编号	1
日期	2024-08-10

本地安全检测报告

• 版权声明

本地安全漏洞检测工具为本团队编写。

• 适用声明

本地安全漏洞检测工具可用于测试Linux系操作系统中是否存在可利用的中高风险漏洞。本工具支持通过原理扫描发现漏洞、支持通过版本匹配的方式发现CVE漏洞以及支持安全基线检测。

• 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。

• 开发团队 刘鑫、乔嘉琛、谢幸

以下贡献者排名不分先后：

一、报告摘要

被扫描平台：　192.168.160.133

用户名	xuj
计算机名	nuc-vmwarevirtualplatform
操作系统名	NAME="优麒麟"
操作系统版本	ubuntukylin-22.04-pro
系统架构	amd64
内核版本	linux 5.15.0-107-generic

- CWE ID 119
- CWE ID 079
- CWE ID 020
- CWE ID 200
- CWE ID 125
- CWE ID 089
- CWE ID 416
- CWE ID 190
- CWE ID 352
- CWE ID 022
- CWE ID 078
- CWE ID 787
- CWE ID 287
- CWE ID 476
- CWE ID 732
- CWE ID 434
- CWE ID 611
- CWE ID 094

- CWE ID 798
- CWE ID 400
- CWE ID 772
- CWE ID 426
- CWE ID 502
- CWE ID 269
- CWE ID 295

Executive Summary

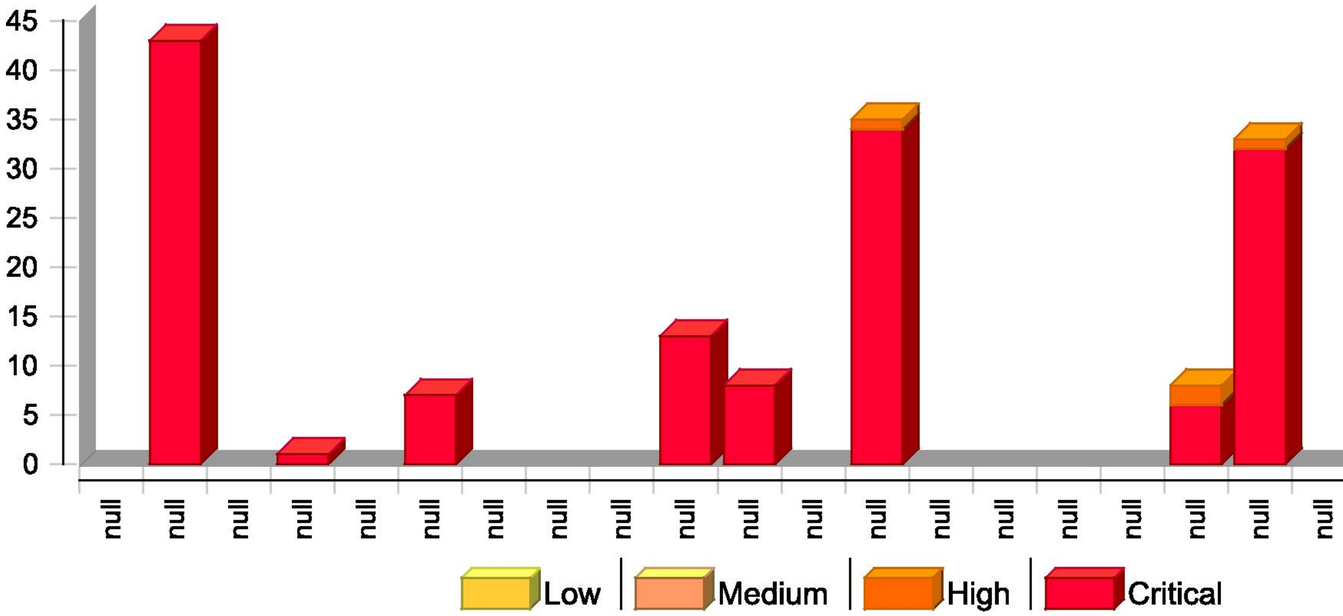
2019 CWE Top 25 最危险的软件错误列举了最普遍$s 最危险的缺陷,其中的错误可导致软件漏洞如国家漏洞 (U5Ii 数据库 (National Vulnerability Database) 所示) 这些缺陷出现频繁 容易查找且易于被利用 由于它们将频繁地允许攻击者全控制软件 窃取数据或使软件全无法运行,因此具有危险性 此列表 CWE 团队将启 ıjnJ 发式公式与数据驱动型方法结合使用而得出的,数据驱动型方法利用的常见的漏洞和风险 (CVE) 国家漏洞数据库 (National Vulnerability Database, NVD) 和常见的漏洞评分系统 (CVSS) 因 CWE 分类具有层次结构, Fortify 将 Top 25 条目子项的所有 CWE ID 视作条目上下文的一部分,因为层次结构中存在 "CHILD-OF" 关

