WordPress Security Analysis (Passive)

http://acunetix.com

This report details the results of a passive (non-intrusive) security analysis of the target WordPress site.

WordPress Version:

???

Unable to determine

WordPress Core Version

Reputation Check

PASSED

Google Check:	OK
Spamhaus Check:	OK
Compromised Hosts:	OK
Dshield Blocklist:	OK
Shadowserver C&C:	OK

Server information

Web Server:	**nginx**
X-Powered-By:	**None**
IP Address:	**54.208.84.166**
Hosting Provider:	**Amazon.com.**
Shared Hosting:	**5 sites found on IP**

WordPress Plugins

The following plugins were detected through analysis of the HTML source from the sites main page.

?	**docembdr**	
✓	**wordpress-seo 9.4**	latest release (9.4) https://yoa.st/1uj
?	**acx-forms**	

Plugins are a source of many security vulnerabilities within WordPress installations, always keep them updated to the latest version available and check the developers plugin page for information about security related updates and fixes.

There are likely more plugins installed than those listed here as the detection method used here is passive. While these results give an indication of the status of plugin updates, a more comprehensive assessment should be undertaken by brute forcing the plugin paths using a **dedicated tool**.

WordPress Theme

The theme has been found by examining the path `/wp-content/themes/ *theme name* /`

acunetix

While plugins get a lot of attention when it comes to security vulnerabilities, themes are another source of security vulnerabilities within WordPress installations, always keep them updated to the latest version available and check the developers theme page for information about security related updates and fixes.

The theme listed here is the **active theme** found in the HTML source of the page. A comprehensive assessment should include checking for other themes that are installed but not active as these can also contain exploitable security vulnerabilities. In a "black box" assessment or penetration test detection of all themes can be undertaken by **brute forcing the theme path**. Remove all unused themes to minimise the attack surface of the WordPress installation. Remove all unused themes to minimise the attack surface of the WordPress installation.

User Enumeration

✔ It was **not possible to easily enumerate usernames** from the user ID's. This is a good thing, as it can add difficulty to brute force password attacks if the username is not able to be determined.

It is recommended to rename the `admin` user account to reduce the chance of brute force attacks occurring. As this will reduce the chance of automated password attackers gaining access.

Keep in mind that if the author archives are enabled it is usually **possible to enumerate all users** within a WordPress installation. Including a renamed `admin` account.

Only the first two user ID's were tested during this scan. Try the **advanced membership options** or a dedicated tool for more detailed enumeration of users, themes and plugins.

Directory Indexing

In the test we attempted to list the directory contents of the uploads and plugins folders to determine if **Directory Indexing** is enabled. This vulnerability type is known as information leakage and can reveal sensitive information regarding your site configuration or content.

/wp-content/uploads/	**Indexing Disabled**
/wp-content/plugins/	**Indexing Disabled**

Directory indexing was tested on the `/wp-content/uploads/` and `/wp-content/plugins/` directores. Note that other directories may have this web server feature enabled, so ensure you check other folders in your installation. It is good practice to ensure directory indexing is disabled for your full WordPress installation either through the web server configuration or `.htaccess`.

Linked Sites

Google Safe browse checks have been performed on each of the linked sites. Links with poor reputation could be a threat to users of the site. Hosting and location are also included in the results.

	Externally Linked Host	Hosting Provider	Country
	online.acunetix.com	Amazon.com, Inc.	United-States

Search performed against Google Safe Browse website security testing
Check for malicious URL against multiple malware scanners using Virus Total

Loaded Resources

Compromised sites will often be linked to malicious `javascript` or `iframes` in an attempt to attack users of your WordPress installation. Look over the listed resources, you should be familiar with all scripts and investigate ones you are not sure. In addition removal of unneeded javascript will speed up your website.

