WordPress Security – “Beyond The Plugins”

Steve Schwartz

AVT Marketing

704-288-5705

Steve@AVTmarketing.com

Three Step Approach

- “Not So” Common Sense Approach
- Quick Nod to the Plugins
- Advanced Stuff

The stories you are about to hear are mostly true…

Names have been changed to protect the innocent.

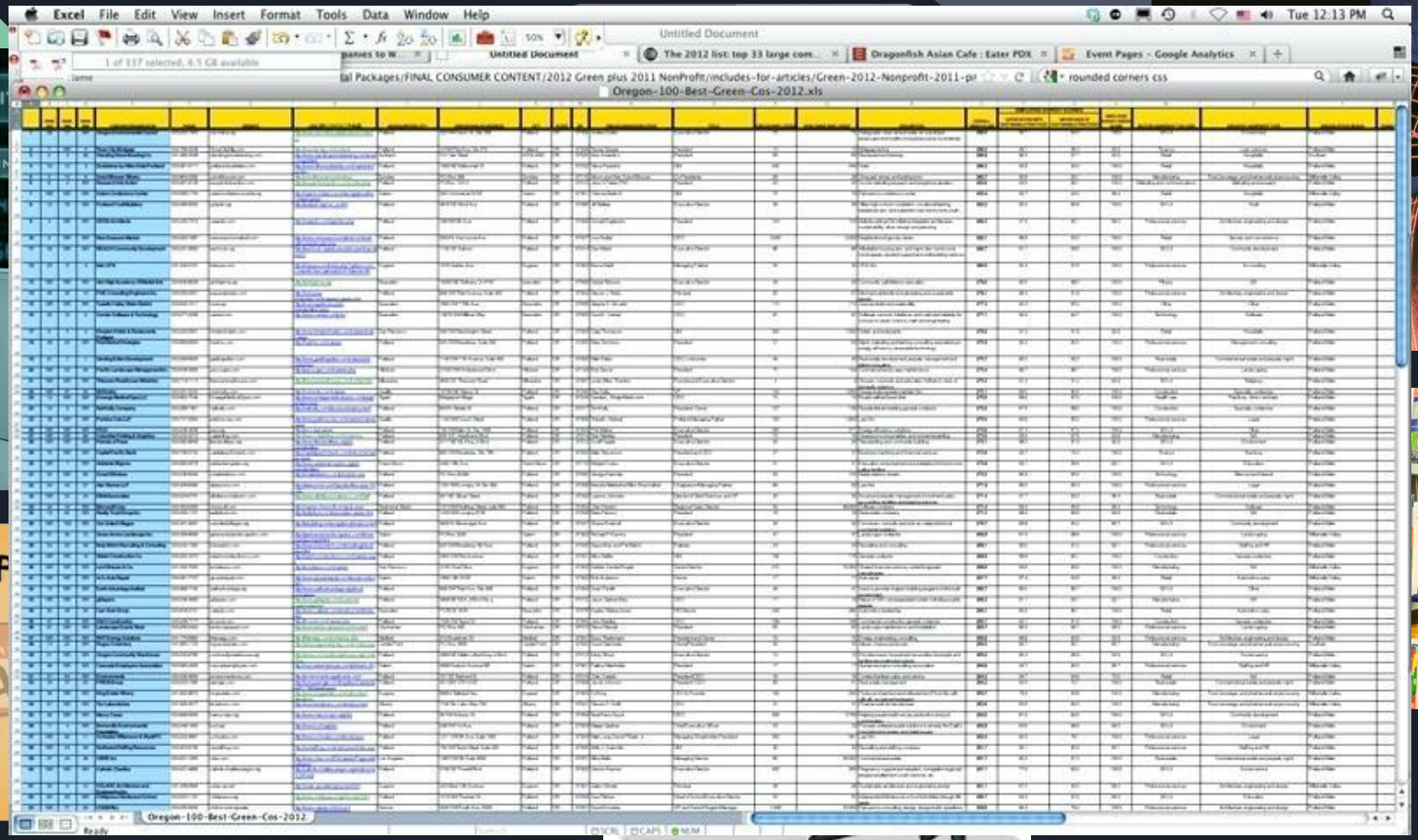
Meet Mary

facebook

