Coverage of Detectify

Executive summary

This is an overview of the tests that Detectify will perfom during a security scan.

500+
fuzzed tests

380+
passive tests

50+
other tests

Fuzzed tests

ACME-Challenge Path Reflection XSS

Apache Superset RCE

Apache Tomcat Open Redirect

Apereo CAS XSS

Atlassian Confluence ShareLinks SSRF

Composr Plupload Flash XSS

CORS Bypass

CVE-2006-3916: Apache Expect-Header XSS

CVE-2009-1975: WebLogic XSS

CVE-2009-2163: SiteCore XSS

CVE-2011-4106: TimThumb RCE

CVE-2012-3414: SWF-Upload Flash XSS

CVE-2012-4000: CKEditor XSS

CVE-2013-4939: Yahoo! YUI IO Flash XSS

CVE-2014-100004: SiteCore Reflected XSS

CVE-2014-4161: SAP NetWeaver SRM Reflected XSS

CVE-2015-2065: WordPress wordpress-video-gallery SQL Injection

CVE-2015-5608: Joomla! com_user Open Redirect

CVE-2016-10134: Zabbix SQL Injection

CVE-2016-2386: SAP NetWeaver UDDI SQL Injection

CVE-2016-2387: SAP NetWeaver ProxyServer-Servlet Reflected XSS

CVE-2016-2389: SAP xMII Path Traversal

CVE-2016-3976: SAP NetWeaver Directory Traversal

CVE-2016-9263: XSF in FlashMediaElement

CVE-2017-10106: Oracle PeopleSoft TestServlet XSS

CVE-2017-10271: WebLogic RCE

CVE-2017-11460: SAP NetWeaver DataArchivingService servlet Reflected XSS

CVE-2017-12615: Tomcat RCE

CVE-2017-12650: WordPress plugin-loganizer Blind SQL Injection

CVE-2017-14619: phpMyFAQ XSS

CVE-2017-15946: Joomla! com_tag SQL Injection

CVE-2017-17671: vBulletin routeString LFI/RCE

CVE-2017-8514: SharePoint XSS

CVE-2017-8917: Joomla! SQL Injection

CVE-2017-9356: SiteCore Reflected XSS

CVE-2017-9506: Jira OAuth SSRF

CVE-2018-6389: WordPress Denial-of-Service

File Upload using PUT-verb

Host / XSS

Image Resize Denial-of-Service

Jira SAML/SSO XSS

Joomla! joomanager Path Traversal

LUA Injection

Magento MLX extension RCE

Microsoft Windows Arbitrary Command Execution

NGINX / WordPress HTTP Response Splitting

NGINX Alias Path Traversal

NGINX Path Traversal

phpMyFAQ Authenticated XSS

Referer / XSS

SAP NetWeaver CAFAdapterTest servlet Reflected XSS

SAP NetWeaver ConfigServlet Arbitrary Command Execution

Spring Boot Actuator SSTI

SWF-Upload Open-Redirect

Unix Arbitrary Command Execution

User-Agent / XSS

Windows HTTP-based NTLM Information Exposure

WordPress buddypress Authenticated Open Redirect

WordPress cta XSS

WordPress flashmediaelement Flash XSS

WordPress formidable Reflected XSS

WordPress mediaelement Flash XSS

WWW Authenticate Bypass

Access Control Bypass

Adobe AEM DAM swfupload XSS

Adobe AEM External Entities Injection (XXE) via Apache JackRabbit

Adobe AEM Foundation player-flv-maxi XSS

Adobe AEM Foundation slideshow XSS

Adobe AEM Foundation strobemediaplayback XSS

Adobe AEM Mobile User-Agent Test XSS

Adobe AEM S7SDK 2.11 XSS

Adobe AEM S7SDK 2.9 XSS

Adobe AEM Server-Side Request Forgery (SSRF) via OpenSocial

Adobe AEM swfupload XSS

Amazon S3 Takeover

AmCharts Reflected XSS

AngularJS Template Injection

Apache .htaccess Exposure

Apache AXIS Information Disclosure

Apache HTTP Server /server-info Exposure

Detectify AB, Långholmsgatan 34, 117 33 / Stockholm,Sweden.
Mail: general@detectify.com / Twitter: @detectify / Facebook: Detectify / Org number: 556985-9084

Apache HTTP Server /server-status Exposure

Apache HTTP Server Icon Leakage

Apache HTTP Server VHOST Disclosure

Apache Maven Disclosure

Apache Struts actionErrors XSS

Apache Struts OGNL Command Injection

Apache Struts setup in Debug-Mode

Apache Tomcat Examples Cookie Disclosure

Apache Tomcat Examples Request Disclosure

Apache Velocity XSS

APPSEC-1378: Magento Web API allows anonymous access

ASP.NET in Debug Mode

Atom /.ftpconfig Information Disclosure

Bitrix Site Manager Log Disclosure

Blind Server Side JavaScript injection (SSJI)

