




## Site Scan 2022-08-28

Tags	Portfolio Work
Published	@August 28, 2022
Public	<input type="checkbox"/>
Last Updated	@August 28, 2022 6:12 PM
Author	 Greg Stevens
Created	@August 28, 2022 5:57 PM
BG Music or Vid	
Description	
Tweet	<input type="checkbox"/>
Featured	<input type="checkbox"/>
Slug	site-scan
Published URL	

### Contents

[Note's Markdown Source from Obsidian](#)

[PDF Export](#)

[From Obsidian \(unpublished\)](#)

[From Notion \(art.stevens.pro\)](#)

[Making of Video](#)

[Mermaid Background](#)

[Mermaid Chart Source Code](#)

[Gist URL to Source Code](#)

[View Gist on GitHub](#)

[Rendered Chart with Mermaid Live Editor](#)

[Live Editor URL \(Play with Themes\)](#)

[Contact Author](#)

### 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://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### From Obsidian (unpublished)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](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)

[https://s3-us-west-2.amazonaws.com/secure.notion-static.com/b5ec3125-e4b6-487e-a746-6bd4abc18906/Site\\_Scan\\_2022-08-28.pdf](https://s3-us-west-2.amazonaws.com/secure.notion-static.com/b5ec3125-e4b6-487e-a746-6bd4abc18906/Site_Scan_2022-08-28.pdf)

## Making of Video

| <https://youtu.be/7-zcO1BAFC0>

<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(""WP Engine recommends Cloudflare when configuring DNS because..." ")
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/411be26f9c1.1.mermaid>

... as a **Notion Bookmark**

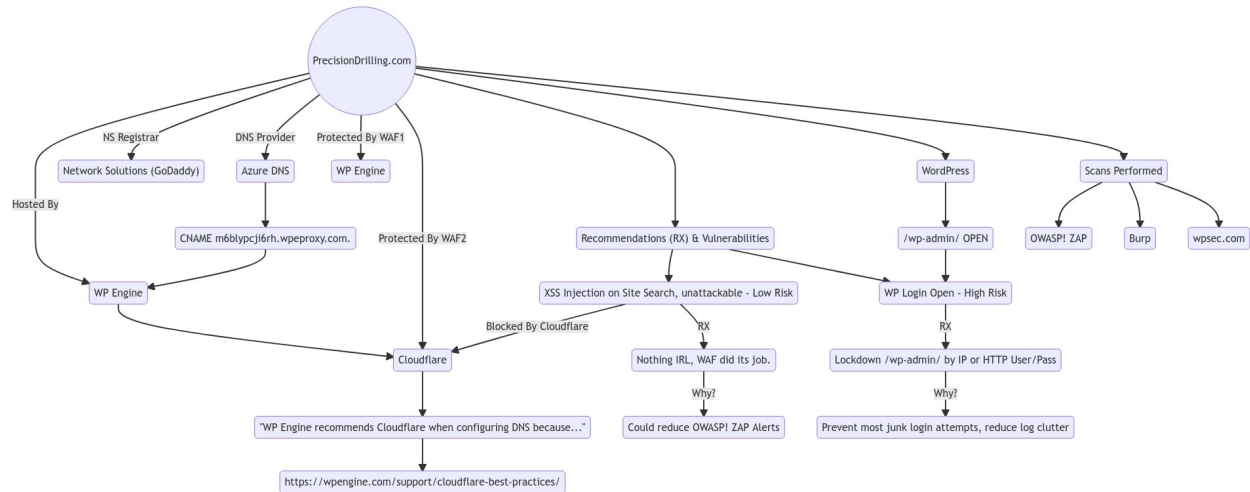
 <https://gist.githubusercontent.com/GregSweats/bada1bb2512a581ce71cfaad82f907a6/raw/411be26f9ca328fcd832424a697db3854ab56694/pd-1.mermaid>

## 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



## Live Editor URL (Play with Themes)

<https://mermaid.live/edit?>

gist=<https://gist.github.com/GregSweats/bada1bb2512a581ce71cfaad82f907a6#pako:eNpVU2FP2zAQ>,

V:-

f37p2zE5VTKBai9rJrYFmUFvg7fbhxUmlbw\_e7G1hLbVDN4AdCJS0Ev4XgYK3r6BFcDLBptrNHmE6P9

=

DL\_dfbPZwdfDMoiVknV8QGI45S85g4hNiLiUsSKsAvXceFAaWo9n73slZuhbOd9f0Cq6c91iFk5cecp6v

lqZkcs9L-

bWdwYCYZ\_g\_PaleZtWErVy3HRy\_ofE4R9XLnOyQ25tSKW4dLA5KsYergyVPO9KYzIK3yNKcqlyleK40

tROKsuJnKowz9yJWW\_N7aMbYqD6uAxuMaStGE0NFipH9mxN7nLfpWajX9Tf-

WRv\_BKSrN8vM8Ijpb3JxIII1bRDgaGLICQ0erWE8Ccv-

snja\_PHB0h1mrJkEHg0dneeLvPn5ImZaCHfTvJd9aCnEoBk3-TXbJcSnSgPhowUsIPZNK-

8K42CkWucimxCL4ildCxDut7Ya9z2m6BPoiy9\_AcpoLrg

## Contact Author

**Greg Stevens**, Dalyle DevOps Inc.

- (403) 213-5644 (best)
- (403) 498-6809 (mobile)
- [greg@dalyle.ca](mailto:greg@dalyle.ca) (mainly unchecked)
- [www.dalyle.ca](http://www.dalyle.ca)
- [www.stevens.pro](http://www.stevens.pro)



DALYLE.CA

*DevOps for All!*