Tom Metzger

opensource.southernerd.us/college/seniorproject

Xpwnd

Push the boundaries of iOS.

Xpwnd is a heavily modified version of the Xcode IDE.
From apps to exploits to jailbreaks and even tweaks, Xpwnd includes everything you need to create amazing content for iOS.

Search less. Develop more.

Jailbreak & Security Research SDKs

Whether you're making the next great jailbreak, turning a bug into an exploit, or creating a tweak, the stock iOS SDK often isn't enough. Additional headers and libraries from Apple as well as from the community are must haves, but not always easy to find or to utilize.

Xpwnd provides two heavily modified versions of the iOS SDK that include all these and more. These SDKs are specially designed to aid whichever direction your projects take you, so that you can spend less time finding the right headers, and more time developing. These SDKs also provide a myriad of project templates - both robust new ones and classic ones revamped, so you don't have to waste time bootstrapping for common project types (such as tweaks, XPC Services, and dynamic libraries - all for iOS).

These headers & libraries include (but aren't limited to):

- `QiLin`
- `CSCommon.h`
- `NSTask.h`
- `patchfinder64`
- `IOKit`
- `MobileGestalt.h`

Achievements

Age-Old Issues Solved

- App icon replacement on macOS
- Adding and configuring Sparse SDKs to Xcode
- Finding path to executable from its handle

Tasks Accomplished

- Xpwnd is in a stable beta state
- Two-tier plugin system
- App that implements plugin system
- Jailbreak that uses the plugin system

In The Works

- Dynamic UI modification via property list definitions
- Self-signing imported resources
- Repo system for Outlet / Plug releases

What's Coming Next

- Theos build support for Xpwnd
- Object-oriented plugin system
- Colorful console output

Fusebox

Power the future of jailbreaking.

Fusebox is the world's first forward-thinking jailbreak tool.
By utilizing an extensive two-tier plugin system and providing a robust set of developer tools, Fusebox makes it easy for developers to build modular jailbreaks, and easy for users to acquire them.

Better. Safer. Simpler.

A New Way To Jailbreak

Fusebox lets users jailbreak their device like never before. It features a two-tier plugin system, which allows developers to modularize their jailbreaks so that exploits are easily replaceable in the future. With Fusebox's repo system, you can install and update jailbreaks from trusted sources - never again will you have to download an IPA file from an unvetted website or try to build from source code. All jailbreaks hosted on a repo are required to be open source, creating a safer experience for users, as well as a better learning environment for new developers.

Outlets & Plugs.

Two-Tier Plugin System

With its two-tier plugin system, Fusebox makes it simple for developers to manage and add features to your jailbreak on the fly using dynamic libraries. At the bottom tier, Plugs contain the specific implementation of exploits or utilities, allowing Plugs that achieve the same task to be interchangeable. Outlets then allow you to abstract away the specifics of an exploit type's implementation, in order to focus solely on the control flow of the jailbreak and execute each Plug as needed. Fusebox also includes a mechanism to allow Outlets to define user-visible preferences.

Integration made easy.

Fusebox Developer SDK

Making a jailbreak is hard enough without also having to learn how to write it to be compatible with someone else's API. That's why Fusebox also comes with an SDK that abstracts away the specifics, and provides a nice, clean interface to integrate the plugin system into your jailbreak.

The Fusebox SDK also provides easy-to-use project templates to make integrating the plugin system effortless. They also feature post-build scripts that automatically handle packaging everything when you're ready to test or release.