BINNEN ZONDER KLOPPEN

WordPress geeft gegevens prijs

WordPress geldt als een veelzijdig en eenvoudig te beheren CMS. Maar veel beheerders vergeten de krachtige interfaces te beveiligen en geven zo ongewild toegang tot niet openbare content en bestanden.

Mirko Dölle, Jan Mahn en Noud van Kruysbergen

WordPress is het wereldwijd meest gebruikte contentmanagementsysteem (CMS). Het wordt door grote bedrijven net zo goed gebruikt als voor particuliere websites. Veel providers bieden WordPress als kant-en-klaar pakket inclusief webserver aan, en voor de basisbediening heb je geen informaticacursus nodig. Maar het systeem heeft zijn gebreken. Veel WordPress-installaties geven via de achterdeur bijvoorbeeld toegang tot gegevens die de beheerder eigenlijk helemaal niet wilde openbaren.

De oorzaak voor de onbedoelde loslippigheid is de programmeerinterface JSON-API. Daarmee kun je WordPress verbinden met andere programma's. Helaas vertelt de officiële documentatie niet luid en duidelijk dat die interface zonder extra maatregelen niet tegen leesbenaderingen beveiligd is.

UIT DE SCHOOL GEKLAPT

Via dat kanaal kunnen nieuwsgierigen bijvoorbeeld muzieknummers vóór de geplande releasedatum downloaden of vertrouwelijke interne documenten in handen krijgen. De achterdeur maakt het hackers ook mogelijk om vooraf en zonder juridische risico's waardevolle informatie over het CMS te verzamelen, die ze dan bijvoorbeeld voor brute-force-aanvallen op wachtwoorden kunnen gebruiken. Voor een efficiënte brute-force wordt bij voorkeur de tweede interface XML-RPC gebruikt.

Het vinden van kwetsbare WordPress-installaties is kinderspel. De IoT-zoekmachine Shodan.io heeft bijvoorbeeld een aparte categorie voor WordPress. Voor het zoeken heb je wel een betaald account nodig. Anders kun je gewoon met je favoriete zoekmachine zoeken op de termen wp-content, wp-include of wp-login – alle drie zijn ontegenzeggelijk aanwijzingen dat de website WordPress gebruikt. Als je wilt weten of een website door WordPress geleverd wordt, hoef je meestal alleen blik op de url van een ingebed plaatje te werpen. Bevat die 'wp-content', dan is dat een onmiskenbaar teken.

OPEN ACHTERDEURTJES

Je kunt met de browser heel simpel achterhalen of de beheerders vergeten hebben om de API-achterdeurtjes te sluiten. Je hoeft alleen maar naar de subdirectory /wp-json te proberen te gaan. Krijg je dan een JSON-structuur te zien, dan staat de API meestal helemaal open. Wanneer de JSON-API niet onder wp-json antwoordt, moet je er op andere plaatsen naar zoeken.

Op de website van de Amerikaanse zangeres Laura Brehm, staat de API in /index.php/wp-json. Dat is makkelijk te ontdekken als je in de HTML-code van de pagina op wp-json zoekt.

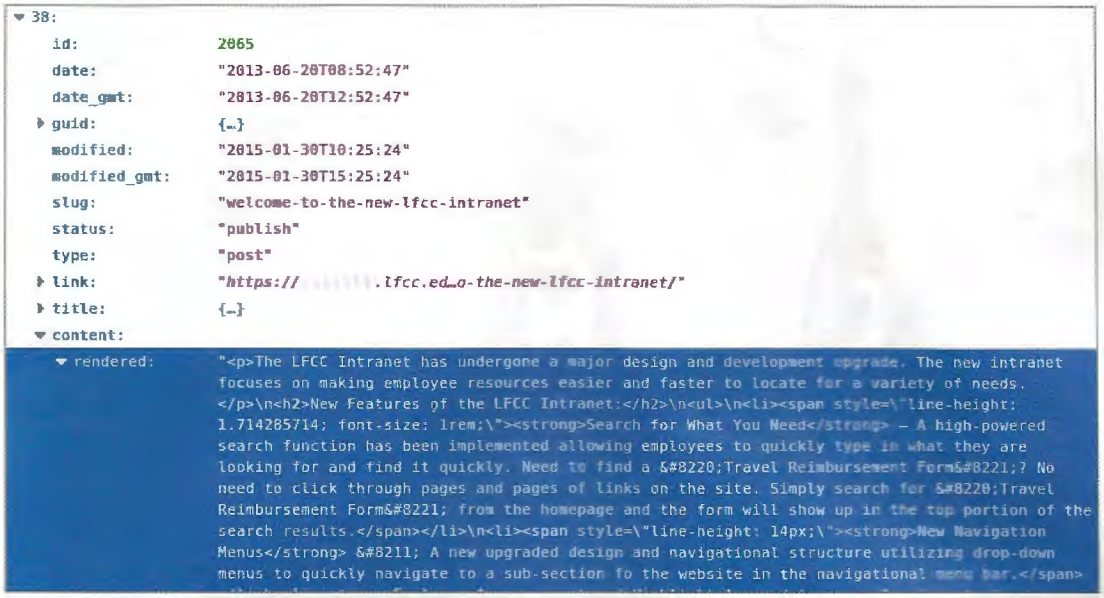
Heb je de API gelokaliseerd, dan kun je via de browser verder rondkijken. Een blik in /index.php/wp-json/wp/v2/media bracht een paar vergeten, high-res foto's van de zangeres aan het licht. Dat is een standaard probleem van vrijwel alle WordPress-installaties, die we in het kader van ons onderzoek onderzocht hebben. Vaak worden foto's in de originele resolutie geüpload, die WordPress dan naar verschillende standaardresoluties terugrekent. De verkleinde foto's worden dan ingebed, maar als je de originele foto's niet verwijdert, zijn ze via de JSON-API te vinden en vrij te downloaden.