系 只使用此 Top 25 列表来合理分配审核尝试时,应小心谨慎,因为接受分析的软件可能与用于定义 Top 25 1U, 的启发式假设不一致例如,这些缺陷中的许多缺陷与 C 类语言相关,接受分析的软件可能并不属于语言的 C 系列 o 因此,许多 CWE 不在范围内

Issues by Priority

12 High	112 Critical
0 Low	0 Medium

Issues by CWE Top 25 2019 Categories



	Fortify Priority				Total Issues	Effort (hrs)
	Critical	High	Medium	Low		
[1] CWE ID 119	0	0	0	0	0	0.0
[2] CWE ID 079	43	0	0	0	43	1.0
[3] CWE ID 020	0	0	0	0	0	0.0
[4] CWE ID 200	1	0	0	0	1	0.1
[5] CWE ID 125	0	0	0	0	0	0.0
[6] CWE ID 089	7	0	0	0	7	0.7
[7] CWE ID 416	0	0	0	0	0	0.0
[8] CWE ID 190	0	0	0	0	0	0.0
[9] CWE ID 352	0	0	0	0	0	0.0

[10] CWE ID 022	13	0	0	0	13	1.2
[11] CWE ID 078	8	0	0	0	8	0.8
[12] CWE ID 787	0	0	0	0	0	0.0
[13] CWE ID 287	34	1	0	0	35	2.1
[14] CWE ID 476	0	0	0	0	0	0.0
[15] CWE ID 732	0	0	0	0	0	0.0
[16] CWE ID 434	0	0	0	0	0	0.0
[17] CWE ID 611	0	0	0	0	0	0.0
[18] CWE ID 094	6	2	0	0	8	0.7
[19] CWE ID 798	32	1	0	0	33	1.8
[20] CWE ID 400	0	0	0	0	0	0.0
[21] CWE ID 772	0	0	0	0	0	0.0
[22] CWE ID 426	0	0	0	0	0	0.0
[23] CWE ID 502	0	9	0	0	9	0.8
[24] CWE ID 269	0	0	0	0	0	0.0
[25] CWE ID 295	0	0	0	0	0	0.0

NOTE:

- Reported issues in the above table may violate more than one CWE Top 25 2019 category. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Executive Summary table.
- For the same reason, the Project-level remediation effort total shown in the Executive Summary removes the effect of any duplication and may be smaller than the sum of the remediation effort per individual category.
- Similarly, the remediation effort per external category is not intended to equal the sum of the remediation effort from the issue details section since individual files may contain issues in multiple Fortify priorities or audit folders.

Below is an enumeration of all issues found in the project. The issues are organized by CWE Top 25 2019, Fortify Priority Order, and vulnerability category. The issues are then further broken down by the package, namespace, or location in which they occur. Issues reported at the same line number with the same category originate from different taint sources.

