Site Scan 2022-08-28

Tags	Portfolio Work
Published	@August 28, 2022
Public	☑
Last Updated	@August 28, 2022 6:04 PM
Author	Greg Stevens
Created	@August 28, 2022 5:57 PM
BG Music or Vid	
Description	
Tweet	□
Featured	□
Slug	site-scan
Published URL	

Contents

Note's Markdown Source from Obsidian

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/c93d3b4a-2cbe-430f-8ec8-e53f210e0679/2022-08-28_PrecisionDrilling.com_Pen_Test_and_Site_Overview.md

https://www.obsidian.md/

PDF Export

From Obsidian (unpublished)

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/5eeafed7-4f2f-4df8-bbc9-9b9de1f521bc/2022-08-28_PrecisionDrilling.com_Pen_Test_and_Site_Overview.pdf

From Notion (art.stevens.pro)

Video

https://youtu.be/7-zcO1BAFC0

Mermaid Background

- Docs
- Live Editor

Mermaid Chart Source Code

```
%% graph TD
flowchart TD
site((PrecisionDrilling.com))

host(WP Engine)
waf1(WP Engine)
waf2(Cloudflare)
dns(Azure DNS)
ns_registrar("Network Solutions (GoDaddy)")
cms(WordPress)
cms_login(/wp-admin/ OPEN)

site -- Hosted By --> host
site -- NS Registrar --> ns_registrar
site -- DNS Provider --> dns
site -- Protected By WAF1 --> waf1
site -- Protected By WAF2 --> waf2





rx("Recommendations (RX) & Vulnerabilities")

vuln1("XSS Injection on Site Search, unattackable - Low Risk")
rx1("Nothing IRL, WAF did its job.")
rx1_why("Could reduce OWASP! ZAP Alerts")

vuln2(WP Login Open - High Risk)
rx2("Lockdown /wp-admin/ by IP or HTTP User/Pass")
rx2_why(Prevent most junk login attempts, reduce log clutter)



site --> rx

vuln1 -- Blocked By Cloudflare --> waf2

rx --> vuln1
vuln1 -- RX --> rx1
rx1 -- Why? --> rx1_why

rx --> vuln2
vuln2 -- RX --> rx2
rx2 -- Why? --> rx2_why
```

```
site --> cms
cms --> cms_login
cms_login --> vuln2


dns_target("CNAME m6blypcji6rh.wpeproxy.com.")
dns --> dns_target
dns_target --> host

%% %% %%
%% cloudflare
%% %% %%
cloudflare_why("&quot;WP Engine recommends Cloudflare when configuring DNS because...&quot; ")
cloudflare_why_src("<https://wpengine.com/support/cloudflare-best-practices/>")

cloudflare_why --> cloudflare_why_src

waf2 --> cloudflare_why

host --> waf2


%% %% %%
%% Scans Done
%% %% %%

scans("Scans Performed")
scan1(OWASP! ZAP)
scan2(Burp)
scan3(wpsec.com)

site --> scans
scans --> scan1
scans --> scan2
scans --> scan3

%% ("<https://wpsec.com/scan/?id=1eb9f5e51054e231071c4cb745ab1413>")
```

Gist URL to Source Code

- *Gist created with vscode plugin GistPad*
- *for loading into mermaid.live*

> https://gist.githubusercontent.com/GregSweats/bada1bb2512a581ce71cfaad82f907a6/raw/411be26f9ca
> 1.mermaid

