اسکریپت های NAMP

WWW.KALIBOYS.COM

نام اسکریپت	توضیحات مربوط به اسکریپت
afp-path-vuln	شناسایی آسیب‌پذیری پیمایش دایرکتوری Mac OS X AFP، CVE-2010-0533.
broadcast-avahi-dos	جستجو برای پیدا کردن میزبان ها در شبکه ی محلی با استفاده از پروتکل کشف سرویس DNS و ارسال یک بسته ی NULL UDP به هر میزبان برای آزمایش در صورتی که بسته ی انکار سرویس Avahi NULL UDP آسیب پذیرباشد(CVE-2011-1002).
clamav-exec	استفاده از سرورهای آسیب پذیر ClamAV برای اجرای دستور clamav نامعتبر است.
distcc-cve2004-2687	شناسایی و استفاده از یک آسیب پذیری کد از راه دور در daemon compiled distcc. این آسیب پذیری در سال ۲۰۰۲ منتشر شد، اما هنوز هم در اجرای کنونی به دلیل پیکربندی نادرست سرویس وجود دارد.
dns-update	تلاش برای به روز رسانی DNS پویا بدون احراز هویت.
firewall-bypass	شناسایی آسیب پذیری در netfilter و دیگر فایروال ها که از برنامه های کمکی برای پورت های باز پویا برای پروتکل هایی مانند ftp و sip استفاده می‌کنند.
ftp-libopie	بررسی اینکه FTPd متمایل به CVE-2010-1938(سرریز پشته جدا از یک OPIE)، آسیب پذیری است که توسط Maksymilian Arciemowicz و Adam "pi3" Zabrocki شناسایی شده است. برای راهنمایی https://nmap.org/r/fbsd-sa-opie رامشاهده کنید. توصیه می‌شود که اگر بر ضد میزبان آسیب‌پذیر اجرا شود، این اسکریپت FTPd را تخریب خواهد کرد.
ftp-proftpd-backdoor	معیارهایی برای وجوددرب‌پشتی ProFTPD 1.3.3c به عنوان OSVDB-ID 69562 گزارش شده است. این اسکریپت به‌طور پیش فرض اقداماتی را برای به کارگیری درب‌پشتی از فرمان id بی-خطراستفاده می کند، اما می تواند با آرگومان‌های اسکریپت ftp-proftpd-backdoor.cmdتغییر کند.
ftp-vsftpd-backdoor	معیارهایی برای وجود درب‌پشتی vsFTPd 2.3.4 در 2011-07-04 گزارش شده است-(CVE 2011-2523). این اسکریپت به‌طور پیش فرض اقداماتی را برای به کارگیری مخفیانه از فرمان id بی‌خطراستفاده می کند، اما می تواند با آرگومان‌های اسکریپت exploit.cmd یا ftp-vsftpd-backdoor.cmd تغییر کند.
ftp-vuln-cve2010-4221	بررسی برای سرریز بافر مبتنی بر پشته در سرورProFTPD ، نسخه‌ی بین 1.3.2rc3 و 1.3.3b. با ارسال تعداد زیادی از رشته‌ی TELNET_IAC ECS، محاسبه اشتباه فرآیند proftpdطول بافر و یک مهاجم از راه دور می‌تواند پشته را تغییر دهد و کد دلخواه را درمحدوده‌ی فرآیند proftpd اجرا کند(CVE-2010-4221) . احراز هویت برای به‌کارگیری از این آسیب پذیری لازم نیست.

http-adobe-coldfusion-apsa1301	اقداماتی برای به‌کارگیری از آسیب پذیری گذرگاه احراز هویت در سرورهای Adobe Coldfusion برای بازیابی مدیریت معتبر کوکی نشست است.
http-aspnet-debug	تعیین اینکه آیا برنامه‌ی ASP.NET دارای اشکال زدایی با استفاده از یک درخواست DEBUG HTTPاست.
http-avaya-ipoffice-users	اقداماتی برای شمارش کاربران در Avaya IP Office systems 7.x.
http-awstatstotals-exec	به‌کارگیری آسیب‌پذیری اجرایی کد از راه دور در Awstats Totals 1.0 تا 1.14 و احتمالا سایر محصولات مبتنی بر آن(CVE: 2008-3922) .
