AWVS AcuSensor 功能分析

Auth : Cryin’
Date : 2016.05.08

AcuSensor

AcuSensor 是 Acunetix Web Vulnerability Scanner 推出的基于交互式应用安全检测(IAST)技术的 Web 漏洞扫描功能，目前支持.net、php 两种语言站点，根据目标站点可以分别配置生成 agent 端。

其中.net 程序的 agent 端是一个客户端 setup 程序，需要在 web 服务器上安装并配置 iis、站点目录等。

php 程序的 agent 是一个 php 文件(配置生存的 php 代码经过混淆),php 文件需要上传至 web 服务器并配置 php.ini 文件 auto_prepend_file 字段,该字段功能是将该 php 文件加入网站文件页眉中。

agent 原理及实现分析

AcuSensor 的 agent 主要作用是对 php 关键函数 SQL_Query、File_Open、Sys_Command、Create_Function、Delete_File 等进行监控。当这些函数执行将参数及相关信息 echo 到 response body 中供扫描器分析。Agent 代码功能及流程如下:

1、判断 http header 字段是否存在及密码正确性，从而执行 agent，直接访问 agent 页面返回 404;

2、根据 Acunetix-Aspect-Queries 字段判断特定任务类型：aspectalerts、filelist 两种，无 Acunetix-Aspect-Queries 则执行一般的 IAST 任务:

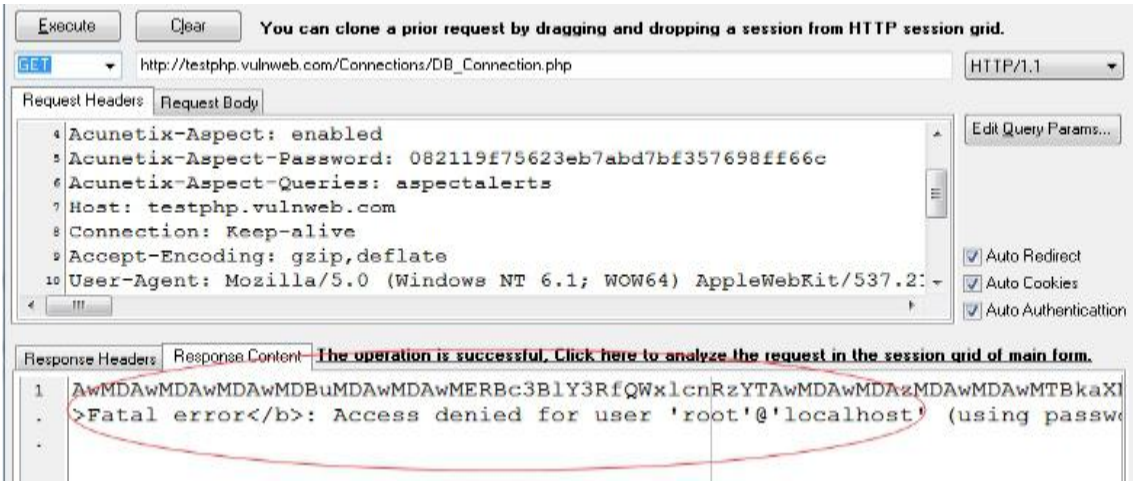
1）aspectalerts：php config 信息等

2）filelist：该页面文件所在目录的所有的文件列表信息

3、判断 HTTP_ACUNETIX_ASPECT 状态是否为 enable,并检查 HTTP_ACUNETIX_ASPECT_PASSWORD 字段是否和预设 password 相同。password 编码后保存在 agent 文件末尾;

4、使用 set_error_handler 函数设置一个用户定义的错误处理函数。根据不同的错误类型在响应内容中 echo 错误信息：

```
switch ($_AAS38) {
    case E_USER_ERROR:
    case E_RECOVERABLE_ERROR:
    case E_ERROR:
        echo "<b>Fatal error</b>: $_AAS39 in <b>" . $_ENV['_AAS29'] . "</b> on line <b>$_AAS41</b><br />\n";
        break;
```



5、使用 token_get_all 将访问的 php 文件源代码进行解析，对 class、函数、参数、注释、T_VARIABLE 等各种字段进行处理并保存在临时文件当中；

