Fortify Audit Workbench

CWE Top 25 2019

seacms-13

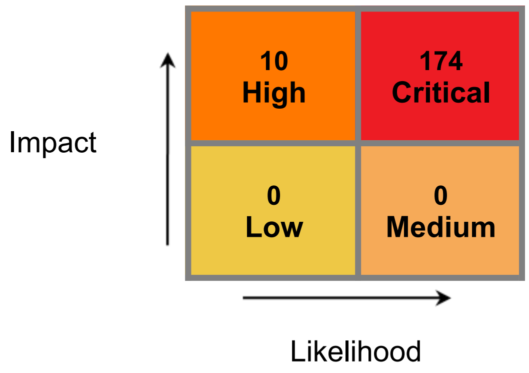
Table of Contents

Executive Summary

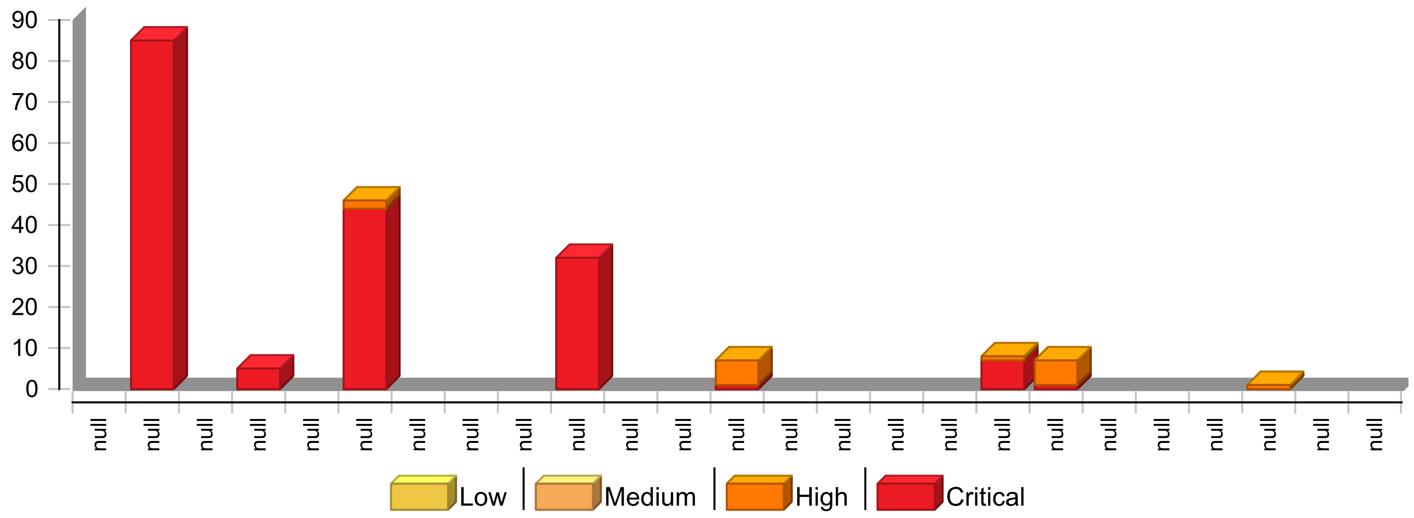
2019 CWE Top 25 最危险的软件错误列举了最普遍、最危险的缺陷，其中的错误可导致软件漏洞（如国家漏洞数据库 (National Vulnerability Database) 所示）。这些缺陷出现频繁、容易查找且易于被利用。由于它们将频繁地允许攻击者完全控制软件、窃取数据或使软件完全无法运行，因此具有危险性。此列表是 CWE 团队将启发式公式与数据驱动型方法结合使用而得出的，数据驱动型方法利用的是常见的漏洞和风险 (CVE)、国家漏洞数据库 (National Vulnerability Database, NVD) 和常见的漏洞评分系统 (CVSS)。因 CWE 分类具有层次结构，Fortify 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 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。因此，许多 CWE 不在范围内。

Project Name:	seacms-13
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
WebInspect Agent:	Results Not Present
Other:	Results Not Present
Remediation Effort (Hrs):	7.4

Issues by Priority



Issues by CWE Top 25 2019 Categories



* The detailed sections following the Executive Summary contain specifics.

Project Description

This section provides an overview of the Fortify scan engines used for this project, as well as the project meta-information.

SCA

Date of Last Analysis:	2024年9月13日 上午10:11	**Engine Version:**	20.1.1.0007
Host Name:	DESKTOP-EKDVM8M	**Certification:**	VALID
Number of Files:	514	**Lines of Code:**	19,618

Rulepack Name	Rulepack Version
Fortify 安全编码规则、核心、JavaScript	2019.4.1.0002
Fortify 安全编码规则、核心、PHP	2019.4.1.0002
Fortify 安全编码规则、核心、SQL	2019.4.1.0002
Fortify 安全编码规则、扩展、配置	2019.4.1.0002
Fortify 安全编码规则、扩展、内容	2019.4.1.0002
Fortify 安全编码规则、扩展、JavaScript	2019.4.1.0002
Fortify 安全编码规则、扩展、SQL	2019.4.1.0002

Issue Breakdown

The following table summarizes the number of issues identified across the different CWE Top 25 2019 categories and broken down by Fortify Priority Order.

	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	85	0	0	0	85	2.8
[3] CWE ID 020	0	0	0	0	0	0.0
[4] CWE ID 200	5	0	0	0	5	0.4
[5] CWE ID 125	0	0	0	0	0	0.0
[6] CWE ID 089	44	2	0	0	46	1.0
[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	32	0	0	0	32	2.3
[11] CWE ID 078	0	0	0	0	0	0.0
[12] CWE ID 787	0	0	0	0	0	0.0
[13] CWE ID 287	1	6	0	0	7	1.0
[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	7	1	0	0	8	0.7
[19] CWE ID 798	1	6	0	0	7	1.0
[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	1	0	0	1	0.2
[24] CWE ID 269	0	0	0	0	0	0.0
[25] CWE ID 295	0	0	0	0	0	0.0

NOTE:

1. 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.
2. 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.
3. 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.