---

http://acunetix.com/

OK | Load: 15ms | Server: 54.208.84.166 nginx | ASN: 14618 Amazon.com, Inc. | Reverse DNS: ec2-54-208-84-166.compute-1.amazonaws.com

https://www.acunetix.com/

OK | Load: 67ms | Server: 54.208.84.166 nginx | ASN: 14618 Amazon.com, Inc. | Reverse DNS: ec2-54-208-84-166.compute-1.amazonaws.com

https://www.googletagmanager.com/gtm.js?id=GTM-K8C34Z4

OK | Load: 243ms | Server: 172.217.12.136 Google Tag Manager (scaffolding) | ASN: 15169 Google LLC | Reverse DNS: lga34s19-in-f8.1e100.net

https://www.acunetix.com/wp-includes/js/wp-emoji-release.min.js?ver=5.0.3

OK | Load: 10ms | Server: 54.208.84.166 nginx | ASN: 14618 Amazon.com, Inc. | Reverse DNS: ec2-54-208-84-166.compute-1.amazonaws.com

https://www.acunetix.com/wp-content/plugins/docembdr/css/docembdr.css?ver=5.0.3

OK | Load: 45ms | Server: 54.208.84.166 nginx | ASN: 14618 Amazon.com, Inc. | Reverse DNS: ec2-54-208-84-166.compute-1.amazonaws.com

https://www.acunetix.com/wp-includes/css/dist/block-library/style.min.css?ver=5.0.3

OK | Load: 54ms | Server: 54.208.84.166 nginx | ASN: 14618 Amazon.com, Inc. | Reverse DNS: ec2-54-208-84-166.compute-1.amazonaws.com

https://www.acunetix.com/wp-content/themes/acunetix/style.css?ver=1.0.0

OK | Load: 54ms | Server: 54.208.84.166 nginx | ASN: 14618 Amazon.com, Inc. | Reverse DNS: ec2-54-208-84-166.compute-1.amazonaws.com

https://www.acunetix.com/wp-content/themes/acunetix/css/bootstrap-xxs.css?ver=1.0.0

OK | Load: 70ms | Server: 54.208.84.166 nginx | ASN: 14618 Amazon.com, Inc. | Reverse DNS: ec2-54-208-84-166.compute-1.amazonaws.com

https://fonts.googleapis.com/css?family=Open+Sans%3A300%2C400%2C600%2C700%2C400italic%2C700italic&ver=5.0.3

OK | Load: 107ms | Server: 173.194.206.95 ESF | ASN: 15169 Google LLC | Reverse DNS: qj-in-f95.1e100.net

https://www.google.com/recaptcha/api.js?ver=5.0.3

OK | Load: 109ms | Server: 172.217.15.68 GSE | ASN: 15169 Google LLC | Reverse DNS: iad23s63-in-f4.1e100.net

https://d3eaqdewfg2crq.cloudfront.net/wp-includes/js/jquery/jquery.js?ver=1.12.4

OK | Load: 87ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://d3eaqdewfg2crq.cloudfront.net/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1

OK | Load: 83ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://d3eaqdewfg2crq.cloudfront.net/wp-content/themes/acunetix/js/base-js-combined.min.js

OK | Load: 83ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://d3eaqdewfg2crq.cloudfront.net/wp-content/themes/acunetix/js/top_search.js

OK | Load: 80ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://d3eaqdewfg2crq.cloudfront.net/wp-content/themes/acunetix/js/general.js

OK | Load: 88ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://d3eaqdewfg2crq.cloudfront.net/wp-includes/js/wp-embed.min.js?ver=5.0.3

OK | Load: 89ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://d3eaqdewfg2crq.cloudfront.net/wp-content/plugins/acx-forms/js/jquery.validate.min.js?ver=1.0.0

OK | Load: 88ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://d3eaqdewfg2crq.cloudfront.net/wp-includes/js/jquery/ui/widget.min.js?ver=1.11.4

OK | Load: 89ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://d3eaqdewfg2crq.cloudfront.net/wp-content/plugins/acx-forms/forms/ovs-signup2/js/cryptojs-sha256.js?ver=5.0.3

OK | Load: 93ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://d3eaqdewfg2crq.cloudfront.net/wp-content/plugins/acx-forms/forms/ovs-signup2/js/libphonenumber-js.min.js?ver=5.0.3