Blind SQL Injection in Microsoft SQL Server

Blind SQL Injection in MySQL

Blind SQL Injection in PostgreSQL

BookContent Flash XSS

Bower Disclosure

CGIEmail: Path Traversal

CKEditor Samples API DOM XSS

CKEditor Samples Posted-Data XSS

CKEditor Spellchecker XSS

CKEditor wiris Plugin XSS

CKFinder Disclosure

Command Injection

Concerto XSS

Core Dump Disclosure

cPanel Open Redirect

CSRF Token Leakage via IFRAME Covert Channel

CSS based XSS &amp: UI-redressing

CVE-2001-1013: Apache HTTP Server Local Username Enumeration

CVE-2005-3299: phpMyAdmin LFI

CVE-2006-3918: Apache HTTP Server Expect Header XSS

CVE-2008-0252: CherryPy Path Traversal

CVE-2009-1151: phpMyAdmin RCE

CVE-2010-2861: Adobe ColdFusion Path Traversal

CVE-2011-2505: phpMyAdmin RCE

CVE-2011-4107: phpMyAdmin XXE

CVE-2012-0053: Apache HttpOnly Cookie Disclosure

CVE-2012-1823: Remote Code Execution

CVE-2012-1823: Remote Code Execution (Kingcope)

CVE-2012-3414: SWFUpload Flash XSS

CVE-2012-4000: FCKEditor XSS

CVE-2012-5159: phpMyAdmin server_sync Backdoor

CVE-2013-0156: Ruby on Rails RCE

CVE-2013-0235: WordPress Pingback SSRF

CVE-2013-0262: Rack File Disclosure

CVE-2013-1808: ZeroClipboard Flash XSS

CVE-2014-3704: Drupalgeddon

CVE-2014-6271: Shellshock

CVE-2015-0235: GHOST check in WordPress pingback

CVE-2015-1397: Magento Shoplift SQL Injection

CVE-2015-1427: ElasticSearch RCE

CVE-2015-2080: Jetleak

CVE-2015-3429: WordPress Twenty Fifteen DOM XSS

CVE-2015-7297: Joomla! Unauthenticated SQL Injection

CVE-2015-7808: vBulletin 5.1.2 Unserialize Code Execution

CVE-2015-8103: Jenkins Deserialization RCE

CVE-2015-8562: Joomla! Unauthenticated RCE

CVE-2016-0957: Adobe AEM Felix Console Exposure

CVE-2016-10033: WordPress RCE

CVE-2016-4566: WordPress plupload.swf Flash XSS

CVE-2016-5110: LiteSpeed HTTP Header Injection

CVE-2016-6195: vBulletin SQL Injection

CVE-2016-8869 &amp: CVE-2016-8870: Joomla! Privilege Escalation

CVE-2017-5611: WordPress Content Injection

CVE-2017-5614: CGIEmail Open Redirect

CVE-2017-5615: CGIEmail HTTP Response Splitting

CVE-2017-5616: CGIEmail XSS

CVE-2017-5638: Apache Struts Content-Type RCE

CVE-2017-7269: Microsoft IIS RCE

CVE-2017-8295: WordPress Unauthorized Password Reset

CVE-2017-9791: Apache Struts RCE

CVS Entries Exposure

Django Tastypie XXE

Dockerfile Disclosure

DOM based Open-Redirect

DOM based XSS

DOM XSS in Grafana

Dot PHPS Source Code Disclosure

Drupal Backup Disclosure

Drupal Database Disclosure

Drupal error_log Disclosure

Eclipse build.properties Disclosure

Eclipse build.xml Disclosure

EdgeCast CDN XSS

Fontlist Flash XSS

Form Upload accept PHP

Ganglia Open Redirect

HelpJuice XSS

Host-header XSS

HTML Injection

HTTP OPTIONS

Index Backup Disclosure

Information Disclosure in unzip.php

Internal IP Disclosure

Java Remote Code Execution

JBoss Unauthenticated Console

Jira XSS via SAML SSO plugin

Jobportals XSS

Joomla! Backup Disclosure

Joomla! com_advertisementboard SQL Injection

Joomla! com_extrasearch SQL Injection

Joomla! com_filecabinet SQL Injection

Joomla! com_frontpage SQL Injection

Joomla! com_jcart SQL Injection

Joomla! com_jdownloads SQL Injection

Joomla! com_news SQL Injection

Joomla! com_opencart SQL Injection

Joomla! com_phocadownload SQL Injection

Joomla! com_publication SQL Injection

Joomla! com_simplemembership SQL Injection

Joomla! com_vikrentcar SQL Injection

Joomla! com_vikrentitems SQL Injection

Joomla! com_webgrouper SQL Injection

Joomla! Flash XSS in flashmediaelement.swf

Joomla! Security Check SQL Injection

Joomla! vik SQL Injection

Joomla! Xtec XSS

Jplayer XSS

JWPlayer Reflected XSS

LDAP Injection

Local File Inclusion (LFI)