http-axis2-dir-traversal	به‌کارگیری آسیب‌پذیری پیمایش دایرکتوری در Apache Axis2 نسخه‌ی 1.4.1 با ارسال یک درخواست خاص به پارامترxsd (OSVDB-59001). به طور پیش‌فرض، برای بازیابی فایل پیکربندی سرویس '/conf/axis2.xml' با استفاده از مسیر '/axis2/services/' برای بازگشت نام کاربری و گذرواژه حساب کاربری تلاش خواهد کرد.
http-cookie-flags	بررسی کوکی‌ها توسط سرویس‌های HTTP تنظیم می‌شوند. گزارشاتی در مورد هر کدام از کوکی‌های نشست بدون پرچم httponly وجود دارد. گزارشاتی در مورد هر کدام از کوکی‌های نشست، در سرتاسر SSL، بدون پرچم امن به کار برده می‌شود. اگر http-enum.nse نیز اجرا شود، هر مسیر جالبی که توسط آن پیدا می شود علاوه بر ریشه بررسی می شود.
http-cross-domain-policy	فایل سیاستی دامنه‌ی مقابل(/crossdomain.xml) و فایل سیاست دسترسی مشتری (/clientaccesspolicy.xml) را در برنامه های وب بررسی کرده و دامنه های قابل اعتماد را لیست می کند. تنظیمات مجاز بیش‌ازحد، می‌تواند سبب حملات جعل درخواست از سایت دیگر شود و ممکن است به مهاجمان اجازه دسترسی به داده‌های حساس را بدهد. این اسکریپت برای شناسایی تنظیمات مجاز و قابل استفاده اسامی‌دامنه محتمل برای خرید به منظور به‌کارگیری برنامه‌ها، قابل‌استفاده است.
http-csrf	این اسکریپت آسیب پذیری های جعل درخواست از سایت دیگر(CSRF) را تشخیص می دهد.
http-dlink-backdoor	شناسایی درب‌پشتی میان‌افزار برروی برخی روترهای D-Link با تغییرعامل کاربر به یک مقدار "سری". به‌کاربردن "سری" عامل‌کاربری احرازهویت را کنارگذاشته و اجازه دسترسی مدیر به روتر را می‌دهد.
http-dombased-xss	به دنبال مکان‌هایی است که اطلاعات تحت کنترل مهاجم در DOM ممکن است برای تاثیر بر اجرای جاوا اسکریپت به روش‌های خاصی مورد استفاده قرار گیرد .این حمله در اینجا توضیح داده شده‌است: http://www.webappsec.org/projects/articles/071105.shtml
http-enum	شمارش دایرکتوری‌های به کار رفته توسط برنامه‌های رایج وب و سرورها.
http-fileupload-exploiter	فرم‌های آپلود فایل بی‌اعتبار در برنامه های وب با استفاده از تکنیک های مختلف مانند تغییر سرآیند نوع‌محتوا یا ایجاد فایل های تصویری معتبر بسته‌های اطلاعاتی در پیام را به کارمی‌گیرد.
http-frontpage-login	بررسی اینکه آیا ماشین‌های هدف برای ورود فرانت‌پیج ناشناس، آسیب‌پذیر هستند یا خیر.

http-git	بررسی برای یافتن منبع Git سند وبسایت (<something>/.git/ root و بازیابی اطلاعات پس-گرفته‌شده تاحدامکان، از جمله زبان / چارچوب، راه‌های‌دور، آخرین پیام فرستاده‌شده و شرح منبع.
http-huawei-hg5xx-vuln	شناسایی مودم‌های Huawei مدل‌های HG530x، HG520x، HG510x(و احتمالاً سایرین...)برای آسیب پذیری اعتبار راه‌دور و افشای اطلاعات آسیب‌پذیر هستند. همچنین اعتبار PPPoEو دیگر مقادیر پیکربندی موردنظر را برمی‌گزینند.
http-iis-webdav-vuln	بررسی برای آسیب‌پذیری IIS 5.1/6.0 که به کاربران دل‌خواه اجازه دسترسی به فایل‌های WebDAV ایمن را با جستجو به دنبال پوشه‌ی محافظت شده با رمز عبور و تلاش برای دسترسی به آن را می‌دهد. این آسیب پذیری در بیانیه‌ی امنیتی مایکروسافت MS09-020، https://nmap.org/r/ms09-020 قرار گرفته است.