OK | Load: 93ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://d3eaqdewfg2crq.cloudfront.net/wp-content/plugins/acx-forms/forms/ovs-signup2/js/acx-form-ovs-signup.js?ver=5.0.3

OK | Load: 91ms | Server: 99.84.106.190 nginx | ASN: 16509 Amazon.com, Inc. | Reverse DNS: server-99-84-106-190.iad79.r.cloudfront.net

https://js.maxmind.com/js/apis/geoip2/v2.1/geoip2.js?ver=2.1.0

OK | Load: 97ms | Server: 104.16.38.47 cloudflare | ASN: 13335 Cloudflare, Inc. | Reverse DNS:

https://www.gstatic.com/recaptcha/api2/v1546842739564/recaptcha__en.js

OK | Load: 152ms | Server: 172.217.10.3 sffe | ASN: 15169 Google LLC | Reverse DNS: lga34s12-in-f3.1e100.net

https://dev.visualwebsiteoptimizer.com/j.php?a=342577&u=https%3A%2F%2Fwww.acunetix.com%2F&r=0.8252712748944759

OK | Load: 136ms | Server: 50.97.40.233 None | ASN: 36351 SoftLayer Technologies Inc. | Reverse DNS: e9.28.6132.ip4.static.sl-reverse.com

https://connect.facebook.net/en_US/fbevents.js

OK | Load: 113ms | Server: 31.13.66.19 None | ASN: 32934 Facebook, Inc. | Reverse DNS: xx-fbcdn-shv-01-iad3.fbcdn.net

https://geoip-js.maxmind.com/geoip/v2.1/country/me?referrer=https%3A%2F%2Fwww.acunetix.com

OK | Load: 191ms | Server: 104.16.38.47 cloudflare | ASN: 13335 Cloudflare, Inc. | Reverse DNS:

https://fonts.gstatic.com/s/opensans/v15/mem8YaGs126MiZpBA-UFVZ0d.woff

OK | Load: 213ms | Server: 172.217.11.35 sffe | ASN: 15169 Google LLC | Reverse DNS: lga25s61-in-f3.1e100.net

https://fonts.gstatic.com/s/opensans/v15/mem5YaGs126MiZpBA-UN_r8OUuhv.woff

OK | Load: 239ms | Server: 172.217.11.35 sffe | ASN: 15169 Google LLC | Reverse DNS: lga25s61-in-f3.1e100.net

https://fonts.gstatic.com/s/opensans/v15/mem5YaGs126MiZpBA-UNirkOUuhv.woff

OK | Load: 273ms | Server: 172.217.11.35 sffe | ASN: 15169 Google LLC | Reverse DNS: lga25s61-in-f3.1e100.net

https://fonts.gstatic.com/s/opensans/v15/mem5YaGs126MiZpBA-UN7rgOUuhv.woff

OK | Load: 276ms | Server: 172.217.11.35 sffe | ASN: 15169 Google LLC | Reverse DNS: lga25s61-in-f3.1e100.net

https://cse.google.com/cse/cse.js?cx=014967287653641589399:rfsaq_jzpxi

OK | Load: 262ms | Server: 172.217.9.238 gws | ASN: 15169 Google LLC | Reverse DNS: lga34s11-in-f14.1e100.net

https://www.googleadservices.com/pagead/conversion_async.js

OK | Load: 253ms | Server: 172.217.9.226 cafe | ASN: 15169 Google LLC | Reverse DNS: lga34s11-in-f2.1e100.net

https://www.google-analytics.com/analytics.js

OK | Load: 218ms | Server: 216.58.219.206 Golfe2 | ASN: 15169 Google LLC | Reverse DNS: lga25s40-in-f14.1e100.net

https://sjs.bizographics.com/insight.min.js

OK | Load: 434ms | Server: 104.73.132.120 None | ASN: 16625 Akamai Technologies, Inc. | Reverse DNS: a104-73-132-120.deploy.static.akamaitechnologies.com