Local Username Disclosure in entropysearch.cgi

Locomotive CMS XSS

Magento Admin Panel XSS

Magento Admin Path Disclosure

Magento Admin Uploader XSS

Magento Backup Disclosure

Magento Configuration Disclosure

Magento Customer Information Leak via RSS and Privilege Escalation

Magento Downloader / Connect Manager Disclosure

Magento Downloader XSS

Magento MAGMI Config XSS

Magento Stored XSS

Magento Unrestricted Cron Script

MediaWiki Backup Disclosure

Microsoft ASP.NET Remote Code Execution

Microsoft IIS Tilde File Enumeration

Microsoft IIS Tilde File Enumeration

Microsoft Windows Remote Command Execution

MongoDB Operator Injection

Moodle Block-Accessability Open-Redirect

Moodle Flowplayer Flash XSS

Movable Type Backup Disclosure

Moxieplayer Open Redirect

MyBB &lt:= 1.8.3 Remote Code Execution

Nagios Authentication Bypass

NextJS XSS

Detectify AB, Långholmsgatan 34, 117 33 / Stockholm,Sweden.
Mail: general@detectify.com / Twitter: @detectify / Facebook: Detectify / Org number: 556985-9084

NTOPNG Reflected XSS
Open Redirect in awstats.pl
Open Redirect in TenderApp
OpenVPN Access Server CRLF Injection
OSVDB-83814: Magento XXE
Parameter based HTTP Response Splitting (HRS)
Parameter based Open-Redirect
Parameter based SQL Injection
Path based XSS
Path Traversal
Perl Remote Code Execution
Pharmacy Hack
PHP based RCE with malicious URL rewrites
PHP Null Session
PHP Object Injection
PHP Remote Code Execution
phpMyAdmin File Disclosure
phpMyAdmin Unauthenticated Access
Proxy Server via CONNECT-verb
Proxy Server via Host-header
Python Eve Werkzeug RCE
Python Flask/Werkzeug RCE
Python Object Transformation
Query based XSS
Referer-header XSS
Reflected Flash XSS
Reflected XSS
Reflected XSS in cshopcart.cgi
Reflected XSS in FusionCharts
Reflected XSS in FusionCharts3
Reflected XSS in FusionWidgets
Reflected XSS in Ganglia
Reflected XSS in hazel.cgi
Reflected XSS in hyperseek.cgi
Reflected XSS in JW-Player
Reflected XSS in PowerCharts
Reflected XSS in testcgi.exe
Relative Path Overwrite (RPO)
Remote File Inclusion (RFI)
Rosetta Flash XSS
Server Side Includes (SSI)
Server Side Template Injection
SharePoint XSS
ShareThis XSS
SSH Private Key Exposure
SWFUpload Open Redirect
Teamcity ZeroClipboard Flash XSS
TYPO3 Flash Player XSS
TYPO3 Flowplayer Flash XSS
TYPO3 SVG XSS
TYPO3 SWF-Upload XSS
Unauthenticated / Exposed Memcache
Unix Remote Command Execution
Uploadify Flash XSS
URL based HTTP Response Splitting (HRS)
URL based Open-Redirect
URL based SQL injection
User-Agent-header XSS
VBS based XSS
Web Cache Deception
WordPress ad-inserter LFI
WordPress adrotate SQL Injection
WordPress adrotate XSS
WordPress all-in-one-schemaorg-rich-snippets XSS
WordPress all-in-one-seo-pack XSS
WordPress allow-php-in-posts-and-pages SQL Injection
WordPress appointments Object Injection
WordPress apptha-slider-gallery LFI
WordPress apptha-slider-gallery SQL Injection
WordPress booking Authenticated XSS
WordPress bridge DOM XSS
WordPress caldera-forms Flash XSS
WordPress contus-hd-flv-player SQL Injection
WordPress couponer SQL Injection
WordPress cp-multi-view-calendar SQL Injection
WordPress cp-multi-view-calendar XSS
WordPress crayon-highlight XSS
WordPress crelly-slider Authenticated XSS
WordPress dm-albums RFI
WordPress dsubscribers SQL Injection
WordPress duplicate-page Authenticated XSS
WordPress easy-contact-form-lite SQL Injection
WordPress easy-social-share-buttons XSS
WordPress enhanced-tooltipglossary XSS
WordPress esig-redirect-after-signing XSS
WordPress evarisk SQL Injection
WordPress event-espresso Blind SQL Injection
WordPress ewww-image-optimizer RCE
WordPress facebook-opengraph-meta-plugin SQL Injection
WordPress faq-wd XSS
WordPress file-groups SQL Injection
WordPress firestats XSS
WordPress flickr-gallery Object Injection
WordPress flickr-picture-backup RFI
WordPress fluid-responsive-slideshow XSS
WordPress forum-server SQL Injection
WordPress gadgetry XSS
WordPress gallery-album Authenticated SQL Injection
WordPress gallery-video SQL Injection
WordPress github-btn XSS
WordPress global-content-blocks SQL Injection
WordPress google-pagespeed-insights Authenticated XSS
WordPress gotmls Authenticated XSS
WordPress grand-media XSS
WordPress gtranslate Open Redirect
WordPress image-export LFI
WordPress instalinker XSS
WordPress jetpack Reflected XSS
WordPress js-appointment SQL Injection
WordPress loco-translate Authenticated XSS
WordPress mainwp XSS
WordPress max-mega-menu Authenticated XSS
WordPress media-library-categories SQL Injection
WordPress multi-device-switcher Open Redirect
WordPress my-tickets Authenticated XSS
WordPress my-wp-translate Authenticated XSS
WordPress mydbr XSS
WordPress myflash LFI
WordPress myflash RFI
WordPress mygallery RFI
WordPress nelio-ab-testing Path Traversal
WordPress nextgen SQL Injection
WordPress ninja-forms Authenticated XSS
WordPress odihost-newsletter SQL Injection
WordPress Open Redirect
WordPress oqey-headers SQL Injection
WordPress participants-database XSS
WordPress photoracer SQL Injection
WordPress pica-photo-gallery SQL Injection
WordPress pinfinity XSS
WordPress Plugin 404 to 301 Unauthenticated Stored Cross-Site Scripting (XSS)
WordPress pootle-button Authenticated XSS
WordPress popup-by-supsystic Authenticated XSS
WordPress pretty-link Authenticated XSS
WordPress proplayer SQL Injection
WordPress registrationmagic Object Injection
WordPress revolution-slider LFI
WordPress robo-gallery RCE
WordPress Rosetta Flash XSS
WordPress search-autocomplete SQL Injection
WordPress search-everything (&lt:= 8.1.6) SQL Injection
WordPress simple-membership Authenticated XSS
WordPress smush LFI
WordPress sniplets RFI
WordPress soundcloud-is-gold XSS
WordPress spider-event-calendar Blind SQL Injection
WordPress spiffy-calendar XSS
WordPress stop-user-enumeration Bypass
WordPress stream Unauthenticated Events Export
WordPress super-captcha SQL Injection
WordPress theme-my-login Authentication Bypass
WordPress Plugins using TimThumb
WordPress tracking-code-manager XSS
WordPress ultimate-form-build Authenticated SQL Injection
WordPress ultimate-form-builder-lite XSS
WordPress ungallery LFI
WordPress upm-polls SQL Injection
WordPress userpro XSS