Issue Details

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

[2] CWE ID 079

CWE-79 用于识别“在 Web 页面生成期间对输入进行不当转义处理 ('Cross-Site Scripting')”缺陷。

出现这些缺陷是因为“软件将用户可控制的输入放入用作将提供给其他用户的 Web 页面的输出之前，无法或错误地转义处理了此输入”。

Cross-Site Scripting: Persistent
Remediation Effort(Hrs): 0.3

Critical

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/functions.php:677	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA
admin/ebak/class/functions.php:677	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/functions.php:677	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/functions.php:677	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA

[2] CWE ID 079

CWE-79 用于识别“在 Web 页面生成期间对输入进行不当转义处理 ('Cross-Site Scripting')”缺陷。

出现这些缺陷是因为“软件将用户可控制的输入放入用作将提供给其他用户的 Web 页面的输出之前，无法或错误地转义处理了此输入”。

Cross-Site Scripting: Persistent ***Remediation Effort(Hrs): 0.3***		**Critical**
Package: admin.ebak.class		
Location	**Analysis Info**	**Analyzer**
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA
admin/ebak/class/functions.php:896	**Sink:** builtin_echo() **Enclosing Method:** ebak_echobakst() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/functions.php:896	**Sink:** builtin_echo() **Enclosing Method:** ebak_echobakst() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 2.6***		**Critical**
Package: <none>		
Location	**Analysis Info**	**Analyzer**
desktop.php:13	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_REQUEST['url'] **In** desktop.php:4	SCA
Package: admin		
Location	**Analysis Info**	**Analyzer**
admin/admin_datarelate.php:713	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['page'] **In** admin/admin_datarelate.php:700	SCA
admin/admin_ip.php:58	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_POST['ip'] **In** admin/admin_ip.php:8	SCA
admin/admin_makehtml2.php:525	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['password'] **In** admin/admin_makehtml2.php:11	SCA
admin/admin_makehtml2.php:553	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_SERVER['HTTP_REFERER'] **from** getreferer() **In** admin/admin_reslib2.php:151	SCA
admin/admin_makehtml2.php:553	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_SERVER['HTTP_REFERER'] **from** getreferer() **In** admin/config.php:215	SCA

[2] CWE ID 079

CWE-79 用于识别“在 Web 页面生成期间对输入进行不当转义处理 ('Cross-Site Scripting')”缺陷。

出现这些缺陷是因为“软件将用户可控制的输入放入用作将提供给其他用户的 Web 页面的输出之前，无法或错误地转义处理了此输入”。

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 2.6***		**Critical**
Package: admin		
Location	**Analysis Info**	**Analyzer**
admin/admin_makehtml2.php:553	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_SERVER['HTTP_REFERER'] **from** getreferer() **In** admin/admin_makehtml2.php:153	SCA
admin/admin_makehtml2.php:589	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_SERVER['HTTP_REFERER'] **from** getreferer() **In** admin/admin_makehtml2.php:153	SCA
admin/admin_makehtml2.php:589	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_SERVER['HTTP_REFERER'] **from** getreferer() **In** admin/admin_reslib2.php:151	SCA
admin/admin_makehtml2.php:589	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_SERVER['HTTP_REFERER'] **from** getreferer() **In** admin/config.php:215	SCA
admin/admin_makehtml2.php:656	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['password'] **In** admin/admin_makehtml2.php:11	SCA
admin/admin_notify.php:55	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_POST['notify1'] **In** admin/admin_notify.php:7	SCA
admin/admin_notify.php:60	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_POST['notify2'] **In** admin/admin_notify.php:8	SCA
admin/admin_notify.php:65	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_POST['notify3'] **In** admin/admin_notify.php:9	SCA
admin/admin_ping.php:61	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_POST['weburl'] **In** admin/admin_ping.php:7	SCA
admin/admin_ping.php:62	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_POST['token'] **In** admin/admin_ping.php:8	SCA
admin/admin_reslib2.php:639	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['password'] **In** admin/admin_reslib2.php:11	SCA

[2] CWE ID 079

CWE-79 用于识别“在 Web 页面生成期间对输入进行不当转义处理 ('Cross-Site Scripting')”缺陷。

出现这些缺陷是因为“软件将用户可控制的输入放入用作将提供给其他用户的 Web 页面的输出之前，无法或错误地转义处理了此输入”。

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 2.6***	**Critical**

Package: admin

Location	Analysis Info	Analyzer
admin/admin_reslib2.php:642	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['password'] **In** admin/admin_reslib2.php:11	SCA
admin/admin_reslib2.php:972	**Sink:** builtin_echo() **Enclosing Method:** intodatabase() **Source:** Read $_GET['password'] **from** intodatabase() **In** admin/admin_reslib2.php:969	SCA
admin/admin_reslib2.php:975	**Sink:** builtin_echo() **Enclosing Method:** intodatabase() **Source:** Read $_GET['password'] **from** intodatabase() **In** admin/admin_reslib2.php:969	SCA
admin/admin_reslib2.php:978	**Sink:** builtin_echo() **Enclosing Method:** intodatabase() **Source:** Read $_GET['password'] **from** intodatabase() **In** admin/admin_reslib2.php:969	SCA
admin/admin_reslib2.php:981	**Sink:** builtin_echo() **Enclosing Method:** intodatabase() **Source:** Read $_GET['password'] **from** intodatabase() **In** admin/admin_reslib2.php:969	SCA
admin/admin_safe.php:130	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_COOKIE['t00ls_s'] **from** getsetting() **In** admin/admin_safe.php:277	SCA
admin/admin_safe.php:160	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_POST['path'] **In** admin/admin_safe.php:153	SCA
admin/admin_safe.php:212	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_POST['path'] **In** admin/admin_safe.php:153	SCA
admin/admin_safe.php:212	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_SERVER['HTTP_HOST'] **In** admin/admin_safe.php:43	SCA

