Ant web application system

使用指导手册

Version:v1.0
Powered by：hanlu
Email:317096829@qq.com

“Ant”系统概述

Ant web application system 是一个带有漏洞的web应用系统，这里面包含了常见的web安全漏洞。

“Ant”的主要目的是帮助渗透测试学习人员在安全的环境里面对web安全漏洞进行学习。

Ant的代码是开源的，你可以在：

https://github.com/zhuifengshaonianhanlu/ant-web-application-system

下载安装包（源代码）。

“Ant”系统介绍-漏洞列表

- Burt Force(暴力破解漏洞)
- XSS(跨站脚本漏洞)
- CSRF(跨站请求伪造)
- SQL-Inject(SQL注入漏洞)
- Sys-Command-Inject(系统命令注入漏洞)
- Files Inclusion(文件包含漏洞)
- Unsafe file downloads(不安全的文件下载漏洞)
- Unsafe file uploads(不安全的文件上传漏洞)
- Over Permisson(越权漏洞)
- ../../../(目录遍历)
- I can see your ABC(敏感信息泄露)
- More...(找找看?..有彩蛋!)

“Ant” -安装指导

Ant web application system是在php+mysql下开发的，因此要运行ant你需要提前安装好“php+mysql+中间件”的环境。
建议在你的测试环境直接使用 **XAMPP**或者**wampserver**来搭建你的基础环境。

XAMPP和WAMPSERVER都是包含了“PHP+MYSQL+APache”的集成软件。
你可以直接通过搜索引擎找到它们并下载安装。

XAMPP中文站点：http://www.xampps.com/（新版本的XAMPP使用MariaDB代替了MYSQL，但由于MariaDB基本兼容MYSQL所以使用MariaDB的XAMPP也可以正常的运行Ant）
WAMPSERVER站点：http://www.wampserver.com/en/

“Ant”-安装指导 for windows

Windows下安装步骤：

1.下载“XAMPP”,并安装，并通过其控制面板开启“mysql” “apache”服务；

2.下载Ant源码包，解压，并建议重命名为“ant”,拷贝到xampp的站点根目录xampp\htdocs下;

3.浏览器访问：http://127.0.0.1/ant/即可打开首页，首次访问会提示“需要初始化”

4.点击“初始化”进入install初始化界面;

5.打开inc/config.inc.php文件对数据库连接参数进行配置：

```
define('DBHOST', 'localhost');//将localhost修改为数据库服务器的地址
define('DBUSER', 'root');//将root修改为连接mysql的用户名
define('DBPW', 'root');//将root修改为连接mysql的密码
define('DBNAME', 'ant');//自定义，建议不修改
define('DBPORT', '3306');//将3306修改为mysql的连接端口，默认tcp3306
```

6.修改完配置文件后，点击“安装/初始化”按钮，开始自动安装

7.提示安装成功，即可以成功访问，如果提示失败，请根据提示信息进行对应的处理。

“Ant”-安装指导 for Linux

Linux下安装步骤：

1.使用: wget https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/5.6.14/下载5.6.14版本的XAMPP

下载下来的文件为：xampp5.6.14.run(你也可以下载当前最新的版本)

2.安装命令：./xampp5.6.14.run　默认的目录为/opt/lampp下

3.下载Ant源码包，解压，并建议重命名为“ant”,拷贝到/opt/lampp/htdocs下;

4.浏览器访问：http://127.0.0.1/ant/即可打开首页，首次访问会提示“需要初始化”

5.点击“初始化”进入install初始化界面;

6.打开inc/config.inc.php文件对数据库连接参数进行配置：

```
define('DBHOST', 'localhost');//将localhost修改为数据库服务器的地址
define('DBUSER', 'root');//将root修改为连接mysql的用户名
define('DBPW', 'root');//将root修改为连接mysql的密码
define('DBNAME', 'ant');//自定义，建议不修改
define('DBPORT', '3306');//将3306修改为mysql的连接端口，默认tcp3306
```

7.修改完配置文件后，点击“安装/初始化”按钮，开始自动安装

8.提示安装成功，即可以成功访问，如果提示失败，请根据提示信息进行对应的处理。

“Ant” -使用指导

通过首页的漏洞列表，你可以进入你需要练习的项目：

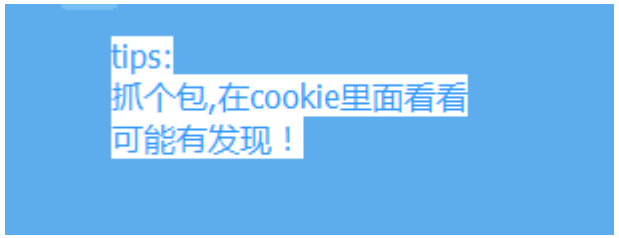
Vulnerability List :

Burt force	Cross-Site Scripting	Cross-site request forgery	SQL-Inject
Sys-Command-Inject	File Inclusion	Unsafe file downloads	Unsafe file uploads
Over permission	../../../	I can see your ABC	More...

“Ant” -使用指导

在漏洞项目页，你可以通过左边栏目来了解该漏洞的概述以及进行该项目对应的练习

如果你对这个栏目没有头绪，你可以选择右边空白处，会有小提示
或者直接ctrl+a全选页面也可以看到



具体的项目测试方法和原理，就留给大家自行测试吧!

谢 谢

在Ant项目的测试过程中，你可能会遇到一些问题

欢迎加入Ant-web安全学习群（群号：558531827,或扫描上面二维码）,和大家一起交流。

如果你对Ant有什么建议，也欢迎发邮件给317096829@qq.com