WordPress videojs-html5-video-player-for-wordpress XSS

WordPress wd-instagram-feed XSS

WordPress webplayer SQL Injection

WordPress woocommerce SQL Injection

WordPress woocommerce-pdf-invoices-packing-slips Authenticated XSS

WordPress wordpress-donation-plugin SQL Injection

WordPress wordpress-video-gallery SQL Injection

WordPress wordtube RFI

WordPress wp-database-backup RCE

WordPress wp-ds-faq SQL Injection

WordPress wp-hide-security-enhancer LFI

WordPress wp-members Authenticated XSS

WordPress wp-menu-creator SQL Injection

WordPress wp-mobile-detector RCE

WordPress wp-special-textboxes Authenticated XSS

WordPress wp-symposium SQL Injection

WordPress wp-table RFI

WordPress wp-ultimate-form-builder SQL Injection

WordPress wpdiscuz XSS

WordPress wpforum SQL Injection

WordPress wpml XSS

WordPress wpml XSS

WordPress XCloner - Backup and Restore LFI

WordPress xcloner-backup-and-restore XSS

WPVDB-7019: WordPress alo-easymail XSS

WPVDB-8190: WordPress alo-easymail XSS

WPVDB-8544: WordPress wp-live-chat-support XSS

WPVDB-8568: WordPress colorway XSS

WPVDB-8585: WordPress aryo-activity-log XSS

XPATH Injection

XSS via TRACE-verb

XSS via TRACK-verb

YaBB Open Redirect

YaBB Reflected XSS

Zabbix SQL Injection

External Link using &quot:target _blank&quot:

CVE-2016-9263: XSF in FlashMediaElement

XSF in Moxie

Expect / XSS

Host Header Poisoning

Edge Side Includes

Parameter-based SSRF

Boolean-Based SQL Injection

Python RCE

Blind Unix-based Arbitrary Command Execution

Unix Arbitrary Command Execution

Ruby Path Traversal

Ruby RCE

HubSpot Open Redirect

CVE-2012-0053: Apache HttpOnly Cookie Disclosure

CVE-2016&ndash:3714: ImageTragick

CVE-2016-8869 &amp: CVE-2016-8870: Joomla! Privilege Escalation

CVE-2002-1717: Microsoft FrontPage Information Exposure

CVE-2014-4663: TimThumb RCE

CVE-2011-4106: TimThumb RCE

WordPress Registration Enabled

WordPress mgl-instagram-gallery XSS

WordPress revslider Path Traversal

WordPress Themes using TimThumb

UnZIP Path Traversal

WordPress download-monitor Log Exposure

WordPress gadgetry-parent XSS

CVE-2014-5465: WordPress force-download Path Traversal

CVE-2017-16842: WordPress wordpress-seo XSS

CVE-2015-2065: WordPress video-gallery SQL Injection

WordPress webplayer SQL Injection

WordPress theme-my-login Authentication Bypass

CVE-2017-16562: WordPress userpro Authentication Bypass

CVE-2017-15919: WordPress ultimate-form-builder-lite SQL Injection

WordPress caldera-forms Flash XSS

CVE-2018-7543: WordPress duplicator XSS

CVE-2017-17092: WordPress Authenticated XSS

CVE-2016-6195: vBulletin SQL Injection

CVE-2017-5966: SiteCore Reflected XSS

Sitecore Open Redirect

Preemtech XSS

CVE-2017-3546: Oracle PeopleSoft IMServlet SSRF

CVE-2014-4210: Oracle WebLogic SSRF

CVE-2017-10246: Oracle E-Business Suite SSRF

CVE-2017-3549: Oracle EBS SQL Injection

CVE-2016-0457: Oracle E-Business XXE

One2Com Blind SQL-Injection

CVE-2014-3744: NodeJS Directory Traversal

MyDBR Path Traversal

Magento Invoice IDOR

Kirby CMS Path Traversal

Kentico CMS XSS

CVE-2014-7981: Joomla! SQL Injection

CVE-2018-6582: Joomla! zhgooglemap SQL Injection

CVE-2018-7318: Joomla! checklist SQL Injection

CVE-2018-7312: Joomla! abook SQL Injection

CVE-2018-7314: Joomla! prayercenter SQL Injection

CVE-2018-7178: Joomla! saxumpicker SQL Injection

CVE-2018-7179: Joomla! squadmanagment SQL Injection

CVE-2018-7179: Joomla! saxumnumerology SQL Injection

CVE-2018-7180: Joomla! saxumastro SQL Injection

Joomla! ekrishta SQL Injection

CVE-2018-7315: Joomla! ekrishta SQL Injection

Evoluted XSS

CVE-2007-2440: Caucho Resin Path Traversal

EPiServer XXE

EPiServer API XSS

CVE-2015-1427: ElasticSearch RCE

Citrix XenMobile XXE

Caddy Open Redirect

CVE-2015-8398: Atlassian Confluence Reflected XSS

Atlassian Confluence status-list XSS

Atlassian Confluence Enterprise Wiki XSS

Adobe AEM Default Credentials

Liferay Portal SSRF

CVE-2018-9205: Drupal avatar_uploader Path Traversal

CVE-2018-7600: Drupal RCE (Drupalgeddon 2)