Package: admin.ebak

Location	Analysis Info	Analyzer
admin/ebak/ChangeDb.php:185	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['act'] **In** admin/ebak/ChangeDb.php:7	SCA

[2] CWE ID 079

CWE-79 用于识别“在 Web 页面生成期间对输入进行不当转义处理 ('Cross-Site Scripting')”缺陷。

出现这些缺陷是因为“软件将用户可控制的输入放入用作将提供给其他用户的 Web 页面的输出之前，无法或错误地转义处理了此输入”。

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 2.6***		**Critical**
Package: admin.ebak.class		
Location	**Analysis Info**	**Analyzer**
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_GET['change'] **from** ebak_delbakpath() **In** admin/ebak/class/combakfun.php:546	SCA
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_POST['mydbname'] **In** admin/ebak/phome.php:199	SCA
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_POST['mydbname'] **In** admin/ebak/phome.php:205	SCA
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_POST['mydbname'] **In** admin/ebak/phome.php:211	SCA
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_POST['mydbname'] **In** admin/ebak/phome.php:217	SCA
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_POST['mydbname'] **In** admin/ebak/phome.php:236	SCA
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_GET **In** admin/ebak/phome.php:283	SCA
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_SERVER['HTTP_REFERER'] **from** ebak_checkshowkey() **In** admin/ebak/class/connect.php:400	SCA
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_SERVER['HTTP_REFERER'] **from** ebak_checkshowkey() **In** admin/ebak/class/connect.php:404	SCA
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_SERVER['HTTP_REFERER'] **from** ebak_checkshowkey() **In** admin/ebak/class/connect.php:409	SCA
admin/ebak/class/functions.php:164	**Sink:** builtin_echo() **Enclosing Method:** printerror() **Source:** Read $_SERVER['HTTP_HOST'] **from** ebak_ereturndomain() **In** admin/ebak/class/connect.php:420	SCA

[2] CWE ID 079

CWE-79 用于识别“在 Web 页面生成期间对输入进行不当转义处理 ('Cross-Site Scripting')”缺陷。

出现这些缺陷是因为“软件将用户可控制的输入放入用作将提供给其他用户的 Web 页面的输出之前，无法或错误地转义处理了此输入”。

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 2.6***		**Critical**
Package: admin.ebak.class		
Location	**Analysis Info**	**Analyzer**
admin/ebak/class/functions.php:401	**Sink:** builtin_echo() **Enclosing Method:** ebak_dozip() **Source:** Read $_GET['p'] **In** admin/ebak/phome.php:262	SCA
admin/ebak/class/functions.php:401	**Sink:** builtin_echo() **Enclosing Method:** ebak_dozip() **Source:** Read $_GET['p'] **In** admin/ebak/phome.php:262	SCA
admin/ebak/class/functions.php:525	**Sink:** builtin_echo() **Enclosing Method:** ebak_doebak() **Source:** Read $_POST **In** admin/ebak/phomebak.php:180	SCA
admin/ebak/class/functions.php:677	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** Read $_GET['mypath'] **In** admin/ebak/phomebak.php:187	SCA
admin/ebak/class/functions.php:677	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** Read $_GET['fnum'] **In** admin/ebak/phomebak.php:190	SCA
admin/ebak/class/functions.php:677	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** Read $_GET['stime'] **In** admin/ebak/phomebak.php:191	SCA
admin/ebak/class/functions.php:677	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** Read $_GET['thenof'] **In** admin/ebak/phomebak.php:189	SCA
admin/ebak/class/functions.php:677	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** Read $_GET['collation'] **from** ebak_bakexe() **In** admin/ebak/class/functions.php:581	SCA
admin/ebak/class/functions.php:695	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** Read $_GET['mypath'] **In** admin/ebak/phomebak.php:187	SCA
admin/ebak/class/functions.php:695	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexe() **Source:** Read $_GET['stime'] **In** admin/ebak/phomebak.php:191	SCA
admin/ebak/class/functions.php:868	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** Read $_GET['stime'] **In** admin/ebak/phomebak.php:205	SCA

[2] CWE ID 079

CWE-79 用于识别“在 Web 页面生成期间对输入进行不当转义处理 ('Cross-Site Scripting')”缺陷。

出现这些缺陷是因为“软件将用户可控制的输入放入用作将提供给其他用户的 Web 页面的输出之前，无法或错误地转义处理了此输入”。

Cross-Site Scripting: Reflected
Remediation Effort(Hrs): 2.6

Critical

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/functions.php:868	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** Read $_GET['mypath'] **In** admin/ebak/phomebak.php:199	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** Read $_GET['fnum'] **In** admin/ebak/phomebak.php:202	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** Read $_GET['stime'] **In** admin/ebak/phomebak.php:205	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** Read $_GET['collation'] **from** ebak_bakexet() **In** admin/ebak/class/functions.php:751	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** Read $_GET['mypath'] **In** admin/ebak/phomebak.php:199	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** Read $_GET['auf'] **In** admin/ebak/phomebak.php:203	SCA
admin/ebak/class/functions.php:879	**Sink:** builtin_echo() **Enclosing Method:** ebak_bakexet() **Source:** Read $_GET['thenof'] **In** admin/ebak/phomebak.php:201	SCA
admin/ebak/class/functions.php:910	**Sink:** builtin_echo() **Enclosing Method:** ebak_echoredatast() **Source:** Read $_GET['p'] **In** admin/ebak/inc/footer.php:15	SCA
admin/ebak/class/functions.php:1294	**Sink:** builtin_echo() **Enclosing Method:** ebak_changelanguage() **Source:** Read $_GET **In** admin/ebak/phome.php:297	SCA
admin/ebak/class/functions.php:1409	**Sink:** builtin_echo() **Enclosing Method:** ebak_changedbserver() **Source:** Read $_GET **In** admin/ebak/phome.php:305	SCA

