phpMyXSS 的设计与实现

摘要：本文主要介绍 phpMyXSS 从设计到实现的过程，文章也将对源码中一些比较不好理解的地方和各个文件的作用做出解释。phpMyXSS 也算是 XSS 利用平台这“车轮”中的其中一个，但我相信这一平台和其它 XSS 利用平台比较起来必有些标新立异的地方。设计的初衷还是看到了 Beef 中强大的在线主机管理，但是 Beef 的安装和使用却补容易，所以索性做个轻量级的 Beef，再加上常用 XSS 平台的功能，便有了现在的 phpMyXSS。phpMyXSS 相比于常见的 XSS 利用平台主要是多了一个在线主机管理还有利用模块数量的增加。phpMyXSS 不管在程序代码/文件结构还是 UI 上都下了一番功夫的，界面采用自适应网页设计，文件结构和代码结构部分参考了 WordPress 还有多个 XSS 平台的源码。现在 phpMyXSS 基本能在手机、电脑和平板上实现通用，由于时间仓促，前端的只保证了对 Google Chrome 和 Mozilla Firefox 的兼容，所以使用上为了保证流畅性不管在手机、平板还是电脑上请都尽量使用这两款浏览器。还有感谢精弘网络技术部各位同学长期来对作者各项软硬件上的支持。

关键词：phpMyXSS、XSS、利用、平台

第一章　引言

1.1 开发背景

在 2013 年 OWASP（开放式 Web 应用程序安全项目）所统计的所有安全威胁中，XSS(跨站脚本攻击)排名第三，而 CSRF(跨站请求伪造)的排名也逐年上升，这两个是网站网页应用中常见的漏洞，造成的危害更是不容小觑。为了更方便地进行黑盒等各种测试，就需要一款强大的漏洞利用的测试框架。这不仅可以在在安全测试方面大大减少安全工作人员的工作量，在调查或者追踪网络犯罪方面也能发挥巨大的作用。也为网络安全的检测提供更加丰富且易于上手的方法。

1.2 意义及现状

跨站脚本（Cross-site scripting，因为 CSS 在网页设计领域已经被广泛指层叠样式表 Cascading Style Sheets，所以将 Cross 改以发音相近的 X 做为缩写。通常简称为 XSS 或跨站脚本或跨站脚本攻击）是一种网站应用程序的安全漏洞攻击，是代码注入的一种。它允许恶意用户将代码注入到网页上，其他用户在观看网页时就会受到影响。这类攻击通常包含了 HTML 以及用户端脚本语言。XSS 攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是 JavaScript，但实际上也可以包括 Java， VBScript， ActiveX， Flash 或者甚至是普通的 HTML。攻击成功后，攻击者可能得到包括但不限于更高的权限（如执行一些操作）、私密网页内容、会话和 cookie 等各种内容。
JavaScript 语言刚推出时，人们也察觉到准许网页服务器传送可运行的代码给一个浏览器的安全风险（即使仅是在一个浏览器的沙盒里）。它所造成的一个关键的问题在于用户同时打开多个浏览器视窗时，在某些例子里，网页里的片断代码被允许从另一个网页或对象取出数据，而因为恶意的网站可以用这个方法来尝试窃取机密信息，所以在某些情形，这应是完全

被禁止的。为了解决这个问题，浏览器采用了同源决策——仅允许来自相同域名系统和使用相同协议的对象与网页之间的任何交互。这样一来，恶意的网站便无法借由 JavaScript 在另一个浏览器窃取机密数据。此后，为了保护用户免受恶意的危害，其他的浏览器与服务端指令语言采用了类似的访问控制决策。
XSS 漏洞可以追溯到 1990 年代。大量的网站曾遭受 XSS 漏洞攻击或被发现此类漏洞，如 Twitter ，Facebook，MySpace ，Orku ,新浪微博和百度贴吧 。研究表明，最近几年 XSS 已经超过缓冲区溢出成为最流行的攻击方式，有 68%的网站可能遭受此类攻击。
然而以前对跨站脚本的检查与测试却不是那么容易，安全人员需要编写大量的代码才能实现理想的功能，因此后来出现了 XSS 安全测试平台。类似于一个代码库，提供各种较完善的安全测试脚本以及模块，方便安全人员进行调用测试。
国外比较知名的 XSS 安全测试平台有 Xenotix XSS Exploit Framework、XSS ChEF、BeEF 等。BeEF 侧重于利用浏览器的漏洞，以评估目标的安全状态。该项目由 BeEF 团队独家开发用作合法的安全渗透测试研究。它能够连接一个或多个浏览器作为利用它们作为滩头阵地发动指挥命令模块，并从浏览器框架内进一步对系统的安全性进行测试。
而在国内，XSS 安全测试平台流行于 2012 出现于乌云漏洞报告平台的 XSS Platform，本人也有幸成为第一批的试用用户，亲身了解并体会了许多 WEB 应用的脆弱和安全问题，漏洞危害巨大。而在此期间，也出现了 xssing，xssf 等测试平台。然而国内的平台更多是专注于 COOKIE 的获取与劫持，对于其它浏览器命令执行,HTTP 请求记录等方面缺乏足够的支持。国外的平台操作繁琐,可参考的中文文档少,更多的是直接在 PC 端,不带上电脑就难以对程序进行操作。
CSRF（Cross-site request forgery 跨站请求伪造，也被称为“one click attack”或者 session riding，通常缩写为 CSRF 或者 XSRF，是一种对网站的恶意利用。尽管听起来像跨站脚本（XSS），但它与 XSS 非常不同左。XSS 利用站点内的信任用户，而 CSRF 则通过伪装来自受信任用户的请求来利用受信任的网站。与 XSS 攻击相比，CSRF 攻击往往不大流行（因此对其进行防范的资源也相当稀少）和难以防范，所以被认为比 XSS 更具危险性。理所当然，phpMyXSS 也通过模块结合了 CSRF 的功能。

1.3 设计目标

开发一套较为成熟的 web 安全测试框架，集成 XSSPlatform 与 BeEF、CSRF，添加 HTTPRequest 跟踪分析，伪造图片，自定义模块，访问统计分析等功能，为信息安全领域的安全工程师提供一套更加完善并易于上手的 Web 安全测试平台，增加网络安全，减少网络安全事故的发生。

第二章　开发环境、工具及编程语言

2.1 开发环境

2.1.1 Ubuntu 14.04 LTS (Trusty Tahr) (Linux version 3.13.0-36-generic)

Ubuntu 是一个以桌面应用为主的 GNU/Linux 操作系统。Ubuntu 的目标在于为一般用户提供一个最新同时又相当稳定，主要以自由软件建构而成的操作系统。Ubuntu 目前具有庞大的社群力量支持，用户可以方便地从社群获得帮助。
Ubuntu 计划强调易用性和国际化，以便能为尽可能多的人所用。在发布 5.04 版时，Ubuntu 就已经把万国码（UTF-8 Unicode）作为系统默认编码，用以应对各国各地区不同的语言文字，试图给用户提供一个无乱码的交流平台。它在语言支持方面，算是 Linux 发布版中相当好的。
我们选择 Ubuntu 的主要原因还是因为 Ubuntu 完善的套件管理。Ubuntu 的套件管理系统与 Debian 的类似，所有软件分为 main、restricted、universe 和 multiverse 等 4 类，每一类为一个“组件（component）”，代表着不同的使用许可和可用的支持级别。一般来说，官方支持的 main 组件主要用来满足大多数个人电脑用户的基本要求，restricted（“版权限制”）组件主要用来提高系统的可用性，因此通常需要安装这两类组件中的软件。main 即“基本”组件，其中只包含符合 Ubuntu 的许可证要求并可以从 Ubuntu 团队中获得支持的软件，致力于满足日常使用，位于这个组件中的软件可以确保得到技术支持和及时的安全更新。此组件内的软件是必须符合 Ubuntu 版权要求（Ubuntu license requirements）的自由软件，而 Ubuntu 版权要求大致上与 Debian 自由软件指导纲要（Debian Free Software Guidelines）相同。
安装软件时可以通过运行 apt-get 命令，或使用图形接口的 Synaptic 工具或“软件中心”来完成。与 Windows 不同，Ubuntu 的用户通常不必四处搜索、逐一下载或购买相应的安装程序。Ubuntu 能够使用的软件大多存放在被称为“软件源”的服务器中，用户只要运行相应的 apt-get 指令（或使用 Synaptic 工具进行相关操作），系统就会自动查找、下载和安装软件了。所以在配置服务器环境的时候十分方便简洁，只需几条命令就能将电脑打造成一台本地的服务器，而且还保证了软件的版本更新速度。

2.1.2 Apache HTTP Server/2.4.7 (Ubuntu)

Apache HTTP Server（简称 Apache）是 Apache 软件基金会的一个开放源代码的网页服务器，可以在大多数电脑操作系统中运行，由于其跨平台和安全性。被广泛使用，是最流行的 Web 服务器端软件之一。它快速、可靠并且可通过简单的 API 扩充，将 Perl / Python 等解释器编译到服务器中。
Apache 源于 NCSAhttpd 服务器，经过多次修改，成为世界上最流行的 Web 服务器软件之一。Apache 取自“a patchy server”的读音，意思是充满补丁的服务器，因为它是自由软件，所以不断有人来为它开发新的功能、新的特性、修改原来的缺陷。Apache 的特点是简单、速度快、性能稳定，并可做代理服务器来使用。
本来它只用于小型或试验 Internet 网络，后来逐步扩充到各种 Unix 系统中，尤其对 Linux 的支持相当完美。Apache 有多种产品，可以支持 SSL 技术，支持多个虚拟主机。Apache 是以进程为基础的结构，进程要比线程消耗更多的系统开支，不太适合于多处理器环境，因此，在一个 Apache Web 站点扩容时，通常是增加服务器或扩充群集节点而不是增加处理器。到目前为止 Apache 仍然是世界上用的最多的 Web 服务器，市场占有率达 60%左右。世界上很多著名的网站如 Amazon、Yahoo!、W3 Consortium、Financial Times 等都是 Apache 的

产物，它的成功之处主要在于它的源代码开放、有一支开放的开发队伍、支持跨平台的应用（可以运行在几乎所有的 Unix、Windows、Linux 系统平台上）以及它的可移植性等方面。Apache 支持许多特性，大部分通过编译的模块实现。这些特性从服务器端的编程语言支持到身份认证方案。一些通用的语言接口支持 Perl，Python，Tcl， 和 PHP。流行的认证模块包括 mod_access，mod_auth 和 mod_digest。其他的例子有 SSL 和 TLS 支持（mod_ssl），代理服务器（proxy）模块，很有用的 URL 重写（由 mod_rewrite 实现），定制日志文件（mod_log_config），以及过滤支持（mod_include 和 mod_ext_filter）。Apache 日志可以通过网页浏览器使用免费的脚本 AWStats 或 Visitors 来进行分析。
Apache 的 2.x 版本核心在 Apache 1.x 版本之上作出了重要的加强。这包括：多线程，更好的支持非 UNIX 平台（例如 Windows），新的 Apache API，以及 IPv6 支持。

Apache HTTP Server 拥有以下特性：

- 支持最新的 HTTP/1.1 通信协议
- 拥有简单而强有力的基于文件的配置过程
- 支持通用网关接口
- 支持基于 IP 和基于域名的虚拟主机
- 支持多种方式的 HTTP 认证
- 集成 Perl 处理模块
- 集成代理服务器模块
- 支持实时监视服务器状态和定制服务器日志
- 支持服务器端包含指令(SSI)
- 支持安全 Socket 层(SSL)
- 提供用户会话过程的跟踪
- 支持 FastCGI
- 通过第三方模块可以支持 JavaServlets

2.1.3 PHP 5.5.9

2004 年 7 月，PHP5 正式版本的发布，标志着一个全新的 PHP 时代的到来。它的核心是第二代 Zend 引擎，并引入了对全新的 PECL 模块的支持。PHP5 的最大特点是引入了面向对象的全部机制，并且保留了向下的兼容性。程序员不必再编写缺乏功能性的类，并且能够以多种方法实现类的保护。另外，在对象的集成等方面也不再存在问题。使用 PHP5 引进了类型提示和异常处理机制，能更有效的处理和避免错误的发生。
在不断更新的同时，PHP5 依然保留对旧有的 PHP4 程序可以运行于 PHP5 的平台上而不会出现较大问题。随着 MySQL 数据库的发展，PHP5 还绑定了新的 MySQLi 扩展模块，它提供了一些更加有效的方法和实用工具用于处理数据库操作。这些方法大都以面向对象的方式实现，同时也极大地提高了基于数据库的 Web 项目的执行速度。
另外，PHP5 中还改进了创建动态图片的功能，能够支持多种图片格式（如
PNG、GIF、TTIF、JPGE 等）。PHP5 以及内置了对 GD2 库的支持，因此安装 GD2 库（主要

指 UNIX 系统中）也不再是件难事，这使得处理图像十分简单和高效。
大多数 Web 程序开发者依然将 XML 作为一个彻底的简单数据库使用。PHP5 中也采用了一系列简单易用、功能强大的方法处理 XML 文档。

5.0.0	2004 年 07 月 13 日	Zend Engine II with a new object model.
5.1.0	2005 年 11 月 24 日	Performance improvements with introduction of compiler variables in re-engineered PHP Engine.
5.2.0	2006 年 11 月 02 日	默认打开"过滤"的扩展。
5.2.8	2008 年 12 月 08 日	emergent bug fix。
5.2.9	2009 年 02 月 26 日	解决了 5.2.*的超过了 50 多个错误和多个安全问题，增加了稳定性。
5.2.10	2009 年 06 月 18 日	这个版本修正了大量的 bug 和安全漏洞，并升级了时区数据库。
5.2.17	2011 年 01 月 06 日	修正了一个浮点数转化的 Bug。
5.3.0	2009 年 06 月 30 日	支持命名空间;使用 XMLReader 和 XMLWriter 增强 XML 支持;支持 SOAP ,延迟静态绑定，跳转标签（有限的 goto），闭包，Native PHP archives。
5.3.3	2010 年 07 月 22 日	使用命名空间的类中，与类同名的成员函数不再作为构造函数。
5.3.6	2011 年 03 月 17 日	修正一系列 Bug。
5.3.10	2012 年 02 月 02 日	修正了 Stefan Esser 报告的任意远程代码执行漏洞，CVE-2012-0830。
5.4.0	2012 年 03 月 01 日	支持 Trait、简短数组表达式。移除了 register_globals , safe_mode , allow_call_time_pass_reference , session_register() , session_unregister() , magic_quotes 以及 session_is_registered() 。加入了内建的 Web 服务器。增强了性能，减小内存使用量。
5.5.0	2013 年 06 月 20 日	支持 generators，用于异常处理的 finally ，将 OpCache（基于 Zend Optimizer+）加入官方发布中。

2.2 开发工具

2.2.1 Eclipse 3.8 (PDT: Eclipse PHP Development Tools)

Eclipse 是著名的跨平台开源集成开发环境（IDE）。最初主要用来 Java 语言开发，目前亦有人通过插件使其作为 C++、Python、PHP 等其他语言的开发工具。
Eclipse 的本身只是一个框架平台，但是众多插件的支持，使得 Eclipse 拥有较佳的灵活性。许多软件开发商以 Eclipse 为框架开发自己的 IDE!
Eclipse 的基础是富客户机平台（即 RCP）。RCP 包括下列组件：

- 核心平台（启动 Eclipse，运行插件）
- OSGi（标准集束框架）
- SWT（可移植构件工具包）
- JFace（文件缓冲，文本处理，文本编辑器）
- Eclipse 工作台（即 Workbench，包含视图（views）、编辑器（editors）、视角（perspectives）、和向导（wizards））

Eclipse 采用的技术是 IBM 公司开发的（SWT），这是一种基于 Java 的窗口组件，类似 Java 本身提供的 AWT 和 Swing 窗口组件；不过 IBM 声称 SWT 比其他 Java 窗口组件更有效率。
Eclipse 的用户界面还使用了 GUI 中间层 JFace，从而简化了基于 SWT 的应用程序的构建。

PHP 开发工具计划（PDT）：努力为 Eclipse 平台提供一个全功能 PHP 的集成开发环境（IDE）。
The PHP IDE project delivers a PHP Integrated Development Environment framework for the Eclipse platform. This project encompasses the development components necessary to develop PHP-based Web Applications and facilitates extensibility. It leverages the existing Web Tools Project in providing developers with PHP capabilities.

2.2.2 Gedit (Version 3.10.4)

gedit 是一个 GNOME 桌面环境下兼容 UTF-8 的文本编辑器。它简单易用，有良好的语法高亮，对中文支持很好，支持包括 GB2312、GBK 在内的多种字符编码。gedit 是一款自由软件。
gedit 包含语法高亮和标签编辑多个文件的功能。利用 GNOME VFS 库，它还可以编辑远程文件。它支持完整的恢复和重做系统以及查找和替换。
它还支持包括多语言拼写检查和一个灵活的插件系统，可以动态地添加新特性。例如 snippets 和外部程序的集成。
gedit 还包括一些小特性，包括行号显示，括号匹配，文本自动换行，自动完成，代码折叠，批量缩进，批量注解，嵌入式终端，当前行高亮以及自动文件备份。
由于是为 X Window System 设计，它使用 GTK+ 2.0 和 GNOME 2.0 库，能支持视窗桌面环境下的拖放功能；并可在 GNOME 中的说明文件获取此编辑器的使用方法。
近来以 Gedit 为架构基础的新一代编辑器 gPHPedit ;将提升 PHP 与 HTML 及 CSS 开发编辑方面的支持。

2.3 编程语言

2.3.1 php

PHP（全称：PHP：Hypertext Preprocessor，即“PHP：超文本预处理器”）是一种开源的通用计算机脚本语言，尤其适用于网络开发并可嵌入 HTML 中使用。PHP 的语法借鉴吸收 C 语言、Java 和 Perl 等流行计算机语言的特点，易于一般程序员学习。PHP 的主要目标是允许网络开发人员快速编写动态页面，但 PHP 也被用于其他很多领域。
PHP 最初是由勒多夫在 1995 年开始开发的。而现在 PHP 的标准由 PHP Group 和开放源代码社群维护。PHP 以 PHP License 作为许可协议，不过因为这个协议限制了 PHP 名称的使用，所以和开放源代码许可协议 GPL 不兼容。
PHP 的应用范围相当广泛，尤其是在网页程序的开发上。一般来说 PHP 大多运行在网页服务器上，通过运行 PHP 代码来产生用户浏览的网页。PHP 可以在多数的服务器和操作系统上运行，而且使用 PHP 完全是免费的。根据 2007 年 4 月的统计数据，PHP 已经被安装在超过 2000 万个网站和 100 万台服务器上。
PHP 是一个应用范围很广的语言，特别是在网络程序开发方面。一般来说 PHP 大多在服务器端运行，通过运行 PHP 的代码来产生网页提供浏览器读取，此外也可以用来开发命令行脚本程序和用户端的 GUI 应用程序。PHP 可以在许多的不同种的服务器、操作系统、平台上运行，也可以和许多数据库系统结合。使用 PHP 不需要任何费用，官方组织 PHP Group 提供了完整的程序源代码，允许用户修改、编译、扩充来使用。
和客户端的 JavaScript 不同的是，PHP 代码是运行在服务端的。如果在服务器上建立了如上例类似的代码，则在运行该脚本后，客户端就能接收到其结果，但他们无法得知其背后的代码是如何运作的。甚至可以将 web 服务器设置成让 PHP 来处理所有的 HTML 文件，这么一来，用户就无法得知服务端到底做了什么。
PHP 能做任何事。PHP 主要是用于服务端的脚本程序，因此可以用 PHP 来完成任何其它的 CGI 程序能够完成的工作，例如收集表单数据，生成动态网页，或者发送 / 接收 Cookies。但 PHP 的功能远不局限于此。

PHP 脚本主要用于以下三个领域：

- 服务端脚本。这是 PHP 最传统，也是最主要的目标领域。开展这项工作需要具备以下三点：PHP 解析器（CGI 或者服务器模块）、web 服务器和 web 浏览器。需要在运行 web 服务器时，安装并配置 PHP，然后，可以用 web 浏览器来访问 PHP 程序的输出，即浏览服务端的 PHP 页面。如果只是实验 PHP 编程，所有的这些都可以运行在自己家里的电脑中。请查阅安装一章以获取更多信息。
- 命令行脚本。可以编写一段 PHP 脚本，并且不需要任何服务器或者浏览器来运行它。通过这种方式，仅仅只需要 PHP 解析器来执行。这种用法对于依赖 cron（Unix 或者 Linux 环境）或者 Task Scheduler（Windows 环境）的日常运行的脚本来说是理想的选择。这些脚本也可以用来处理简单的文本。请参阅 PHP 的命令行模式以获取更多信息。
- 编写桌面应用程序。对于有着图形界面的桌面应用程序来说，PHP 或许不是一种最好的语言，但是如果用户非常精通 PHP，并且希望在客户端应用程序中使用 PHP 的一些高级特性，可以利用 PHP-GTK 来编写这些程序。用这种方法，还可以编写跨平台的应用程序。PHP-GTK 是 PHP 的一个扩展，在通常发布的 PHP 包中并不包含它。如果对

PHP-GTK 感兴趣，请访问其» 网站以获取更多信息。
PHP 能够在所有的主流操作系统上使用，包括 Linux、Unix 的各种变种（包括 HP-UX、Solaris 和 OpenBSD）、Microsoft Windows、Mac OS X、RISC OS 等。今天，PHP 已经支持了大多数的 web 服务器，包括 Apache、Microsoft Internet Information Server（IIS）、Personal Web Server（PWS）、Netscape 以及 iPlant server、Oreilly Website Pro Server、Caudium、Xitami、OmniHTTPd 等。对于大多数的服务器，PHP 提供了一个模块；还有一些 PHP 支持 CGI 标准，使得 PHP 能够作为 CGI 处理器来工作。
综上所述，使用 PHP，可以自由地选择操作系统和 web 服务器。同时，还可以在开发时选择使用面对过程和面对对象，或者两者混和的方式来开发。尽管 PHP 4 不支持 OOP 所有的标准，但很多代码仓库和大型的应用程序（包括 PEAR 库）仅使用 OOP 代码来开发。PHP 5 弥补了 PHP 4 的这一弱点，引入了完全的对象模型。
使用 PHP，并不局限于输出 HTML。PHP 还能被用来动态输出图像、PDF 文件甚至 Flash 动画（使用 libswf 和 Ming）。还能够非常简便的输出文本，例如 XHTML 以及任何其它形式的 XML 文件。PHP 能够自动生成这些文件，在服务端开辟出一块动态内容的缓存，可以直接把它们打印出来，或者将它们存储到文件系统中。
PHP 最强大最显著的特性之一，是它支持很大范围的数据库。使用任何针对某数据库的扩展（例如 mysql）编写数据库支持的网页非常简单，或者使用抽象层如 PDO，或者通过 ODBC 扩展连接到任何支持 ODBC 标准的数据库。其它一些数据库也可能会用 cURL 或者 sockets，例如 CouchDB。
PHP 还支持利用诸如 LDAP、IMAP、SNMP、NNTP、POP3、HTTP、COM（Windows 环境）等不计其数的协议的服务。还可以开放原始网络端口，使得任何其它的协议能够协同工作。PHP 支持和所有 web 开发语言之间的 WDDX 复杂数据交换。关于相互连接，PHP 已经支持了对 Java 对象的即时连接，并且可以透明地将其用作 PHP 对象。
PHP 具有极其有效的文本处理特性，包括 Perl 兼容正则表达式（PCRE）以及许多扩展和工具可用于解析和访问 XML 文档。PHP 将所有的 XML 功能标准化于坚实的 libxml2 扩展，并且还增加了 SimpleXML，XMLReader 以及 XMLWriter 支持以扩充其功能。