http-internal-ip-disclosure	تعیین می کند که آیا سرور وب هنگام ارسال درخواست HTTP / 1.0 بدون سرآیند میزبان، آدرس IP داخلی خود را از افشا می کند.
http-jsonp-detection	تلاش برای یافتن نقاط انتهایی JSONP در سرورهای وب. نقاط انتهایی JSONP می تواند برای عبور از محدودیت های سیاستی خاستگاه مشترک در مرورگرهای وب استفاده شود.
http-litespeed-sourcecode-download	به کارگیری آسیب‌پذیری مسموم بایت صفر در Litespeed Web Servers 4.0.x قبل از 4.0.15 برای بازیابی کد منبع اسکریپت هدف با ارسال یک درخواست HTTP با یک بایت صفر به دنبال یک پسوند فایل txt. (CVE-2010-2333).
http-majordomo2-dir-traversal	به‌کارگیری اسیب پذیری پیمایش موجود در Majordomo2 برای بازیابی فایل‌های راه‌دور. (CVE-2011-0049).
http-method-tamper	تلاش برای عبور از منابع حفاظت شده ی گذرواژه(وضعیت HTTP 401) با دستکاری کلمه‌ی HTTP، انجام می‌شود. اگر آرایه ای از مسیر ها برای بررسی تعیین نشده باشد، سرور وب را جابه‌جا خواهد کرد وبررسی در برابر هر منبع حفاظت شده گذرواژه که آن را پیدا می کند، انجام می دهد.
http-passwd	بررسی می‌کند که آیا سرور وب در برابر پیمایش دایرکتوری، با تلاش برای بازیابی /etc/passwd یا boot.ini\ آسیب‌پذیر است یا خیر.
http-phpmyadmin-dir-traversal	به‌کارگیری آسیب‌پذیری پیمایش دایرکتوری در phpMyAdmin 2.6.4-pl1(و احتمالا سایر نسخه ها) برای بازیابی فایل های راه‌دور در سرور وب.
http-phpself-xss	جابه‌جایی سرور وب و تلاش برای یافتن آسیب‌پذیری فایل‌های PHPبرای عبور معکوس اسکریپت نویسی در سایت از طریق متغیر $_SERVER["PHP_SELF"].
http-shellshock	تلاش برای به‌کارگیری از آسیب پذیری"shellshock" (CVE-2014-6271 و CVE-2014-7169) در برنامه های وب.
http-slowloris-check	معبارهای سرور وب برای آسیب پذیری به حمله Slowloris DoS بدون انجام حمله DoS.
http-sql-injection	Spider های یک سرور HTTP به دنبال URL هایی است که حاوی آسیب پذیری درخواست ها برای حمله تزریق SQL است.

http-stored-xss	رفع فیلتر '<'(علامت بزرگتر). نشانه‌ای از آسیب‌پذیری XSSپنهانی.
http-tplink-dir-traversal	به‌کارگیری آسیب‌پذیری پیمایش دایرکتوری موجود در چندین روتر بی‌سیم TP-Link. مهاجمان ممکن است از این آسیب‌پذیری برای خواندن هر کدام از فایل‌های پیکربندی و رمز عبور از راه دور و بدون احراز هویت استفاده کنند.
http-trace	درخواست TRACE HTTPرا ارسال نموده و نشان می‌دهد که آیا متد TRACEفعال شده‌است یا خیر. اگر اشکال‌زدایی فعال باشد، فیلدهای سرآیندی را که درپاسخ تغییر کرده اند، را باز می‌گرداند.
http-vmware-path-vuln	بررسی برای آسیب‌پذیری پیمایش مسیر در VMWare ESX، ESXi، و سرور(CVE-2009-3733).
http-vuln-cve2006-3392	به‌کارگیری افشای فایل در Webmin (CVE-2006-3392).
http-vuln-cve2009-3960	به‌کارگیری cve-2009-3960 ونیز با عنوان Adobe XML External Entity Injection، شناخته می‌شود.
