

RIPS

下载+安装

安装解析 PHP 文件的本地网络服务器（如果您开发 PHP 应用程序应该已经可用）。[在此处](#)下载最新版本。将所有文件提取到本地网络服务器文档根目录（例如/var/www/rips/）转到<http://localhost/rips/>并开始扫描。

- subdirs：扫描所有子目录。
- verbosity level：选择扫描结果的详细程度，缺省为1(建议就使用1)。
- vuln type：选择需要扫描的漏洞类型。支持命令注入、代码执行、SQL注入等十余种漏洞类型，缺省为全部扫描。
- code style：选择扫描结果的显示风格（支持9种语法高亮）。
- /regex/：使用正则表达式过滤结果。

输入目录后可以查看扫描结果

路径/文件: C:\phpstudy_pro\Vulnerable-Web-Application

详细程度: 1. 仅受污染的用户

漏洞类型: 全部

扫描

代码风格: 艾蒂

自下而上

/正则表达式/

搜索

子目录

视图

文件

用户输入

统计数

职能

RIPS

0.55

文件: C:\phpstudy_pro\Vulnerable-Web-Application\CommandInjection\command_injection.php

跨站脚本

用户输入到达敏感接收器。 如需更多信息, 请按左侧的帮助图标。

25: 回声 回声 shell_exec (['用户名']) ;

要求: 24: if (isset (\$_GET ['用户名']))

命令执行

用户输入到达敏感接收器。 如需更多信息, 请按左侧的帮助图标。

25: shell_exec 回 显 shell_exec (\$_GET ['用户名']) ;

要求: 24: if (isset (\$_GET ['用户名']))

全部藏起来

文件: C:\phpstudy_pro\Vulnerable-Web-Application\CommandInjection\command_injection.php

跨站脚本

用户输入到达敏感接收器。 如需更多信息, 请按左侧的帮助图标。

25: 回声 回声 shell_exec (目标) ;

结果

命令执行: 4

文件包含: 4

文件操作: 3

SQL注入: 5

跨站脚本: 19

和: 35

扫描文件: 28

包括成功: 0/4 (0%)

考虑的水槽: 298

用户自定义函数: 3

独特来源: 12

敏感水槽: 148

信息: 检测到 phpinfo()

信息: 使用 DBMS MySQL、MySQL 扩展

Execution/C/ 获得下一代 撕裂.php

使用最先进的代码分析!

扫描时间: 2.523 秒

点击右上角 user input 可以查看web输入

files

user input

stats

functions

x

user input

x

type[parameter]

t:

\$_COOKIE

6

\$_COOKIE[id]

3

\$_COOKIE[security]

2

\$_FILES[uploaded]

9

\$_GET

6

\$_GET[1]

2

\$_GET[Change]

3

\$_GET[Login]

3

\$_GET[Submit]

3

\$_GET[callback]

5

\$_GET[clear_log]

4

\$_GET[default]

4

\$_GET[1+1]

2

(98%)



ions

ror

se

level=debug