Package: admin.ebak.inc

Location	Analysis Info	Analyzer
admin/ebak/inc/footer.php:34	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['t'] **In** admin/ebak/inc/footer.php:12	SCA

[2] CWE ID 079

CWE-79 用于识别“在 Web 页面生成期间对输入进行不当转义处理 ('Cross-Site Scripting')”缺陷。

出现这些缺陷是因为“软件将用户可控制的输入放入用作将提供给其他用户的 Web 页面的输出之前，无法或错误地转义处理了此输入”。

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 2.6***	**Critical**

Package: admin.ebak.inc

Location	Analysis Info	Analyzer
admin/ebak/inc/footer.php:34	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['stime'] **In** admin/ebak/inc/footer.php:7	SCA
admin/ebak/inc/footer.php:42	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['p'] **In** admin/ebak/inc/footer.php:15	SCA
admin/ebak/inc/footer.php:42	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['p'] **In** admin/ebak/inc/footer.php:15	SCA
admin/ebak/inc/footer.php:42	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['t'] **In** admin/ebak/inc/footer.php:12	SCA
admin/ebak/inc/footer.php:42	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['stime'] **In** admin/ebak/inc/footer.php:7	SCA

Package: admin.ebak.lang.gbutf8.temp

Location	Analysis Info	Analyzer
admin/ebak/lang/gbutf8/temp/eChangeTable.php:128	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['savefilename'] **In** admin/ebak/lang/gbutf8/temp/eChangeTable.php:128	SCA

Package: admin.editor.php

Location	Analysis Info	Analyzer
admin/editor/php/file_manager_json.php:133	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['path'] **In** admin/editor/php/file_manager_json.php:40	SCA
admin/editor/php/file_manager_json.php:133	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['path'] **In** admin/editor/php/file_manager_json.php:41	SCA
admin/editor/php/file_manager_json.php:133	**Sink:** builtin_echo() **Enclosing Method:** () **Source:** Read $_GET['dir'] **In** admin/editor/php/file_manager_json.php:19	SCA

[2] CWE ID 079

CWE-79 用于识别“在 Web 页面生成期间对输入进行不当转义处理 ('Cross-Site Scripting')”缺陷。

出现这些缺陷是因为“软件将用户可控制的输入放入用作将提供给其他用户的 Web 页面的输出之前，无法或错误地转义处理了此输入”。

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 2.6***		**Critical**
Package: admin.editor.php		
Location	**Analysis Info**	**Analyzer**
admin/editor/php/upload_json .php:125	**Sink:** `builtin_echo()` **Enclosing Method:** `()` **Source:** `Read $_GET['dir']` **In** `admin/editor/php/upload_json.php:86`	SCA
admin/editor/php/upload_json .php:125	**Sink:** `builtin_echo()` **Enclosing Method:** `()` **Source:** `Read $_FILES['imgFile']['name']` **In** `admin/editor/php/upload_json.php:60`	SCA

[3] 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

[4] 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”。

Privacy Violation
Remediation Effort(Hrs): 0.3

Critical

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/connect.php :173	**Sink:** setcookie() **Enclosing Method:** esetcookie() **Source:** Read $password1 **from** make_password() **In** admin/ebak/class/functions.php:234	SCA
admin/ebak/class/connect.php :173	**Sink:** setcookie() **Enclosing Method:** esetcookie() **Source:** Read $password1 **from** make_password() **In** admin/ebak/class/functions.php:230	SCA
admin/ebak/class/functions.php:401	**Sink:** builtin_echo() **Enclosing Method:** ebak_dozip() **Source:** Read $password1 **from** make_password() **In** admin/ebak/class/functions.php:234	SCA
admin/ebak/class/functions.php:401	**Sink:** builtin_echo() **Enclosing Method:** ebak_dozip() **Source:** Read $password1 **from** make_password() **In** admin/ebak/class/functions.php:230	SCA

System Information Leak: External
Remediation Effort(Hrs): 0.1

Critical

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/eginfofun.php:247	**Sink:** phpinfo() **Enclosing Method:** eginfo_getzend() **Source:**	SCA

[5] 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

[6] CWE ID 089

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): 0.9***		**Critical**
Package: admin.ebak.class		
Location	**Analysis Info**	**Analyzer**
admin/ebak/class/db_sql.php:46	**Sink:** mysql_query() **Enclosing Method:** do_dosetdbchar() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA
admin/ebak/class/db_sql.php:46	**Sink:** mysql_query() **Enclosing Method:** do_dosetdbchar() **Source:** Read $_GET['collation'] **from** ebak_bakexet() **In** admin/ebak/class/functions.php:751	SCA
admin/ebak/class/db_sql.php:46	**Sink:** mysql_query() **Enclosing Method:** do_dosetdbchar() **Source:** Read $_GET['collation'] **from** ebak_bakexe() **In** admin/ebak/class/functions.php:581	SCA
admin/ebak/class/db_sql.php:46	**Sink:** mysql_query() **Enclosing Method:** do_dosetdbchar() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/db_sql.php:46	**Sink:** mysql_query() **Enclosing Method:** do_dosetdbchar() **Source:** Read $_POST **In** admin/ebak/phome.php:267	SCA
admin/ebak/class/db_sql.php:46	**Sink:** mysql_query() **Enclosing Method:** do_dosetdbchar() **Source:** Read $_POST **In** admin/ebak/phome.php:275	SCA
admin/ebak/class/db_sql.php:79	**Sink:** mysql_query() **Enclosing Method:** do_dbquery_common() **Source:** Read $_POST **In** admin/ebak/phome.php:309	SCA
admin/ebak/class/db_sql.php:79	**Sink:** mysql_query() **Enclosing Method:** do_dbquery_common() **Source:** Read $_POST **In** admin/ebak/phome.php:194	SCA
admin/ebak/class/db_sql.php:83	**Sink:** mysql_query() **Enclosing Method:** do_dbquery_common() **Source:** Read $_POST **In** admin/ebak/phome.php:309	SCA
admin/ebak/class/db_sql.php:83	**Sink:** mysql_query() **Enclosing Method:** do_dbquery_common() **Source:** Read $_POST **In** admin/ebak/phome.php:194	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** Read $_POST['tablename'] **In** admin/ebak/phome.php:235	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** Read $_POST['tablename'] **In** admin/ebak/phome.php:216	SCA