2.3.2 JavaScript

JavaScript，一种直译式脚本语言，是一种动态类型、弱类型、基于原型的语言，内置支持类。它的解释器被称为 JavaScript 引擎，为浏览器的一部分，广泛用于客户端的脚本语言，最早是在 HTML 网页上使用，用来给 HTML 网页增加动态功能。然而现在 JavaScript 也可被用于网络服务器，如 Node.js。
一般来说，完整的 JavaScript 包括以下几个部分：

- ECMAScript，描述了该语言的语法和基本对象
- 文档对象模型（DOM），描述处理网页内容的方法和接口
- 浏览器对象模型（BOM），描述与浏览器进行交互的方法和接口

它的基本特点如下：

- 是一种解释性脚本语言（代码不进行预编译）。
- 主要用来向 HTML 页面添加交互行为。

• 可以直接嵌入 HTML 页面，但写成单独的 js 文件有利于结构和行为的分离。

JavaScript 常用来完成以下任务：

• 嵌入动态文本于 HTML 页面
• 对浏览器事件作出响应
• 读写 HTML 元素
• 在数据被提交到服务器之前验证数据
• 检测访客的浏览器信息
• 控制 cookies，包括创建和修改等

不同于服务器端脚本语言，例如 PHP 与 ASP，JavaScript 主要被作为客户端脚本语言在用户的浏览器上运行，不需要服务器的支持。所以在早期程序员比较青睐于 JavaScript 以减少对服务器的负担，而与此同时也带来另一个问题：安全性。而随着服务器的强壮，虽然现在的程序员更喜欢运行于服务端的脚本以保证安全，但 JavaScript 仍然以其跨平台、容易上手等优势大行其道。同时，有些特殊功能（如 AJAX）必须依赖 Javascript 在客户端进行支持。随着引擎如 V8 和框架如 Node.js 的发展，及其事件驱动及异步 IO 等特性，JavaScript 逐渐被用来编写服务器端程序。

2.4 相关库或软件

2.4.1 jQuery

jQuery 是一套跨浏览器的 JavaScript 库，简化 HTML 与 JavaScript 之间的操作。由 John Resig 在 2006 年 1 月的 BarCamp NYC 上发布第一个版本。目前是由 Dave Methvin 领导的开发团队进行开发。全球前 10000 个访问最高的网站中，有 65%使用了 jQuery，是目前最受欢迎的 JavaScript 库。

jQuery 是开源软件，使用 MIT 许可证授权。jQuery 的语法设计使得许多操作变得容易，如操作文档对象（document）、选择 DOM 元素、创建动画效果、处理事件、以及开发 Ajax 程序。jQuery 也提供了给开发人员在其上创建插件的能力。这使开发人员可以对底层交互与动画、高级效果和高级主题化的组件进行抽象化。模块化的方式使 jQuery 函数库能够创建功能强大的动态网页以及网络应用程序。

微软和诺基亚已宣布在他们的平台上绑定 jQuery。微软最初在 Visual Studio 中集成了 jQuery 以便在微软自己的 ASP.NET AJAX 框架和 ASP.NET MVC Framework 中使用，而诺基亚则在他的 Web 运行时组件开发平台中集成了 jQuery。MediaWiki 自从 1.16 版本后也开始使用 jQuery。

jQuery 1.3 版以后，引入全新的 CSS 选择器引擎 Sizzle。同时不再提供 Packed 版本，因为解压缩的消耗的时间，远大于所节省的下载时间，且不利于 Debug，且已有 Google AJAX Libraries API 等公开站台提供 jQuery 的 js 的引用服务，故 Packed 版本原本的优点已荡然无存。

jQuery 有下列特色:

- 跨浏览器的 DOM 元素选择
- DOM 巡访与更改：支持 CSS 1-3
- 事件（Events）
- CSS 操纵
- 特效和动画（移动显示位置、淡入、淡出）
- Ajax
- 延伸性（Extensibility）
- 工具：例如浏览器版本（已取消内置，改由 jQuery Migrate plugin 外挂提供）和 `each` 函数。
- JavaScript 插件
- 轻量级

jQuery 1.8.0 版时（内置 Sizzle.js）：

文件	行数	大小
jquery-1.8.0.min.js	2	91KB
jquery-1.8.0.js	9228	254KB

- DHTML DOM 选择器与链式语法

经由 jQuery 的 DHTML DOM 选择器，可以更容易的操作在复杂的树状 HTML 中的任何 DHTML DOM 对象，并可用链式语法对同一对象的不同属性进行操作。

例如：

```
$("p.surprise").addClass("ohmy").show("slow");
```

相当于

1. 查找 HTML 的<p>标签，且其 class 为"surprise"的 DHTML DOM 对象
2. 将其 Class 属性多加上一个"ohmy"（通常是配 CSS 的定义做显示时的配色修改）
3. 打开显示

- CSS 1-3 选择器：支持 CSS 选择器选定 DOM 对象。
- 跨浏览器：跨浏览器的 AJAX 解决方式，支持 Internet Explorer 6.0+、Opera 9.0+、Firefox 2+、Safari 2.0+、Google Chrome 1.0+
- 简单：较其它 JavaScript 库更易于入门。

2.4.2 Bootstrap

Bootstrap 是 Twitter 推出的一个开源的用于前端开发的工具包。它由 Twitter 的设计师 Mark Otto 和 Jacob Thornton 合作开发，是一个 CSS/HTML 框架。Bootstrap 提供了优雅的 HTML 和 CSS 规范，它即是由动态 CSS 语言 Less 写成。Bootstrap 一经推出后颇受欢迎，一直是

GitHub 上的热门开源项目，包括 NASA 的 MSNBC（微软全国广播公司）的 Breaking News 都使用了该项目。
Bootstrap 是基于 jQuery 框架开发的，它在 jQuery 框架的基础上进行了更为个性化和人性化的完善，形成一套自己独有的网站风格，并兼容大部分 jQuery 插件。
Bootstrap 中包含了丰富的 Web 组件，根据这些组件，可以快速的搭建一个漂亮、功能完备的网站。其中包括以下组件：下拉菜单、按钮组、按钮下拉菜单、导航、导航条、面包屑、分页、排版、缩略图、警告对话框、进度条、媒体对象等。
Bootstrap 自带了 13 个 jQuery 插件，这些插件为 Bootstrap 中的组件赋予了“生命”。其中包括：模式对话框、标签页、滚动条、弹出框等。

2.4.3 phpMailer

PHPMailer 是一个用于发送电子邮件的 PHP 函数包。

它提供的功能包括：

*.在发送邮时指定多个收件人，抄送地址，暗送地址和回复地址
*.支持多种邮件编码包括：8bit，base64，binary 和 quoted-printable
*.支持 SMTP 验证
*.支持冗余 SMTP 服务器
*.支持带附件的邮件和 Html 格式的邮件
*.自定义邮件头
*.支持在邮件中嵌入图片
*.调试灵活
*.经测试兼容的 SMTP 服务器包括：Sendmail,qmail,Postfix,Imail,Exchange 等
*.可运行在任何平台之上

2.4.4 PDO

PDO 扩展为 PHP 访问数据库定义了一个轻量级的、一致性的接口，它提供了一个数据访问抽象层，这样，无论使用什么数据库，都可以通过一致的函数执行查询和获取数据。PDO 随 PHP5.1 发行，在 PHP5.0 的 PECL 扩展中也可以使用，无法运行于之前的 PHP 版本。

2.4.5 phpass

phpass (pronounced "pH pass") is a portable public domain password hashing framework for use in PHP applications. It is meant to work with PHP 3 and above, and it has actually been tested with at least PHP 3.0.18 through 5.4.x so far. (PHP 3 support is likely to be dropped in next revision.)

2.4.6 jsPacker

jsPacker 是一个用于混淆和压缩 JS 代码的 PHP 函数包。
Github 地址：https://github.com/UlisesFreitas/jsPacker

2.4.7 Git

Git 是一个分布式版本控制 / 软件配置管理软件，原是 Linux 内核开发者林纳斯·托瓦兹（Linus Torvalds）为更好地管理 Linux 内核开发而设计。
Git 是用于 Linux 内核开发的版本控制工具。与 CVS、Subversion 一类的集中式版本控制工具不同，它采用了分布式版本库的作法，不需要服务器端软件，就可以运作版本控制，使得源代码的发布和交流极其方便。Git 的速度很快，这对于诸如 Linux 内核这样的大项目来说自然很重要。Git 最为出色的是它的合并追踪（merge tracing）能力。
实际上内核开发团队决定开始开发和使用 Git 来作为内核开发的版本控制系统的时候，世界上开源社群的反对声音不少，最大的理由是 Git 太艰涩难懂，从 Git 的内部工作机制来说，的确是这样。但是随着开发的深入，Git 的正常使用都由一些友善的命令稿来执行，使 Git 变得非常好用。现在，越来越多的著名项目采用 Git 来管理项目开发，例如：wine、U-boot 等。
作为开源自由原教旨主义项目，Git 没有对版本库的浏览和修改做任何的权限限制，通过其他工具也可以达到有限的权限控制，比如：gitosis、CodeBeamer MR。原本 Git 的使用范围只适用于 Linux/Unix 平台，但在 Windows 平台下的使用也日渐成熟，这主要归功于 Cygwin、msysgit 环境，以及 TortoiseGit 这样易用的 GUI 工具。Git 的源代码中也已经加入了对 Cygwin 与 MinGW 编译环境的支持且逐渐完善，为 Windows 用户带来福音。

2.4.8 GitHub

GitHub 是一个共享虚拟主机服务，用于存放使用 Git 版本控制的软件代码和内容项目。它由 GitHub 公司（曾称 Logical Awesome）的开发者 Chris Wanstrath、PJ Hyett 和 Tom Preston-Werner 使用 Ruby on Rails 编写而成。
GitHub 同时提供付费账户和为开源项目提供的免费账户。根据在 2009 年的 Git 用户调查，GitHub 是最流行的 Git 存取站点。除了允许个人和组织建立和存取代码库以外，它也提供了一些方便社会化软件开发的功能，包括允许用户跟踪其他用户、组织、软件库的动态，对软件代码的改动和 bug 提出评论等。
GitHub 也提供了图表功能，用于显示开发者们怎样在代码库上工作以及软件的开发活跃程度。
GitHub 也提供一个粘贴箱风格的站点 Gist，供软件代码库使用的 Wiki，以及通过 git 版本库进行编辑和管理的网页托管功能。
許多赫赫有名的程式庫、開發框架都採用 GitHub 作為为主版本控制平台。

第三章　功能设计

3.1 登录管理

（1）用户登录判断
（2）用户密码加密
（3）用户权限判断

3.2 项目管理

（1）列出所有项目
（2）添加项目功能（可自选模块）
（3）删除项目功能
（4）编辑项目功能（可自选模块）

3.3 项目操作

（1）开始项目
（2）停止项目
（3）查看脚本地址
（4）查看项目记录（分页显示）
（5）删除项目记录
（6）全（不）选项目记录
（7）批量删除项目记录

3.4 模块管理

（1）列出所有模块（分页显示）
（2）添加模块功能
（3）删除模块功能
（4）编辑模块功能
（7）模块分类功能

3.5 模块操作

（1）编辑模块
（2）查看模块信息
（3）添加模块
（4）删除模块
（5）全（不）选模块
（6）批量删除模块

3.6 主机管理

（1）列出所有主机功能（分页显示）
（2）删除主机功能
（3）主机分类功能
（4）删除不在线主机功能

3.7 主机操作

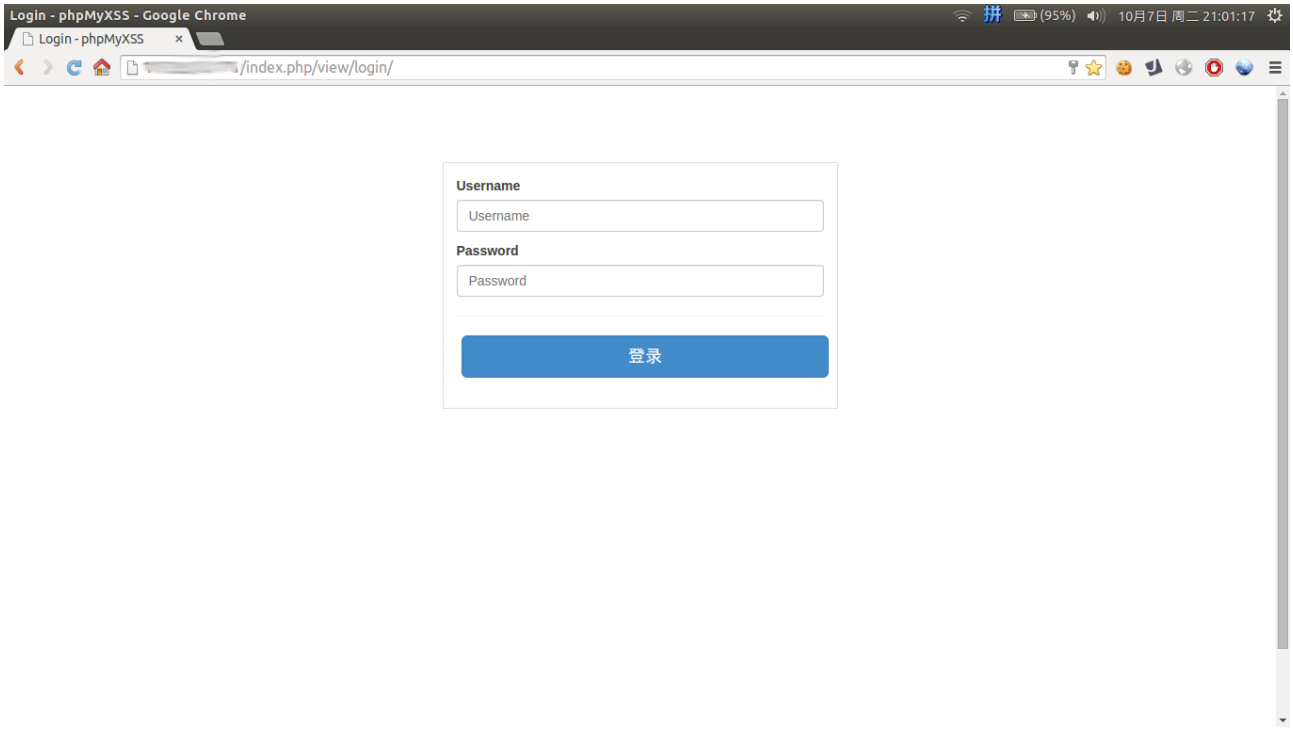
（1）查看主机
（2）管理主机
（3）删除主机
（4）删除主机独立会话
（5）全（不）选主机
（6）自动加载模块
（7）自动更新记录状态
（8）自定义执行 JS 代码

3.8 其它模块

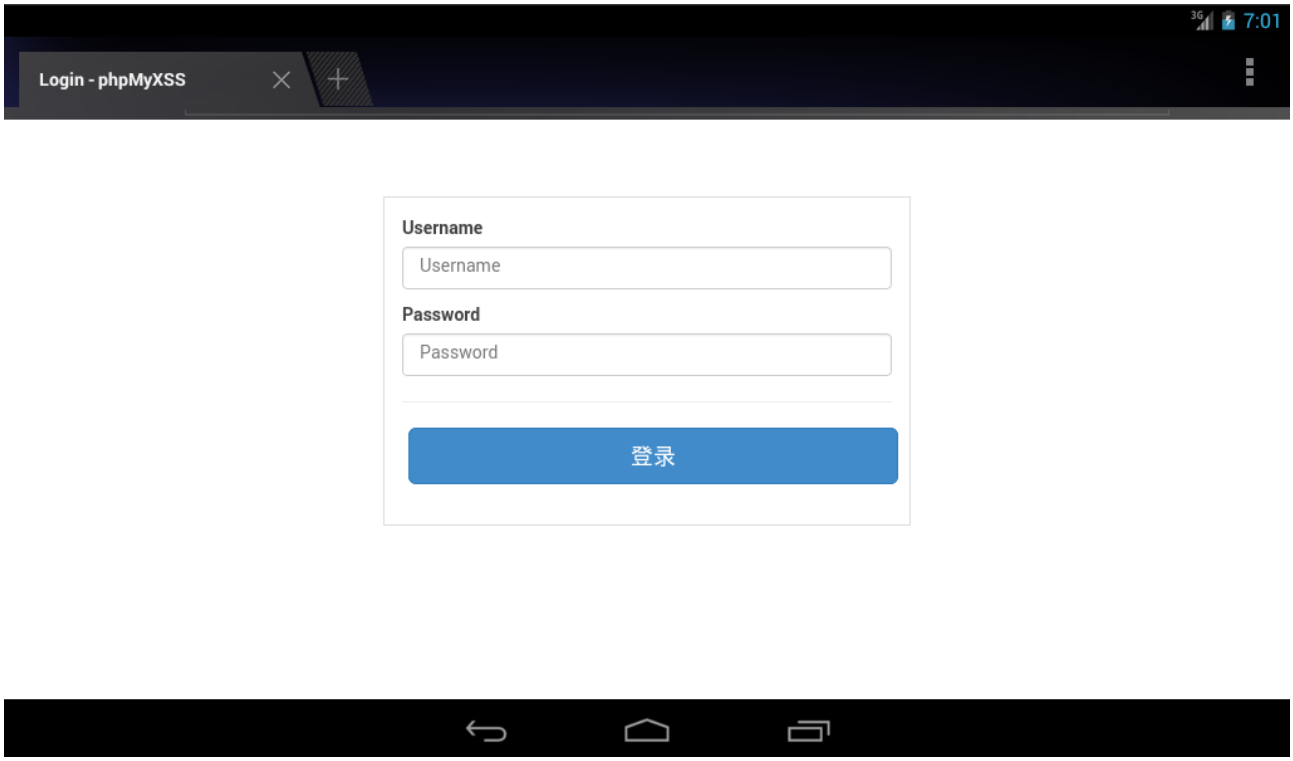
（1）获取模块列表 API
（2）获取模块详细信息 API
（3）获取主机记录 API