[1] CWE ID 119

CWE-119 用于识别“在内存缓冲区边界内不当地限制操作”缺陷。

出现这些缺陷是因为“软件在内存缓冲区上执行操作，但它可以从缓冲区的预期边界外部的内存位置读取或写入信息”。

No Issues

Cross-Site Scripting: Persistent

Remediation Effort(Hrs): 0.3

Critical

Package: dvwa.includes

Location	Analysis Info	Analyzer
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** PDO.prepare() **In** vulnerabilities/sqli/source/impossible.php:13	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** mysqli_query() **In** vulnerabilities/brute/source/medium.php:15	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** mysqli_query() **In** vulnerabilities/sqli/source/medium.php:10	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** mysqli_query() **In** vulnerabilities/sqli/source/low.php:9	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** mysqli_query() **In** vulnerabilities/brute/source/low.php:13	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** PDO.prepare() **In** vulnerabilities/brute/source/impossible.php:53	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** PDOStatement.fetch() **In** vulnerabilities/sqli/source/impossible.php:16	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** PDOStatement.fetch() **In** vulnerabilities/brute/source/impossible.php:57	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** mysqli_query() **In** vulnerabilities/brute/source/high.php:20	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** mysqli_query() **In** vulnerabilities/sqli/source/high.php:9	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** mysqli_query() **from** dvwaguestbook() **In** dvwa/includes/dvwaPage.inc.php:502	SCA

Cross-Site Scripting: Reflected *Remediation Effort(Hrs): 0.8*		Critical
Package: dvwa.includes		
Location	**Analysis Info**	**Analyzer**
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/high.php:5	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_POST['id'] **In** vulnerabilities/sqli/source/medium.php:5	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/low.php:5	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_POST['include'] **In** vulnerabilities/csp/source/low.php:15	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_POST['include'] **In** vulnerabilities/csp/source/high.php:10	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_GET['id'] **In** vulnerabilities/sqli/source/impossible.php:8	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_GET['name'] **In** vulnerabilities/xss_r/source/high.php:8	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_GET['username'] **In** vulnerabilities/brute/source/medium.php:5	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_POST['include'] **In** vulnerabilities/csp/source/medium.php:16	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_POST['include'] **In** vulnerabilities/csp/source/impossible.php:11	SCA
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_POST['password_new'] **In** vulnerabilities/captcha/source/low.php:8	SCA

Cross-Site Scripting: Reflected
Remediation Effort(Hrs): 0.8

Critical

Package: dvwa.includes

Location	Analysis Info	Analyzer
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_GET['username'] **In** vulnerabilities/brute/source/high.php:8	SCA
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_POST['username'] **In** vulnerabilities/brute/source/impossible.php:8	SCA
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_GET['name'] **In** vulnerabilities/xss_r/source/medium.php:8	SCA
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_GET['name'] **In** vulnerabilities/xss_r/source/low.php:8	SCA
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/impossible.php:8	SCA
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_POST['password_conf'] **In** vulnerabilities/captcha/source/low.php:9	SCA
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/medium.php:5	SCA
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_FILES['uploaded']['name'] **In** vulnerabilities/upload/source/impossible.php:9	SCA
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_GET['username'] **In** vulnerabilities/brute/source/low.php:5	SCA
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_REQUEST['id'] **In** vulnerabilities/s qli/source/low.php:5	SCA
dvwa/includes/dvwaPage.inc.p hp:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_POST['password_new'] **In** vulnerabilities/captcha/source/medium.php:8	SCA

Cross-Site Scripting: Reflected

Remediation Effort(Hrs): 0.8

Critical

Package: dvwa.includes

Location	Analysis Info	Analyzer
dvwa/includes/dvwaPage.inc.php:316	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_POST['password_conf'] **In** vulnerabilities/captcha/source/medium.php:9	SCA
dvwa/includes/dvwaPage.inc.php:326	**Sink:** builtin_echo() **Enclosing Method:** dvwahtmlecho() **Source:** Read $_COOKIE['security'] **from** dvwasecuri tylevelget() **In** dvwa/includes/dvwaPage.inc.php:1 36	SCA
dvwa/includes/dvwaPage.inc.php:406	**Sink:** builtin_echo() **Enclosing Method:** dvwasourcehtmlecho() **Source:** Read $_POST['id'] **In** vulnerabilities/sqli/session-input.php:12	SCA
dvwa/includes/dvwaPage.inc.php:406	**Sink:** builtin_echo() **Enclosing Method:** dvwasourcehtmlecho() **Source:** Read $_GET['security'] **In** vulnerabilities/view_source.php:12	SCA
dvwa/includes/dvwaPage.inc.php:406	**Sink:** builtin_echo() **Enclosing Method:** dvwasourcehtmlecho() **Source:** Read $_GET['id'] **In** vulnerabilities/view_ source.php:11	SCA