http-vuln-cve2010-0738	بررسی اینکه آیا هدف JBoss برای عبور از احراز هویت کنسول jmx آسیب پذیر است(CVE-2010-0738).
http-vuln-cve2010-2861	اجرای حمله پیمایش دایرکتوری دربرابر سرور ColdFusion و تلاش برای درهم کردن گذرواژه را برای کاربر مدیر. سپس استفاده از مقدار بیشتری(مخفی در صفحه وب) برای درهم کردن SHA1 HMAC ایجاد می‌کند که سرور وب برای احراز هویت به عنوان مدیر نیاز دارد. شما می توانید این مقدار را به سرور ColdFusion به عنوان مدیر بدون شکستن درهم‌ریختگی رمز عبور منتقل کنید.
http-vuln-cve2011-3192	شناسایی آسیب‌پذیری انکار سرویس در روشی که سرور وب Apache درخواست برای چند دامنه ساده/ مشترک یک صفحه را کنترل می‌کند.
http-vuln-cve2011-3368	معیارهایی برای آسیب‌پذیری CVE-2011-3368(گذرگاه پروکسی معکوس) در حالت پروکسی معکوس سرور Apache HTTP. اسکریپت ۳ معیار را اجرا خواهد کرد: • معیار loopbackبا ۳ بسته‌اطلاعاتی برای کنترل قوانین بازنویسی شده متفاوت • معیار میزبان‌های داخلی. با توجه به Contextis، ما انتظار یک تاخیر قبل‌از خطای سرور را داریم. • معیار وب سایت خارجی .این به این معنا نیست که شما می‌توانید به یک IP شبکه محلی دسترسی پیدا کنید، اما در هر حال این یک مساله مرتبط است.
http-vuln-cve2012-1823	شناسایی نصب PHP-CGI که برای CVE-2012-1823 آسیب پذیر است، این آسیب پذیری بحرانی به مهاجمان اجازه می دهد تا کد منبع را بازیابی و کد را از راه دور اجرا کنند.
http-vuln-cve2013-0156	شناسایی آسیب پذیری سرورهای Ruby on Rails برای تزریق شیء، اجرای دستورات از راه دور و حملات انکار سرویس(CVE-2013-0156) .

http-vuln-cve2013-6786	شناسایی تغییر مسیر URL و آسیب پذیری XSS در سرور وب سرور Allegro RomPager . این آسیب‌پذیری در CVE-2013-6786 اختصاص یافته‌است.
http-vuln-cve2013-7091	۰روز در تاریخ ۶ دسامبر ۲۰۱۳ توسط rubina119 منتشر شد و در Zimbra 7.2.6 اصلاح شد.
http-vuln-cve2014-2126	شناسایی اینکه آیا تجهیزات Cisco ASA برای افزایش ویژه‌ی آسیب‌پذیری Cisco ASA ASDM آسیب‌پذیر است یا خیر(CVE-2014-2126) .
http-vuln-cve2014-2127	شناسایی اینکه آیا تجهیزات Cisco ASA برای افزایش ویژه‌ی آسیب‌پذیری Cisco ASA SSL VPN آسیب‌پذیر است یا خیر(CVE-2014-2127) .
http-vuln-cve2014-2128	شناسایی اینکه آیا تجهیزات Cisco ASA برای عبور از احراز هویت آسیب‌پذیری Cisco ASA SSL VPN آسیب‌پذیر است یا خیر(CVE-2014-2128) .
http-vuln-cve2014-2129	شناسایی اینکه آیا تجهیزات Cisco ASA برای انکارسرویس آسیب‌پذیری Cisco ASA SSL VPN آسیب‌پذیر است یا خیر(CVE-2014-2129) .
http-vuln-cve2014-3704	به‌کارگیری CVE-2014-3704، و نیز با عنوان 'Drupageddon' در Drupal شناخته می‌شود. نسخه‌های 7.32 > از هسته Drupalنیز تحت‌تاثیر قرار خواهند گرفت.
http-vuln-cve2014-8877	به‌کارگیری آسیب‌پذیری تزریق کد از راه دور (CVE-2014-8877) در پلاگین مدیریت CM وردپرس. نسخه های 2.0.0 =< که شناخته شده اند تحت تاثیر قرار می گیرند.