第四章　前端设计

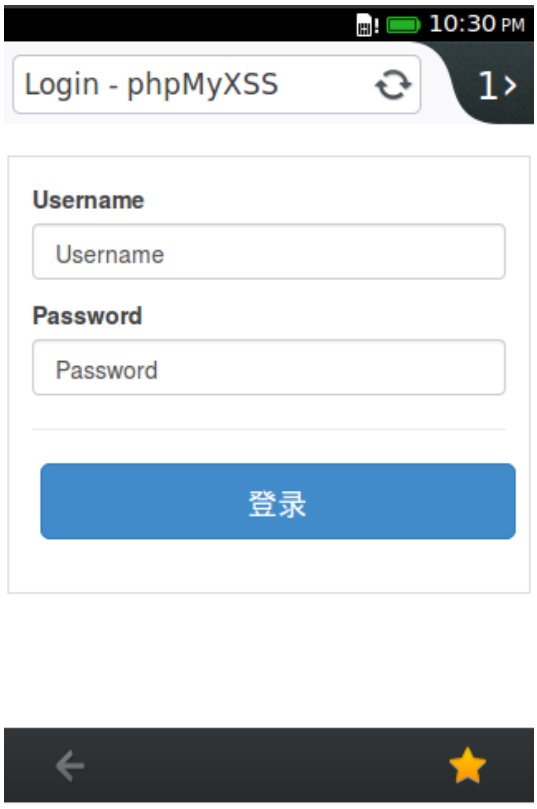
4.1 登录相关



登录界面（电脑）

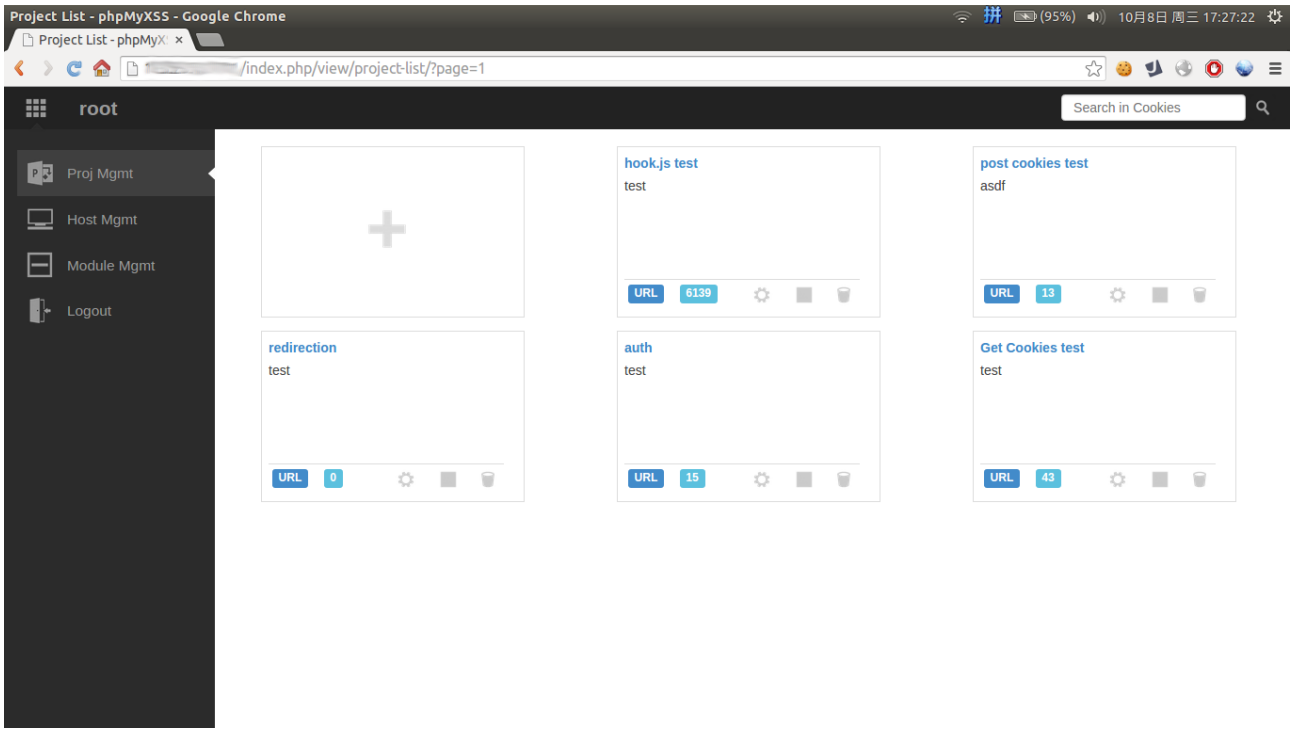


登录界面（平板）

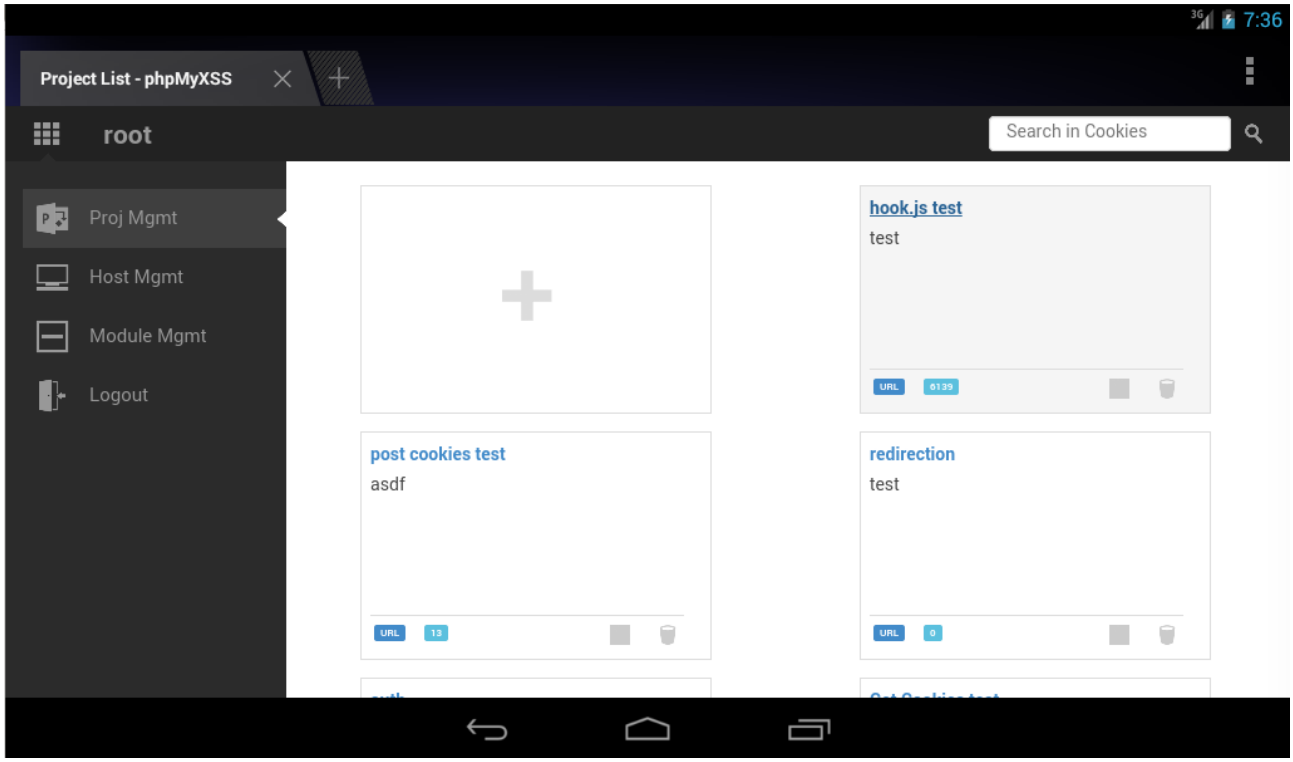


登录界面（手机）

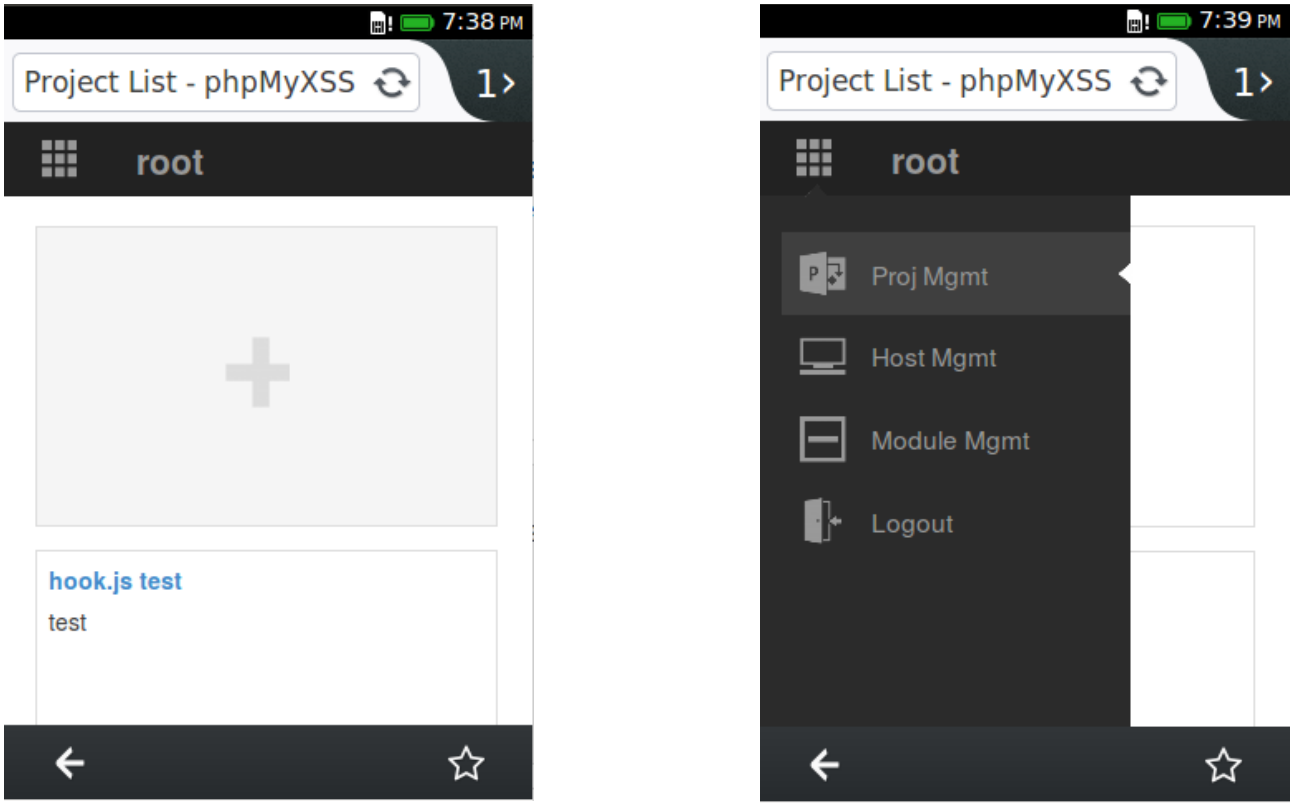
4.2 项目管理相关



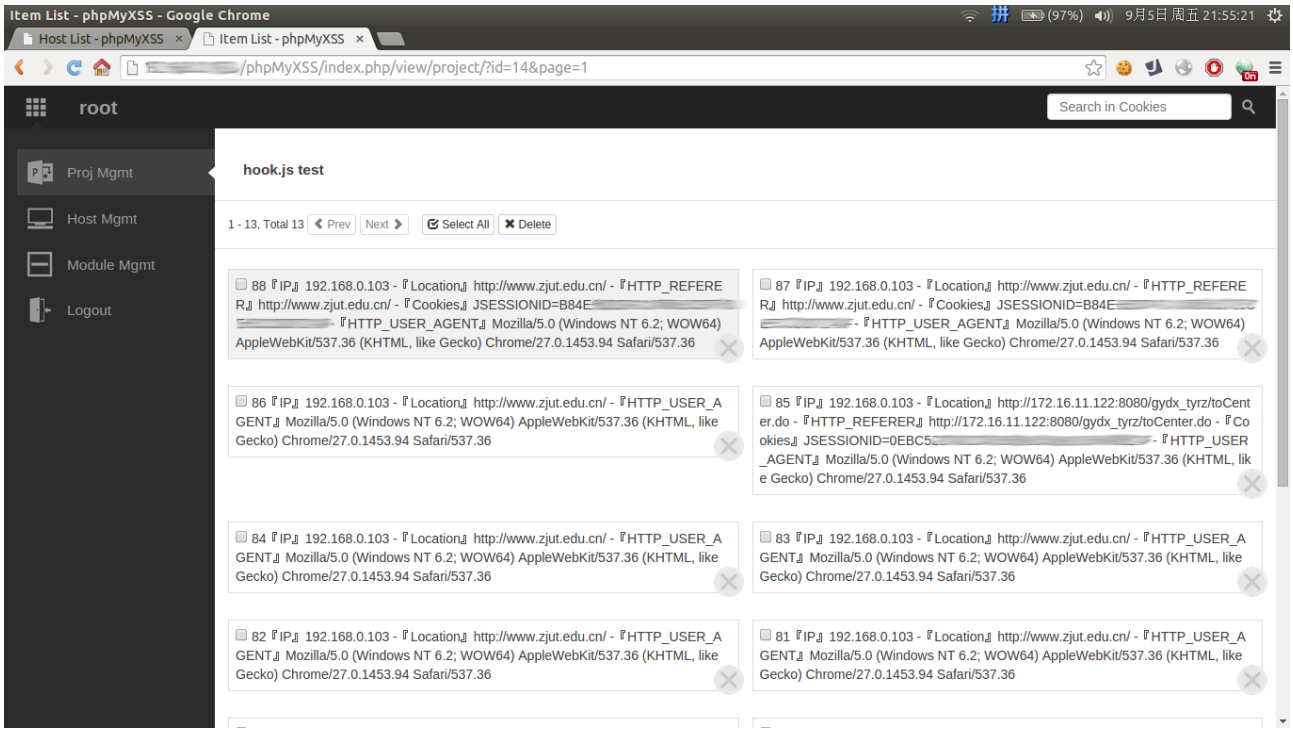
项目列表（电脑）



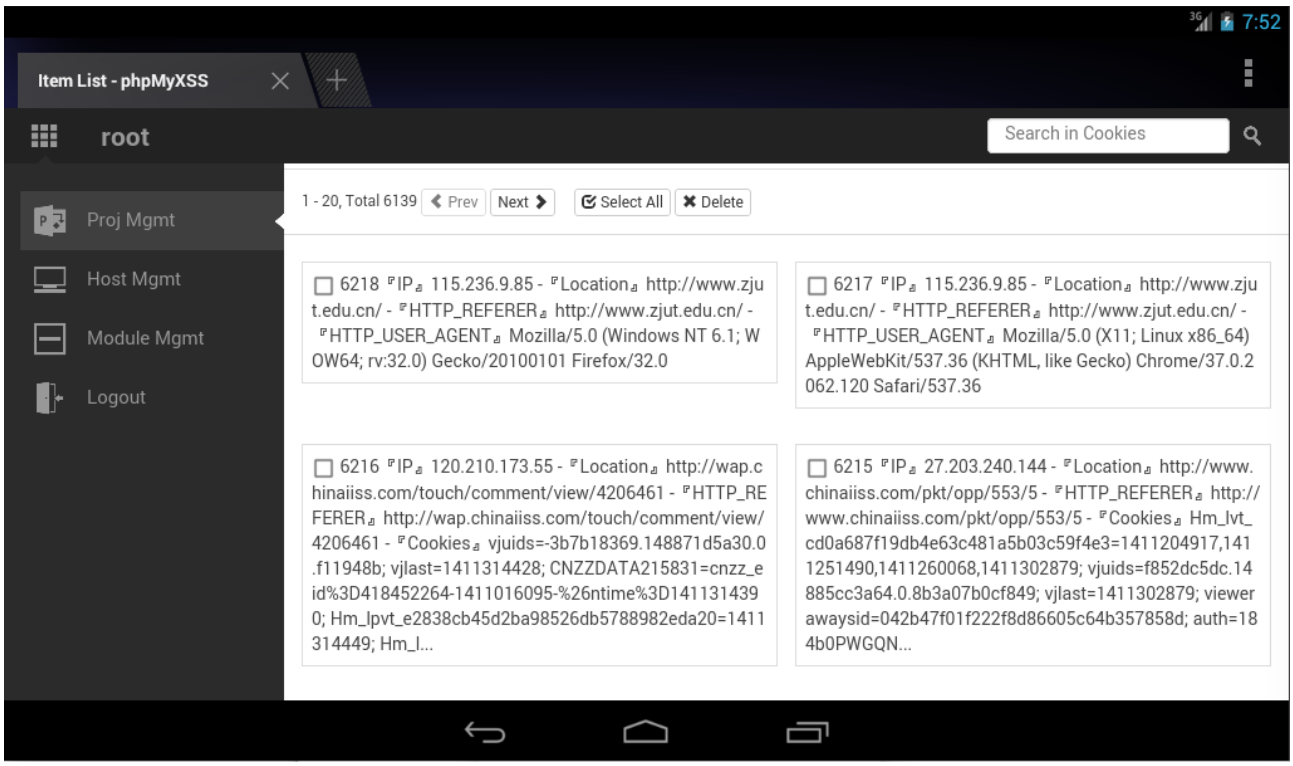
项目列表（平板）



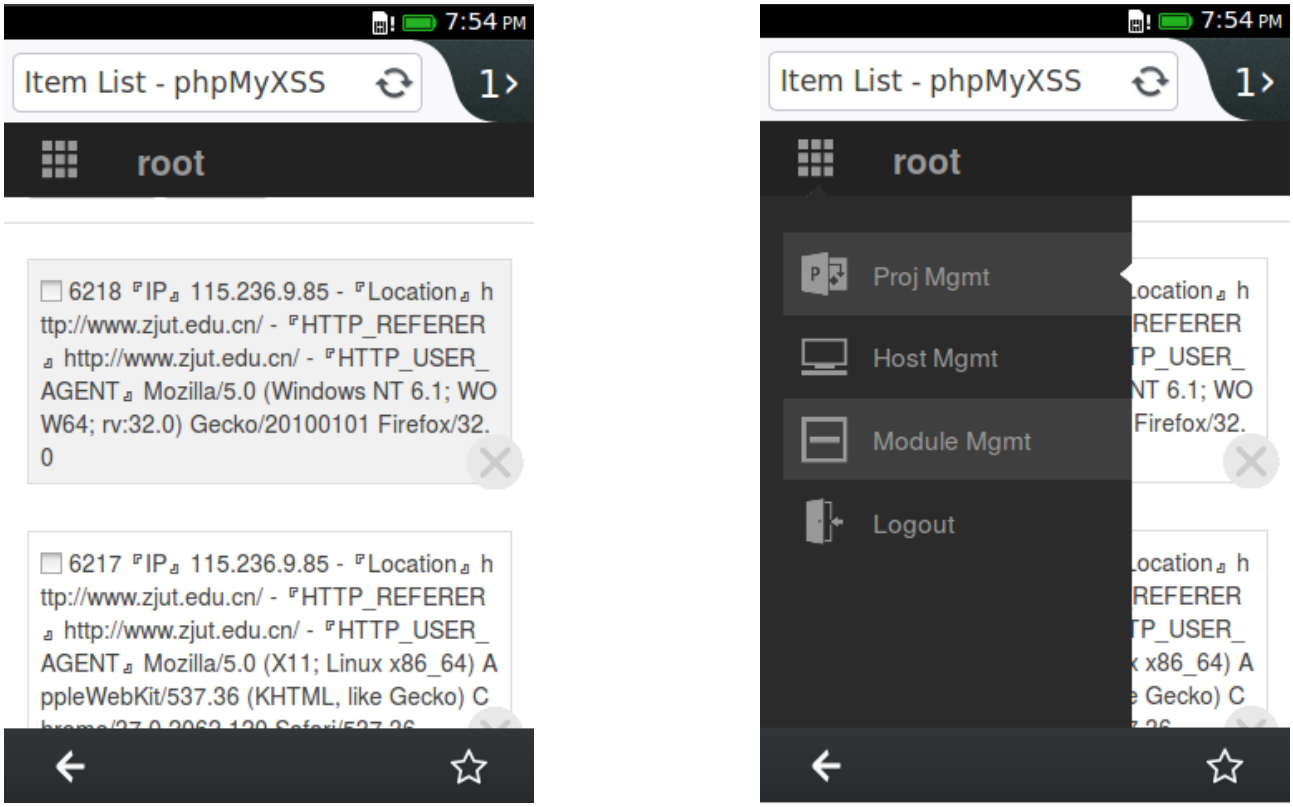
项目列表（手机）



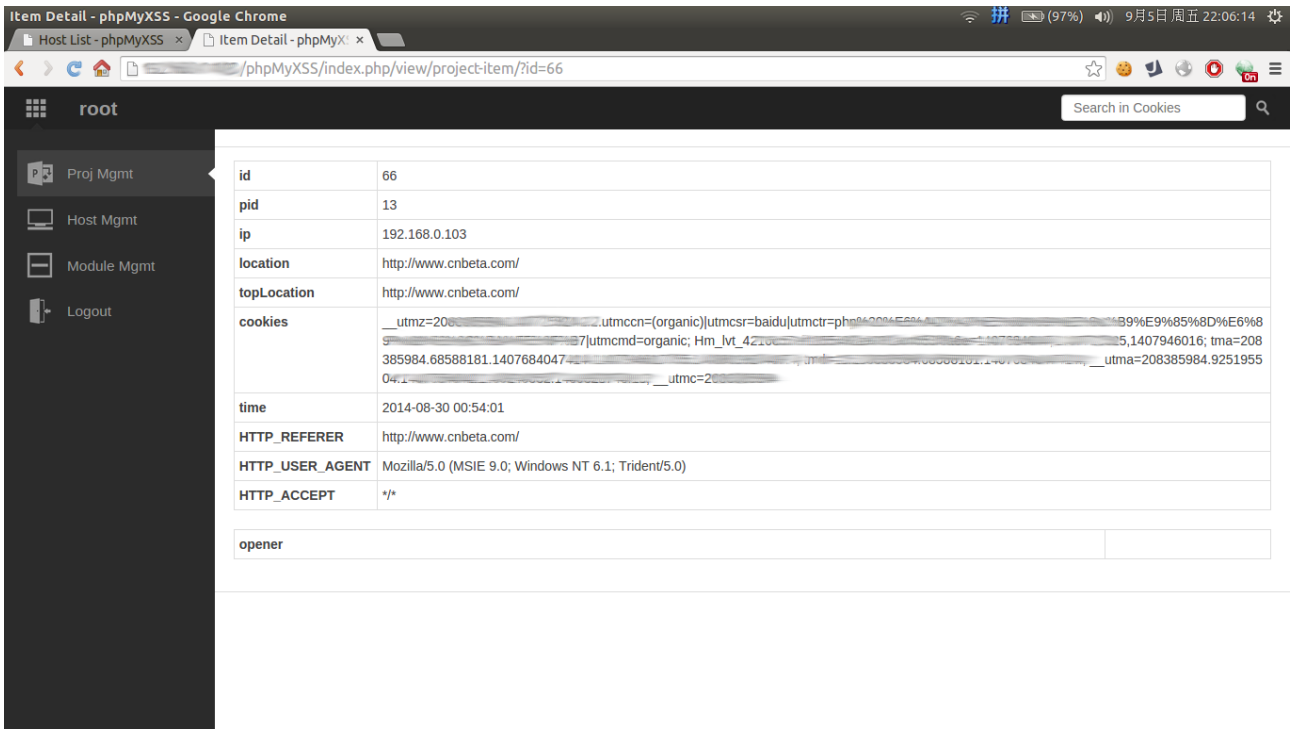
项目记录列表（电脑）



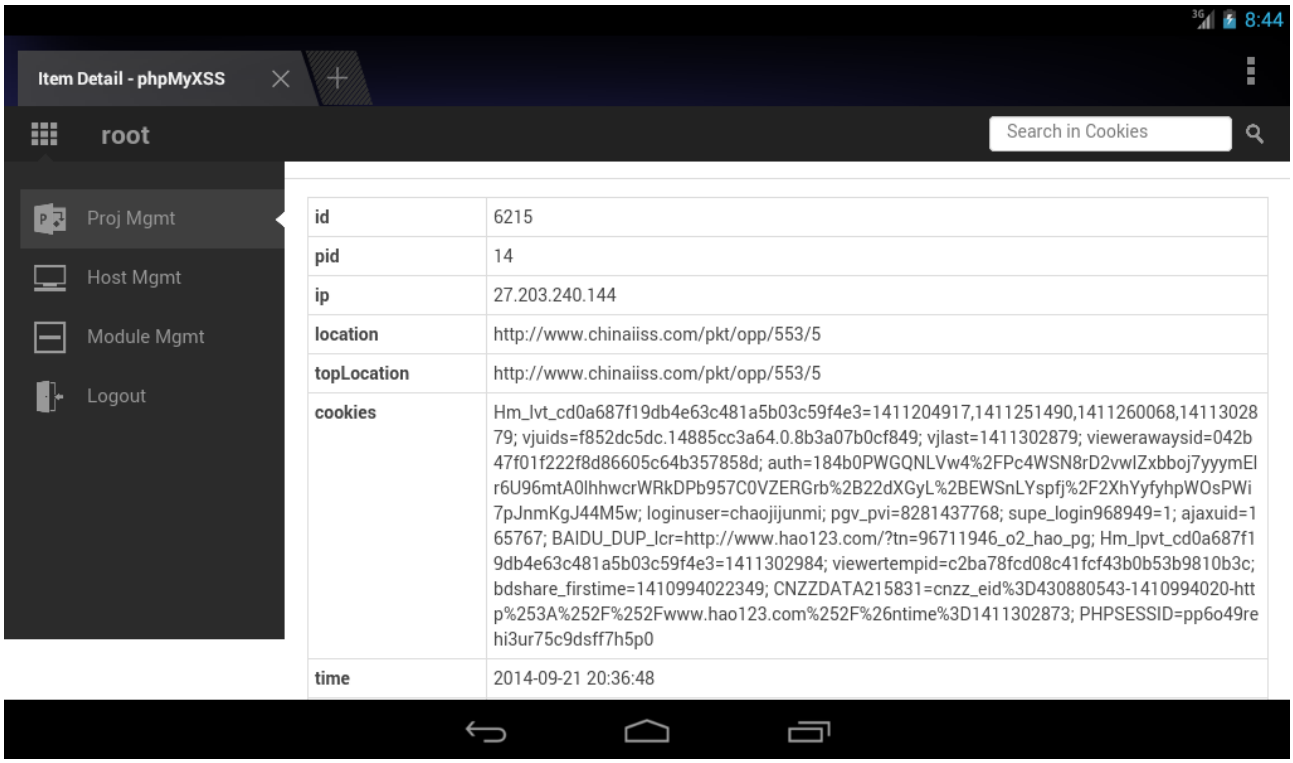
项目记录列表（平板）



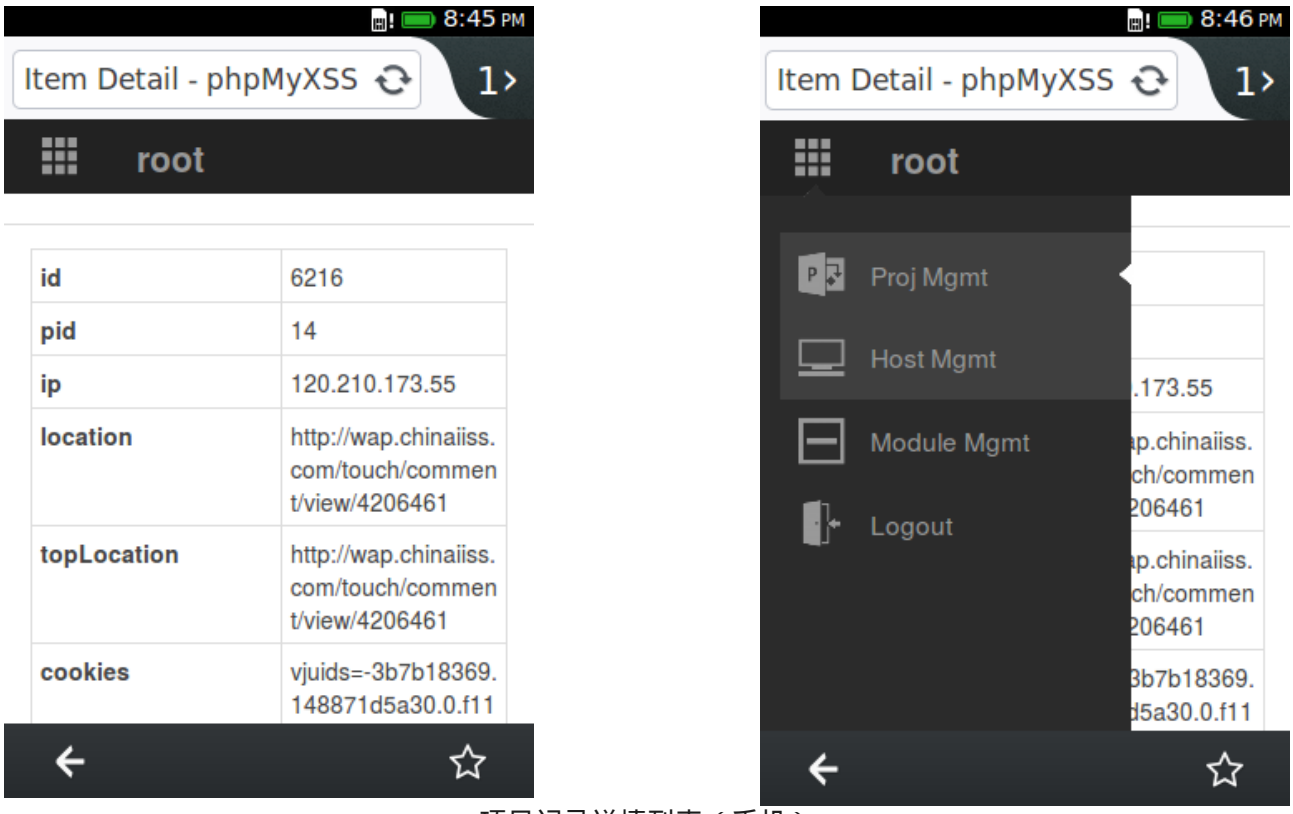
项目记录列表（手机）



项目记录详情列表（电脑）

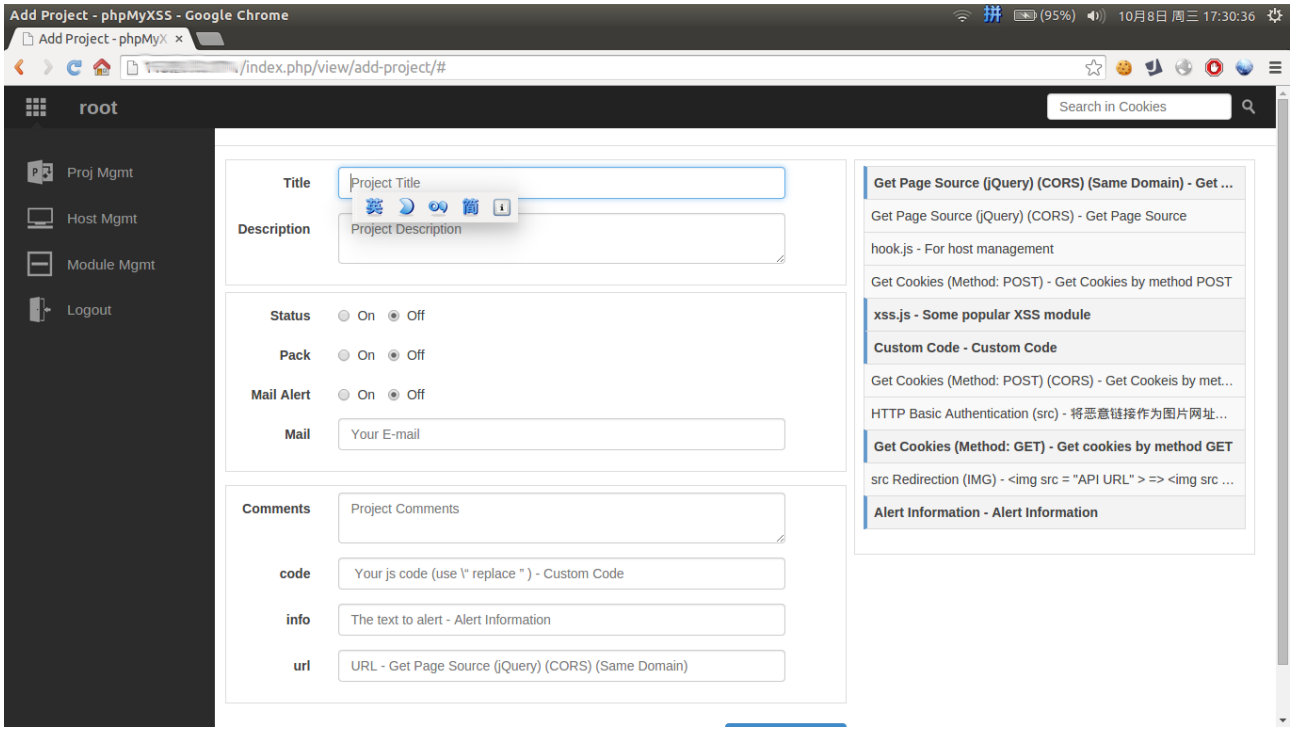


项目记录详情列表（平板）

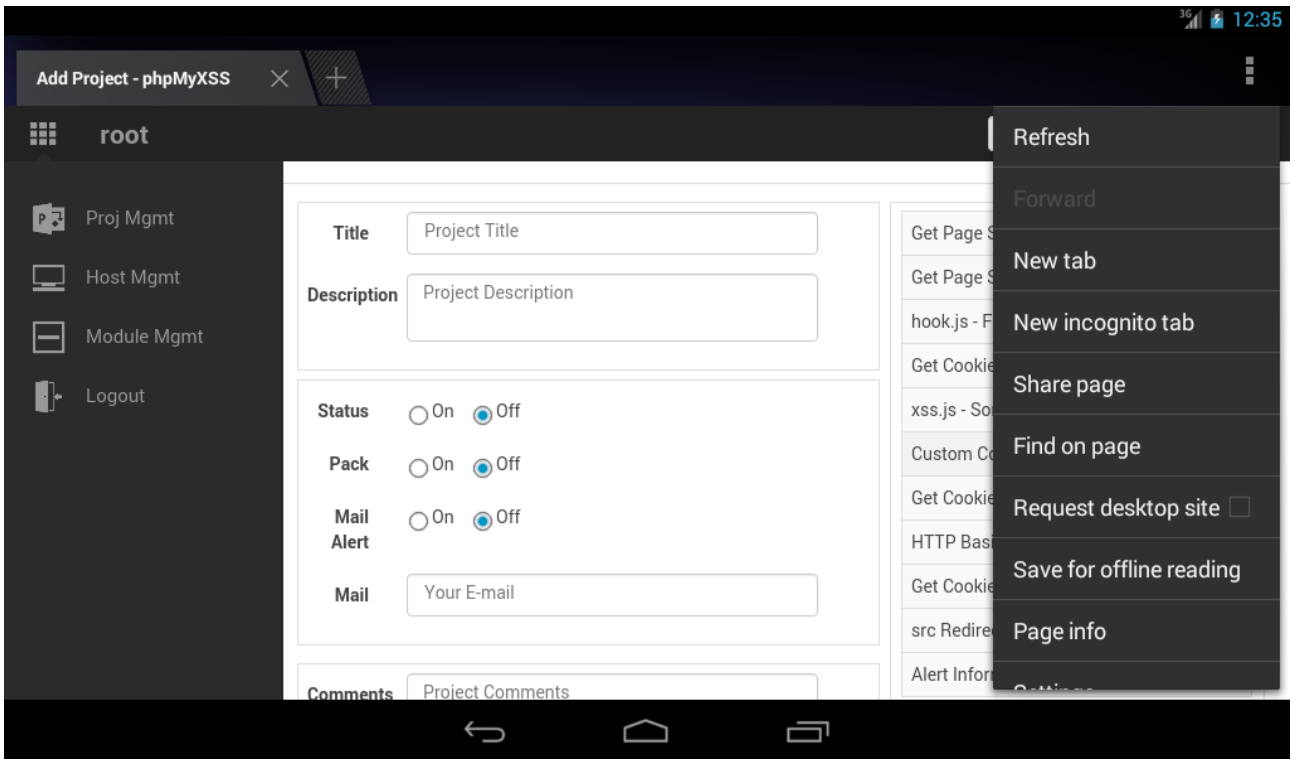