[6] CWE ID 089

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): 0.9***		**Critical**
Package: admin.ebak.class		
Location	**Analysis Info**	**Analyzer**
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** Read $_POST['tablename'] **In** admin/ebak/phome.php:198	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** Read $_POST['tablename'] **In** admin/ebak/phome.php:210	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** Read $_POST['tablename'] **In** admin/ebak/phome.php:204	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** Read $_POST['newtablepre'] **In** admin/ebak/phome.php:219	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** Read $_GET['auf'] **In** admin/ebak/phomebak.php:203	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** Read $_POST **In** admin/ebak/phome.php:275	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** Read $_POST **In** admin/ebak/phome.php:267	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** Read $_POST['mydbchar'] **In** admin/ebak/phome.php:230	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA
admin/ebak/class/db_sqli.php:47	**Sink:** mysqli_query() **Enclosing Method:** do_dosetdbchar() **Source:** Read $_POST **In** admin/ebak/phome.php:275	SCA
admin/ebak/class/db_sqli.php:47	**Sink:** mysqli_query() **Enclosing Method:** do_dosetdbchar() **Source:** Read $_POST **In** admin/ebak/phome.php:267	SCA

[6] CWE ID 089

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): 0.9***		**Critical**
Package: admin.ebak.class		
Location	**Analysis Info**	**Analyzer**
admin/ebak/class/db_sqli.php :47	**Sink:** mysqli_query() **Enclosing Method:** do_dosetdbchar() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA
admin/ebak/class/db_sqli.php :47	**Sink:** mysqli_query() **Enclosing Method:** do_dosetdbchar() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/db_sqli.php :47	**Sink:** mysqli_query() **Enclosing Method:** do_dosetdbchar() **Source:** Read $_GET['collation'] **from** ebak_bakexet() **In** admin/ebak/class/functions.php:751	SCA
admin/ebak/class/db_sqli.php :47	**Sink:** mysqli_query() **Enclosing Method:** do_dosetdbchar() **Source:** Read $_GET['collation'] **from** ebak_bakexe() **In** admin/ebak/class/functions.php:581	SCA
admin/ebak/class/db_sqli.php :87	**Sink:** mysqli_query() **Enclosing Method:** do_dbquery_common() **Source:** Read $_POST **In** admin/ebak/phome.php:194	SCA
admin/ebak/class/db_sqli.php :87	**Sink:** mysqli_query() **Enclosing Method:** do_dbquery_common() **Source:** Read $_POST **In** admin/ebak/phome.php:309	SCA
admin/ebak/class/db_sqli.php :91	**Sink:** mysqli_query() **Enclosing Method:** do_dbquery_common() **Source:** Read $_POST **In** admin/ebak/phome.php:194	SCA
admin/ebak/class/db_sqli.php :91	**Sink:** mysqli_query() **Enclosing Method:** do_dbquery_common() **Source:** Read $_POST **In** admin/ebak/phome.php:309	SCA
admin/ebak/class/db_sqli.php :123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** mysql_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sql.php:115	SCA
admin/ebak/class/db_sqli.php :123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** Read $_POST['tablename'] **In** admin/ebak/phome.php:198	SCA
admin/ebak/class/db_sqli.php :123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** Read $_POST['tablename'] **In** admin/ebak/phome.php:235	SCA
admin/ebak/class/db_sqli.php :123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** Read $_POST['tablename'] **In** admin/ebak/phome.php:204	SCA

[6] CWE ID 089

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): 0.9 — **Critical**

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/db_sqli.php:123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** Read $_POST['tablename'] **In** admin/ebak/phome.php:216	SCA
admin/ebak/class/db_sqli.php:123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** Read $_POST['tablename'] **In** admin/ebak/phome.php:210	SCA
admin/ebak/class/db_sqli.php:123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** Read $_POST['newtablepre'] **In** admin/ebak/phome.php:219	SCA
admin/ebak/class/db_sqli.php:123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** mysqli_query() **from** mysqlquery.query() **In** admin/ebak/class/db_sqli.php:123	SCA
admin/ebak/class/db_sqli.php:123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** Read $_GET['auf'] **In** admin/ebak/phomebak.php:203	SCA
admin/ebak/class/db_sqli.php:123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** Read $_POST **In** admin/ebak/phome.php:267	SCA
admin/ebak/class/db_sqli.php:123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** Read $_POST **In** admin/ebak/phome.php:275	SCA
admin/ebak/class/db_sqli.php:123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** Read $_POST['mydbchar'] **In** admin/ebak/phome.php:230	SCA

SQL Injection
Remediation Effort(Hrs): 0.2 — **High**

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/db_sql.php:115	**Sink:** mysql_query() **Enclosing Method:** query() **Source:** fread() **from** readfiletext() **In** admin/ebak/class/functions.php:266	SCA
admin/ebak/class/db_sqli.php:123	**Sink:** mysqli_query() **Enclosing Method:** query() **Source:** fread() **from** readfiletext() **In** admin/ebak/class/functions.php:266	SCA