Package: external.phpids.0.6.docs.examples

Location	Analysis Info	Analyzer
external/phpids/0.6/docs/examples/example.php:82	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_COOKIE **In** external/phpids/0.6/docs/examples/example.php:45	SCA
external/phpids/0.6/docs/examples/example.php:82	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_REQUEST **In** external/phpids/0.6/docs/examples/example.php:42	SCA
external/phpids/0.6/docs/examples/example.php:82	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET **In** external/phpids/0.6/docs/examples/example.php:43	SCA
external/phpids/0.6/docs/examples/example.php:82	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_POST **In** external/phpids/0.6/docs/examples/example.php:44	SCA

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 0.8***		**Critical**
Package: vulnerabilities.csp.source		
Location	**Analysis Info**	**Analyzer**
vulnerabilities/csp/source/jsonp.php:12	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['callback'] **In** vulnerabilities /csp/source/jsonp.php:5	SCA

- ## CWE ID 020

CWE-20 用于识别“不当的输入验证”缺陷。

出现这些缺陷是因为“产品没有验证或不正确地验证可能会影响程序控制流或数据流的输入”。

No Issues

- ## CWE ID 200

CWE-200 用于识别“信息暴露”缺陷。

“信息暴露是向没有直接被授予信息访问权限的操作者有意或无意泄漏信息”。

System Information Leak: External ***Remediation Effort(Hrs): 0.1***		**Critical**
Package: <none>		
Location	**Analysis Info**	**Analyzer**
phpinfo.php:8	**Sink:** phpinfo() **Enclosing Method:** () **Source:**	SCA

- ## CWE ID 125

CWE-125 用于识别“超界读取”缺陷。

出现这些缺陷是因为“软件在预期的缓冲区末端之后或开始位置之前读取数据”。

No Issues

CWE-89 用于识别“对 SQL 命令中使用的特殊元素进行不当转义处理 ('SQL Injection')”缺陷。

出现这些缺陷是因为“软件使用来自上游组件的受外部影响的输入来构造一个完整或部分的 SQL 命令，但是当将其发送给下游组件时，软件无法或错误地转义处理了可以修改预期 SQL 命令的特殊元素”。

SQL Injection ***Remediation Effort(Hrs): 0.7***		**Critical**
Package: dvwa.includes.DBMS		
Location	**Analysis Info**	**Analyzer**
dvwa/includes/DBMS/MySQL.php:60	**Sink:** mysqli_query() **Enclosing Method:** () **Source:** Read $_SERVER['SCRIPT_NAME'] **In** dvwa/includes/DBMS/MySQL.php:51	SCA
dvwa/includes/DBMS/PGSQL.php:66	**Sink:** pg_query() **Enclosing Method:** () **Source:** Read $_SERVER['PHP_SELF'] **In** dvwa/includes/DBMS/PGSQL.php:56	SCA
dvwa/includes/DBMS/PGSQL.php:66	**Sink:** pg_query() **Enclosing Method:** () **Source:** Read $_SERVER['SERVER_NAME'] **In** dvwa/includes/DBMS/PGSQL.php:56	SCA
Package: vulnerabilities.brute.source		
Location	**Analysis Info**	**Analyzer**
vulnerabilities/brute/source/low.php:13	**Sink:** mysqli_query() **Enclosing Method:** () **Source:** Read $_GET['username'] **In** vulnerabilities/brute/source/low.php:5	SCA
Package: vulnerabilities.sqli.source		
Location	**Analysis Info**	**Analyzer**
vulnerabilities/sqli/source/low.php:9	**Sink:** mysqli_query() **Enclosing Method:** () **Source:** Read $_REQUEST['id'] **In** vulnerabilities/sqli/source/low.php:5	SCA

Package: vulnerabilities.sqli_blind.source		
Location	**Analysis Info**	**Analyzer**
vulnerabilities/sqli_blind/source/high.php:9	**Sink:** `mysqli_query()` **Enclosing Method:** `()` **Source:** `Read $_COOKIE['id']` **In** `vulnerabilities/sqli_blind/source/high.php:5`	SCA
vulnerabilities/sqli_blind/source/low.php:9	**Sink:** `mysqli_query()` **Enclosing Method:** `()` **Source:** `Read $_GET['id']` **In** `vulnerabilities/sqli_blind/source/low.php:5`	SCA