项目记录详情列表（手机）

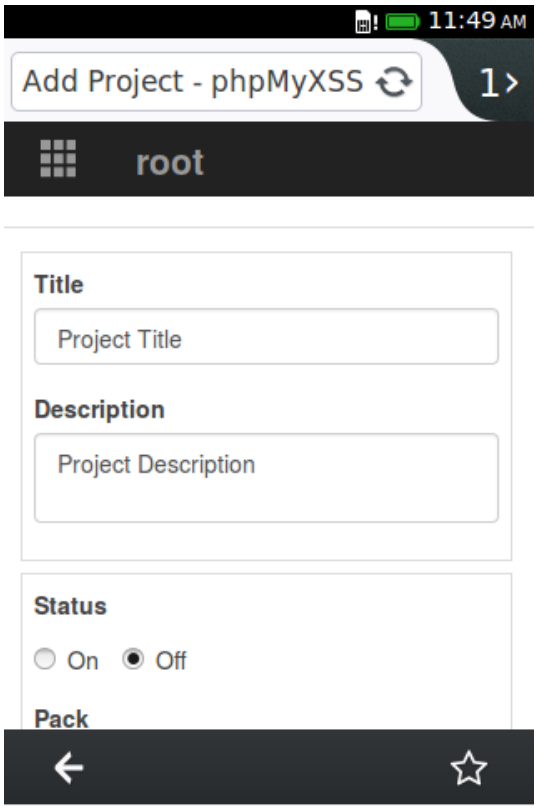
4.3 项目操作相关

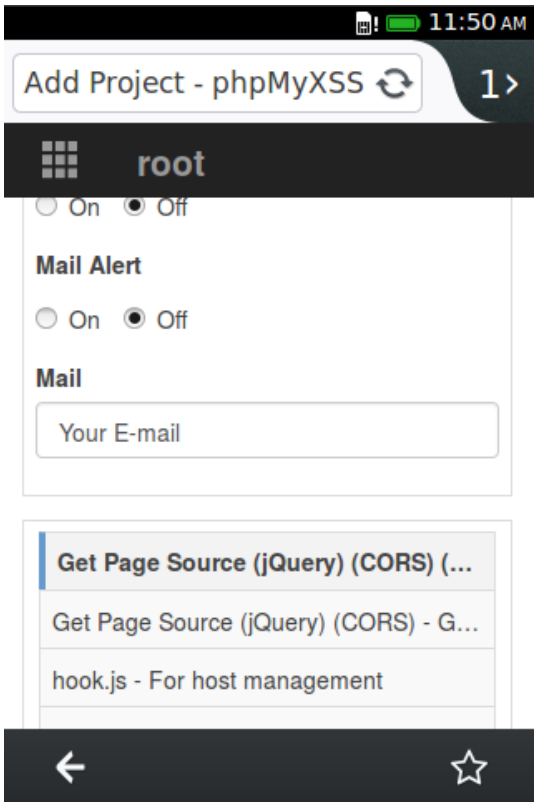


添加项目（电脑）

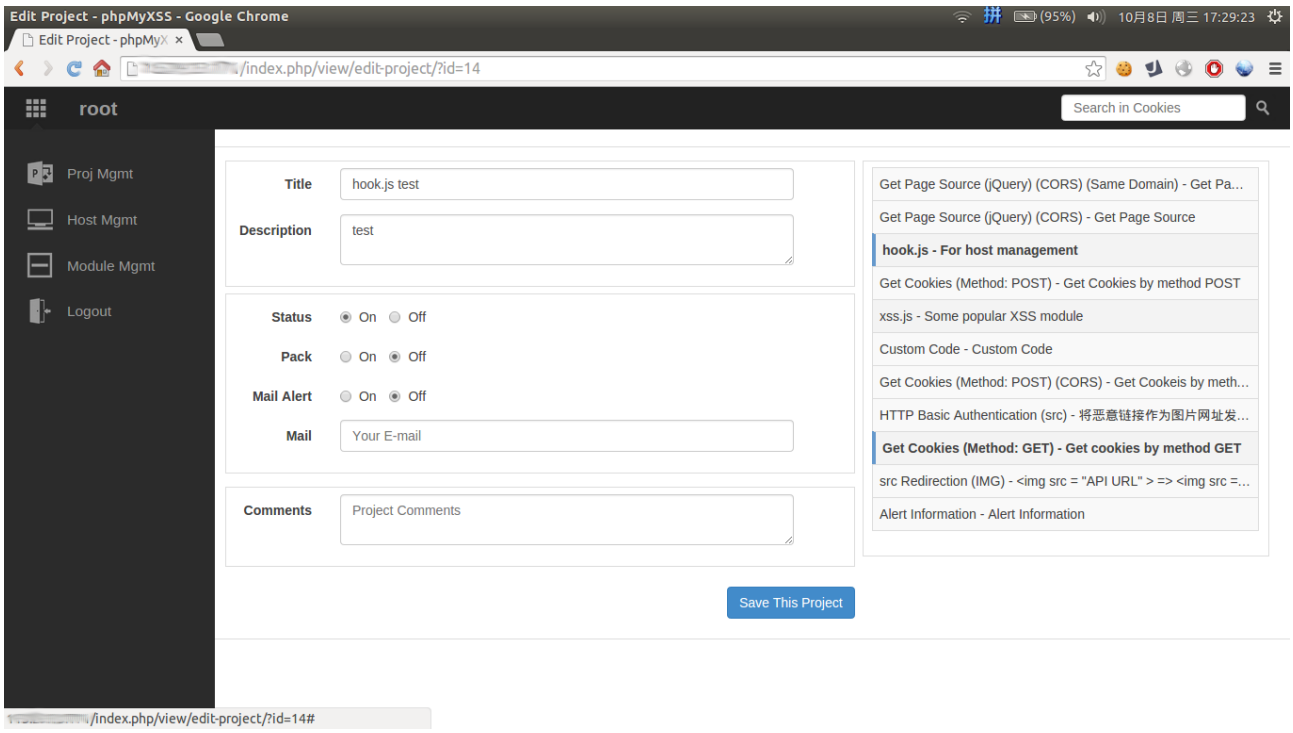


添加项目（平板）

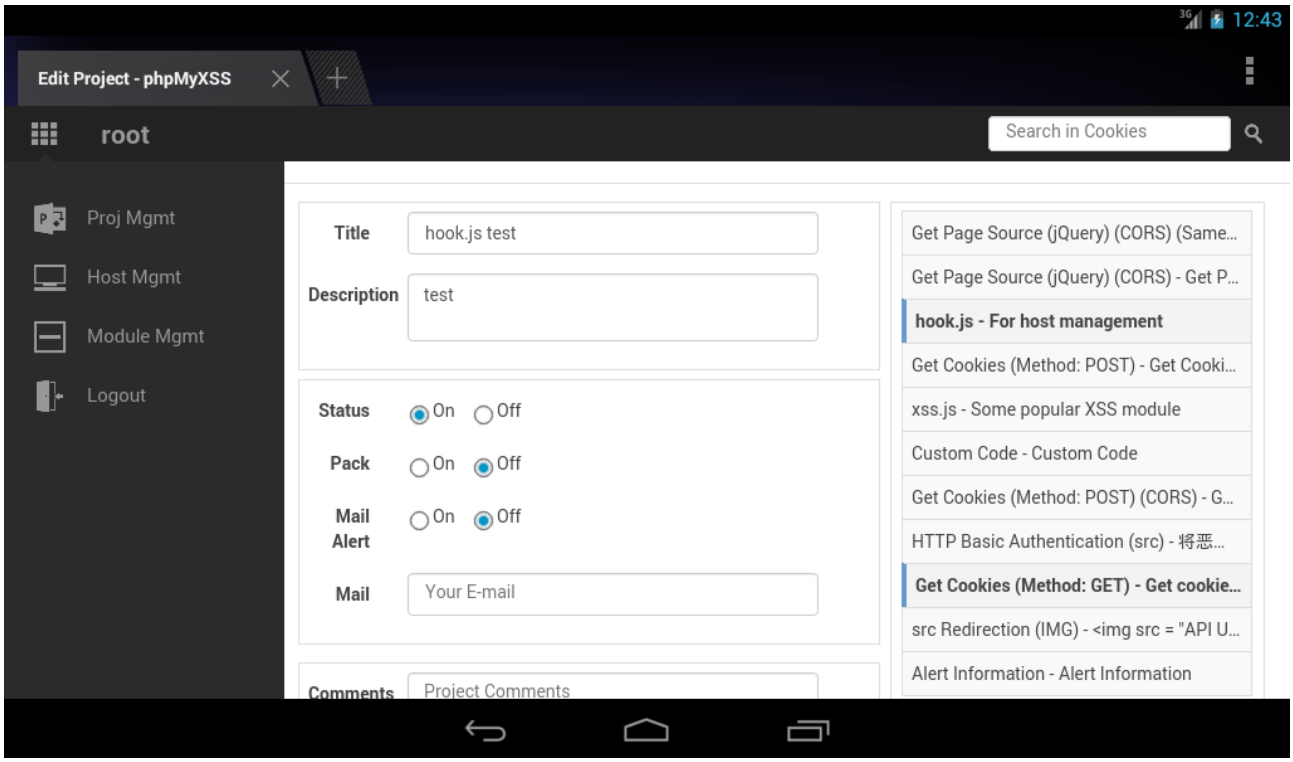




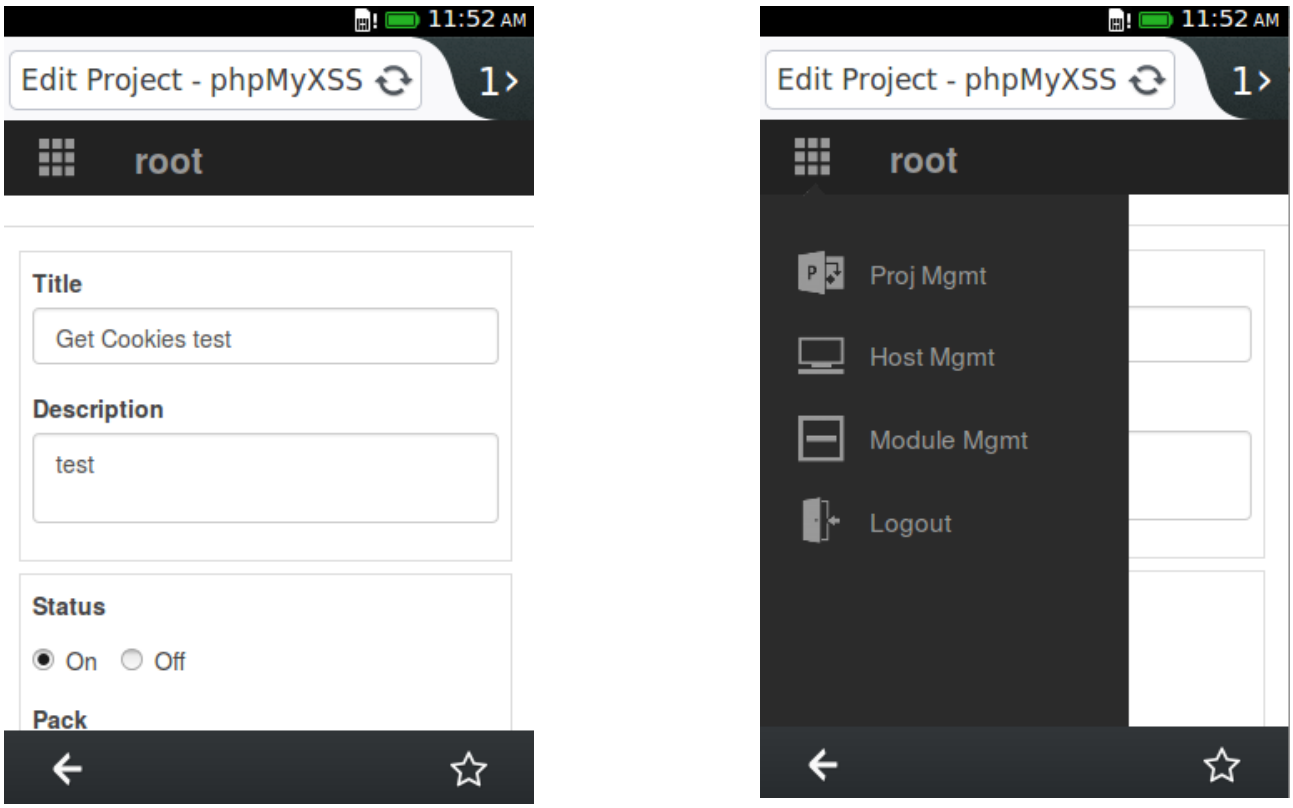
添加项目（手机）



编辑项目（电脑）

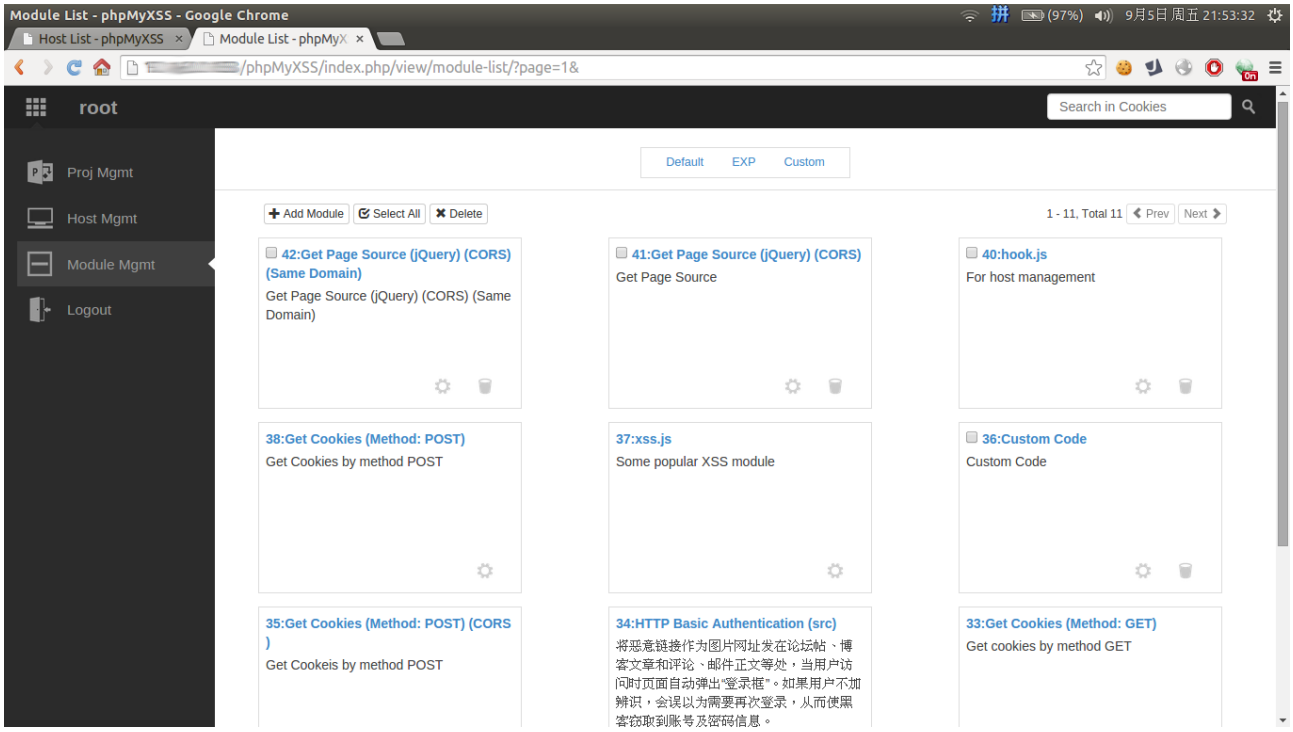


编辑项目（平板）

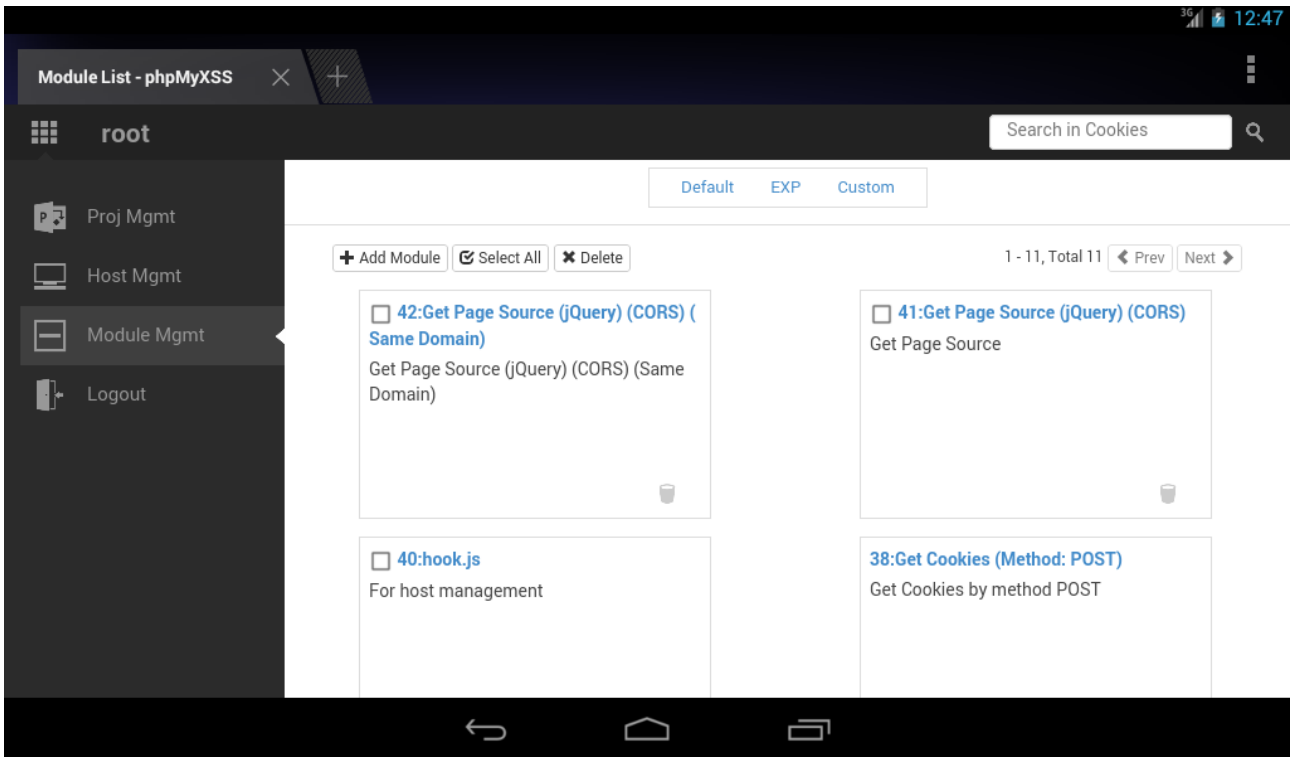


编辑项目（手机）

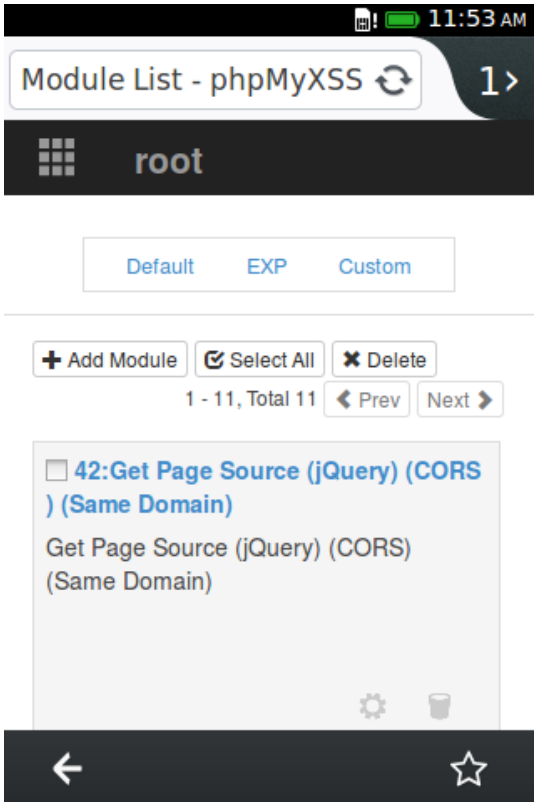
4.4 模块管理相关

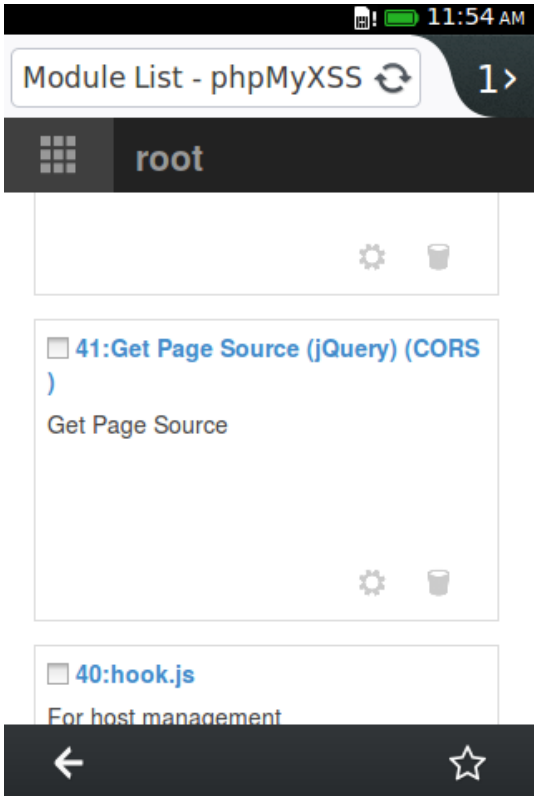


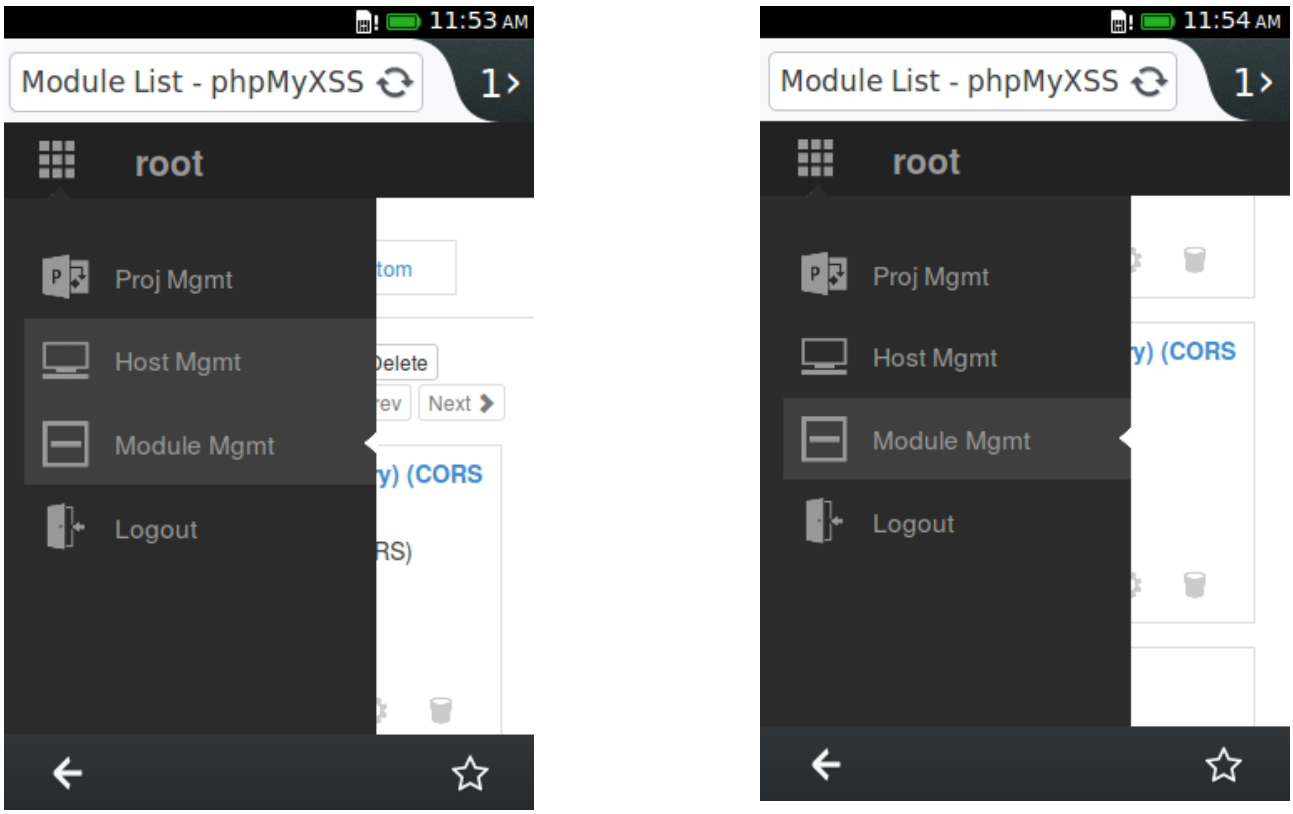
模块列表（电脑）


12:47
Module List - phpMyXSS
root
Search in Cookies
Proj Mgmt
Host Mgmt
Module Mgmt
Logout
Default
EXP
Custom
Add Module