Laravel Log Path Traversal

CVE-2018-8947: Laravel Log Path Traversal

CVE-2017-12629: Apache Solr RCE

ASP-Nuke Open Redirect

CVE-2015-1164: Node serve-static Open Redirect

CVE-2017-9841: PHP-Unit RCE

SAP B2B/B2C CRM LFI

VideoJS Flash XSS

Clipboard Flash XSS

CopyToClipboard Flash XSS

CVE-2013-1636: Open Flash Chart XSS

Microsoft IIS Tilde File Enumeration

Passive tests

Adminer Exposure
AdRoll CSP Bypass
Ansible Tower Exposure
Apple .DS_Store Directory Listing
Atom Synchronization Exposure
Bitrix Path Disclosure
CKEditor AJAX-File-Manager Exposure
CKEditor Samples API DOM XSS #1
CKEditor Samples API DOM XSS #2
CORS Wildcard Policy
CVE-2017-1001000: WordPress Content Injection / Authentication Bypass
CVE-2017-12149: Potential JBoss RCE
CVE-2017-14725: WordPress Open Redirect
CVE-2017-16510: WordPress SQL Injection
CVE-2017-5611: WordPress 4.7.0 &amp: 4.7.1 Authentication Bypass
Dropwizard Exposure
Drupal Username Enumeration
EPiServer Image Resizer Exposure
Exposure of /.mysql_history
Exposure of /.pgsql_history
Exposure of /.sqlite_history
Fantastico Filename Listing
Frames Lacking Sandbox Attribute
GitLab CI Configuration Exposure
Google Ads CSP Bypass
Google Analytics CSP Bypass
Google cAdvisor Exposure
Hadoop Namenode Exposure
HasiCorp Consul Exposure
HTML Comments
Jaeger UI Exposure
jQuery Mobile 1.2 XSS
jQuery Mobile XSS
Kubernetes Console Exposure
Lacking Redirect to HTTPS
Lynk Zipper Information Disclosure
Microsoft SharePoint files Disclosure
Microsoft SharePoint layouts Disclosure
Microsoft SharePoint lists-api Disclosure
Microsoft SharePoint master-page Disclosure
Microsoft SharePoint site-collection Disclosure
Microsoft SharePoint site-pages Disclosure
Mixpanel CSP Bypass
Node Exporter Exposure
Node.JS Source Code Exposure
Oracle WebLogic Admin Console Exposure
Oracle WebLogic T3 Enabled
phpMyAdmin Exposure
phpMyAdmin Lacking Authentication
Piwik Exposure
Plesk Test Page Exposure
Prometheus Alertmanager Exposure
Prometheus Exposure
Prometheus Information Disclosure
Prometheus Metrics Disclosure
README.md Disclosure
Referrer-Policy / Invalid Directive
Referrer-Policy / Missing Header
Rocket Chat NoSQL Injection
SAP ICF Information Exposure
Script Integrity Attribute Not Implemented
SnoopServlet Information Exposure
Spring Boot Actuator /trace
SSH .known_hosts Exposure
Strict-Transport-Security / Invalid Directive
Strict-Transport-Security / Low Timeout
Strict-Transport-Security / Missing Header
Strict-Transport-Security / Served via HTTP
WebLogic Console Exposure
WordPress caldera-forms Authenticated XSS
WordPress Database Exposure
WordPress duplicate-page 2.3 Authenticated XSS
WordPress duplicate-page 2.4 Authenticated XSS
WordPress duplicator Stored XSS
WordPress file-manager Exposure
WordPress functions.php Full Path Disclosure
WordPress hrm Authenticated SQL Injection
WordPress instagram-feed Authenticated XSS
WordPress invite-anyone Object Injection
WordPress ninja-forms 3.1.8 Authenticated XSS
WordPress ninja-forms 3.2.12 Authenticated XSS
WordPress qards SSRF
WordPress shortcodes-ultimate Authenticated Command Execution
WordPress simple-login-log SQL Injection
WordPress tablespress Authenticated XXE
WordPress upme Authentication Bypass
WordPress userpro Authentication Bypass
WordPress wordcamp CSV Formula Injection
WordPress wordpress-seo XSS
WordPress work-the-flow-file-upload Arbitrary File Upload
WordPress wp-all-import XSS
WordPress wp-custom-fields-search XSS
WordPress wpforms-lite Authenticated XSS
WordPress wp-support-plus-responsive-ticket-system CSRF/RCE
X-Content-Type-Options / Invalid Directive
X-Content-Type-Options / Missing Header
X-Frame-Options / Invalid Directive
X-Frame-Options / Lacking Header
X-Frame-Options / Reflecting Host-Header
X-Frame-Options / Reflecting Referer-Header
X-XSS-Protection / Disabled Auditor
X-XSS-Protection / Invalid Directive
X-XSS-Protection / Missing Header
Adobe AEM CQ5 Custom Scripts Exposure
Adobe AEM CQ5 JsonRendererServlet Exposure
Adobe AEM CQ5 Package Manager Exposure
Adobe AEM CQ5 Query-Builder Exposure
Adobe AEM CRX Browser Exposure
Adobe AEM CRX DE Console Exposure
Adobe AEM CRX Explorer Console Exposure
Adobe AEM CRX Namespace Editor Exposure
Adobe AEM CRX Package Manager Exposure
Adobe AEM CRX Statistics Exposure
Adobe AEM Disk Usage Information Disclosure
Adobe ColdFusion Admin Panel Disclosure
Adobe ColdFusion Source Code Disclosure
Adobe ColdFusion Stack Trace
Apache Solr
Application Serving Empty Documents
ASP.NET Source Code Disclosure
ASP.NET Stack Trace
AWStats Open Access
Caddy Directory Listing
Content-Security-Policy Bypass
Content-Type-Options
Cookie lacking HttpOnly-flag
Cookie lacking Secure-flag
CSRF via GET-verb
CSRF via Login Form
CVE-2011-4969: jQuery XSS
CVE-2013-6837: jQuery prettyPhoto XSS
CVE-2014-1869: ZeroClipboard Flash XSS
CVE-2016&ndash:3714: ImageTragick
Database Error Message Disclosure
DC-2017-04-003: Magento RCE
Deprecated Drupal
Deprecated JavaScript Framework
Deprecated Joomla! Version
Deprecated Version of Microsoft Windows
Deprecated WordPress
Directory Listing Enabled
Disclosure of .cer File
Disclosure of .cert File
Disclosure of .cfg File
Disclosure of .conf File
Disclosure of .config File
Disclosure of .crt File
Disclosure of .pem File
Disclosure of .pfx File
E-Mail Address Disclosure