https://bat.bing.com/bat.js

OK | Load: 218ms | Server: 204.79.197.200 None | ASN: 8068 Microsoft Corporation | Reverse DNS: a-0001.a-msedge.net

https://js.hs-scripts.com/4595665.js

OK | Load: 189ms | Server: 104.17.213.204 cloudflare | ASN: 13335 Cloudflare, Inc. | Reverse DNS:

https://connect.facebook.net/signals/config/539967686106303?v=2.8.37&r=stable

OK | Load: 85ms | Server: 31.13.66.19 None | ASN: 32934 Facebook, Inc. | Reverse DNS: xx-fbcdn-shv-01-iad3.fbcdn.net

https://dev.visualwebsiteoptimizer.com/5.0/va-3d21b22b243806407666de89d24a2e04.js

OK | Load: 56ms | Server: 50.97.40.233 None | ASN: 36351 SoftLayer Technologies Inc. | Reverse DNS: e9.28.6132.ip4.static.sl-reverse.com

https://dev.visualwebsiteoptimizer.com/5.0/track-3d21b22b243806407666de89d24a2e04.js

OK | Load: 104ms | Server: 50.97.40.233 None | ASN: 36351 SoftLayer Technologies Inc. | Reverse DNS: e9.28.6132.ip4.static.sl-reverse.com

https://dev.visualwebsiteoptimizer.com/analysis/2.0/opa-223743be8b39a88528aec7917bf9d592.js

OK | Load: 122ms | Server: 50.97.40.233 None | ASN: 36351 SoftLayer Technologies Inc. | Reverse DNS: e9.28.6132.ip4.static.sl-reverse.com

https://www.acunetix.com/undefined

OK | Load: 305ms | Server: 54.208.84.166 nginx | ASN: 14618 Amazon.com, Inc. | Reverse DNS: ec2-54-208-84-166.compute-1.amazonaws.com

https://dev.visualwebsiteoptimizer.com/analysis/worker-68f4c079a93008e8e04f81f6476e5cc4.js

OK | Load: 42ms | Server: 50.97.40.233 None | ASN: 36351 SoftLayer Technologies Inc. | Reverse DNS: e9.28.6132.ip4.static.sl-reverse.com

https://js.hs-analytics.net/analytics/1547744100000/4595665.js

OK | Load: 64ms | Server: 104.17.71.176 cloudflare | ASN: 13335 Cloudflare, Inc. | Reverse DNS:

https://www.google.com/cse/static/element/785fcc06555bb453/cse_element__en.js?usqp=CAI%3D

OK | Load: 15ms | Server: 172.217.15.68 sffe | ASN: 15169 Google LLC | Reverse DNS: iad23s63-in-f4.1e100.net

https://www.google.com/cse/static/element/785fcc06555bb453/default+en.css

OK | Load: 46ms | Server: 172.217.15.68 sffe | ASN: 15169 Google LLC | Reverse DNS: iad23s63-in-f4.1e100.net

https://www.google.com/cse/static/style/look/v2/default.css

OK | Load: 47ms | Server: 172.217.15.68 sffe | ASN: 15169 Google LLC | Reverse DNS: iad23s63-in-f4.1e100.net

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1070114355/?random=1547744290795&cv=9&fst=1547744290795&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=768&u_w=1024&u_ah=768&u_aw=1024&u_cd=32&u_his=1&u_tz=0&u_java=false&u_nplug=0&u_nmime=0>m=2wg170&frm=0&url=https%3A%2F%2Fwww.acunetix.com%2F&tiba=Website%20security%20-%20keep%20in%20check%20with%20Acunetix&async=1&rfmt=3&fmt=4

OK | Load: 89ms | Server: 172.217.10.2 cafe | ASN: 15169 Google LLC | Reverse DNS: lga34s12-in-f2.1e100.net

https://dev.visualwebsiteoptimizer.com/j.php?a=342577&u=https%3A%2F%2Fwww.acunetix.com%2Fundefined&r=0.07772120484150946

