

SandCat PHP ve Konfigürasyon Güvenliği

MUSTAFA SERHAT DÜNDAR, <SERHAT AT SERHATDUNDAR DOT COM>,
21/06/2009

TANIM :

Syhunt firmasının en iyi ürünlerinden olan Sandcat'in, tamamen php scriptler için yazılmış hali "SandCat for PHP".

VULNERABILITY CHECKS

- ☒ Cross-Site Scripting (XSS)
- ☒ File Inclusion
- ☒ SQL Injection
- ☒ Command Execution
- ☒ Weak XSS Validation

OTHER CHECKS

- ☒ Key HTML Tags
- ☒ Key AJAX / JavaScript
- ☒ Entry Points - User Input
- ☒ Entry Points - Indirect User Input
- ☒ Interesting Keywords

Custom PHP extension: Specify

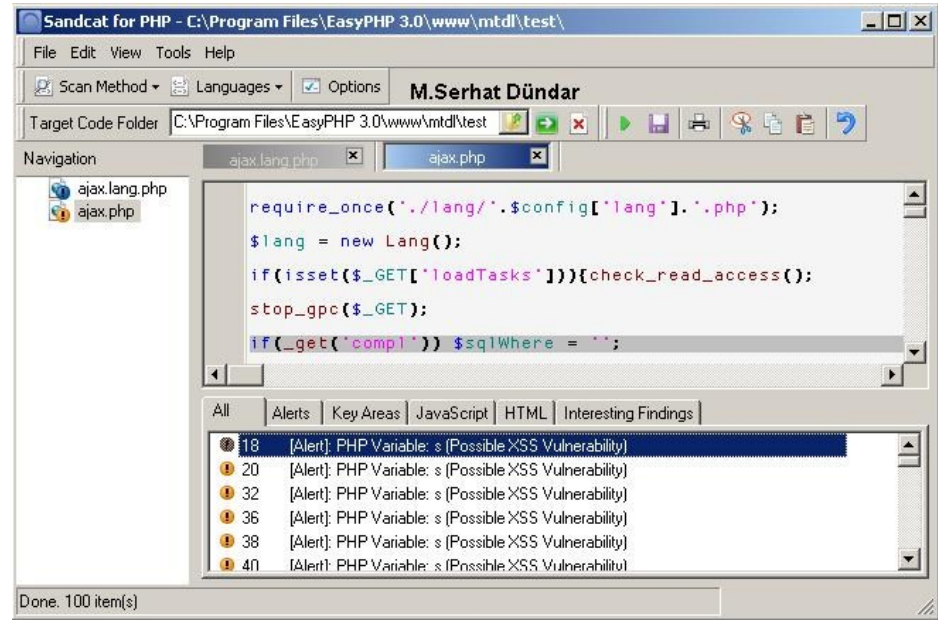
Custom PHP include extension: Specify

** Sandcat'in paranoyak yapısını unutmamak lazım. Bütün \$Post \$Get \$Sesion \$Cookie karakterleri, echo komutu ve daha bir çoğu muhtemel tehlike onun için.

* Program sadece local olarak çalışmakta.

* Ücretsiz sürümünde tek seferde sadece 2 dosya için tarama yapabilirsiniz. Fakat tarama yapacağınız toplam dosya sayısı sınırsızdır.

Örnek bir php dosyasına ait analiz :

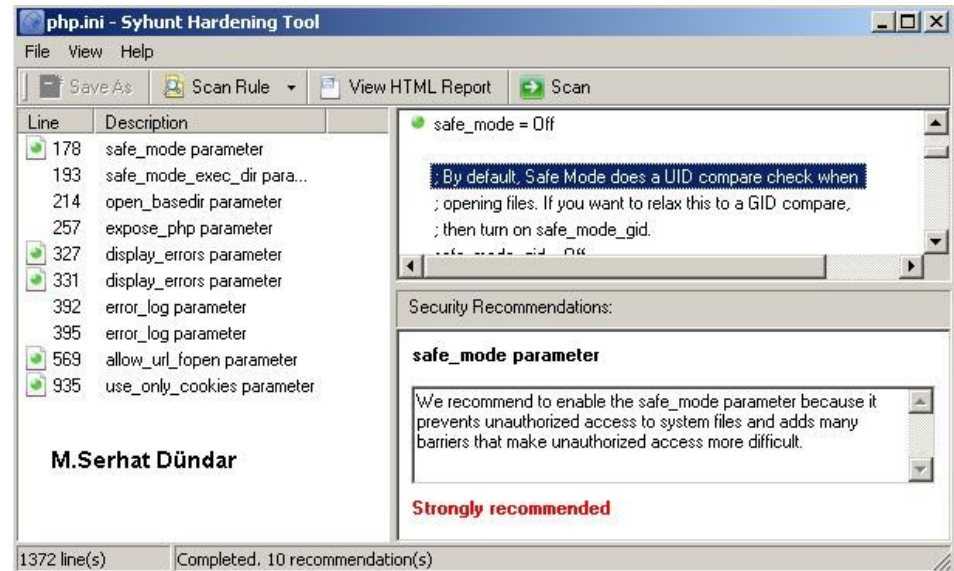


KONFIGÜRASYON DOSYALARININ GÜVENLİĞİ

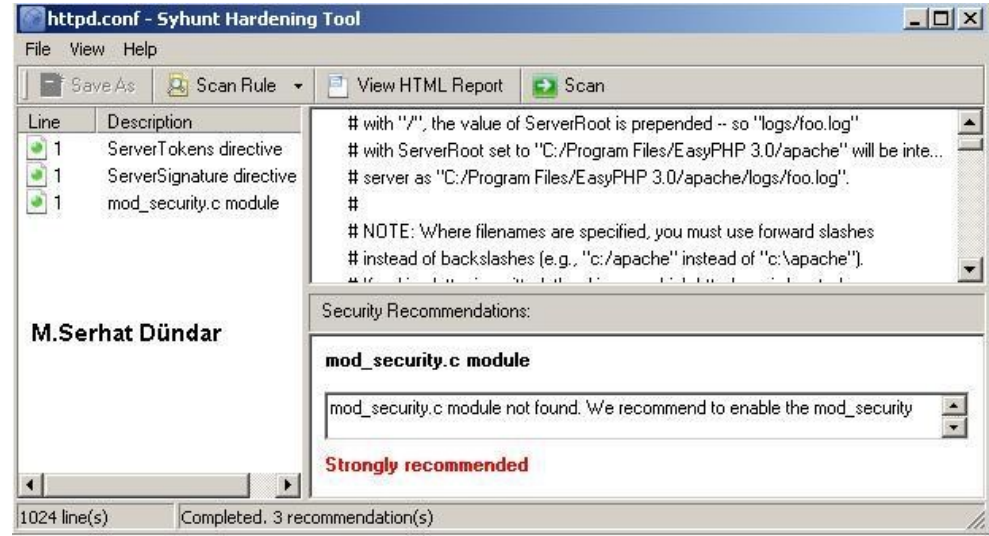
Sandcat'in bize sunduğu özellikler arasına Syhunt Hardening Tool'da bulunmakta.

Bu özellik ile php.ini, httpd.conf gibi konfigürasyon dosyalarının güvenlik ayarlarını otomatik olarak denetleyebiliyoruz.

Örnek bir php.ini dosyasına ait analiz :



Örnek bir httpd.conf dosyasına ait analiz :



Download :

<http://www.syhunt.com/>

M.SERHAT DÜNDAR