CWE-416 用于识别“释放后使用’’缺陷。

出现这些缺陷是因为“在内存释放后引用内存会导致程序崩溃、使用异常值或执行代码’’。

No Issues

[8] CWE ID 190

CWE-190 用于识别“整数溢出或环绕’’缺陷。

出现这些缺陷是因为“当逻辑假设结果值将始终大于初始值时，软件执行可产生整数溢出或环绕的计算。当计算用于资源管理或执行控制时，这将产生其他缺陷’’。

No Issues

[9] CWE ID 352

CWE-352 用于识别 "Cross-Site Request Forgery (CSRF)" 缺陷。

出现这些缺陷是因为“Web 应用程序不验证或无法确定格式标准的、有效的持续请求是否是提交请求的用户有意提供的’’。

No Issues

Path Manipulation
Remediation Effort(Hrs): 1.2

Critical

Package: external.phpids.0.6.lib.IDS.Filter

Location	Analysis Info	Analyzer
external/phpids/0.6/lib/IDS/Filter/Storage.php:305	**Sink:** file_get_contents() **Enclosing Method:** getfilterfromjson() **Source:** Read $_REQUEST **from** idscomponent.detect() **In** external/phpids/0.6/docs/examples/cakephp/id s.php:125	SCA

Package: vulnerabilities

Location	Analysis Info	Analyzer
vulnerabilities/view_help.p h p:15	**Sink:** file_get_contents() **Enclosing Method:** () **Source:** Read $_GET['id'] **In** vulnerabilities/view_help.php:11	SCA
vulnerabilities/view_source.php:53	**Sink:** file_get_contents() **Enclosing Method:** () **Source:** Read $_GET['id'] **In** vulnerabilities/view_source.php:11	SCA
vulnerabilities/view_source.php:53	**Sink:** file_get_contents() **Enclosing Method:** () **Source:** Read $_GET['security'] **In** vulnerabilities /view_source.php:12	SCA
vulnerabilities/view_source.php:58	**Sink:** file_get_contents() **Enclosing Method:** () **Source:** Read $_GET['security'] **In** vulnerabilities /view_source.php:12	SCA
vulnerabilities/view_source.php:58	**Sink:** file_get_contents() **Enclosing Method:** () **Source:** Read $_GET['id'] **In** vulnerabilities/view_source.php:11	SCA
vulnerabilities/view_source _ all.php:13	**Sink:** file_get_contents() **Enclosing Method:** () **Source:** Read $_GET['id'] **In** vulnerabilities/view_source_all.php:11	SCA
vulnerabilities/view_source _ all.php:17	**Sink:** file_get_contents() **Enclosing Method:** () **Source:** Read $_GET['id'] **In** vulnerabilities/view_source_all.php:11	SCA
vulnerabilities/view_source _ all.php:21	**Sink:** file_get_contents() **Enclosing Method:** () **Source:** Read $_GET['id'] **In** vulnerabilities/view_source_all.php:11	SCA
vulnerabilities/view_source _ all.php:25	**Sink:** file_get_contents() **Enclosing Method:** ()	SCA

	Source: Read $_GET['id'] **In** vulnerabilities/view_source_all.php:11	

Path Manipulation *Remediation Effort(Hrs): 1.2*	Critical
Package: vulnerabilities.upload.source	

Location	Analysis Info	Analyzer
vulnerabilities/upload/source/impossible.php:40	**Sink:** rename() **Enclosing Method:** () **Source:** Read $_FILES['uploaded']['name'] **In** vulnerabilities/upload/source/impossible.php:9	SCA
vulnerabilities/upload/source/impossible.php:40	**Sink:** rename() **Enclosing Method:** () **Source:** Read $_FILES['uploaded']['name'] **In** vulnerabilities/upload/source/impossible.php:9	SCA
vulnerabilities/upload/source/impossible.php:51	**Sink:** unlink() **Enclosing Method:** () **Source:** Read $_FILES['uploaded']['name'] **In** vulnerabilities/upload/source/impossible.php:9	SCA

CWE-78 用于识别“对 OS 命令中使用的特殊元素进行不当转义处理（‘OS Command Injection’）”缺陷。

出现这些缺陷是因为“软件使用来自上游组件的受外部影响的输入来构造一个完整或部分的 OS 命令，但是当将其发送给下游组件时，软件无法或错误地转义处理了可以修改预期 OS 命令的特殊元素”。