Als je de JSON-API verder onderzoekt, ontdek je in /index.php/wp-json/wp/v2/users op de website van Laura Brehm, dat er bij die WordPress-installatie maar één enkele gebruiker is, laura. Een belangrijke clou waarmee hackers vervolgens via de eveneens openstaande XML-RPC-interface een brute-force-aanval op het wachtwoord kunnen starten met een paar honderd pogingen per aanroep.

Andere WordPress-sites werken met de e-mailadressen van de gebruikers als gebruikersnaam of als WordPress-slug. Daartoe behoort een site die zich met de Aziatische pokervariant Teen Patti bezig houdt. Die nalatigheid maakt wp/v2/users van de JSON-API tot een door machines leesbare zelfbedieningswinkel voor spammers.

OPEN DEUR

Voor het Lord Fairfax Community College in de Verenigde Staten werd die configuratiefout echt fataal. Daar had de beheerder geprobeerd op de van buitenaf bereikbare intranetserver een beveiligd gebied in te richten door de pagina via een plug-in van een login te voorzien. Die zorgde er echter alleen voor dat je naar de WordPress-login werd omgeleid als je content via het front-end opvraagt. De JSON-API werd door de omleiding niet beveiligd, zodat iedereen daar toegang toe had en zo via de link /wp-json/wp/v2/pages alle pagina's, via /wp-json/wp/v2/posts alle forumposts en via /wp-json/wp/v2/comments alle commentaren kon lezen. Via /wp-json/wp/v2/media waren alle bestanden bereikbaar.



De nieuwe intranetserver van het Lord Fairfax Community College was niet alleen toegankelijk vanaf internet, maar via de onbeschermde JSON-API van WordPress had iedereen ook toegang tot meer dan 2500 documenten, scans, roosters en mailinglijsten.

Op die manier hadden we vrij toegang tot meer dan 2500 interne protocollen, mailinglijsten, dienstroosters van het systeembeheer, telefoonlijsten, Dropbox-links, links naar documenten op Google Docs en gearchiveerde stukken vanaf 2008.

GOUDMIJN

Bij veel openstaande WordPress-installaties is de mediadatabase een ware goudmijn. Die wordt bij bedrijven vaak als tussenstation voor de interne data-uitwisseling misbruikt. Dat is gebaseerd op de foutieve aanname dat content die niet in een gepubliceerde forumpost gelinkt is, voor derden onvindbaar zou zijn. Dat klopt ook voor het front-end van de website, je kunt immers niet zomaar een directory-listing van de directory /wp-content opvragen.

Maar die listing staat wel in de mediadatabase, die je via de API kunt bereiken. Bij onze onderzoekingen vonden we interne foto's van bedrijven, bij verschillende muzikanten muziekbestanden, foto's en video's van toekomstige projecten en in een enkel geval zelfs een back-up van de complete webserver als zip-bestand. En dat overkomt niet alleen kleine ondernemingen. Het Italiaanse consultancybedrijf Media-Engine, die voor vele bekende ondememingen zoals Red Bull, Armani, Continental, BMW, Maserati, Allianz, UniCredit en Virgin werkt, heeft eveneens een WordPress-CMS met openstaande JSON-API. Daar vonden we in de posts en in de mediadatabase onder andere concepten en ontwerpen voor toekomstige website-uitingen, die vermoedelijk niet voor de buitenwereld bedoeld waren.

Een schoolvoorbeeld van hoe WordPress interne gegevens lekt, is de website van de Zwitserse firma Akiro. Toen we die bij onze onderzoekingen tegenkwamen, bestond de website schijnbaar alleen uit het bedrijfslogo en de verplichte bedrijfsgegevens – verder stond er geen informatie in. Maar via de openstaande JSON-API ontdekten we dat er nog een productcatalogus en een heleboel oude pagina's gepubliceerd waren. Daaronder bevond zich ook een contactformulier dat zich nota bene ook nog voor spam en phishing liet misbruiken – en begin september ook inderdaad voor een massamailing van reclame voor een louche loterij gebruikt werd.

OPLOSSING

Er zijn verschillende manieren om de API te beveiligen tegen externe blikken. Sommigen raden aan om hem helemaal uit te schakelen. Maar dat werkt niet als je de moderne editor Gutenberg gebruikt, die van de API gebruik maakt. Het beste kun je er een authenticatie aan koppelen.

Een manier is om alle paden onder '/wp-json' direct door de webserver te laten beveiligen met HTTP Basic Auth. Maar het kan ook door een bestand van WordPress aan te passen: open functions.php in het gebruikte theme en voeg daar de functie `add_filter()` aan toe, die we bij de link op deze pagina voor je hebben klaargezet. Bij een eventuele update moet je dat dan opnieuw doen. Het kan nog makkelijker met de plug-in Disable WP REST API.

Natuurlijk hebben we alle eigenaren van de in dit artikel genoemde WordPress-installaties vooraf over de bestaande problemen en de aankomende publicatie geïnformeerd. Toch waren sommige JSON-API's bij redactiesluiting nog steeds bereikbaar – blijkbaar zien de eigenaren het gevaar er niet van in. ct

www.ct.nl/softlink/
2103102

Als de beheerder e-mailadressen gebruikt als gebruikersnamen voor WordPress, wordt de onbeschermde JSON-API een door machines leesbare zelfbedieningswinkel voor spammers.