OK | Load: 47ms | Server: 50.97.40.233 None | ASN: 36351 SoftLayer Technologies Inc. | Reverse DNS: e9.28.6132.ip4.static.sl-reverse.com

https://www.google.com/cse/cse.js?cx=014967287653641589399:rfsaq_jzpxi

OK | Load: 30ms | Server: 172.217.15.68 sffe | ASN: 15169 Google LLC | Reverse DNS: iad23s63-in-f4.1e100.net

https://geoip-js.maxmind.com/geoip/v2.1/country/me?referrer=https%3A%2F%2Fwww.acunetix.com

OK | Load: 40ms | Server: 104.16.38.47 cloudflare | ASN: 13335 Cloudflare, Inc. | Reverse DNS:

https://www.acunetix.com/wp-content/themes/acunetix/fnt/glyphicons-halflings-regular.woff

OK | Load: 33ms | Server: 54.208.84.166 nginx | ASN: 14618 Amazon.com, Inc. | Reverse DNS: ec2-54-208-84-166.compute-1.amazonaws.com

https://cse.google.com/cse/cse.js?cx=014967287653641589399:rfsaq_jzpxi

OK | Load: 65ms | Server: 172.217.9.238 gws | ASN: 15169 Google LLC | Reverse DNS: lga34s11-in-f14.1e100.net

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1070114355/?random=1547744291075&cv=9&fst=1547744291075&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=768&u_w=1024&u_ah=768&u_aw=1024&u_cd=32&u_his=1&u_tz=0&u_java=false&u_nplug=0&u_nmime=0>m=2wg170&frm=1&url=https%3A%2F%2Fwww.acunetix.com%2F&ref=https%3A%2F%2Fwww.acunetix.com%2F&tiba=Page%20Not%20Found%20%7C%20Acunetix&async=1&rfmt=3&fmt=4

OK | Load: 73ms | Server: 172.217.10.2 cafe | ASN: 15169 Google LLC | Reverse DNS: lga34s12-in-f2.1e100.net

https://www.acunetix.com/undefined

OK | Load: 292ms | Server: 54.208.84.166 nginx | ASN: 14618 Amazon.com, Inc. | Reverse DNS: ec2-54-208-84-166.compute-1.amazonaws.com

https://dev.visualwebsiteoptimizer.com/j.php?a=342577&u=https%3A%2F%2Fwww.acunetix.com%2Fundefined&r=0.39595034904778004

OK | Load: 39ms | Server: 50.97.40.233 None | ASN: 36351 SoftLayer Technologies Inc. | Reverse DNS: e9.28.6132.ip4.static.sl-reverse.com

https://www.google.com/cse/cse.js?cx=014967287653641589399:rfsaq_jzpxi

OK | Load: 25ms | Server: 172.217.15.68 sffe | ASN: 15169 Google LLC | Reverse DNS: iad23s63-in-f4.1e100.net

https://geoip-js.maxmind.com/geoip/v2.1/country/me?referrer=https%3A%2F%2Fwww.acunetix.com

	Load:	Server: 104.16.38.47	ASN: 13335		Reverse DNS:
OK	59ms	cloudflare	Cloudflare, Inc.		

https://cse.google.com/cse/cse.js?cx=014967287653641589399:rfsaq_jzpxi

	Load:	Server: 172.217.9.238	ASN: 15169		Reverse DNS:
OK	51ms	gws	Google LLC		lga34s11-in-f14.1e100.net

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1070114355/?random=1547744291436&cv=9&fst=1547744291436&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=768&u_w=1024&u_ah=768&u_aw=1024&u_cd=32&u_his=1&u_tz=0&u_java=false&u_nplug=0&u_nmime=0>m=2wg170&frm=1&url=https%3A%2F%2Fwww.acunetix.com%2F&ref=https%3A%2F%2Fwww.acunetix.com%2Fundefined&tiba=Page%20Not%20Found%20%7C%20Acunetix&async=1&rfmt=3&fmt=4

	Load:	Server: 172.217.10.2	ASN: 15169		Reverse DNS:
OK	59ms	cafe	Google LLC		lga34s12-in-f2.1e100.net