Command Injection *Remediation Effort(Hrs): 0.8*	Critical
Package: vulnerabilities.exec.source	

Location	Analysis Info	Analyzer
vulnerabilities/exec/source/high.php:26	**Sink:** shell_exec() **Enclosing Method:** () **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/high.php:5	SCA
vulnerabilities/exec/source/high.php:30	**Sink:** shell_exec() **Enclosing Method:** () **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/high.php:5	SCA
vulnerabilities/exec/source/	**Sink:** shell_exec()	SCA

impossible.php:22	**Enclosing Method:** () **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/impossible.php:8	
vulnerabilities/exec/source/impossible.php:26	**Sink:** shell_exec() **Enclosing Method:** () **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/impossible.php:8	SCA
vulnerabilities/exec/source/low.php:10	**Sink:** shell_exec() **Enclosing Method:** () **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/low.php:5	SCA
vulnerabilities/exec/source/low.php:14	**Sink:** shell_exec() **Enclosing Method:** () **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/low.php:5	SCA
vulnerabilities/exec/source/medium.php:19	**Sink:** shell_exec() **Enclosing Method:** () **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/medium.php:5	SCA
vulnerabilities/exec/source/medium.php:23	**Sink:** shell_exec() **Enclosing Method:** () **Source:** Read $_REQUEST['ip'] **In** vulnerabilities/exec/source/medium.php:5	SCA

[12] CWE ID 787

CWE-787 用于识别"超界写入"缺陷。

出现这些缺陷是因为"软件在期望的缓冲区末端之后或开始位置之前写入数据"。

No Issues

Key Management: Hardcoded Encryption Key
Remediation Effort(Hrs): 1.7
Critical

Package: external.phpids.0.6.tests.coverage

Location	Analysis Info	Analyzer
external/phpids/0.6/tests/coverage/container-min.js:7	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:7	**Sink:** FieldAccess: key **Enclosing Method:**	SCA

	lambda() **Source:**	
external/phpids/0.6/tests/coverage/container-min.js:7	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:7	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing**	SCA

	Method: lambda() **Source:**	
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA

Key Management: Hardcoded Encryption Key

Remediation Effort(Hrs): 1.7

Critical

Package: external.phpids.0.6.tests.coverage

Location	Analysis Info	Analyzer
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:**	SCA

	lambda() **Source:**	
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:15	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:15	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:15	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA

Key Management: Hardcoded Encryption Key

Remediation Effort(Hrs): 1.7

Critical

Package: external.phpids.0.6.tests.coverage

Location	Analysis Info	Analyzer
external/phpids/0.6/tests/coverage/container-min.js:16	**Sink:** FieldAccess: key **Enclosing Method:** lambda()	SCA

	Source:	
external/phpids/0.6/tests/coverage/container-min.js:16	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA

Password Management: Password in Configuration File ***Remediation Effort(Hrs): 0.3***	**Critical**

Package: external.phpids.0.6.lib.IDS.Config

Location	Analysis Info	Analyzer
external/phpids/0.6/lib/IDS/Config/Config.ini:63	**Sink:** password **Enclosing Method:** () **Source:**	SCA
external/phpids/0.6/lib/IDS/Config/Config.ini:80	**Sink:** password **Enclosing Method:** () **Source:**	SCA

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 0.2***	**High**

Package: config

Location	Analysis Info	Analyzer
config/config.inc.php:21	**Sink:** ArrayAccess: $_DVWA **Enclosing Method:** () **Source:**	SCA