[7] CWE ID 416

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

[10] CWE ID 022

CWE-22 用于识别“对受限目录的路径名进行不当限制 ('Path Traversal')”缺陷。

出现这些缺陷是因为“软件使用外部输入来构造用于识别位于受限制父级目录下的文件或目录的路径名称，但是软件无法对路径名称中的特殊元素进行妥善转义处理，使得路径名称解析为受限制目录之外的位置”。

Path Manipulation *Remediation Effort(Hrs): 2.3*	Critical

Package: admin

Location	Analysis Info	Analyzer
admin/admin_safe.php:94	**Sink:** `file_get_contents()` **Enclosing Method:** `()` **Source:** `Read $_GET['file']` **In** `admin/admin_safe.php:89`	SCA
admin/admin_safe.php:240	**Sink:** `file_get_contents()` **Enclosing Method:** `scan()` **Source:** `Read $_POST['path']` **In** `admin/admin_safe.php:153`	SCA

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/delpath.php:36	**Sink:** `unlink()` **Enclosing Method:** `wm_chief_file()` **Source:** `Read $_GET['path']` **In** `admin/ebak/phome.php:252`	SCA
admin/ebak/class/delpath.php:41	**Sink:** `rmdir()` **Enclosing Method:** `wm_chief_path()` **Source:** `Read $_GET['path']` **In** `admin/ebak/phome.php:252`	SCA
admin/ebak/class/eginfofun.php:214	**Sink:** `file()` **Enclosing Method:** `eginfo_testcj()` **Source:** `Read $_SERVER['HTTP_HOST']` **from** `eginfo_returndomain()` **In** `admin/ebak/class/eginfofun.php:270`	SCA
admin/ebak/class/eginfofun.php:214	**Sink:** `file()` **Enclosing Method:** `eginfo_testcj()` **Source:** `Read $_SERVER['PHP_SELF']` **from** `eginfo_returnhttppath()` **In** `admin/ebak/class/eginfofun.php:286`	SCA
admin/ebak/class/functions.php:260	**Sink:** `unlink()` **Enclosing Method:** `delfiletext()` **Source:** `Read $_GET` **In** `admin/ebak/phome.php:283`	SCA
admin/ebak/class/functions.php:260	**Sink:** `unlink()` **Enclosing Method:** `delfiletext()` **Source:** `Read $_GET['f']` **In** `admin/ebak/phome.php:257`	SCA
admin/ebak/class/functions.php:265	**Sink:** `fopen()` **Enclosing Method:** `readfiletext()` **Source:** `Read $_GET['mypath']` **In** `admin/ebak/phomebak.php:199`	SCA
admin/ebak/class/functions.php:265	**Sink:** `fopen()` **Enclosing Method:** `readfiletext()` **Source:** `Read $_GET['mypath']` **In** `admin/ebak/phomebak.php:187`	SCA

[10] CWE ID 022

CWE-22 用于识别“对受限目录的路径名进行不当限制 ('Path Traversal')”缺陷。

出现这些缺陷是因为“软件使用外部输入来构造用于识别位于受限制父级目录下的文件或目录的路径名称，但是软件无法对路径名称中的特殊元素进行妥善转义处理，使得路径名称解析为受限制目录之外的位置”。

Path Manipulation
Remediation Effort(Hrs): 2.3 | **Critical**

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/functions.php:265	**Sink:** fopen() **Enclosing Method:** readfiletext() **Source:** Read $_POST **In** admin/ebak/phome.php:301	SCA
admin/ebak/class/functions.php:290	**Sink:** fopen() **Enclosing Method:** writefiletext_n() **Source:** Read $_POST **In** admin/ebak/phomebak.php:180	SCA
admin/ebak/class/functions.php:290	**Sink:** fopen() **Enclosing Method:** writefiletext_n() **Source:** Read $_GET['mypath'] **In** admin/ebak/phomebak.php:199	SCA
admin/ebak/class/functions.php:290	**Sink:** fopen() **Enclosing Method:** writefiletext_n() **Source:** Read $_GET['mypath'] **In** admin/ebak/phomebak.php:187	SCA
admin/ebak/class/functions.php:290	**Sink:** fopen() **Enclosing Method:** writefiletext_n() **Source:** Read $_POST **In** admin/ebak/phome.php:279	SCA
admin/ebak/class/functions.php:290	**Sink:** fopen() **Enclosing Method:** writefiletext_n() **Source:** Read $_POST **In** admin/ebak/phome.php:301	SCA
admin/ebak/class/functions.php:295	**Sink:** chmod() **Enclosing Method:** writefiletext_n() **Source:** Read $_POST **In** admin/ebak/phomebak.php:180	SCA
admin/ebak/class/functions.php:295	**Sink:** chmod() **Enclosing Method:** writefiletext_n() **Source:** Read $_GET['mypath'] **In** admin/ebak/phomebak.php:187	SCA
admin/ebak/class/functions.php:295	**Sink:** chmod() **Enclosing Method:** writefiletext_n() **Source:** Read $_GET['mypath'] **In** admin/ebak/phomebak.php:199	SCA
admin/ebak/class/functions.php:295	**Sink:** chmod() **Enclosing Method:** writefiletext_n() **Source:** Read $_POST **In** admin/ebak/phome.php:301	SCA
admin/ebak/class/functions.php:295	**Sink:** chmod() **Enclosing Method:** writefiletext_n() **Source:** Read $_POST **In** admin/ebak/phome.php:279	SCA
admin/ebak/class/functions.php:314	**Sink:** mkdir() **Enclosing Method:** domkdir() **Source:** Read $_POST **In** admin/ebak/phomebak.php:180	SCA

[10] CWE ID 022

CWE-22 用于识别“对受限目录的路径名进行不当限制 ('Path Traversal')”缺陷。

出现这些缺陷是因为“软件使用外部输入来构造用于识别位于受限制父级目录下的文件或目录的路径名称，但是软件无法对路径名称中的特殊元素进行妥善转义处理，使得路径名称解析为受限制目录之外的位置”。