http-vuln-cve2015-1427	این اسکریپت تلاش می کند تا یک آسیب پذیری را شناسایی کند، CVE-2015-1427، که به مهاجمان اجازه می دهد تا ویژگی های وسیله‌ی نفوذ این API را برای به دست آوردن اجرای کد از راه دور غیرمجازاستفاده کنند(RCE) .
http-vuln-cve2015-1635	بررسی برای آسیب‌پذیری اجرای کد از راه دور(MS15-034) در سیستم های ویندوز مایکروسافت (CVE2015-2015-1635).
http-vuln-cve2017-1001000	تلاش برای شناسایی آسیب‌پذیری افزایش ویژه در وردپرس 4.7.0 و 4.7.1 که به کاربران غیرمجاز، اجازه تزریق محتوا در پست‌ها را می‌دهد.
http-vuln-cve2017-5638	شناسایی اینکه آیا URL مشخص شده برای آسیب‌پذیری اجرای کد از راه دور Apache Struts آسیب‌پذیر است با خیر(CVE-2017-5638) .
http-vuln-cve2017-5689	شناسایی اینکه آیا سیستم باتکنولوژی مدیریت فعال داخلی برای افزایش ویژه‌ی آسیب‌پذیری INTEL-SA-00075 آسیب‌پذیر است یا خیر(CVE2017-5689) .
http-vuln-cve2017-8917	آسیب‌پذیری تزریق SQLکه بر جوملا اثر می‌گذارد! 3.7.x قبل از 3.7.1 اجازه می‌دهد تا کاربران غیرمجاز دستورها SQL دل‌خواه را اجرا کنند. این آسیب‌پذیری ناشی از یک جز جدید، که در نسخه 3.7. معرفی شد، در دسترس عموم قرار گرفت، که به این معنی است که می توان آن را توسط هر فرد مخربی که از سایت بازدید می‌کند، مورد بهره‌برداری قرار داد.
http-vuln-misfortune-cookie	شناسایی آسیب‌پذیری کوکی RomPager 4.07 Misfortune توسط به‌کارگیری ایمن آن.

http-vuln-wnr1000-creds	یک آسیب پذیری در سری WNR 1000 کشف شده است که به مهاجم اجازه می دهد تا مجوزهای مدیریت را با رابط روتر بازیابی کند. تست شده برروی نسخه‌ی نرم‌افزار(ها)ی دائمی: V1.0.2.60_60.0.86(آخرین) و V1.0.2.54_60.0.82NA
http-wordpress-users	شمارش کاربران در نصب وردپرس blog/CMS با به‌کارگیری آسیب‌پذیری افشاء اطلاعات موجود در نسخه‌های 2.6، 3.1، 3.1.1، 3.1.3 و 3.2-beta2 و احتمالات دیگر.
ipmi-cipher-zero	برای آسیب‌پذیری عبور از احرازهویت توسط استفاده از به‌رمز درآوردن صفر.
irc-botnet-channels	بررسی سرور IRC برای کانال‌هایی که معمولا برای بات‌نت‌های مخرب استفاده می‌شوند.
irc-unrealircd-backdoor	بررسی اینکه که سرورIRC با اجرای فرمان بر مبنای زمان (ping) و بررسی اینکه چقدر طول می‌کشد تا واکنش نشان دهد، درب‌پشتی می‌شود.
mysql-vuln-cve2012-2122	
netbus-auth-bypass	بررسی اینکه آیا سرور NetBus برای آسیب‌پذیری عبور احرازهویت که اجازه دسترسی کامل بدون دانستن گذرواژه را می دهد، آسیب‌پذیراست.
puppet-naivesigning	شناسایی اینکه آیا امضای‌خام برروی سرور puppet فعال است. این امر مهاجمان را قادر می‌سازد تا هر گونه درخواست امضای گواهی را ایجاد کرده و آن را امضا کرده و به آن‌ها اجازه جعل بعنوان عامل puppet داده شود. این می تواند پیکربندی عوامل و همچنین هر گونه اطلاعات حساس دیگر موجود در فایل های پیکربندی را فاش کند.
qconn-exec	تلاش برای شناسایی این که آیاروح QNX QCONN استماع به کاربران غیرمجازاجازه می‌دهد تا دستورها سیستم عملکردی دل‌خواه را اجرا کنند.