6、对于临时文件中需要监控的函数则替换为自定义函数，自定义函数中再调用监控函数。然后执行临时 php 文件；

7、 使用 debug_backtrace 跟踪 php 程序执行的 bug 信息，获取当前函数、class、args、object、line、file 信息，如图：

PHP debug_backtrace() 函数生成一个 backtrace。

该函数返回一个关联数组。下面是可能返回的元素：

名称	类型	描述
function	字符串	当前的函数名。
line	整数	当前的行号。
file	字符串	当前的文件名。
class	字符串	当前的类名
object	对象	当前对象。
type	字符串	当前的调用类型，可能的调用： • 返回: "->" - 方法调用 • 返回: "::" - 静态方法调用 • 返回 nothing - 函数调用
args	数组	如果在函数中，列出函数参数。如果在被引用的文件中，列出被引用的文件名。

8、对于返回的信息进行格式化，如：

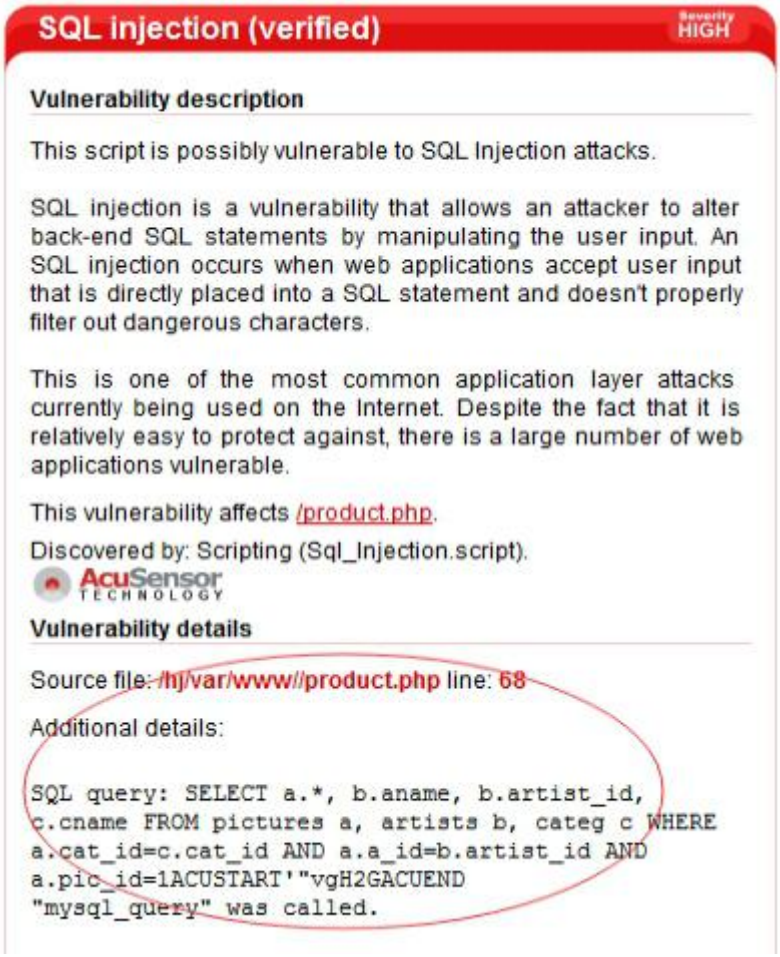
00000010PHP_File_Includes00000014database_connect.php00000018/hj/var/www//product.php00000001s0000001A"require_once" was called.

其中 00000010 为 16 进制，表示后面数据的长度，该串数字后可能出现""、"s"、"n"、"a"，分别标识 16 进制数后面的数据是 string、null、array 类型。