Path Manipulation ***Remediation Effort(Hrs): 2.3***	**Critical**

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/functions.php:316	**Sink:** chmod() **Enclosing Method:** domkdir() **Source:** Read $_POST **In** admin/ebak/phomebak.php:180	SCA
admin/ebak/class/phpzip.inc.php:28	**Sink:** fopen() **Enclosing Method:** zip() **Source:** Read $_GET['p'] **In** admin/ebak/phome.php:262	SCA
admin/ebak/class/phpzip.inc.php:39	**Sink:** fopen() **Enclosing Method:** zip() **Source:** Read $_GET['p'] **In** admin/ebak/phome.php:262	SCA

Package: admin.editor.php

Location	Analysis Info	Analyzer
admin/editor/php/file_manager_json.php:28	**Sink:** mkdir() **Enclosing Method:** () **Source:** Read $_GET['dir'] **In** admin/editor/php/file_manager_json.php:19	SCA
admin/editor/php/upload_json.php:104	**Sink:** mkdir() **Enclosing Method:** () **Source:** Read $_GET['dir'] **In** admin/editor/php/upload_json.php:86	SCA
admin/editor/php/upload_json.php:111	**Sink:** mkdir() **Enclosing Method:** () **Source:** Read $_GET['dir'] **In** admin/editor/php/upload_json.php:86	SCA
admin/editor/php/upload_json.php:117	**Sink:** move_uploaded_file() **Enclosing Method:** () **Source:** Read $_FILES['imgFile']['name'] **In** admin/editor/php/upload_json.php:60	SCA
admin/editor/php/upload_json.php:117	**Sink:** move_uploaded_file() **Enclosing Method:** () **Source:** Read $_GET['dir'] **In** admin/editor/php/upload_json.php:86	SCA
admin/editor/php/upload_json.php:120	**Sink:** chmod() **Enclosing Method:** () **Source:** Read $_FILES['imgFile']['name'] **In** admin/editor/php/upload_json.php:60	SCA
admin/editor/php/upload_json.php:120	**Sink:** chmod() **Enclosing Method:** () **Source:** Read $_GET['dir'] **In** admin/editor/php/upload_json.php:86	SCA

[11] CWE ID 078

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”。

No Issues

[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

[13] CWE ID 287

CWE-287 用于识别“不正确的身份验证”缺陷。

出现这些缺陷是因为“在操作者宣称拥有给定身份时，软件无法或不能充分证明此声明是正确的”。

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

Package: admin

Location	Analysis Info	Analyzer

admin/admin_safe.php:32	`Sink: FieldAccess: $password`
	`Enclosing Method: ()`
	`Source:`
		SCA

Password Management: Empty Password ***Remediation Effort(Hrs): 0.5***	**High**

Package: admin.ebak.class

Location	Analysis Info	Analyzer

admin/ebak/class/combakfun.php:184	`Sink: ArrayAccess: $add`
	`Enclosing Method: ebak_setdb()`
	`Source:`
		SCA

admin/ebak/class/connect.php:25	`Sink: FieldAccess: $phome_db_password`
	`Enclosing Method: ()`
	`Source:`
		SCA

admin/ebak/class/connect.php:63	`Sink: FieldAccess: $defphome_db_password`
	`Enclosing Method: ()`
	`Source:`
		SCA

Package: data

Location	Analysis Info	Analyzer

data/config.user.inc.php:18	`Sink: FieldAccess: $cfg_smtp_password`
	`Enclosing Method: ()`
	`Source:`
		SCA

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 0.3***	**High**

Package: admin.ebak.class

Location	Analysis Info	Analyzer

admin/ebak/class/config.php:24	`Sink: FieldAccess: $set_password`
	`Enclosing Method: ()`
	`Source:`
		SCA

Package: admin.ebak.lang.gbutf8.pub

Location	Analysis Info	Analyzer

admin/ebak/lang/gbutf8/pub/m.php:62	`Sink: ArrayAccess`
	`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

[15] CWE ID 732

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

[18] CWE ID 094

CWE-94 用于识别“对代码生成进行不当控制 ('Code 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代码片段，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代码片段的语法或行为的特殊元素”。

Dangerous File Inclusion *Remediation Effort(Hrs): 0.5*	Critical

Package: admin.ebak

Location	Analysis Info	Analyzer
admin/ebak/ChangeTable.php:224	**Sink:** builtin_include() **Enclosing Method:** () **Source:** Read $_GET['savefilename'] **In** admin/ebak/ChangeTable.php:214	SCA

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/functions.php:537	**Sink:** builtin_include() **Enclosing Method:** ebak_bakexe() **Source:** Read $_GET['mypath'] **In** admin/ebak/phomebak.php:187	SCA
admin/ebak/class/functions.php:707	**Sink:** builtin_include() **Enclosing Method:** ebak_bakexet() **Source:** Read $_GET['mypath'] **In** admin/ebak/phomebak.php:199	SCA
admin/ebak/class/functions.php:1175	**Sink:** builtin_include() **Enclosing Method:** ebak_redata() **Source:** Read $_POST['mypath'] **In** admin/ebak/phomebak.php:211	SCA
admin/ebak/class/functions.php:1321	**Sink:** builtin_include() **Enclosing Method:** ebak_setgotobak() **Source:** Read $_GET['savename'] **In** admin/ebak/phome.php:287	SCA
admin/ebak/class/functions.php:1338	**Sink:** builtin_include() **Enclosing Method:** ebak_pathgotoredata() **Source:** Read $_GET['mypath'] **In** admin/ebak/phome.php:292	SCA

Dynamic Code Evaluation: Code Injection *Remediation Effort(Hrs): 0.2*	Critical

Package: admin.editor

Location	Analysis Info	Analyzer
admin/editor/kindeditor-min.js:2	**Sink:** environment~object.eval() **Enclosing Method:** _json() **Source:** Read f.responseText **from** onreadystatechange() **In** admin/editor/kindeditor-min.js:2	SCA