rdp-vuln-ms12-020	بررسی اینکه آیا دستگاه دربرابر MS12-020 RDP آسیب‌پذیر است.
realvnc-auth-bypass	آیا یک سرور VNC برای دور زدن احراز هویت RealVNC آسیب پذیر است(CVE-2006-2369).
rmi-vuln-classloader	معیارهایی مبنی بر این که Java rmiregistry اجازه دانلود کلاس را می‌دهد. پیکربندی پیش فرض rmiregistriاجازه می دهد تا کلاس ها را از URL های از راه دور دانلود کنید، که می تواند به اجرای کد از راه دور منجر شود. فروشنده (Oracle/Sun) این را به عنوان یک ویژگی طراحی طبقه بندی می کند.
rsa-vuln-roca	شناسایی آسیب‌پذیری کلید RSA دربرابر حمله‌ی فاکتورگیری برای بازیابی کلیدهای خصوصی (ROCA).
samba-vuln-cve-2012-1182	بررسی اینکه آیا ماشین‌های هدف دربرابر آسیب‌پذیری سرریز پشته ی سامبا CVE-2012-1182، آسیب‌پذیراست.
smb-double-pulsar-backdoor	بررسی اینکه آیا ماشین‌هدف در Double Pulsar SMB اجرا می‌شود.

smb-vuln-conficker	شناسایی سیستم‌های ویندوز مایکروسافت که توسط Conficker worm آلوده می‌شوند. این بررسی خطرناک است و ممکن است سیستم ها را خراب کند.
smb-vuln-cve-2017-7494	بررسی اینکه آیا دستگاه‌های هدف در برابر آسیب‌پذیری بارگذاری کتابخانه اشتراکی دل‌خواه CVE-2017-7494 آسیب‌پذیر هستند.
smb-vuln-cve2009-3103	شناسایی آسیب‌پذیری سیستم‌های ویندوز مایکروسافت برای انکار سرویس(CVE-2009-3103). این اسکریپت، اگر آسیب‌پذیر باشد، این سرویس را خراب خواهد کرد.
smb-vuln-ms06-025	شناسایی سیستم‌های ویندوز مایکروسافت با سرویس Ras RPC دربرابر MS06-025 آسیب‌پذیر هستند.
smb-vuln-ms07-029	شناسایی سیستم‌های ویندوز مایکروسافت با Dns Server RPC دربرابر MS07-029 آسیب‌پذیر هستند.
smb-vuln-ms08-067	شناسایی آسیب‌پذیری سیستم‌های ویندوز مایکروسافت دربرابر آسیب‌پذیری اجرای کد از راه‌دور شناخته شده به عنوان MS08-067. این بررسی خطرناک است و ممکن است سیستم ها را خراب کند.
smb-vuln-ms10-054	معیارهایی که آیا دستگاه‌های هدف دربرابر آسیب‌پذیری تخریب حافظه از راه‌دور SMB ms10-054، آسیب‌پذیر هستند.
smb-vuln-ms10-061	معیارهایی که آیا دستگاه‌های هدف دربرابر آسیب‌پذیری جعل هماهنگ‌کننده‌ی چاپگر ms10-061، آسیب‌پذیر هستند.
smb-vuln-ms17-010	تلاش برای شناسایی این که آیا سرور SMBv1 مایکروسافت در برابر یک آسیب‌پذیری اجرای کد از راه دور آسیب‌پذیر است(ms17-010, a.k.a. EternalBlue) . این آسیب‌پذیری به طورفعال توسط WannaCry و Petya ransomware و سایر بدافزارها مورد استفاده قرارمی‌گیرد.
smb-vuln-regsvc-dos	معیارهایی که آیا ویندوز ۲۰۰۰ مایکروسافت دربرابر تخریب در عامل regsvc توسط عدم ارجاع اشاره-گر تهی، آسیب‌پذیر است. معیارهایی که اگر سرویس آسیب‌پذیر و نیاز به یک حساب مهمان یا بالاتر برای کار داشته باشد، آسیب‌پذیر است.
smb-vuln-webexec	آسیب‌پذیری اجرای کد از راه دور بحرانی در WebExService (WebExec) وجود دارد.