[14] CWE ID 476

CWE-476 用于识别“空指针间接引用”缺陷。

“在应用程序间接引用预期有效但却为空的指针时，会出现空指针间接引用，这通常会导致崩溃或退出”。

No Issues

CWE-732 用于识别“关键资源权限分配错误”缺陷。

出现这些缺陷是因为“软件为安全关键资源指定权限，允许非指定的操作者读取

或修改资源’’。

No Issues

[16] CWE ID 434

CWE-434 用于识别‘‘未限制上传危险类型的文件’’缺陷。

出现这些缺陷是因为‘‘软件允许攻击者上传或传输危险类型的文件，这些文件可在产品环境中自动处理’’。

No Issues

[17] CWE ID 611

CWE-611 用于识别‘‘对 XML 外部实体引用进行不当限制’’缺陷。

出现这些缺陷是因为‘‘软件处理包含带有 URI（可在预期控制范围之外解析文档）的 XML 实体的 XML 文档，这会导致该产品将不正确的文档嵌入其输出中 ’’。

No Issues

Dangerous File Inclusion ***Remediation Effort(Hrs): 0.6***		**Critical**
Package: external.phpids.0.6.lib.IDS		
Location	**Analysis Info**	**Analyzer**
external/phpids/0.6/lib/IDS / Monitor.php:368	**Sink:** builtin_includeonce() **Enclosing Method:** _purifyvalues() **Source:** Read $_REQUEST **from** idscomponent.detect() **In** external/phpids/0.6/docs/examples/cakephp/ids.php:125	SCA
Package: external.phpids.0.6.lib.IDS.Caching		
Location	**Analysis Info**	**Analyze**

		r
external/phpids/0.6/lib/IDS / Caching/Factory.php:76	**Sink:** builtin_includeonce() **Enclosing Method:** factory() **Source:** Read $_REQUEST **from** idscomponent.detect() **In** external/phpids/0.6/docs/examples/cakephp/id s.php:125	SCA

Package: vulnerabilities.fi

Location	Analysis Info	Analyzer
vulnerabilities/fi/index.php :36	**Sink:** builtin_include() **Enclosing Method:** () **Source:** Read $_GET['page'] **In** vulnerabilities/fi/ source/impossible.php:4	SCA
vulnerabilities/fi/index.php :36	**Sink:** builtin_include() **Enclosing Method:** () **Source:** Read $_GET['page'] **In** vulnerabilities/fi/ source/high.php:4	SCA
vulnerabilities/fi/index.php :36	**Sink:** builtin_include() **Enclosing Method:** () **Source:** Read $_GET['page'] **In** vulnerabilities/fi/ source/medium.php:4	SCA
vulnerabilities/fi/index.php :36	**Sink:** builtin_include() **Enclosing Method:** () **Source:** Read $_GET['page'] **In** vulnerabilities/fi/ source/low.php:4	SCA

PHP Misconfiguration: allow_url_fopen Enabled ***Remediation Effort(Hrs): 0.1***	**High**

Package: <none>

Location	Analysis Info	Analyzer
php.ini:4	**Sink:** allow_url_fopen **Enclosing Method:** () **Source:**	SCA

PHP Misconfiguration: allow_url_include Enabled ***Remediation Effort(Hrs): 0.1***	**High**

Package: <none>

Location	Analysis Info	Analyzer
php.ini:5	**Sink:** allow_url_include **Enclosing Method:** () **Source:**	SCA

Key Management: Hardcoded Encryption Key ***Remediation Effort(Hrs): 1.7***	**Critical**

Package: external.phpids.0.6.tests.coverage

Location	Analysis Info	Analyzer

external/phpids/0.6/tests/coverage/container-min.js:7	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()` **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:7	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()` **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:7	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()` **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:7	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()` **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()` **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()` **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()` **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()` **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()` **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()` **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** `FieldAccess: key` **Enclosing Method:** `lambda()`	SCA

	Source:	
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:9	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA

Key Management: Hardcoded Encryption Key

Remediation Effort(Hrs): 1.7

Critical

Package: external.phpids.0.6.tests.coverage

Location	Analysis Info	Analyzer
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA

external/phpids/0.6/tests/coverage/container-min.js:12	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:13	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:15	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA

Key Management: Hardcoded Encryption Key

Remediation Effort(Hrs): 1.7

Critical

Package: external.phpids.0.6.tests.coverage

Location	Analysis Info	Analyzer
external/phpids/0.6/tests/coverage/container-min.js:15	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/co	**Sink:**	SCA

verage/container-min.js:15	FieldAccess: key **Enclosing Method:** lambda() **Source:**	
external/phpids/0.6/tests/coverage/container-min.js:16	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA
external/phpids/0.6/tests/coverage/container-min.js:16	**Sink:** FieldAccess: key **Enclosing Method:** lambda() **Source:**	SCA