AcuSensor 漏洞检测原理

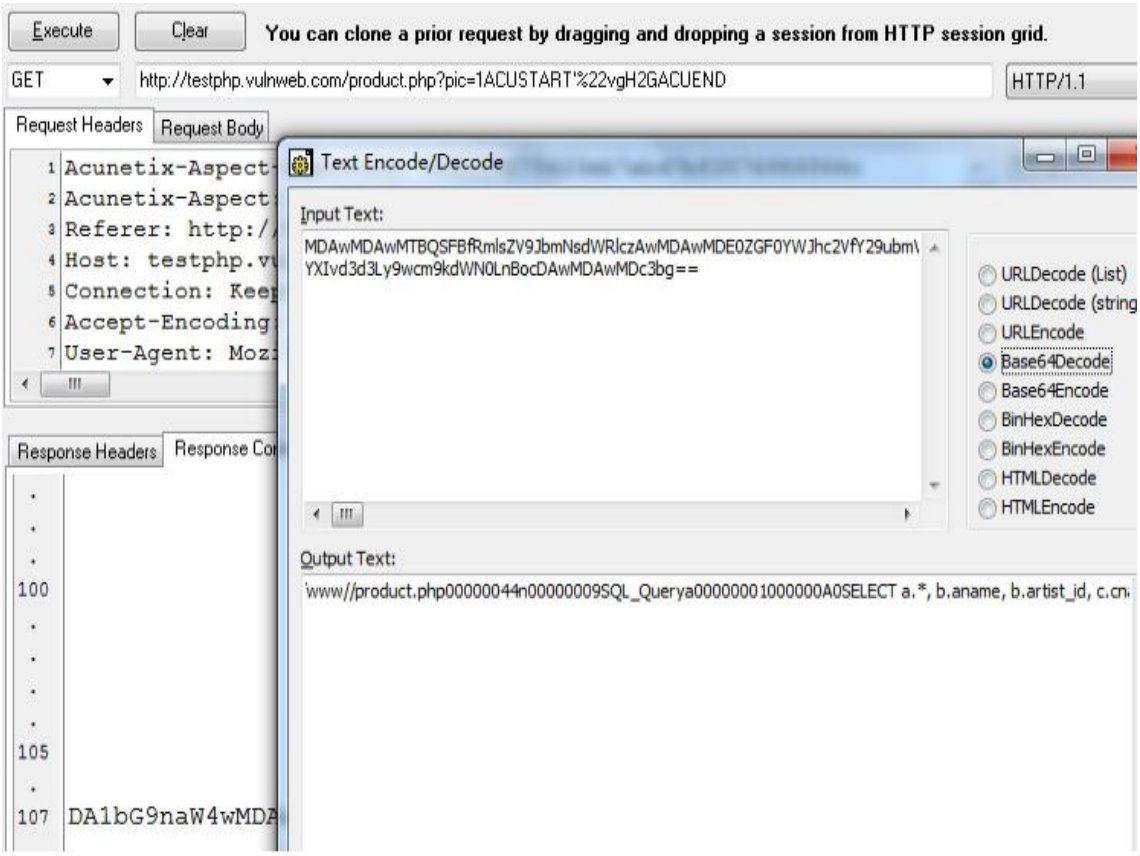
SQL injection 漏洞实例

AcuSensor 在扫描到 sql 注入时会根据 Agent 返回的信息判断漏洞是否真实存在，如真实存在则标注 verified，并给出具体漏洞 php 文件、漏洞产生的对应代码行数



SQL injection 漏洞数据包分析

AcuSensor Agent 将监控到的漏洞信息通过 base64 编码返回到相应消息中，扫描器获取数据得到漏洞详细信息。如图:


Execute
Clear
You can clone a prior request by dragging and dropping a session from HTTP session grid.
GET
http://testphp.vulnweb.com/product.php?pic=1ACUSTART'%22vgH2GACUEND
HTTP/1.1
Request Headers
Request Body
Acunetix-Aspect
Acunetix-Aspect
Referer: http:/
Host: testphp.v
Connection: Kee
Accept-Encoding
User-Agent: Moz
Response Headers
Response Co
100
105
107
DA1bG9naW4wMDA
Text Encode/Decode
Input Text:
MDAwMDAwMTBQSFBfRmlsZV9JbmNsdWRlczAwMDAwMDE0ZGF0YWJhc2VfY29ubm\
YXIvd3d3Ly9wcm9kdWN0LnBocDAwMDAwMDc3bg==
URLDecode (List)
URLDecode (string
URLEncode
Base64Decode
Base64Encode
BinHexDecode
BinHexEncode
HTMLDecode
HTMLEncode
Output Text:
'www//product.php00000044n00000009SQL_Querya00000001000000A0SELECT a.*, b.aname, b.artist_id, c.cn