نماد امن
Namade Amn

گزارش امنیتی دامنه http://testphp.vulnweb.com

دامنه مذکور توسط ابزار های Acunetix، Nmap، SQLmap و Nikto تست گردید که خلاصه آسیب پذیری های دامنه بر اساس ابزار معرفی شده در زیر آمده است:

Acunetix

درباره نرم افزار: این نرم افزار بعنوان یکی از پیشتاز ترین تکنولوژی های اسکن امنیتی نرم افزارهای تحت وب از سال ۱۹۹۷ فعالیت خود را آغاز نموده و بعنوان محبوب ترین نرم افزار آنالیز و تشخیص آسیب پذیری های نرم افزار معرفی شده است. از جمله ویژگی های این نرم افزار شامل:

- تکنولوژی AcuSensor
- تست کننده آسیب پذیری های تزریق SQL و همچنین XSS
- ابزاری برای تست نفوذ (Penetration Testing) همانند HTTP Editor و HTTP Fuzzer
- رکورد شماتیک ماکرو که تست فرم های وب و رمز عبور را آسان می سازد
- پشتیبانی از صفحات دارای CAPTCHA، Single sign-on و همچنین مکانیزم اعتبار سنجی two factor
- گزارش های متعدد پذیریش پرداخت های بانکی PCI
- خزنده (crawler) هوشمند در جهت تشخیص نوع وب سرور، زبان برنامه نویسی
- اسکن نوع های مختلف وب سایت شامل HTML۵، SOAP و AJAX
- اسکن پورت و چک نمودن سرویس های شبکه که بر روی سرور اجرایی می باشند

نتیجه اسکن امنیتی: *۱ آسیب پذیری ریسک بالا / ۲ آسیب پذیری با ریسک متوسط / ۵ آسیب پذیری با ریسک پایین / ۲ آسیب پذیری با ریسک اطلاعاتی*

نام آسیب پذیری	توضیحات
nginx SPDY heap buffer overflow	هکر می تواند موجب سرریز بافر حافظه heap توسط درخواست های طراحی شده و مخرب گردد و در نهایت وب سرور از دسترس خارج می گردد.
HTML form without CSRF protection	هکر می تواند کاربر وب سایت را مجبور به اجرای دستوراتی خارج از درخواست های کاربر نماید و در صورتی که کاربر، مدیر وب سایت باشد می تواند بر روی کل وب سایت / نرم افزار تاثیر گذارد. مسیر های تاثیر پذیر در دامنه شامل: / /guestbook.php

	/hpp /login.php /signup.php
User credentials are sent in clear text	نفر سومی امکان رویت اعتبارات کاربری را با تفسیر درخواست HTTP کاربر خواهد داشت و موجب لو رفتن اطلاعات سیستم و کاربر خواهد شد. مسیر های تاثیر پذیر در دامنه شامل: /login.php /signup.php
Clickjacking: X-Frame-Options header missing	امکان نمایش قالب ها و یا منو هایی بر روی وب سایت اصلی وجود دارد که موجب فریب کاربر و هدایت آن به وب سایت مخرب می گردد و مسیر تاثیر پذیر آن Webserver می باشد.
Broken links	مشکل در پیمایش وب سایت با وجود لینک های شکسته مسیر های تاثیر پذیر در دامنه شامل: /Mod_Rewrite_Shop/Details/color-printer/۳ /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/۱ /Mod_Rewrite_Shop/Details/web-camera-a٤tech/۲ /privacy.php

این گزارش دمو بوده و سایر موارد آسیب پذیر نمایش داده نشده است.