… as a **Notion Bookmark**

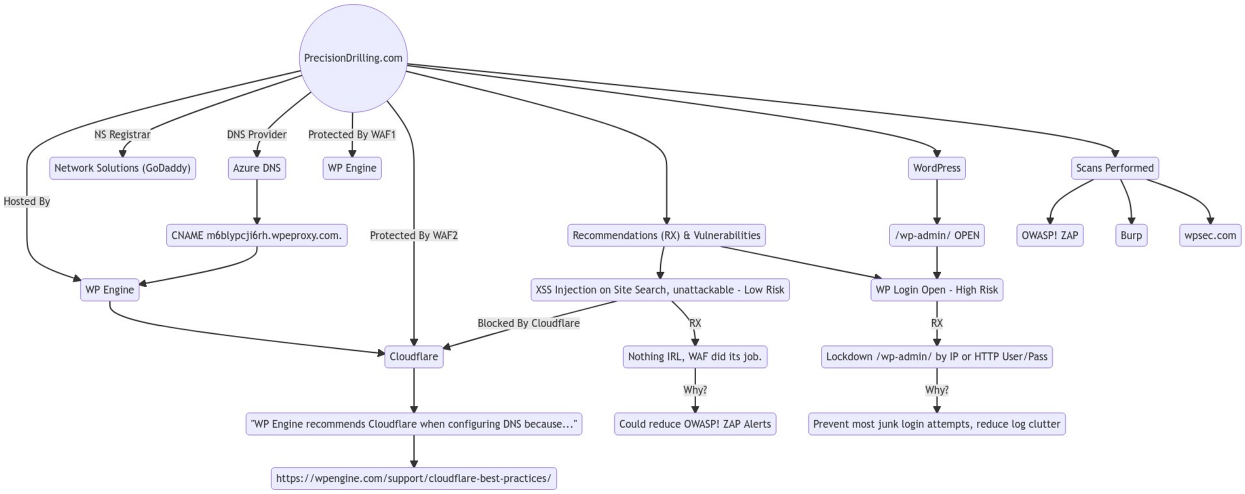
https://gist.githubusercontent.com/GregSweats/bada1bb2512a581ce71cfaad82f907a6/raw/411be26f9ca328fcd832424a697db3854ab56694/pd-1.mermaid

View Gist on GitHub

> https://gist.github.com/GregSweats/bada1bb2512a581ce71cfaad82f907a6#file-pd-1-mermaid

- Chart is rendered by GitHub b/c apparently Mermaid Charts are supported by GitHub?

Rendered Chart with Mermaid Live Editor


PrecisionDrilling.com
NS Registrar
Network Solutions (GoDaddy)
DNS Provider
Azure DNS
Protected By WAF1
WP Engine
Hosted By
CNAME m6blypcji6rh.wpeproxy.com.
Protected By WAF2
WP Engine
Cloudflare
"WP Engine recommends Cloudflare when configuring DNS because..."
https://wpengine.com/support/cloudflare-best-practices/
Recommendations (RX) & Vulnerabilities
XSS Injection on Site Search, unattackable - Low Risk
Blocked By Cloudflare
RX
Nothing IRL, WAF did its job.
Why?
Could reduce OWASP! ZAP Alerts
WordPress
/wp-admin/ OPEN
WP Login Open - High Risk
RX
Lockdown /wp-admin/ by IP or HTTP User/Pass
Why?
Prevent most junk login attempts, reduce log clutter
Scans Performed
OWASP! ZAP
Burp
wpsec.com

Live Editor URL (Play with Themes)

> https://mermaid.live/edit?
> gist=https://gist.github.com/GregSweats/bada1bb2512a581ce71cfaad82f907a6#pako:eNpVU2FP2zAQ
> v-
> f37p2zE5VTKBai9rJrYFmUFvg7fbhxUmlbw_e7G1hLbVDN4AdCJS0Ev4XgYK3r6BFcDLBptrNHmE6P9
> -
> DL_dfbPZwdfDMoiVkNVk8QGl45S85g4hNiLiUsSKsAvXceFAaWo9n73slZuhbOd9f0Cq6c91iFk5cecp6V
> IqZkcs9L-
> bWdwYCZ__g_PaleZtWErVy3HRy_ofE4R9XLnOyQ25tSKW4dLA5KsYergyVPO9KYzlK3yNKcqlyleK40
> tROKsuJnKowz9yJWW_N7aMbYqD6uAxuMaStGE0NFiPh9mxN7nLfpWajX9Tf-
> WRv_BKSrN8vM8IJpb3JxIIl1bRDqaGLlCQ0erWE8Ccv-
> snja_PHbOh1mrJkEHg0dneeLvPn5ImZaCHfTvJd9aCnEoBk3-TXbJcSnSgPhowUslPZNK-
> 8K42CkWucimxCL4iIdCxuDut7Ya9z2m6BPoiy9_AcpoLrg

Contact Author

Greg Stevens, Dalyle DevOps Inc.

- (403) 213-5644 (best)
- (403) 498-6809 (mobile)
- greg@dalyle.ca (mainly unchecked)
- www.dalyle.ca
- www.stevens.pro

DALYLE.CA
DevOps for All!