smb2-vuln-uptime	تلاش برای شناسایی قطعات از دست رفته در سیستم های ویندوز توسط بررسی بازگشت زمان‌فعالیت آپدیت در طول مذاکره پروتکل SMB2 .
smtp-vuln-cve2010-4344	بررسی و/ یا به‌کارگیری سرریز پشته در نسخه‌هایی از Exim قبلی تا نسخه‌ی 4.69 -CVE-2010-4344) و افزایش آسیب‌پذیری ویژه در Exim 4.72 و قبل از آن(CVE-2010-4345).
smtp-vuln-cve2011-1720	بررسی خرابی حافظه در سرور Postfix SMTP هنگام استفاده از مکانیزم‌های احراز هویت کتابخانه Cyrus SASL (CVE-2011-1720). این آسیب پذیری می تواند امکان انکار سرویس و احتمالا اجرای کد از راه دور را بدهد.

smtp-vuln-cve2011-1764	چک کردن آسیب پذیری رشته فرمت در سرور Exim SMTP (نسخه‌ی 4.70 تا 4.75) با پشتیبانی DomainKeys Identified Mail (DKIM) (CVE-2011-1764). مکانیزم ثبت DKIM هنگام مشخص‌کننده‌های قالب رشته، ثبت برخی از قسمت‌های فیلد سرآیند DKIM-Signature را به‌کارنمی‌برد. مهاجم ازراه دور که قادر به ارسال ایمیل است، می‌تواند از این آسیب‌پذیری بهره‌برداری کرده کد دلخواه را با امتیازات Daemon Exim اجرا کند.
ssl-ccs-injection	شناسایی اینکه آیا سرور دربرابر آسیب‌پذیری "تزریق CSS" SSL/TLS آسیب‌پذیری است(CVE-2014-0224)، اولین‌بارتوسط Masashi Kikuchi کشف شد. این اسکریپت برپایه‌ی کد ccsinjection.c توسط Ramon de C Valle نوشته‌شده-است(https://gist.github.com/rcvalle/71f4b027d61a78c42607)
ssl-cert-intaddr	گزارش هر IPv4 خصوصی (RFC1918) که در زمینه های مختلف یک گواهی سرویس SSL یافت می شود. این موارد تنها در صورتی گزارش می‌شوند که خود آدرس هدف خصوصی نباشد. Nmap v7.30 یا بالاتر مورد نیاز است.
ssl-dh-params	شناسایی پارامتر Diffie-Hellman ناپایدار برای خدمات SSL/TLS.
ssl-heartbleed	شناسایی اینکه آیا سرور دربرابر خطای OpenSSL Heartbleed آسیب‌پذیر است-(CVE-2014-0160). این کد براساس اسکریپت پایتون ssltest.py توسط Jared Stafford by نوشته‌شده-است(jspenguin@jspenguin.org).
ssl-known-key	بررسی می‌کند که آیا گواهی SSL که توسط یک میزبان استفاده می‌شود دارای انگشت‌نگاری است که شامل پایگاه‌داده‌ای متشکل از کلیدهای مشکل‌دار است.
ssl-poodle	بررسی می‌کند که آیا رمزنگاری SSLv3 CBC مجاز است(POODLE) .
sslv2-drown	تعیین اینکه آیا سرور از SSLv2 پشتیبانی می‌کند، از چه نوع رمزنگاری پشتیبانی می‌کند، و معیارهایی برای CVE-2015-3197، CVE-2016-0703 و CVE-2016-0800 (DROWN).
supermicro-ipmi-conf	تلاش برای بارگیری فایل پیکربندی محافظت نشده حاوی اعتبارنامه کاربرمتن ساده برحسب کنترل-کنندگان Supermicro Onboard IPMI آسیب پذیراست.
tls-ticketbleed	شناسایی اینکه آیا سرور در برابر خطای F5 Ticketbleed آسیب‌پذیر است.
wdb-version	شناسایی آسیب‌پذیری و جمع‌آوری اطلاعات(مانند شماره‌های نسخه و پشتیبانی سخت‌افزار) از عوامل VxWorks Wind DeBug.

منبع:

https://nmap.org/nsedoc/categories/vuln.html
https://kaliboys.com/nmap-scripts/