Select All
Delete
1 - 11, Total 11
Prev
Next
42:Get Page Source (jQuery) (CORS) (Same Domain)
Get Page Source (jQuery) (CORS) (Same Domain)
41:Get Page Source (jQuery) (CORS)
Get Page Source
40:hook.js
For host management
38:Get Cookies (Method: POST)
Get Cookies by method POST

模块列表（平板）

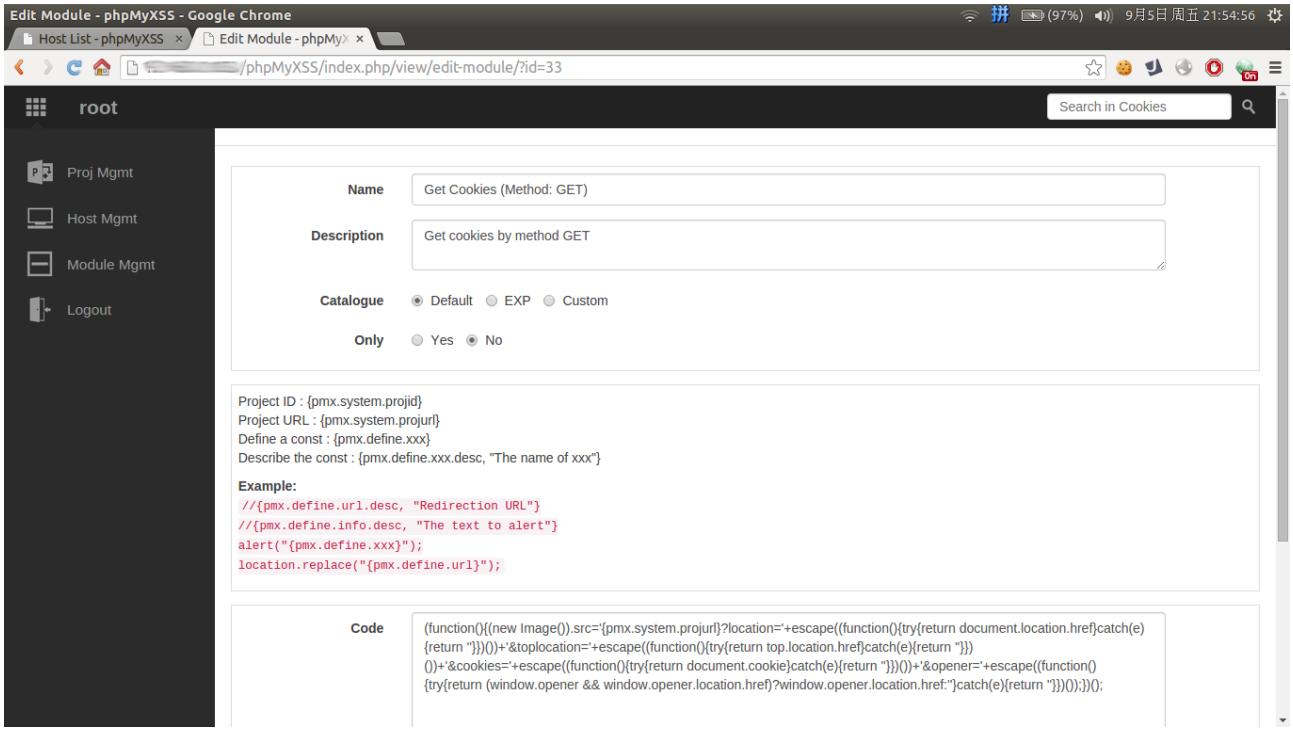

11:53 AM
Module List - phpMyXSS
1
root
Default
EXP
Custom
Add Module
Select All
Delete
1 - 11, Total 11
Prev
Next
42:Get Page Source (jQuery) (CORS) (Same Domain)
Get Page Source (jQuery) (CORS) (Same Domain)


11:54 AM
Module List - phpMyXSS
1
root
41:Get Page Source (jQuery) (CORS)
Get Page Source
40:hook.js
For host management