Embedded JavaScript in PDF
Embedded Metadata in Graphics
Embedded Metadata in PDF
Environment Variable Disclosure
Environment Variable Disclosure in /.env
Environment Variable Disclosure in cgiscript.cgi
Environment Variable Disclosure in info.cgi
Environment Variable Disclosure in printenv.cgi
Environment Variable Disclosure in test.cgi
EPiServer .NET Version Disclosure
EPiServer Logout CSRF
Evaluation of /humans.txt
Evaluation of /manifest.json
Evaluation of /robots.txt
Evaluation of clientaccesspolicy.xml
Evaluation of crossdomain.xml
Execution After Redirect (EAR)
eXist Unauthenticated Access
Exposed S3CMD Attributes
Exposed Selenium Grid Configuration
Express Stack Trace
External Link using &quot:target _blank&quot:
Form Action lack proper Cache-Control Directive
Form Lacking CSRF Token
FrontPage Information Exposure
Full Path Disclosure Vulnerability Hubspot
Git /.git/config Disclosure
Git /.git/HEAD Disclosure
Git /.git/index Disclosure
Git /.gitignore Disclosure
Golang Godeps Disclosure
Golang Stack Trace
Grunt Disclosure
Gulp Disclosure
HAProxy Statistics Disclosure
Heroku Procfile Disclosure
HTML comments
HTML using External Resources
HTTP Stripping
Information Disclosure of sftp-config.json
Information Disclosure via /.bash_history
Java Source Code Disclosure
Java Stack Trace
Jetbrains Data Sources Disclosure
Jetty Config Disclosure
jQuery CORS Requests may lead to XSS
jQuery Migrate Selector Degredation
jQuery Migrate Selector Manipulation
jQuery Migrate XSS
jQuery prettyPhoto Selector Injection
jQuery prettyPhoto XSS
jQuery Selector Injection
KCEditor Filemanager Unauthenticated Access
Login submits via GET
Lua Stack Trace
Magento Admin Panel Disclosure
Magento Package Disclosure
Mercurial Branch-file Disclosure
Mercurial Requires-file Disclosure
Microsoft Exchange IP Disclosure
Microsoft IIS /elmah.axd Information Disclosure
Microsoft IIS /trace.axd Information Disclosure
Microsoft IIS /web.config Disclosure
Microsoft SharePoint all-items Disclosure
Microsoft SharePoint all-pages Disclosure
Microsoft SharePoint all-sites-content Disclosure
MIME text/html set for invalid HTML
Missing Content-Type
Mixed Content
MS15-034: Range-header Integer Overflow
NGINX Status Disclosure
NPM /npm-debug.log Disclosure
NPM /package.json Disclosure
Open Instance of PHPSysInfo
Open Spring Boot Actuator Information Leakage
Oracle Weblogic Admin Console Disclosure
PHP /composer.json Disclosure
PHP /composer.lock Disclosure
PHP Configuration Disclosure
PHP Debug Array via print_r():
PHP Easter Egg
PHP Error-log Disclosure
PHP Laravel Stack Trace
PHP phpinfo()-Disclosure
PHP Source Code Disclosure
PHP Stack Trace
PHP Symfony Debug Toolbar
PHP Zend Stack Trace
Piwik Error Information Disclosure
Proxy Judge Information Disclosure
Public Cacti Instance
Public Predis Example Files
Publicly exposed Webalizer Interface
Python Django Admin Panel
Python Django Stack Trace
Python Source Code Disclosure
Python Stack Trace
Python Werkzeug Debug Console
Roxy File Manager Open Access
Ruby /Gemfile Disclosure
Ruby on Rails /info/properties/ Disclosure
Ruby on Rails /info/routes/ Disclosure
Ruby on Rails CSRF Token Leakage
Ruby on Rails Object Transformation
Ruby Source Code Disclosure
Sensitive Data Disclosure in JSON
Sensitive Form using Plaintext HTTP
Serve Static 1.7.0 Open Redirect
SSL BREACH
SSL Private Key Disclosure
SVN Database Disclosure
SVN Entries Disclosure
Swagger Disclosure
Symfony Debug Toolbar Exposure
Tomcat Default Files
Tor Hostname File Disclosure
Tor Private Key Disclosure
Travis-CI Config Disclosure
Typo-Squatting XSS
Ultimate Bulletin Board Email Disclosure
Unauthenticated Access to Xymon
Unauthenticated Apache Solr
Unauthenticated Ganglia
Unauthenticated JBoss JMX Console
Unencrypted Basic Authentication
Unencrypted Login Form
Vulnerable JavaScript Frameworks
Wildcard Cookie
WooCommerce Electro Electronics Store CSRF
WordPress Authenticated Open-Redirect
WordPress Backup Disclosure
WordPress backup-with-restore Database Disclosure
WordPress backwpup Backup Disclosure
WordPress clean-login CSRF
WordPress Content Injection
WordPress Debug Log Disclosure
WordPress download-monitor Unauthenticated Log Download
WordPress error_log Disclosure
WordPress fluid-responsive-slideshow CSRF
WordPress Full Path Disclosure
WordPress ninjaforms Arbitrary File Upload
WordPress ninjaforms Nonce Leakage
WordPress ninjaforms Unauthenticated Tampering
WordPress plugin-organizer CSRF
WordPress Setup Script Identified
WordPress Theme Database Disclosure
WordPress use-any-font CSRF
WordPress Username Enumeration via author-parameter
WordPress Username Enumeration via REST API
WordPress whizz CSRF
WordPress wp-fastest-cache CSRF
WordPress wp-include/wp-db.php Exposure
WordPress xcloner-backup-and-restore phpinfo() Information Disclosure
WordPress youtube-embed-plus CSRF
WPVDB-8390: WordPress alo-easymail CSRF
WPVDB-8392: WordPress alo-easymail CSRF
WPVDB-8487: WordPress YoastSEO Data Exposure
Zend application.ini Exposure
Sensitive Token Disclosure
Admin Panel Exposure
Slack API Key Disclosure

