IT-Service BW

WordPress Sicherheitsüberprüfung–BlackBox-Test der Seite: EineBeispielDomaine.de

Auftraggeber:
<NamedesAuftraggebers>
<Adresse>
<Telefon/Fax>
<Ansprechpartner>

Auftragnehmer:
IT-Service BW
Juan Roldan Güpner
Fabrikhof1
88410 Bad Wurzach
Tel. 07358 924069

Der Auftraggeber hat dem Auftragnehmer die Erlaubnis erteilt einen BlackBox-Test durchzuführen. Dabei wird die Webseite gescannt, indem nur Zugriffe durchgeführt werden, die von ‚aussen' möglich sind, d.h. ohne sich in das WordPress System einzuloggen.

ZusammenfassungdesErgebnisses:

Das Ergebnis des Sicherheitscans hat ergeben, dass:

- Die Version von WordPress von aussen nicht festgestellt werden kann, dies ist sicherheitstechnisch als sehr gut zu bewerten. Es muss jedoch sichergestellt werden, dass WordPress dann auf den aktuellen Stand ist.
- Das PlugIn `js_composer` ist ggf. nicht auf dem aktuellen Stand.
- Das PlugIn `WP Statistics` ist zwar auf dem aktuellen Stand, jedoch ist eine Sicherheitslücke bekannt, die noch nicht geschlossen wurde. Diese Lücke betrifft den Adminbereich und ist nicht als kritisch zu bewerten.

Fazit:

Es muss überprüft werden, ob WordPress auf dem aktuellen Stand ist und sobald für `WP Statistics` ein Update herauskommt, muss diese installiert werden, um die noch offene Sicherheitslücke zu schließen.

Scan-Protokoll im Detail

```
 [+] URL: http://EineBeispielDomaine.de/

 [+] Started: Wed Aug 16 21:02:22 2017


 [+] robots.txt available under: 'http://EineBeispielDomaine.de/robots.txt'

 [+] Interesting entry from robots.txt: http://EineBeispielDomaine.de/wp-admin/admin-ajax.php

 [+] Interesting header: KEEP-ALIVE: timeout=15

 [+] Interesting header: LINK: <http://EineBeispielDomaine.de/wp-json/>; rel="https://api.w.org/"

 [+] Interesting header: SERVER: Apache

 [+] Interesting header: SET-COOKIE: wfvt_2681142237=5995155941f59; expires=Thu, 17-Aug-2017 04:32:33 GMT; Max-
Age=1800; path=/; httponly

 [+] Interesting header: X-POWERED-BY: PHP/5.6.31

 [+] This site has 'Must Use Plugins' (http://codex.wordpress.org/Must_Use_Plugins)

 [+] XML-RPC Interface available under: http://EineBeispielDomaine.de/xmlrpc.php


 [34m[i] [0m WordPress version can not be detected
```

```
[+] WordPress theme in use: customizr - v3.3.28

[+] Name: customizr - v3.3.28
|  Last updated: 2017-08-02T00:00:00.000Z
|  Location: http://EineBeispielDomaine.de/wp-content/themes/customizr/
|  Readme: http://EineBeispielDomaine.de/wp-content/themes/customizr/readme.txt
[33m[!] [0m The version is out of date, the latest version is 4.0.5
|  Style URL: http://EineBeispielDomaine.de/wp-content/themes/customizr/style.css

[+] Enumerating installed plugins (only ones with known vulnerabilities) ...

 : |=============================================================================================|

[+] We found 2 plugins:

[+] Name: js_composer
|  Location: http://EineBeispielDomaine.de/wp-content/plugins/js_composer/
```

```
[33m[!] [0m We could not determine a version so all vulnerabilities are printed out


[31m[!] [0m Title: Visual Composer <= 4.7.3 - Multiple Unspecified Cross-Site Scripting (XSS)
   Reference: https://wpvulndb.com/vulnerabilities/8208
   Reference: http://codecanyon.net/item/visual-composer-page-builder-for-wordpress/242431
   Reference: https://forums.envato.com/t/visual-composer-security-vulnerability-fix/10494/7
[34m[i] [0m Fixed in: 4.7.4


[+] Name: wp-statistics - v12.0.10
|  Latest version: 12.0.10 (up to date)
|  Last updated: 2017-07-24T17:43:00.000Z
|  Location: http://EineBeispielDomaine.de/wp-content/plugins/wp-statistics/
|  Readme: http://EineBeispielDomaine.de/wp-content/plugins/wp-statistics/readme.txt
|  Changelog: http://EineBeispielDomaine.de/wp-content/plugins/wp-statistics/changelog.txt


[31m[!] [0m Title: WP Statistics 12.0.9 - Authenticated Cross-Site Scripting (XSS)
   Reference: https://wpvulndb.com/vulnerabilities/8866
```

```
    Reference:
https://lorexxar.cn/2017/07/07/WordPress%20WP%20Statistics%20authenticated%20xss%20Vulnerability(WP%20Statistics%20-
=12.0.9)/

    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10991


 [+] Enumerating installed themes (only ones with known vulnerabilities) ...

  : |=============================================================================================|


 [+] No themes found


 [+] Finished: Wed Aug 16 21:21:05 2017

 [+] Requests Done: 1910

 [+] Memory used: 145.531 MB

 [+] Elapsed time: 00:18:42
```