Nmap

درباره نرم افزار: nmap نرم افزاری است که در حقیقت برای مدیران شبکه و سیستمـ طراحی شده است تا بوسیله آن بررسی کنند که در شبکه کدام سرورها در حال کار بوده و چه سرویسهایی را ارائه میکنند. این نرم افزار تکنیکهای گسترده‌ای از انواع اسکن را پشتیبانی میکند. از این تکنیکها میتوان به UDP، TCP Connect، TCP Syn، ftp proxy، Reverse ident، ICMP، FIN، Ack sweep، Xmas Tree، Syn sweep، IP protocol و NULL scan اشاره کرد. این تکنیکها جلوتر شرح داده خواهند شد. بجز این قابلیتها، nmap برخی قابلیتهای پیشرفته مانند تشخیص سیستم عامل میزبان از طریق تکنیک TCP/IP Fingerprinting، اسکن Stealth، dynamic delay، اسکن موازی (Parallel scanning)، تشخیص میزبانهای خاموش با استفاده از اسکن موازی، اسکن decoy،تشخیص فیلتر پورت، اسکن مستقیمـ RPC و مشخصات قابل انعطاف هدف و پورت را ارائه میکند.

۱۲ پورت از ۱۰۰۰ پورت اسکن شده بر روی سرور باز می باشد:

نتیجه اسکن امنیتی: ۴ *آسیب پذیری ریسک بالا* / ۲ *آسیب پذیری با ریسک متوسط*

اسامی پورت ها و سرویس ها
پورت ۲۱ مرتبط با FTP نسخه ProFTPD ۱,۳,۳e دارای آسیب پذیری ریسک بالا
پورت ۲۲ مرتبط با SSH نسخه OpenSSH ۵,۳p۱ Debian ۳ubuntu۷,۱ دارای آسیب پذیری ریسک بالا
پورت ۲۵ نسخه Postfix smptd
پورت ۵۳
پورت ۸۰ نسخه nginx ۱,۴ دارای آسیب پذیری ریسک بالا
پورت ۱۰۶ سرویس pop3pw
پورت ۱۱۰ سرویس pop۳
پورت ۱۴۳ سرویس imap
پورت ۴۵۶ سرویس ssl/smtp
پورت ۹۹۳ سرویس ssl/imap
پورت ۹۹۵ سرویس ssl/pop۳
پورت ۸۴۴۳ نسخه lighttpd

این گزارش دمو بوده و سایر موارد آسیب پذیر نمایش داده نشده است.

SQLmap

درباره نرم افزار: Sqlmap یکی از قدرتمندترین و پر طرفدارترین ابزارهای PenTest می باشد که برای تشخیص و استفاده از آسیب پذیری SQL Injection مورد استفاده قرار می گیرد. این ابزار OpenSource علاوه بر قابلیت پشتیبانی از رنج وسیعی از دیتابیس ها (از جمله MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB SQLite۲)، انواع تکنیک های تزریق را نیز جهت نفوذ بکار می گیرد.

نتیجه اسکن امنیتی: *تمامی پارامتر های موجود در این دامنه بنظر غیر قابل تزریق می رسد و البته پویا نیز نمی باشند.*

این گزارش دمو بوده و سایر موارد آسیب پذیر نمایش داده نشده است.

Nikto

درباره نرم افزار: این نرم افزار متن باز به منظور اسکن آسیب پذیری های وب سرور مورد استفاده قرار می گیرد و شامل تست ۶۷۰۰ برنامه و فایل مخرب، بررسی بروز بودن بر روی ۱۲۵۰ سرور و بررسی بروز بودن نسخه بر روی ۲۷۰ سرور می باشد. همچنین پیکربندی سرور را نیز مورد آنالیز قرار می دهد.

نتیجه اسکن امنیتی: *۶ آسیب پذیری با ریسک متوسط / ۳ آسیب پذیری با ریسک پایین*

نام سرور nginx
خطای clickjacking X-Frame-Options header
آسیب پذیری Cookie created without the secure flag
هدر 'ms-author-via' یافت شد
هدر 'powered-by' با محتوای P..Shop یافت شد
هدر x-powered-by با مقدار Ples..in یافت شد
...

این گزارش دمو بوده و سایر موارد آسیب پذیر نمایش داده نشده است.