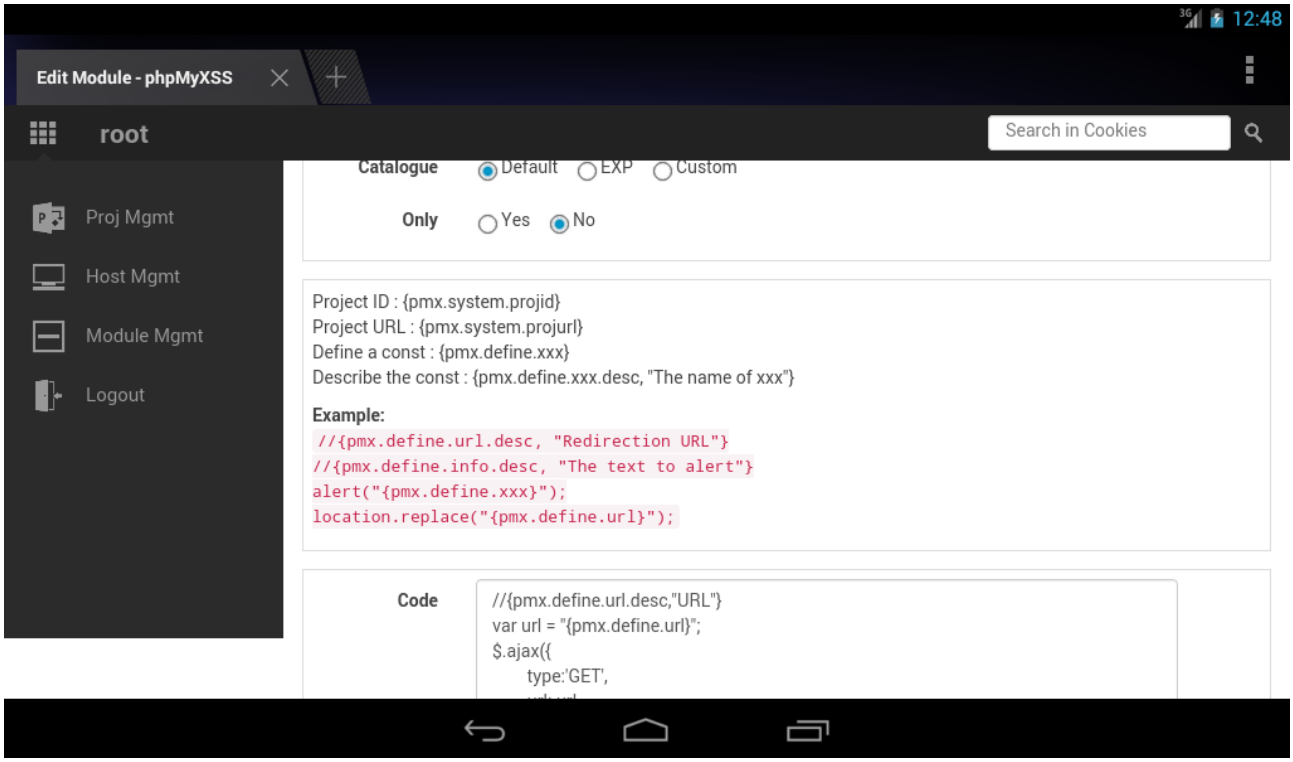


模块列表（手机）

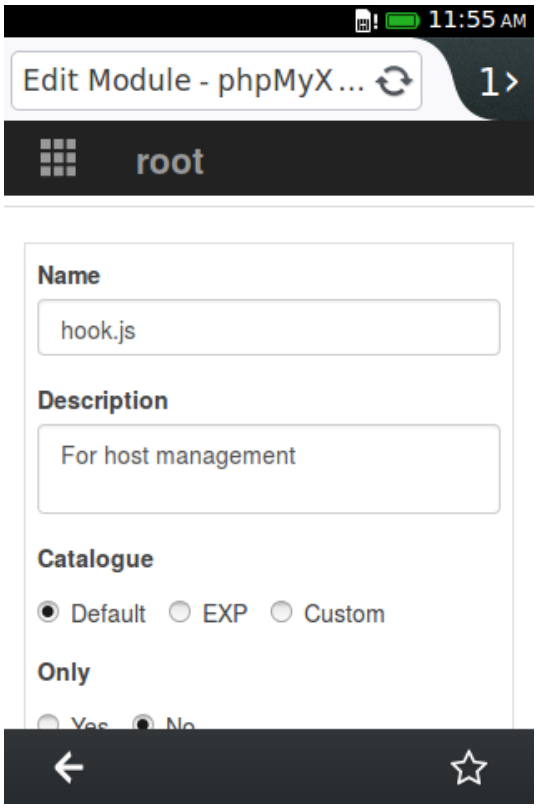
4.5 模块操作相关

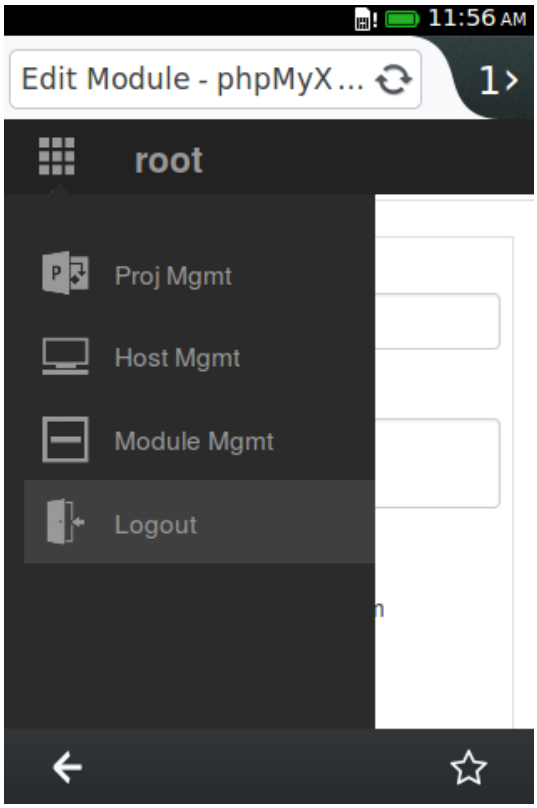


编辑模块（电脑）

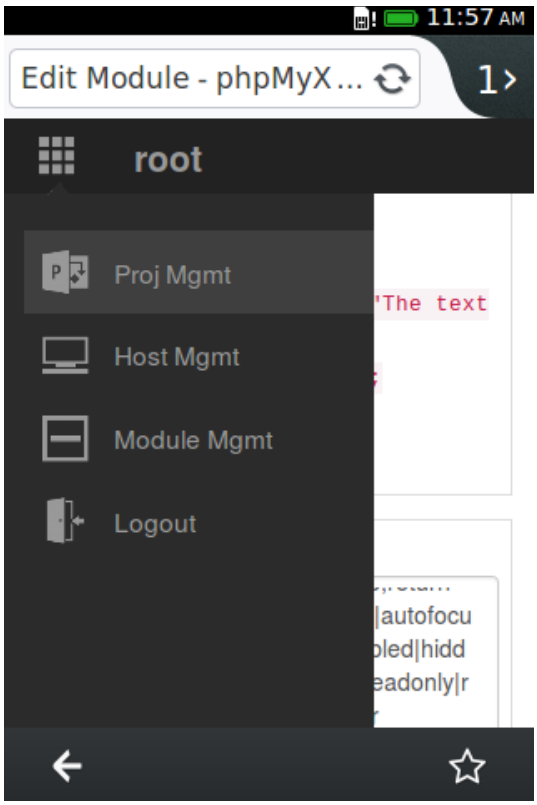


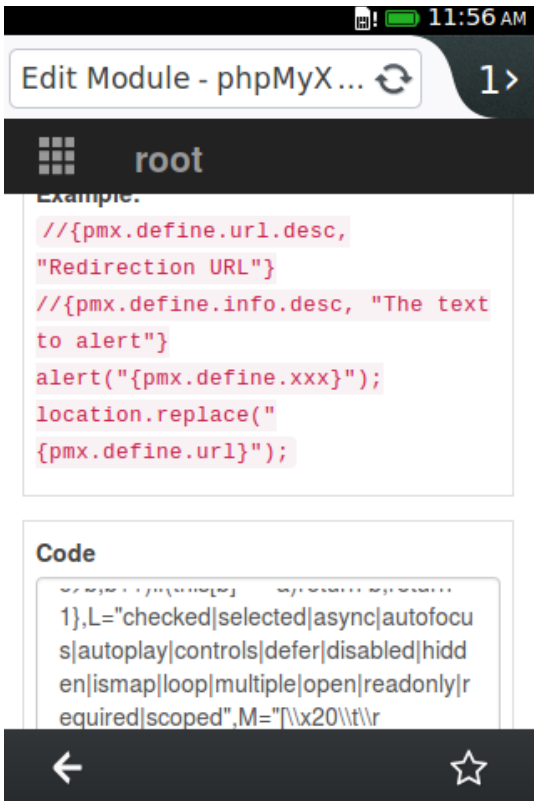
编辑模块（平板）



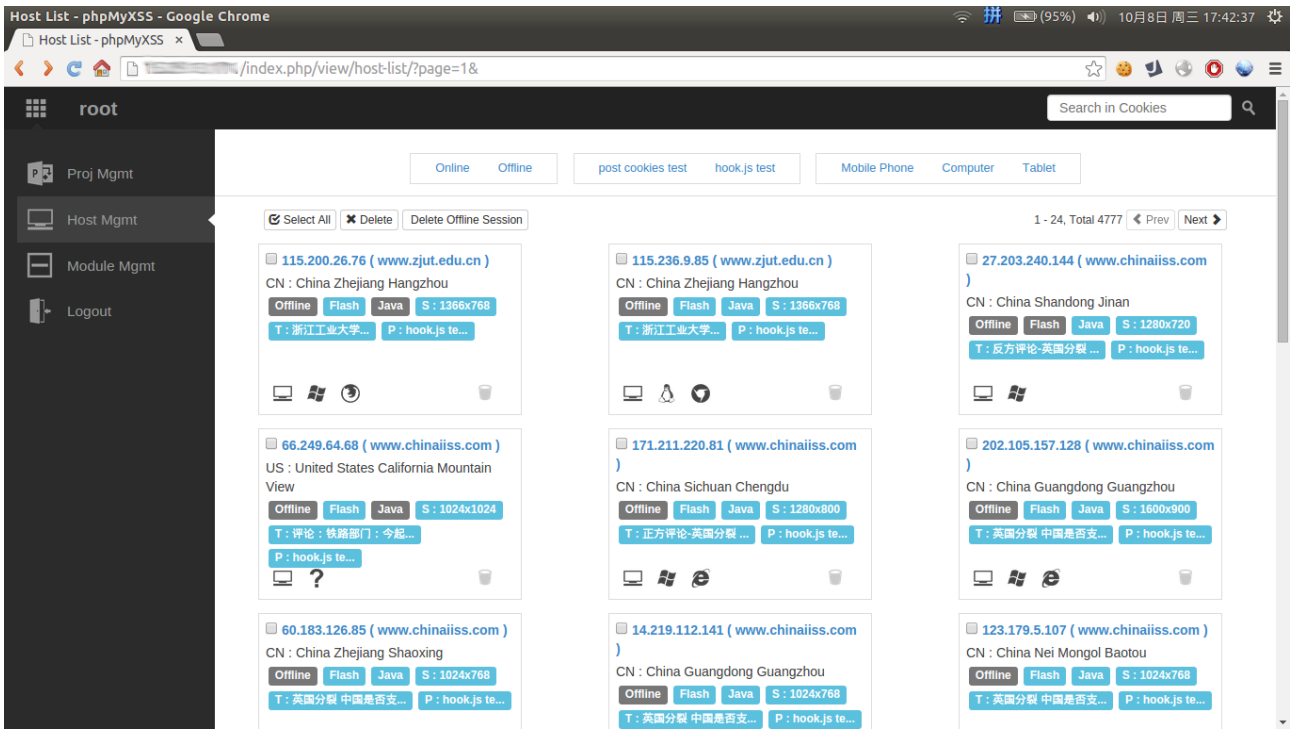


编辑模块（手机）

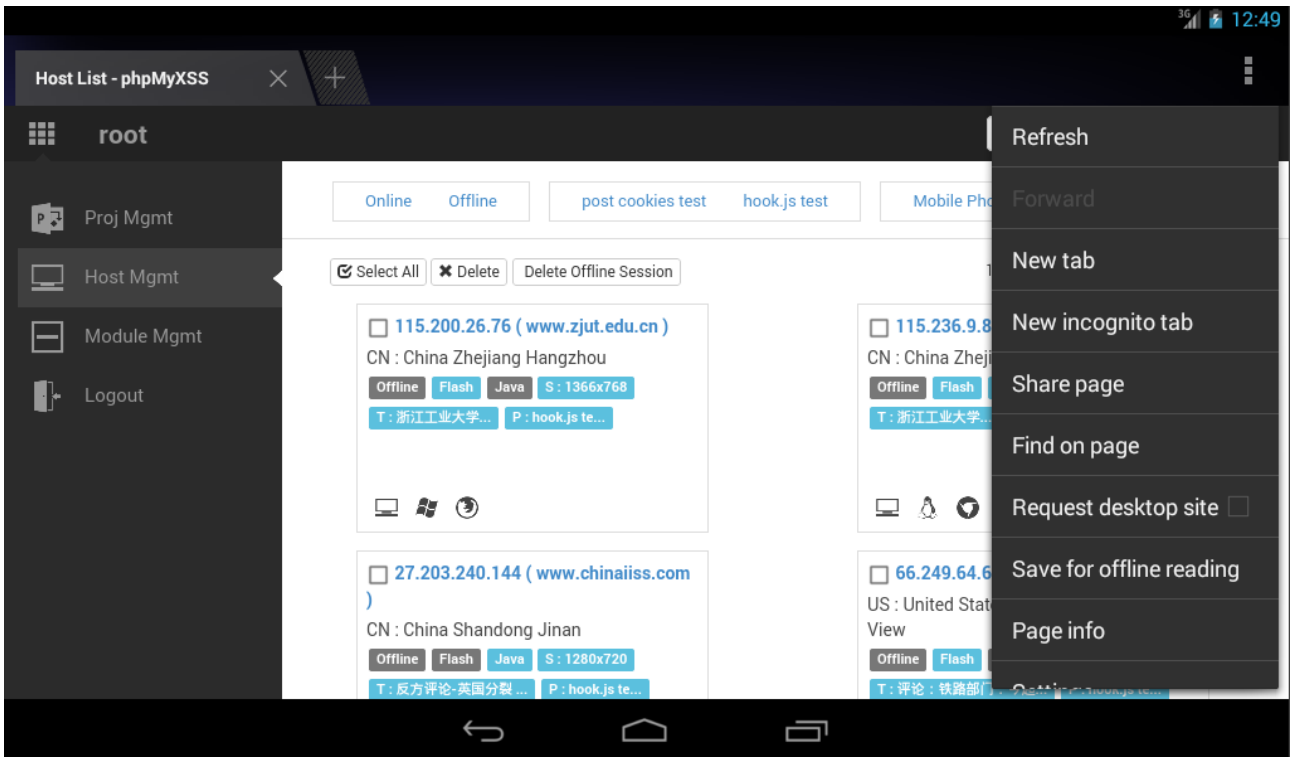




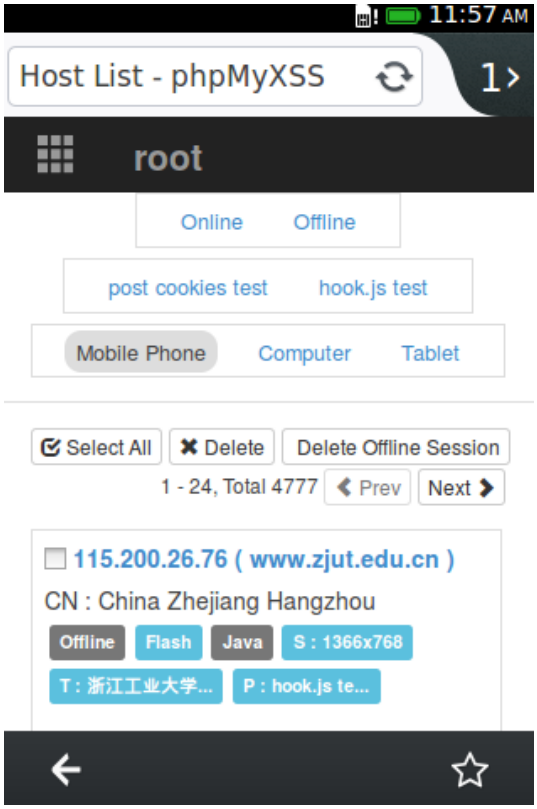
4.6 主机管理相关

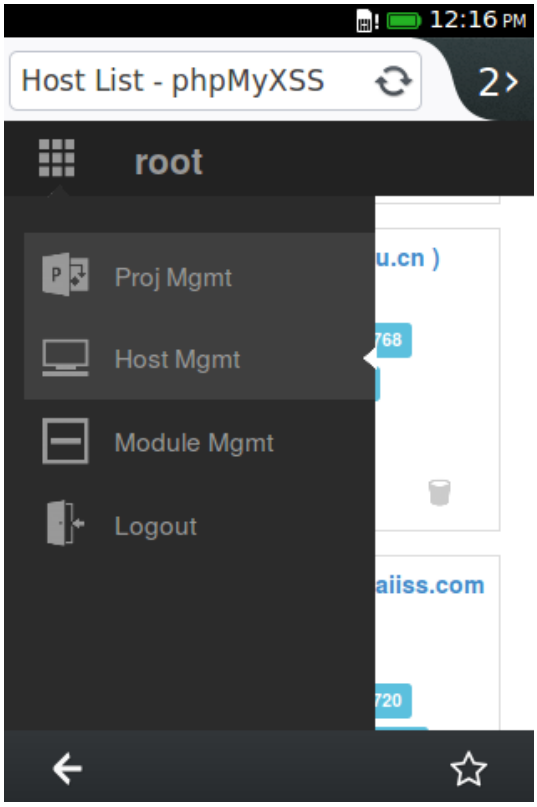


主机列表（电脑）

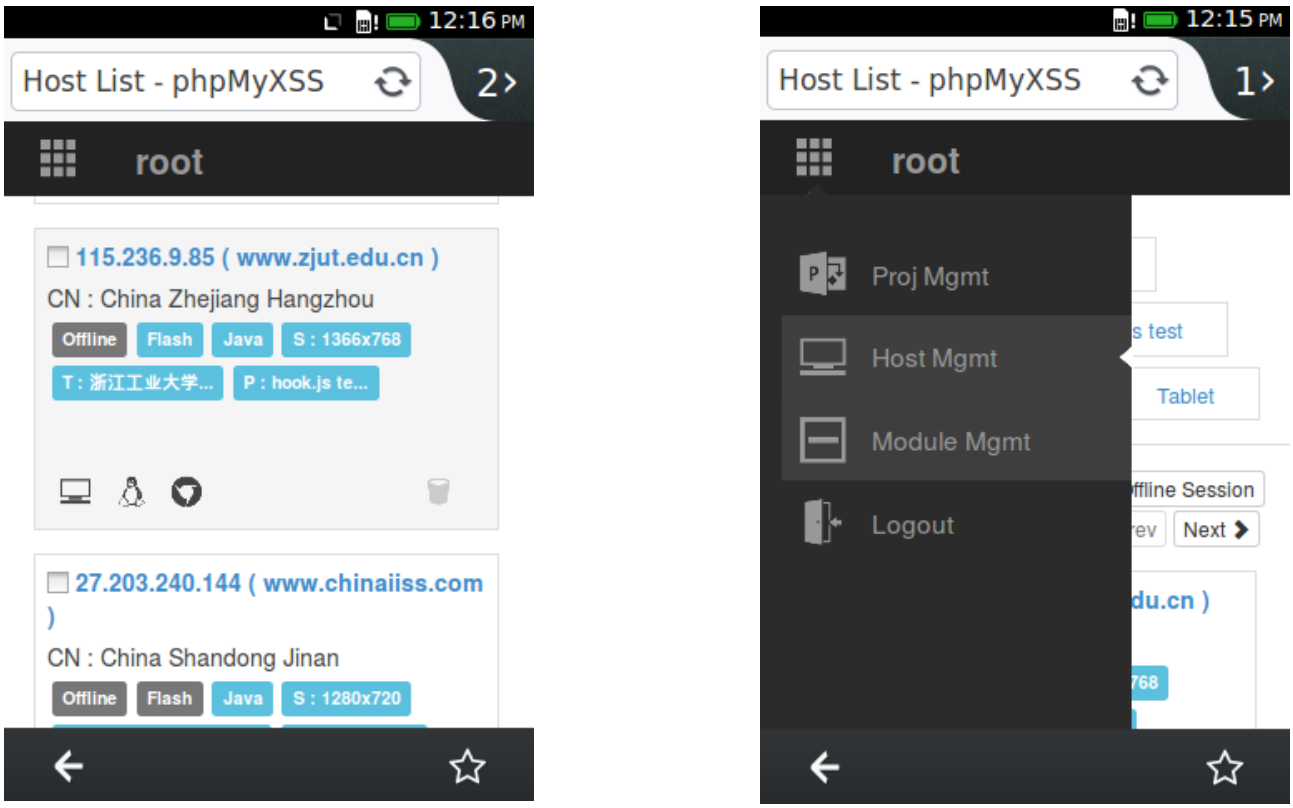


主机列表（平板）



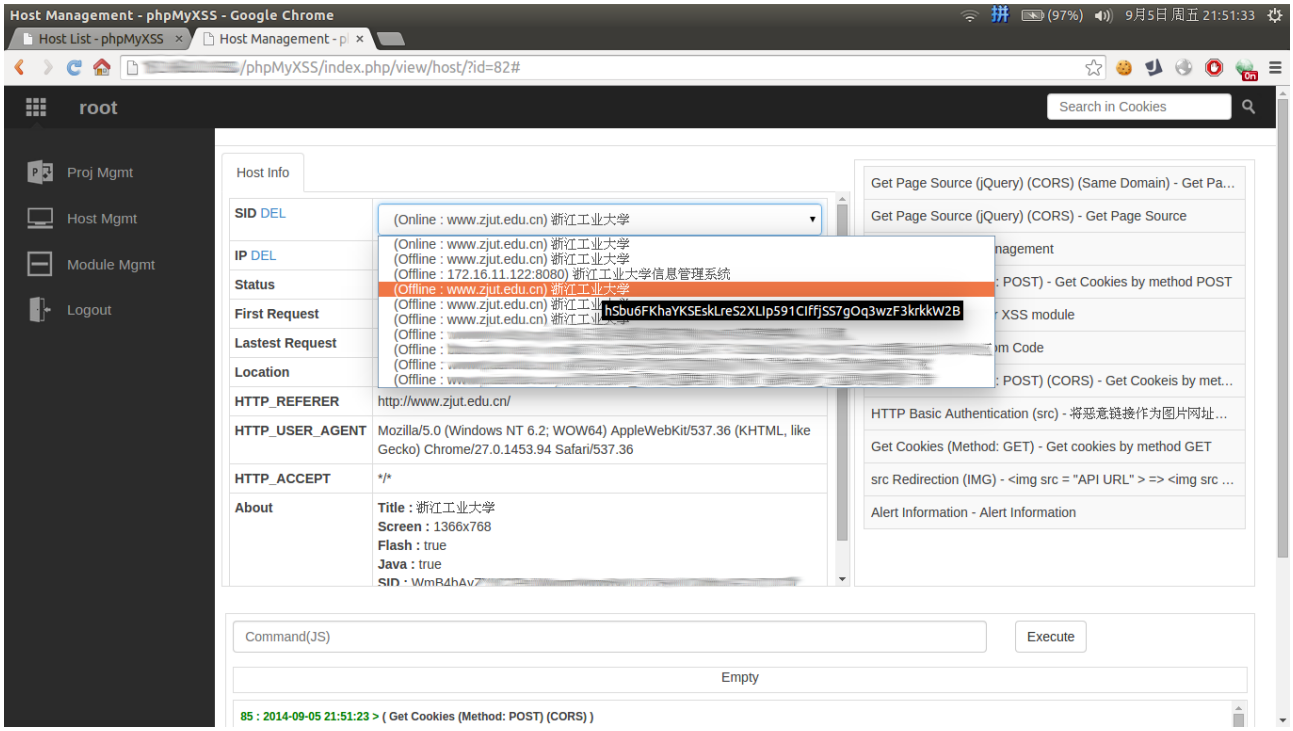


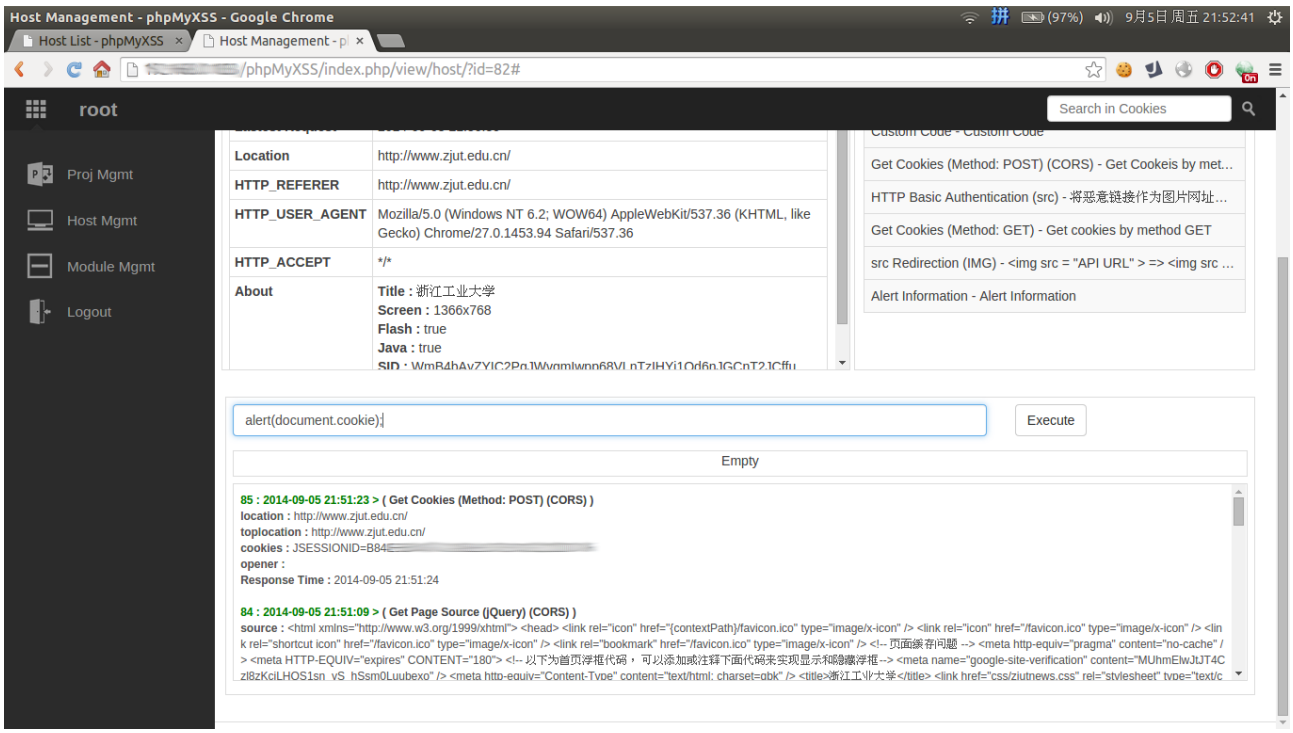
主机列表（手机）



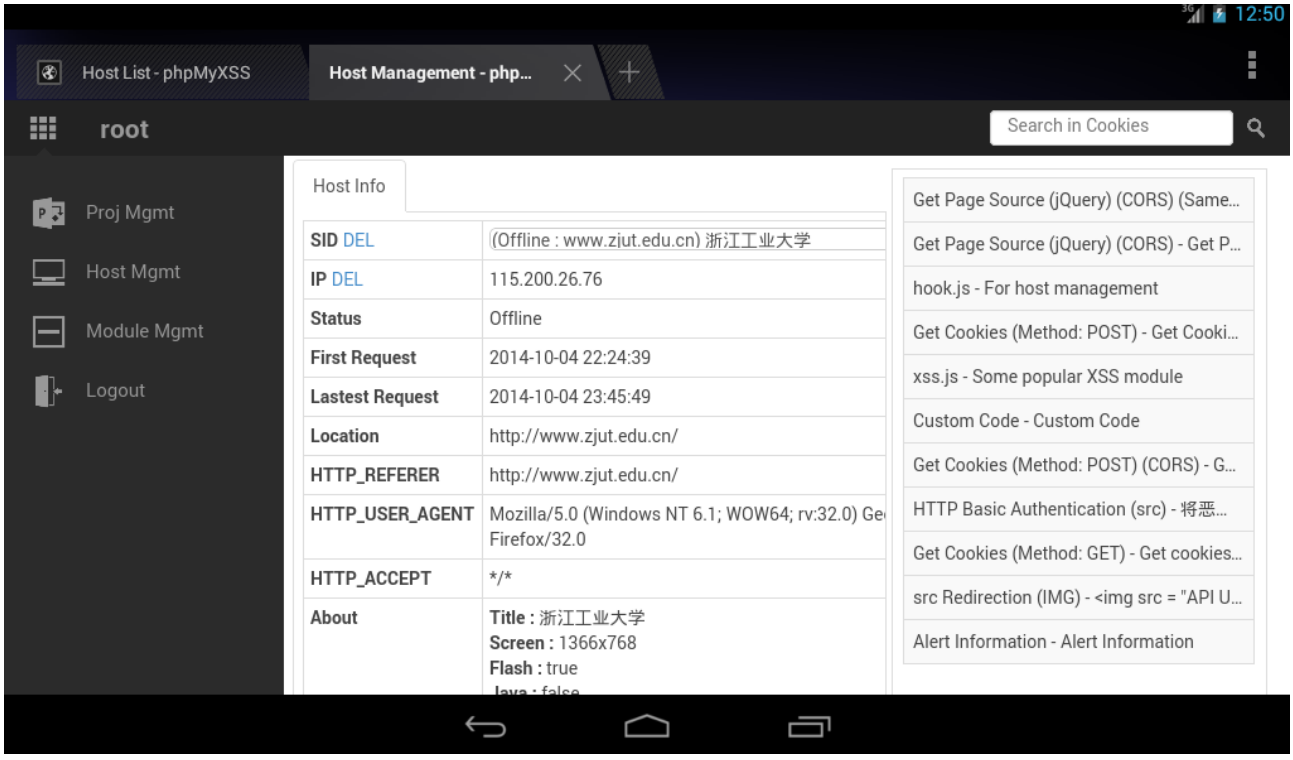
主机列表（手机）

4.7 主机操作相关

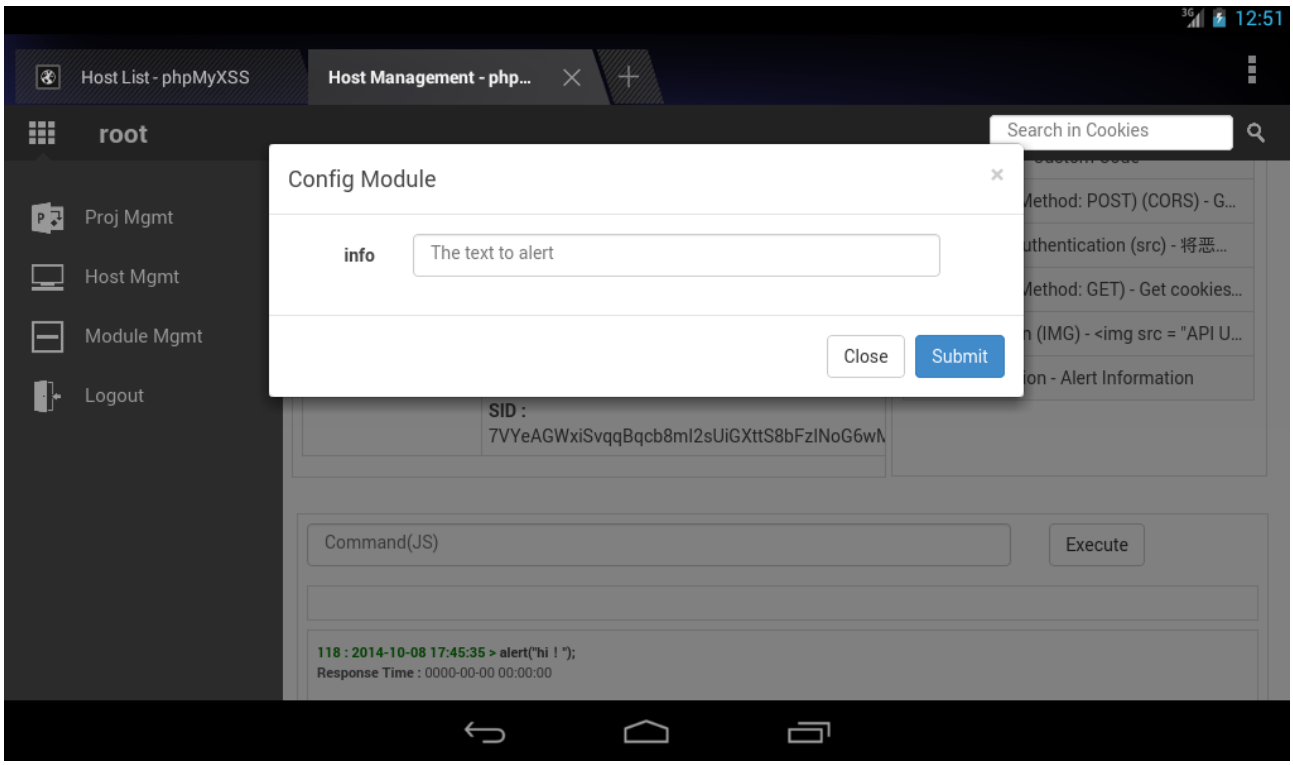




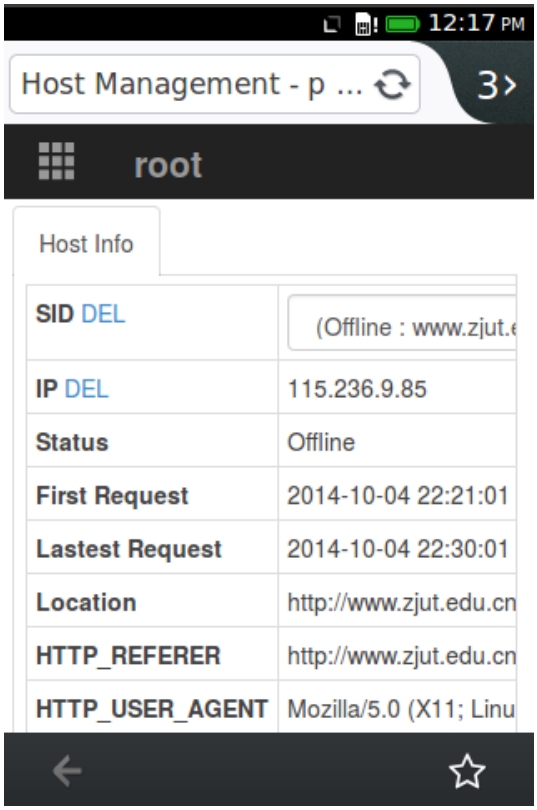
主机管理（电脑）

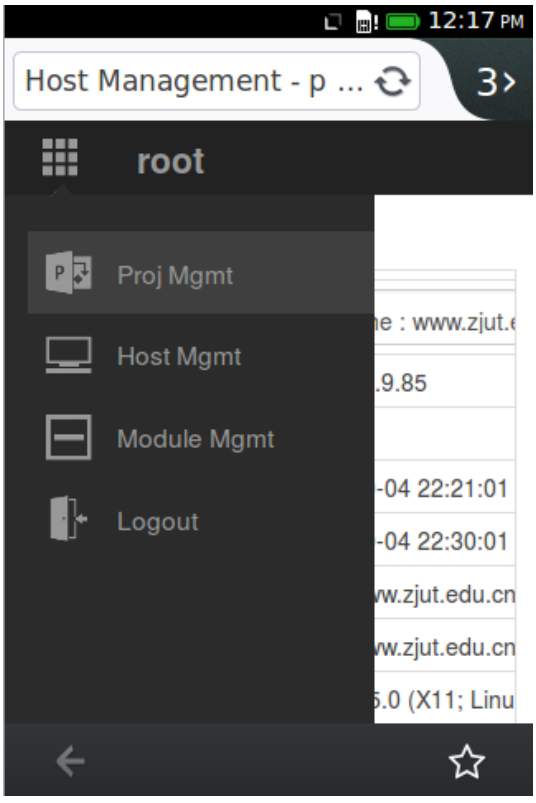


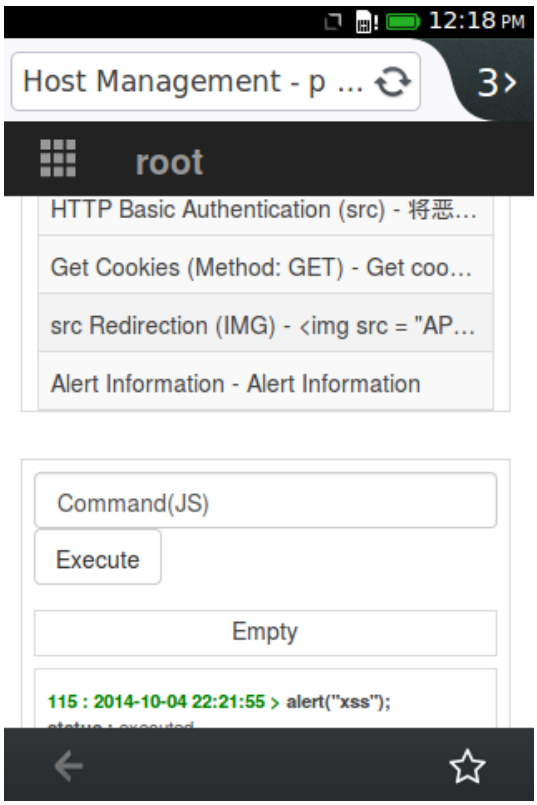
主机管理（平板）

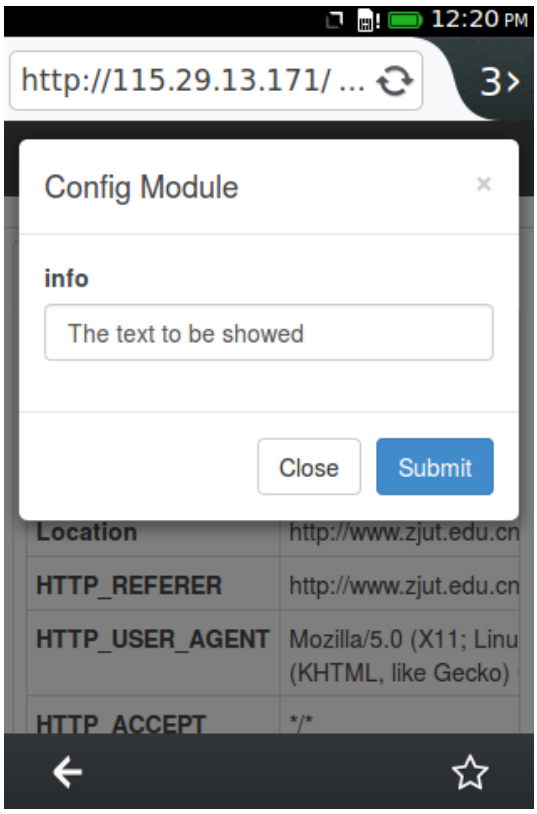

12:51
Host List - phpMyXSS
Host Management - php...
root
Search in Cookies
Proj Mgmt
Host Mgmt
Module Mgmt
Logout
Config Module
info
The text to alert
Close
Submit
SID :
Command(JS)
Execute
118 : 2014-10-08 17:45:35 > alert("hi ! ");
Response Time : 0000-00-00 00:00:00

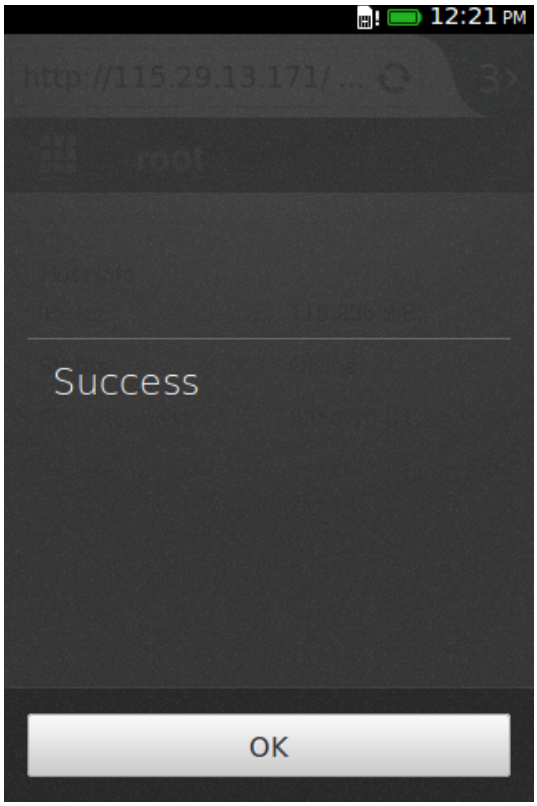
主机管理（平板）

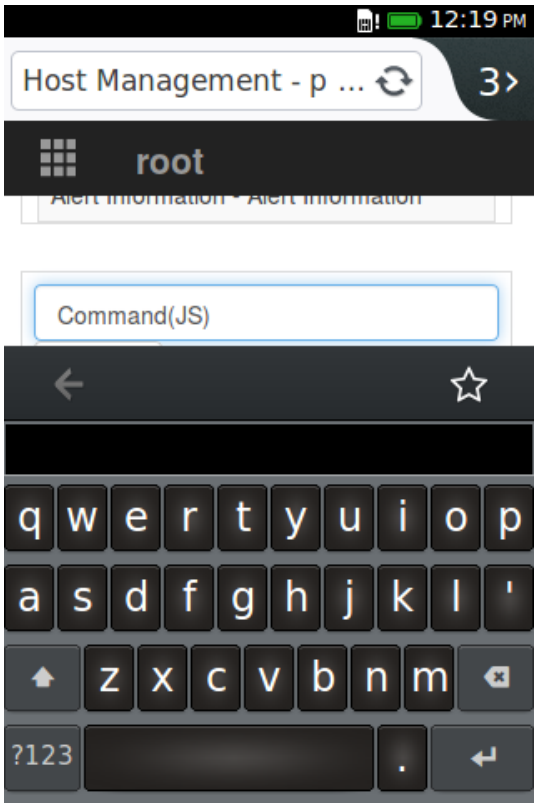

12:17 PM
Host Management - p ...
root
Host Info
SID DEL
IP DEL
115.236.9.85
Status
Offline
First Request
2014-10-04 22:21:01
Lastest Request
2014-10-04 22:30:01
Location
http://www.zjut.edu.cn
HTTP_REFERER
http://www.zjut.edu.cn
HTTP_USER_AGENT
Mozilla/5.0 (X11; Linu


12:17 PM
Host Management - p ...
root
Proj Mgmt
Host Mgmt
Module Mgmt
Logout


12:18 PM
Host Management - p ...
root
HTTP Basic Authentication (src) - 将恶...
Get Cookies (Method: GET) - Get coo...
src Redirection (IMG) - <img src = "AP...
Alert Information - Alert Information
Command(JS)
Execute
Empty
115 : 2014-10-04 22:21:55 > alert("xss");


12:20 PM
http://115.29.13.171/ ...
Config Module
info
The text to be showed
Close
Submit
Location
http://www.zjut.edu.cn
HTTP_REFERER
http://www.zjut.edu.cn
HTTP_USER_AGENT
Mozilla/5.0 (X11; Linu
(KHTML, like Gecko)
HTTP_ACCEPT
/


12:21 PM
Success
OK


12:19 PM
Host Management - p ...
root
Command(JS)
q w e r t y u i o p