Execution After Redirect (EAR)
Application Serving Empty Documents
MIME text/html set for invalid HTML
Missing Content-Type
Unencrypted Basic Authentication
Amazon API-Key Disclosure
Facebook OAuth Token Disclosure
GitHub API Key Disclosure
Google OAuth Token Disclosure
Heroku API Key Disclosure
Twitter OAuth Token Disclosure
Database Error Message Disclosure
Directory Listing Enabled
E-Mail Address Disclosure
Express Stack Trace
Evaluation of /hackers.txt
Spring Boot Configuration Exposure
Spring Boot Beans Exposure
Spring Boot Environment Exposure
Spring Boot Mapping Exposure
WordPress Automatic Updates Disabled
WordPress Configuration Exposure
WordPress revslider Fingerprinting
PHP Configuration Disclosure
PHP APC Exposure
PHP Proberv Exposure
PHP Coredumps Exposure
Xymon Exposure
WordPress bridge DOM XSS
WordPress youtube-embed-plus CSRF
WPVDB-8487: WordPress Yoast-SEO Data Exposure
WordPress wpforms-lite Authenticated XSS
WordPress woocommerce-pdf-invoices-packing-slips Authenticated XSS
WordPress tracking-code-manager XSS
WordPress wp-stream Unauthenticated Export
WordPress spider-event-calendar Blind SQL Injection
WordPress wp-database-backup RCE
WordPress wordcamp-talks Formula Injection
WordPress ultimate-form-builder-lite Authenticated SQL Injection
WordPress ultimate-form-builder-lite XSS
WordPress wp-support-plus-responsive-ticket-system Autenticated RCE
WordPress caldera-forms Authenticated XSS
WordPress upme Authentication Bypass
CVE-2017-10889: WordPress tablespress Authenticated XXE
WordPress ninjaforms Unauthenticated Tampering
WordPress ninjaforms Arbitrary File Upload
WordPress ninjaforms Nonce Leakage
WordPress gravity-forms Debug Log Exposure
CVE-2018-12895: WordPress Authenticated File Deletion
WordPress error_log Disclosure
CVE-2018-11409: Splunk Information Disclosure
Perl Source Code Disclosure
MediaWiki Information Disclosure
Magento Follow Up Email SQL Injection
Indico Information Exposure
ElasticSearch Exposure
Atlassian Bitbucket Authentication Bypass
Mutt Configuration Exposure
CVE-2018-7602: Drupalgeddon3
Laravel Log Exposure
Apache Tomcat Status Exposure
Apache Spark Exposure
Apache Hadoop Exposure
Yii Debugger Exposure
WS-FTP Exposure
Adobe Dreamweaver Information Disclosure
PGP Private Key Disclosure
SVN Database Disclosure
SVN Entries Disclosure
Bazaar Repository Exposure
Evoluted Directory Listing
Bitcoin Wallet Exposure
Exposed S3CMD Attributes
Content-Security-Policy / Lacking Header

SSL tests

CVE-2017-9798: Apache Optionsbleed
CVE-2011-3389: SSL BEAST
CVE-2012-4929: SSL CRIME
CVE-2014-0160: SSL Heartbleed
CVE-2014-8730: SSL POODLE
CVE-2015-0204: SSL FREAK
CVE-2015-4000: SSL Logjam
CVE-2016-0800: SSL DROWN
CVE-2016-2107: SSL LuckyNegative20
CVE-2017-15361: SSL ROCA
Expiring SSL Certificate
Server uses SSLv2
Server uses SSLv3
Server uses TLS 1.0
SSL Certificate bundled with Subject Alternative Names (SAN)
SSL Certificate Information
SSL Certificate is Revoked
SSL Certificate is Self-Signed
SSL Certificate Signed for other Domain
SSL Certificate Signed for Partial Domains
SSL Certificate Signed using an Untrusted Root
SSL Certificate Signed with 1024-bits Key Length
SSL Certificate Signed with 512-bits Key Length
SSL Certificate Signed with Weak Hashing Algorithm
SSL Expired Certificate
SSL is Lacking
SSL using Deprecated Ciphers
SSL using Weak Ciphers
CVE-2017-15361: SSL ROCA

DNS tests

NSEC Walking
DNS DMARC
DNS SPF 10-Request Limit
DNS SPF Evaluation
DNS Zone-Transfer
DNSSEC
Domain Serving Internal Addresses
Domain Takeover
Name Server Recursive Lookups
Name Server Replying with Invalid DNS Status
Name Server Single Record
Name Servers on Redundant Networks
CVE-1999-0532: DNS Zone Transfer
Same Network Scripting
Same Site Scripting
DNS Reserved Range
Domain Takeover / DNS Hijacking

Detectify AB, Långholmsgatan 34, 117 33 / Stockholm,Sweden.
Mail: general@detectify.com / Twitter: @detectify / Facebook: Detectify / Org number: 556985-9084

Third party tests

JavaScript served from Untrusted Parties

SSL Blacklist

VirusTotal File Scan

VirusTotal URL Scanning

Slack Webhook Exposure

Google Groups Exposure

GitLab Public Repository Exposure

Other

Forced Browsing

- *Custom made tests available upon customer request, could include zero days.*
- *New tests added frequently sourced via Detectify Crowdsource*
- *Please note that this overview does not include all Detectify tests.*