分别是：低危、中危、高危。其中属于高危的漏洞类型有：弱口令漏洞、任意文件上传漏洞、SQL注入漏洞；属于中危的漏洞类型有：水平越权漏洞、敏感信息泄露漏洞、未授权访问漏洞；属于低危的漏洞类型有：CORS漏洞。

其中置信度为“低”级别的检测结果将自动降低一级别漏洞危害，若已处于最低漏洞级别则不作降级处理。例如某漏洞为：SQL注入漏洞，本应属于高危漏洞，但其置信度为“低”，故自动降级为中危漏洞。

* **风险等级**

本报告内置无风险、低风险、中风险、高风险四个风险等级，采用打分评级模式，依次对应的分值档位为0、5、10、18。对应漏洞等级分值分别为：低危1分、中危2分、高危6分。例如在某次扫描中共发现一个高危、两个中危、五个低危漏洞，则分值计算方式为：1 x 6 + 2 x 2 + 5 x 1 = 15(分)，其得分大于10并小于18，所以风险等级为“中风险”。

**（报告结束，以下空白）**