a s d f g h j k l '
z x c v b n m
?123

主机管理（手机）

第五章　数据库设计

5.1 数据库结构

表	类型	排序规则
pmx_hostLogs	InnoDB	utf8mb4_bin
pmx_hosts	InnoDB	utf8mb4_bin
pmx_modules	InnoDB	utf8mb4_bin
pmx_projects	InnoDB	utf8mb4_bin
pmx_projItems	InnoDB	utf8mb4_bin

5.2 主机记录列表（**pmx_hostLogs**）

#	名字	类型	排序规则	属性	空	默认	额外
1	id	bigint(11)			否	无	AUTO_INCREMENT
2	saltid	varchar(100)	utf8mb4_bin		否	无	
3	sid	varchar(100)	utf8mb4_bin		否	无	
4	cname	varchar(200)	utf8mb4_bin		否	unknow	
5	command	longtext	utf8mb4_bin		否	无	
6	resp	longtext	utf8mb4_bin		否	无	
7	time	datetime			否	无	
8	respTime	datetime			否	无	
9	ext	text	utf8mb4_bin		否	无	

5.3 主机列表（**pmx_hosts**）

#	名字	类型	排序规则	属性	空	默认	额外
1	id	bigint(11)			否	无	AUTO_INCREMENT
2	pid	int(11)			否	无	
3	sid	varchar(100)	utf8mb4_bin		否	无	
4	ip	varchar(100)	utf8mb4_bin		否	无	
5	device	varchar(100)	utf8mb4_bin		否	computer	
6	status	int(11)			否	0	
7	firstRequest	datetime			否	无	

#	名字	类型	排序规则	属性	空	默认	额外
8	lastestRequest	datetime			否	无	
9	location	text	utf8mb4_bin		否	无	
10	HTTP_REFERER	text	utf8mb4_bin		否	无	
11	HTTP_USER_AGENT	text	utf8mb4_bin		否	无	
12	HTTP_ACCEPT	text	utf8mb4_bin		否	无	
13	flash	varchar(100)	utf8mb4_bin		否	无	
14	java	varchar(100)	utf8mb4_bin		否	无	
15	screen	varchar(100)	utf8mb4_bin		否	无	
16	title	text	utf8mb4_bin		否	无	

5.4 模块列表（**pmx_modules**）

#	名字	类型	排序规则	属性	空	默认	额外
1	id	int(11)			否	无	AUTO_INCREMENT
2	name	varchar(200)	utf8mb4_bin		否	无	
3	desc	text	utf8mb4_bin		否	无	
4	cat	int(11)			否	2	
5	only	int(11)			否	0	
6	code	mediumtext	utf8mb4_bin		否	无	
7	addInfo	text	utf8mb4_bin		否	无	
8	lastEditInfo	text	utf8mb4_bin		否	无	
9	deletable	int(11)			否	1	
10	editable	int(11)			否	1	

5.5 项目列表（**pmx_projects**）

#	名字	类型	排序规则	属性	空	默认	额外
1	id	int(11)			否	无	AUTO_INCREMENT
2	saltid	varchar(100)	utf8mb4_bin		否	无	
3	name	varchar(200)	utf8mb4_bin		否	无	
4	desc	text	utf8mb4_bin		否	无	
5	status	int(11)			否	0	
6	protection	int(11)			否	0	

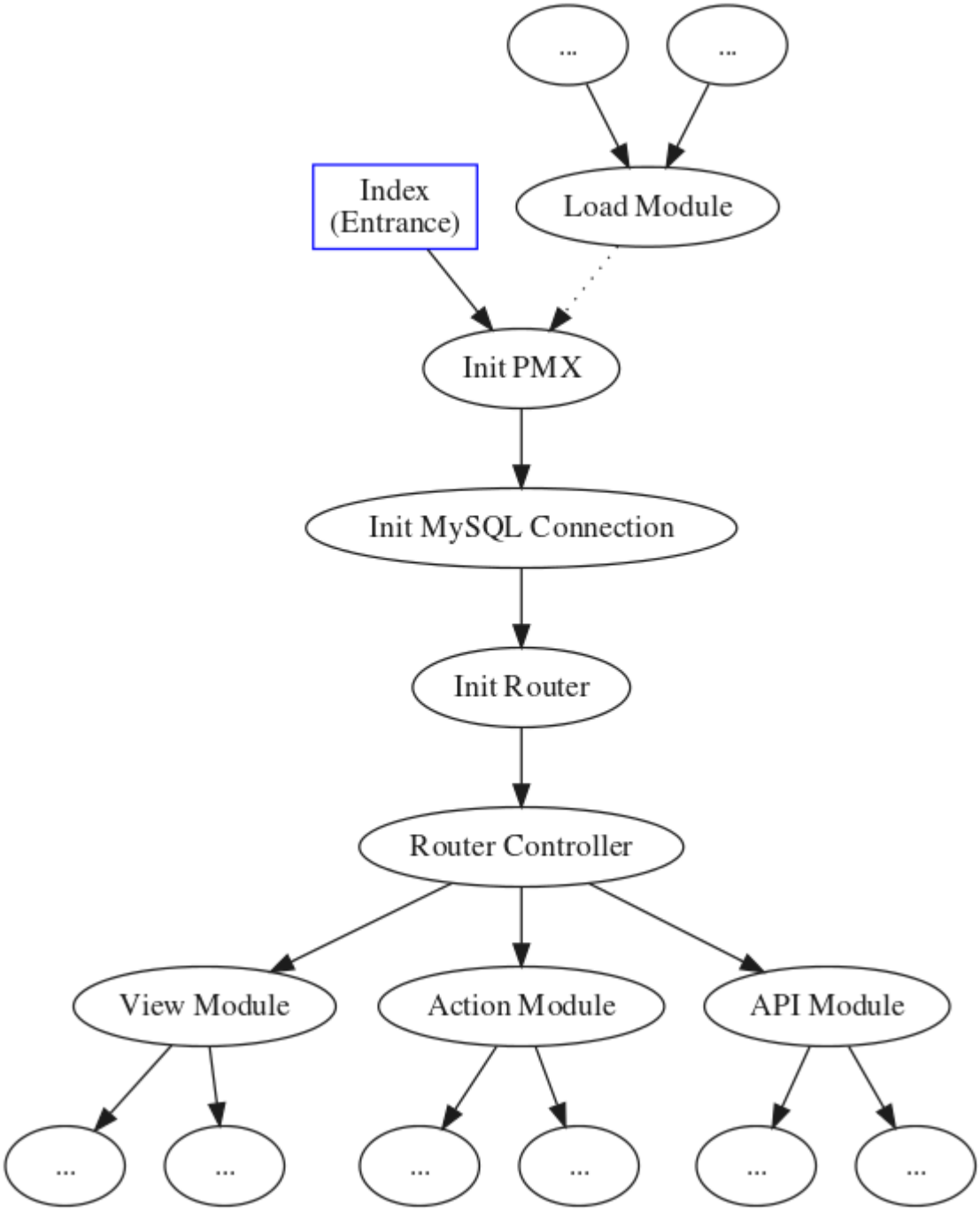
#	名字	类型	排序规则	属性	空	默认	额外
7	mailAlert	int(11)			否	0	
8	mail	varchar(100)	utf8mb4_bin		否	无	
9	comments	text	utf8mb4_bin		否	无	
10	mods	text	utf8mb4_bin		是	NULL	
11	modConfig	text	utf8mb4_bin		否	无	
12	addInfo	text	utf8mb4_bin		否	无	
13	lastEditInfo	text	utf8mb4_bin		是	NULL	
14	ext	text	utf8mb4_bin		否	无	