[18] CWE ID 094

CWE-94 用于识别“对代码生成进行不当控制 ('Code 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代码片段，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代码片段的语法或行为的特殊元素”。

Dynamic Code Evaluation: Code Injection ***Remediation Effort(Hrs): 0.2***		**High**
Package: admin.editor		
Location	**Analysis Info**	**Analyzer**
admin/editor/kindeditor-min.js:2	**Sink:** `environment~object.eval()` **Enclosing Method:** `_json()` **Source:** `Read f.responseText` **from** `onreadystatechange()` **In** `admin/editor/kindeditor-min.js:2`	SCA

[19] CWE ID 798

CWE-798 用于识别“使用硬编码凭证”缺陷。

出现这些缺陷是因为“软件包含硬编码凭证，例如密码或加密密钥，用于自身的入站验证、外部组件的出站通信或者内部数据的加密”。

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

Package: admin

Location	Analysis Info	Analyzer
admin/admin_safe.php:32	**Sink:** FieldAccess: $password **Enclosing Method:** () **Source:**	SCA

Password Management: Empty Password ***Remediation Effort(Hrs): 0.5***	**High**

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/combakfun.php:184	**Sink:** ArrayAccess: $add **Enclosing Method:** ebak_setdb() **Source:**	SCA
admin/ebak/class/connect.php:25	**Sink:** FieldAccess: $phome_db_password **Enclosing Method:** () **Source:**	SCA
admin/ebak/class/connect.php:63	**Sink:** FieldAccess: $defphome_db_password **Enclosing Method:** () **Source:**	SCA

Package: data

Location	Analysis Info	Analyzer
data/config.user.inc.php:18	**Sink:** FieldAccess: $cfg_smtp_password **Enclosing Method:** () **Source:**	SCA

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 0.3***	**High**

Package: admin.ebak.class

Location	Analysis Info	Analyzer
admin/ebak/class/config.php:24	**Sink:** FieldAccess: $set_password **Enclosing Method:** () **Source:**	SCA

Package: admin.ebak.lang.gbutf8.pub

Location	Analysis Info	Analyzer
admin/ebak/lang/gbutf8/pub/m.php:62	**Sink:** ArrayAccess **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

[22] CWE ID 426

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

[23] CWE ID 502

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): 0.2***		**High**
Package: admin		
Location	**Analysis Info**	**Analyzer**
admin/admin_safe.php:277	**Sink:** `unserialize()` **Enclosing Method:** `getsetting()` **Source:** `Read $_COOKIE['t00ls_s']` **from** `getsetting( )` **In** `admin/admin_safe.php:277`	SCA

[24] CWE ID 269

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

Description of Key Terminology

Likelihood and Impact

Likelihood
Likelihood is the probability that a vulnerability will be accurately identified and successfully exploited.

Impact
Impact is the potential damage an attacker could do to assets by successfully exploiting a vulnerability. This damage can be in the form of, but not limited to, financial loss, compliance violation, loss of brand reputation, and negative publicity.

Fortify Priority Order

Critical
Critical-priority issues have high impact and high likelihood. Critical-priority issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to the application. As such, they should be remediated immediately.

SQL Injection is an example of a critical issue.

High
High-priority issues have high impact and low likelihood. High-priority issues are often difficult to detect and exploit, but can result in large asset damage. These issues represent a high security risk to the application. High-priority issues should be remediated in the next scheduled patch release.

Password Management: Hardcoded Password is an example of a high issue.

Medium
Medium-priority issues have low impact and high likelihood. Medium-priority issues are easy to detect and exploit, but typically result in small asset damage. These issues represent a moderate security risk to the application. Medium-priority issues should be remediated in the next scheduled product update.

Path Manipulation is an example of a medium issue.

Low
Low-priority issues have low impact and low likelihood. Low-priority issues can be difficult to detect and exploit and typically result in small asset damage. These issues represent a minor security risk to the application. Low-priority issues should be remediated as time allows.

Dead Code is an example of a low issue.

Remediation Effort

The report provides remediation effort estimates. You can use these estimates to perform a relative comparison of projects and as a starting point for estimates specific to your organization. Remediation effort estimates are provided in the following report sections:

- Executive Summary
- Issue Breakdown
- Issue Details

To determine remediation effort for a collection of issues, Software Security Center weights each issue based on its category (“remediation constant”) and adds an overhead calculation based on the number of distinct files which contain the set of issues. The formula used at each report level is the same:

- Remediation Effort (in mins) = SUM(remediation constant for each issue in the set) + 6 * Number of distinct files in that set of issues.

At the lowest level of detail, issues are grouped based on Fortify category and Fortify priority OR Fortify category and folder name, depending on report options. So, for example, the Issue Details section of the report might show the remediation effort for “SQL Injection, Critical” or “SQL Injection, MyFolder”.

At the Issue Breakdown level, remediation effort is shown at the level of each external (non-Fortify) category (such as “AC-3 Access Enforcement” in the case of NIST, or “A1 Unvalidated Input” in the case of OWASP Top10). Remediation effort is calculated for the set of all issues that fall into that external category (irrespective of Fortify priority or folder name). As an example, if there are two SQL injection vulnerabilities, one critical and one medium, within the same file, the file overhead is only included once.

At the Executive Summary level, all issues of that project which are mapped to the specified external category list (such as NIST or CWE) are used in the remediation effort calculation.

Fortify recommends that you treat the different levels of remediation effort as information relevant at that level only. You cannot add up remediation effort at a lower level and expect it to match the remediation effort at a higher level.

About Fortify Solutions

Fortify is the leader in end-to-end application security solutions with the flexibility of testing on-premise and on-demand to cover the entire software development lifecycle. Learn more at www.microfocus.com/solutions/application-security.