Password Management: Hardcoded Password
Remediation Effort(Hrs): 0.2

High

Package: config

Location	Analysis Info	Analyzer
config/config.inc.php:21	**Sink:** ArrayAccess: $_DVWA **Enclosing Method:** () **Source:**	SCA

[20] CWE ID 400

CWE-400 用于识别"不受控制的资源消耗"缺陷。

出现这些缺陷是因为"软件没有正确限制操作者请求或影响的资源大小或资源量，这样，消耗的资源会比预期更多"。

No Issues

[21] CWE ID 772

CWE-772 用于识别"有效期结束后缺少资源释放"缺陷。

出现这些缺陷是因为"有效期结束后，也就是不再需要资源后，软件无法释放资源"。

No Issues

CWE-426 用于识别“不可信赖的搜索路径’’缺陷。

出现这些缺陷是因为“应用程序使用可指向不受应用程序直接控制的资源的外部提供的搜索路径来搜索关键资源’’。

No Issues

CWE-502 用于识别“不可信赖的数据的反序列化’’缺陷。

出现这些缺陷是因为“应用程序在未充分验证结果数据是否有效的情况下对不受信任的数据进行了反序列化’’。

Object Injection ***Remediation Effort(Hrs): 0.8***		**High**
Package: external.phpids.0.6.lib.IDS		
Location	**Analysis Info**	**Analyzer**
external/phpids/0.6/lib/IDS/Converter.php:632	**Sink:** unserialize() **Enclosing Method:** runcentrifuge() **Source:** Read $_POST **In** external/phpids/0.6/docs/examples/example.php:44	SCA
external/phpids/0.6/lib/IDS/Converter.php:632	**Sink:** unserialize() **Enclosing Method:** runcentrifuge() **Source:** Read $_REQUEST **In** external/phpids/0.6/docs/examples/example.php:42	SCA
external/phpids/0.6/lib/IDS/Converter.php:632	**Sink:** unserialize() **Enclosing Method:** runcentrifuge() **Source:** Read $_COOKIE **from** dvwaphpidstrap() **In** dvwa/includes/dvwaPhpIds.inc.php:65	SCA
external/phpids/0.6/lib/IDS/Converter.php:632	**Sink:** unserialize() **Enclosing Method:** runcentrifuge() **Source:** Read $_GET **In** external/phpids/0.6/docs/examples/example.php:43	SCA
external/phpids/0.6/lib/IDS/Converter.php:632	**Sink:** unserialize() **Enclosing Method:** runcentrifuge() **Source:** Read $_COOKIE **In** external/phpids/0.6/docs/examples/example.php:45	SCA
external/phpids/0.6/lib/IDS/	**Sink:** unserialize()	SCA

Converter.php:632	**Enclosing Method:** runcentrifuge() **Source:** Read $_POST **from** dvwaphpidstrap() **In** dvwa/includes/dvwaPhpIds.inc.php:64	
external/phpids/0.6/lib/IDS/Converter.php:632	**Sink:** unserialize() **Enclosing Method:** runcentrifuge() **Source:** Read $_REQUEST **from** dvwaphpidstrap() **In** dvwa/includes/dvwaPhpIds.inc.php:62	SCA
external/phpids/0.6/lib/IDS/Converter.php:632	**Sink:** unserialize() **Enclosing Method:** runcentrifuge() **Source:** Read $_GET **from** dvwaphpidstrap() **In** dvwa/includes/dvwaPhpIds.inc.php:63	SCA

Package: external.phpids.0.6.lib.IDS.Caching

Location	Analysis Info	Analyzer
external/phpids/0.6/lib/IDS/Caching/Database.php:192	**Sink:** unserialize() **Enclosing Method:** getcache() **Source:** PDO.prepare() **from** ids_caching_database.g etcache() **In** external/phpids/0.6/lib/IDS/Caching/Database.php:186	SCA

CWE-269 用于识别“不正确的权限管理”缺陷。

出现这些缺陷是因为“软件没有正确分配、修改、追踪或检查操作者的权限，给该操作者提供了预期控制范围以外的控制力”。

No Issues

[25] CWE ID 295

CWE-295 用于识别“对证书进行不当验证”缺陷。

出现这些缺陷是因为“软件无法验证或以错误方式验证证书”。

No Issues