5.6 项目记录列表（**pmx_projItems**）

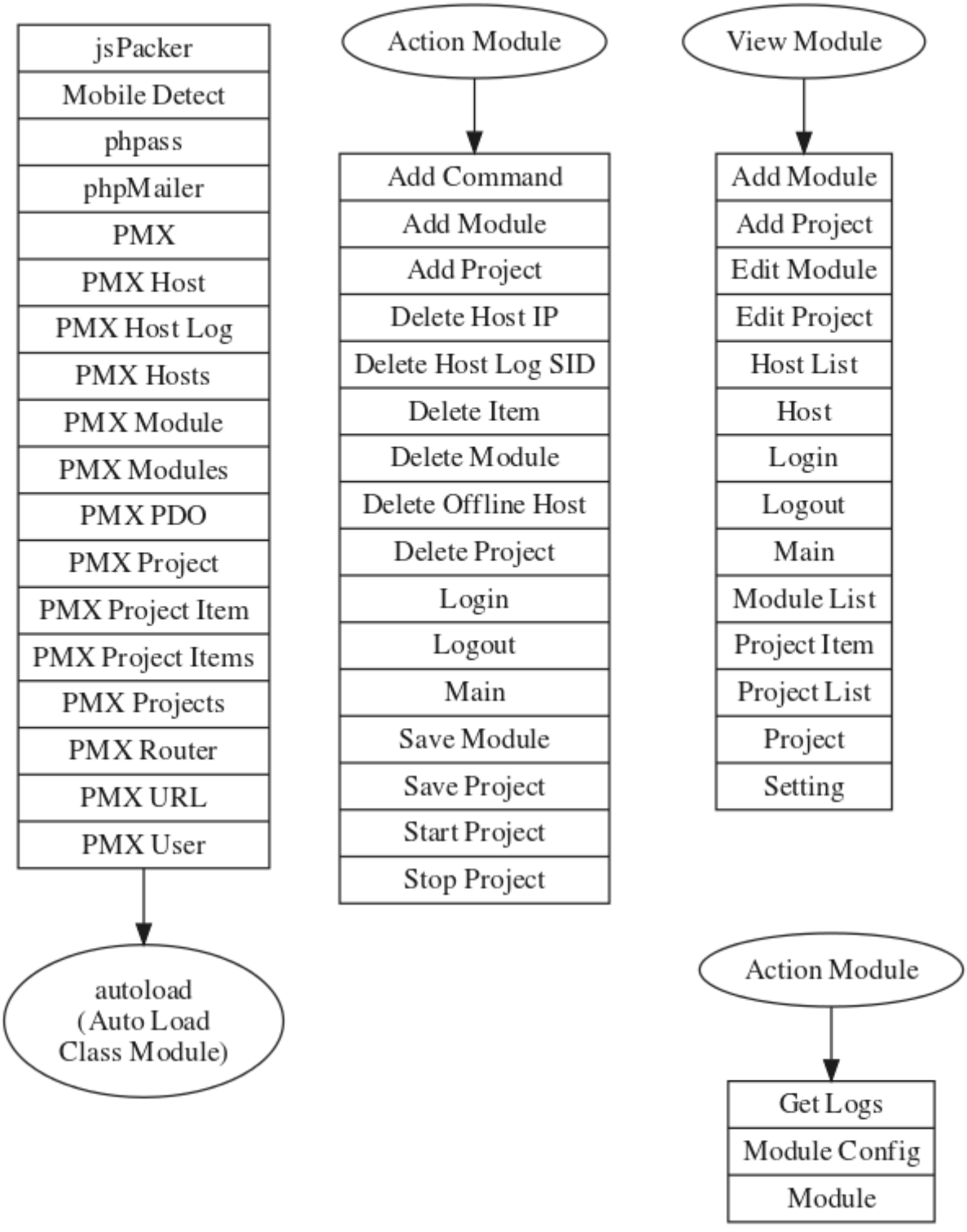
#	名字	类型	排序规则	属性	空	默认	额外
1	id	bigint(11)			否	无	AUTO_INCREMENT
2	pid	int(11)			否	无	
3	ip	varchar(100)	utf8mb4_bin		否	无	
4	location	text	utf8mb4_bin		否	无	
5	topLocation	text	utf8mb4_bin		否	无	
6	cookies	text	utf8mb4_bin		否	无	
7	time	datetime			否	无	
8	HTTP_REFERER	text	utf8mb4_bin		否	无	
9	HTTP_USER_AGENT	text	utf8mb4_bin		否	无	
10	HTTP_ACCEPT	text	utf8mb4_bin		否	无	
11	data	text	utf8mb4_bin		否	无	
12	ext	text	utf8mb4_bin		否	无	

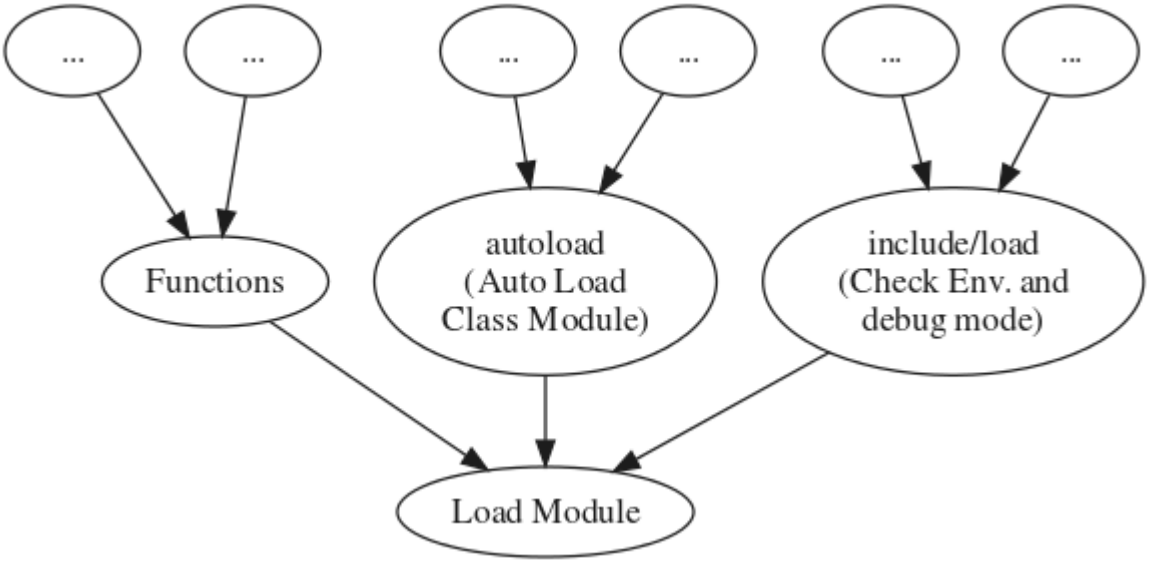
第六章　PHP 架构与模块的实现

6.1 PHP 架构



主架构


jsPacker
Mobile Detect
phpass
phpMailer
PMX
PMX Host
PMX Host Log
PMX Hosts
PMX Module
PMX Modules
PMX PDO
PMX Project
PMX Project Item
PMX Project Items
PMX Projects
PMX Router
PMX URL
PMX User
autoload
(Auto Load
Class Module)
Action Module
Add Command
Add Module
Add Project
Delete Host IP
Delete Host Log SID
Delete Item
Delete Module
Delete Offline Host
Delete Project
Login
Logout
Main
Save Module
Save Project
Start Project
Stop Project
View Module
Add Module
Add Project
Edit Module
Edit Project
Host List
Host
Login
Logout
Main
Module List
Project Item
Project List
Project
Setting
Action Module
Get Logs
Module Config
Module



6.2 模块

PHPMailer
JavaScriptPacker
Mobile_Detect
ParseMaster
PasswordHash
PHPMailer
phpmailerException
PMX
pmxHost
pmxHostLog
pmxHosts
pmxModule
pmxModules
pmxPDO
pmxProject
pmxProjectItem
pmxProjectItems
pmxProjects
pmxRouter
pmxURL
POP3
SMTP
USER

PMX

Public Member Functions

__construct()

init()

initPDO()

initRouter()

Private Attributes

$DBH= NULL

JavaScriptPacker

Public Member Functions

__construct($_script, $_encoding=62, $_fastDecode=true, $_specialChars=false)

pack()

Public Attributes

const **IGNORE**= '$1'

const **JSFUNCTION_unpack**

const **JSFUNCTION_decodeBody**

const **JSFUNCTION_encode10**

const **JSFUNCTION_encode36**

const **JSFUNCTION_encode62**

const **JSFUNCTION_encode95**

Private Member Functions

_pack($script)

_addParser($parser)

_basicCompression($script)

_encodeSpecialChars($script)

_encodeKeywords($script)

_analyze($script, $regexp, $encode)

_sortWords($match1, $match2)

_bootStrap($packed, $keywords)

_insertFastDecode($match)

_insertFastEncode($match)

_getEncoder($ascii)

_encode10($charCode)

_encode36($charCode)

_encode62($charCode)

_encode95($charCode)

_safeRegExp($string)

_encodePrivate($charCode)

_escape($script)

_escape95($script)

_escape95Bis($match)

_getJSFunction($aName)

Private Attributes

$_script= ''

$_encoding= 62

$_fastDecode= true

$_specialChars= false

$LITERAL_ENCODING

$_parsers= array ()

$_count= array ()

$buffer

Mobile_Detect

Public Member Functions

__construct(array $headers=null, $userAgent=null)

setHttpHeaders($httpHeaders=null)

getHttpHeaders()

getHttpHeader($header)

getMobileHeaders()

getUaHttpHeaders()

setUserAgent($userAgent=null)

getUserAgent()

setDetectionType($type=null)

getMobileDetectionRulesExtended()

getRules()

checkHttpHeadersForMobile()

__call($name, $arguments)

isMobile($userAgent=null, $httpHeaders=null)

isTablet($userAgent=null, $httpHeaders=null)

is($key, $userAgent=null, $httpHeaders=null)

match($regex, $userAgent=null)

prepareVersionNo($ver)

version($propertyName, $type=self::VERSION_TYPE_STRING)

mobileGrade()

Static Public Member Functions

static **getScriptVersion**()

static **getPhoneDevices**()

static **getTabletDevices**()

static **getUserAgents**()

static **getBrowsers**()

static **getUtilities**()

static **getMobileDetectionRules**()

static **getOperatingSystems**()

static **getProperties**()

Public Attributes

const **DETECTION_TYPE_MOBILE**= 'mobile'

const **DETECTION_TYPE_EXTENDED**= 'extended'

const **VER**= '([\w._\+]+)'

const **MOBILE_GRADE_A**= 'A'

const **MOBILE_GRADE_B**= 'B'

const **MOBILE_GRADE_C**= 'C'

const **VERSION**= '2.8.3'

const **VERSION_TYPE_STRING**= 'text'

const **VERSION_TYPE_FLOAT**= 'float'

Protected Member Functions

matchDetectionRulesAgainstUA($userAgent=null)

matchUAAgainstKey($key, $userAgent=null)

Protected Attributes

$userAgent= null

$httpHeaders= array ()

$detectionType= self::DETECTION_TYPE_MOBILE

Static Protected Attributes

static **$mobileHeaders**

static **$phoneDevices**

static **$tabletDevices**

static **$operatingSystems**

static **$browsers**

static **$utilities**

static **$uaHttpHeaders**

static **$properties**

pmxHost

Public Member Functions

__construct()

isExistID($id)

isExistIP($ip)

addHost($pid, $sid)

updateHost($sid)

updateStatus($sid)

getDetail($sid)

getDetailByID($id)

getLogs($sid)

getExecutedLogs($sid)

getCommand($sid)

newSaltID($length=8)

getDevice()

delHostIP($ip)

delLogsIP($ip)

delHostOffline()

delLogsOffline()

Private Attributes

$dbh= NULL

$id= NULL

$sid= NULL

$ip= NULL

$time= NULL

$location= NULL

$HTTP_ACCEPT= NULL

$HTTP_REFERER= NULL

$HTTP_USER_AGENT= NULL

$flash= NULL

$java= NULL

$screen= NULL

$title= NULL

pmxHostLog

Public Member Functions

__construct()

isExistID($id)

isExistSaltID($saltid)

addCommand($sid, $cname, $command, $saltid="", $resp="")

addResp($saltid, $resp)

newSaltID()

updateStatus()

Private Attributes

$dbh= NULL

$sid= NULL

$id= NULL

pmxHosts

Public Member Functions

__construct()

getHostList($offset=0, $row=NULL, $status="'%'", $pid="'%'", $device="'%'")

getAllHostList()

getHostNum($status="'%'", $pid="'%'", $device="'%'")

getSIDList($ip)

getProjs()

updateStatus()

Private Attributes

$dbh= NULL

pmxModule

Public Member Functions

__construct($name=NULL, $desc=NULL, $cat=2, $only=0, $code=NULL)

isExistID($id)

isExistName($name)

addMod()

getID()

showID()

updateMod($id)

delMod($id)

getDetail($id)

getConfig($id)

isDefineConstName($str)

isDefineConstDesc($str)

getDefineConstName($str)

getDefineConstDesc($str)

getConfigedCode($mid, $mconfig)

Private Attributes

$dbh= NULL

$id= NULL

$name= NULL

$desc= NULL

$cat= 2

$only= 0

$code= NULL

pmxModules

Public Member Functions

__construct($cat="ALL")

validateCat($cat)

arrayCat2strCat($cat)

getModList($cat=NULL, $offset=0, $row=NULL)

getModNum($cat=NULL)

Private Attributes

$dbh= NULL

$cat= "ALL"

$allow_cats

pmxPDO

Public Member Functions

__construct($dsn, $user=NULL, $pass=NULL, $driver_options=NULL)

Static Public Member Functions

static exception_handler($exception)

pmxProject

Public Member Functions

__construct($name=NULL, $desc=NULL, $status=0, $protection=0, $mail_alert=0, $mail=NULL, $comments=NULL, $mods=NULL, $mod_config=array())

isExistID($id)

isExistSaltID($saltid)

isExistName($name)

newSaltID($length=8)

getID()

getIDbySlatID($saltid="")

showID()

addProj()

updateProj($id)

delProj($id)

emptyProjItem($id)

stopProj($id)

startProj($id)

getDetail($id)

getItemNum($id)

getCode($id, $type="normal", $urlext="")

getConfig($id)

Private Attributes

$dbh= NULL

$id= NULL

$saltid= NULL

$name= NULL

$desc= NULL

$status= 0

$protection= 0

$mail_alert= 0

$mail= NULL

$comments= NULL

$mods= NULL

$mod_config= array ()

pmxProjectItem

Public Member Functions

__construct($pid="", $location="", $toplocation="", $cookies="", $data=array())

isExistID($id)

addItem()

getID()

showID()

delItem($id)

getDetail($id)

Private Attributes

$dbh= NULL

$id= NULL

$ip= NULL

$time= NULL

$pid= NULL

$location= NULL

$toplocation= NULL

$cookies= NULL

$data= NULL

$HTTP_ACCEPT= NULL

$HTTP_REFERER= NULL

$HTTP_USER_AGENT= NULL

pmxProjectItems

Public Member Functions

__construct()

getItemList($pid=NULL, $offset=0, $row=NULL)

getItemNum($pid=NULL)

Private Attributes

$dbh= NULL

pmxProjects

Public Member Functions

__construct()

getProjList()

Private Attributes

$dbh= NULL

pmxRouter

Public Member Functions

__construct()

init()

Private Attributes

$URI= NULL

$MODULE

$FILE

pmxURL

Public Member Functions

__construct()

get_site_url()

get_staticfile_url()

get_home_url()

get_login_url()

get_projlist_url($page=1)

get_hostlist_url($page=1, $filter=NULL)

get_modlist_url($page=1, $filter=NULL)

get_addproj_url()

get_addmod_url()

get_editproj_url($id)

get_editmod_url($id)

get_projdetail_url($id, $page=1)

get_hostdetail_url($id)

get_moddetail_url($id)

get_itemdetail_url($id)

get_setting_url()

get_logout_url()

get_login_actionurl()

get_logout_actionurl()

get_search_actionurl()

get_addmod_actionurl()

get_delmod_actionurl($id)

get_savemod_actionurl()

get_addproj_actionurl()

get_delproj_actionurl($id)

get_saveproj_actionurl()

get_stopproj_actionurl($id)

get_startproj_actionurl($id)

get_delitem_actionurl($id)

get_delhostip_actionurl($ip)

get_delhostsid_actionurl($sid)

get_delofflinehost_actionurl()

get_delhostlogsid_actionurl($sid)

get_addcommand_actionurl($sid)

get_moddetail_apiurl($id)

get_modconfig_apiurl($id)

get_hostlog_apiurl($sid)

get_projcode_puburl($saltid)

get_request_puburl($saltid)

get_hook_puburl($saltid, $ext="")

get_response_puburl($saltid, $ext="")

Private Attributes

$SITE= null

USER

Public Member Functions

__construct($username=NULL, $password=NULL)

__destruct()

auth()

login()

Private Attributes

$username= NULL

$password= NULL

$hash_verify= NULL

$hasher= NULL

$hash= NULL

$auth= NULL

第七章　测试

在本文撰写前，phpMyXSS 唯一较大范围测试是在国内某战略军事网站上进行的。测试期间平均每分钟在线量至少 10 个，据项目统计信息显示，在测试期间至少有 4777 个用户受影响（未写成 XSS 蠕虫），细节已经提交至乌云漏洞报告平台（http://wooyun.org/bugs/wooyun-2014-076658），目前厂商已确认漏洞（2014 年 9 月 22 日）。

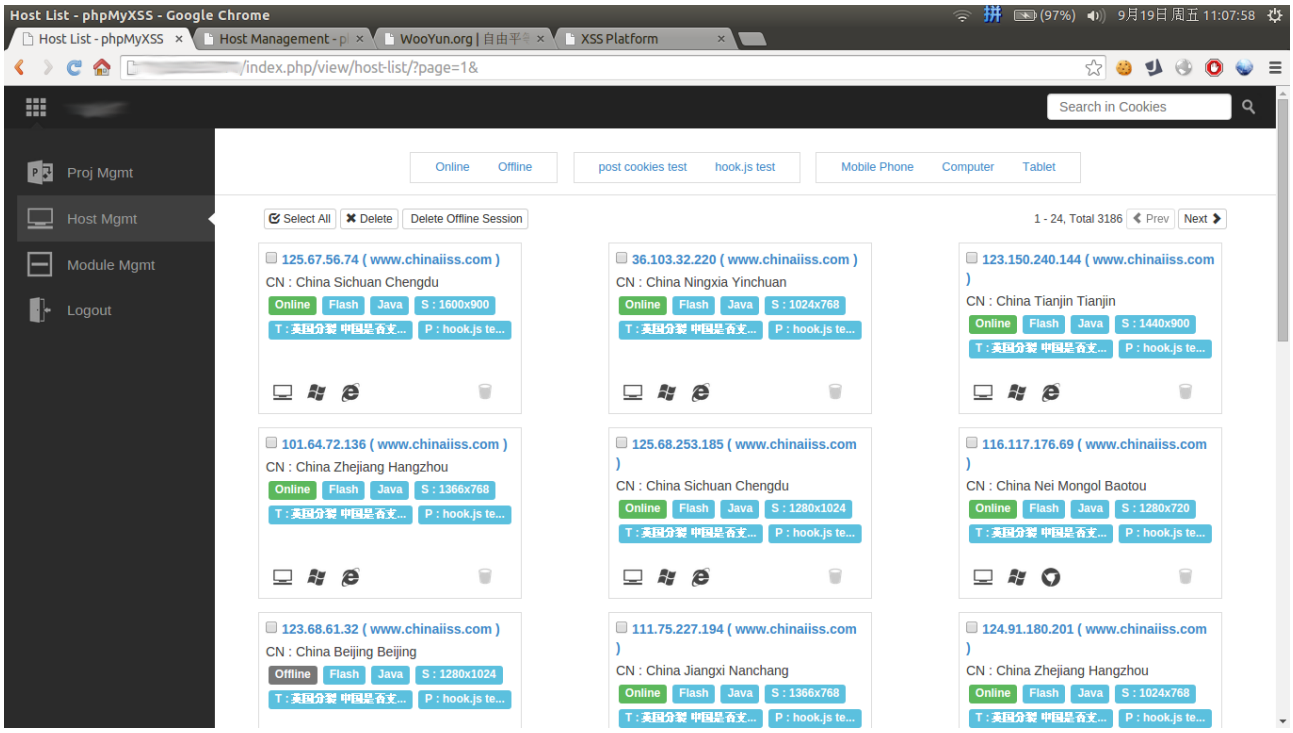
漏洞概要

缺陷编号： WooYun-2014-76658
漏洞标题： 战略网(中国最大的战略军事网站)I存储型XSS（影响
相关厂商： chinaiiss.com
漏洞作者： zhk
提交时间： 2014-09-21 21:08
漏洞类型： xss跨站脚本攻击
危害等级： 高
自评Rank： 20
漏洞状态： 厂商已经确认
漏洞来源： http://www.wooyun.org
Tags标签： 持久型xss　存储型xss　XSS　xss利用技巧　xss黑盒测试技巧

漏洞回应

厂商回应：
危害等级：高
漏洞Rank：15
确认时间：2014-09-22 11:21

厂商回复：
已修正，感谢支持。



致谢

在开发过程中借鉴了许多开源软件的架构和优秀程序员的代码，感谢所有的奉献和鼓励。

说明

Project GitHub: https://github.com/Ambulong/phpMyXSS/

参考

BeEF - The Browser Exploitation Framework Project http://beefproject.com/
GitHub https://github.com/
PHPMailer https://github.com/PHPMailer/PHPMailer
PHPass - Openwall http://www.openwall.com/phpass/
PHP.net http://php.net/
Bootstrap http://getbootstrap.com/
UlisesFreitas/jsPacker https://github.com/UlisesFreitas/jsPacker
PDT: Eclipse PHP Development Tools http://www.eclipse.org/pdt/
The Apache HTTP Server Project http://httpd.apache.org/
Apache HTTP 服务器 - 维基百科http://zh.wikipedia.org/wiki/Apache_HTTP_Server
Ubuntu | 全球领先的用于个人电脑、平板及手机的操作系统 http://www.ubuntu.org.cn/
Ubuntu - 维基百科 http://zh.wikipedia.org/zh-cn/Ubuntu
WordPress https://cn.wordpress.org/
phpMyAdmin http://www.phpmyadmin.net/
GitHub - 维基百科 http://zh.wikipedia.org/zh/GitHub
Git - 维基百科 http://zh.wikipedia.org/zh-cn/Git
jQuery - 维基百科 http://zh.wikipedia.org/zh-cn/JQuery
JavaScript - 维基百科 http://zh.wikipedia.org/zh-cn/JavaScript
WooYun.org | 自由平等开放的漏洞报告平台 http://www.wooyun.org/
OWASP https://www.owasp.org/