starbucks

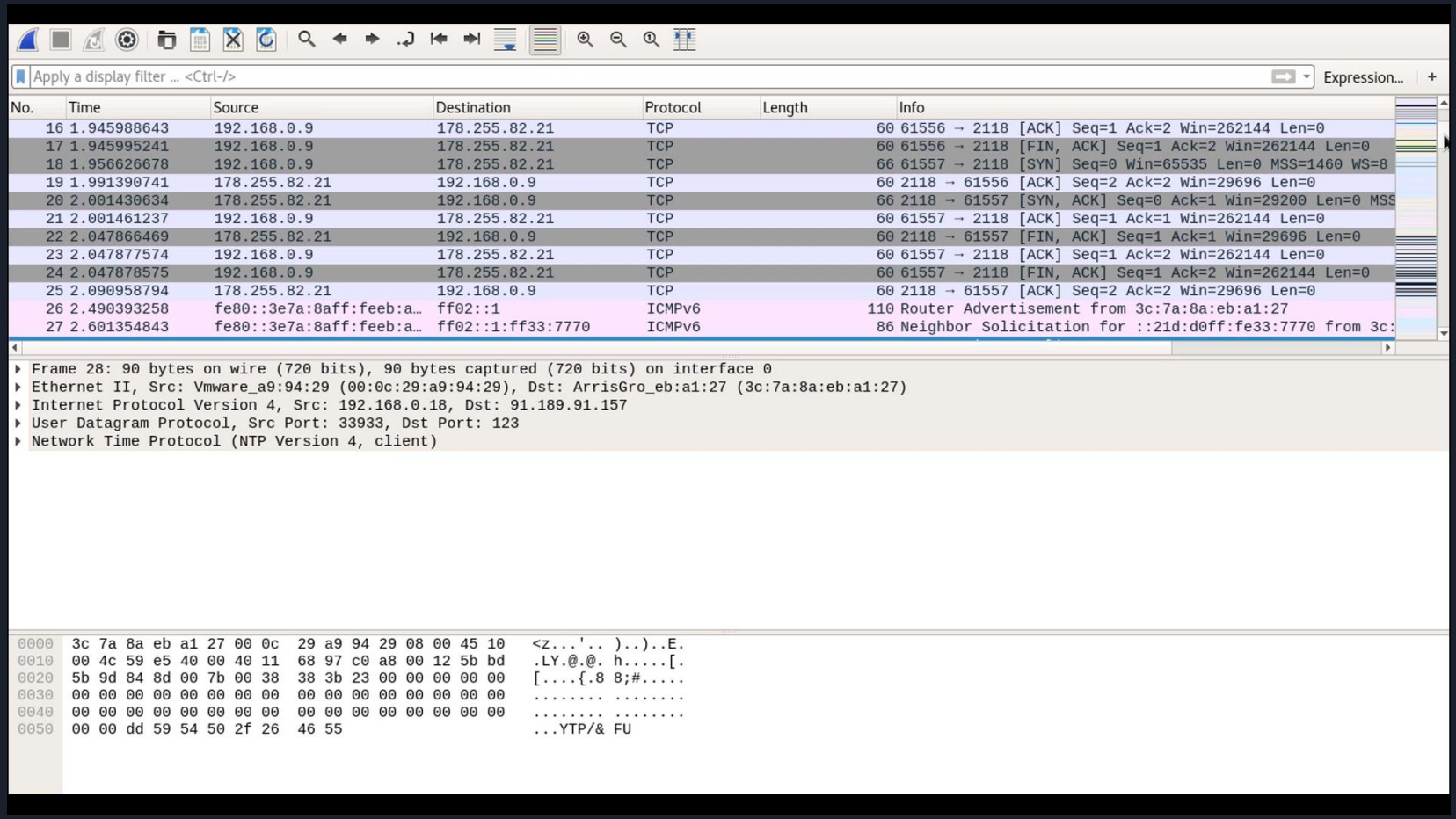
starbucks1

Mary 3 Months Later



So What Happened?

What The Hacker Saw



Simple Fix : Make Site SSL = HTTPS!

Force SSL (when possible) -

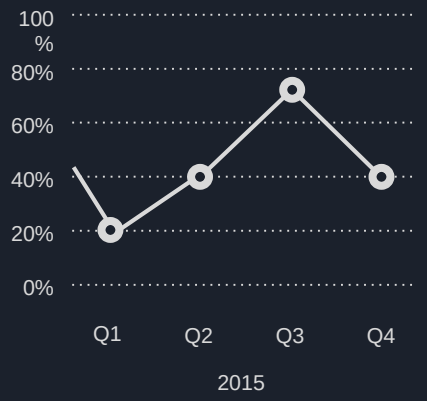
Just add the following options to your wp-config.php file:

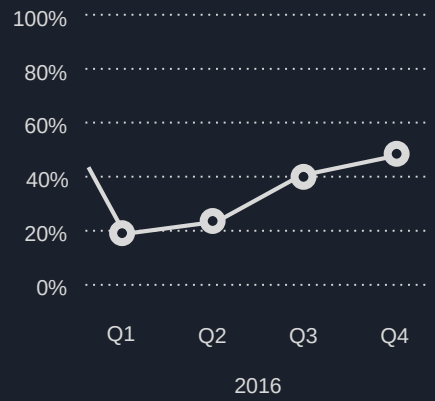
define(‘FORCE_SSL_LOGIN’, true);

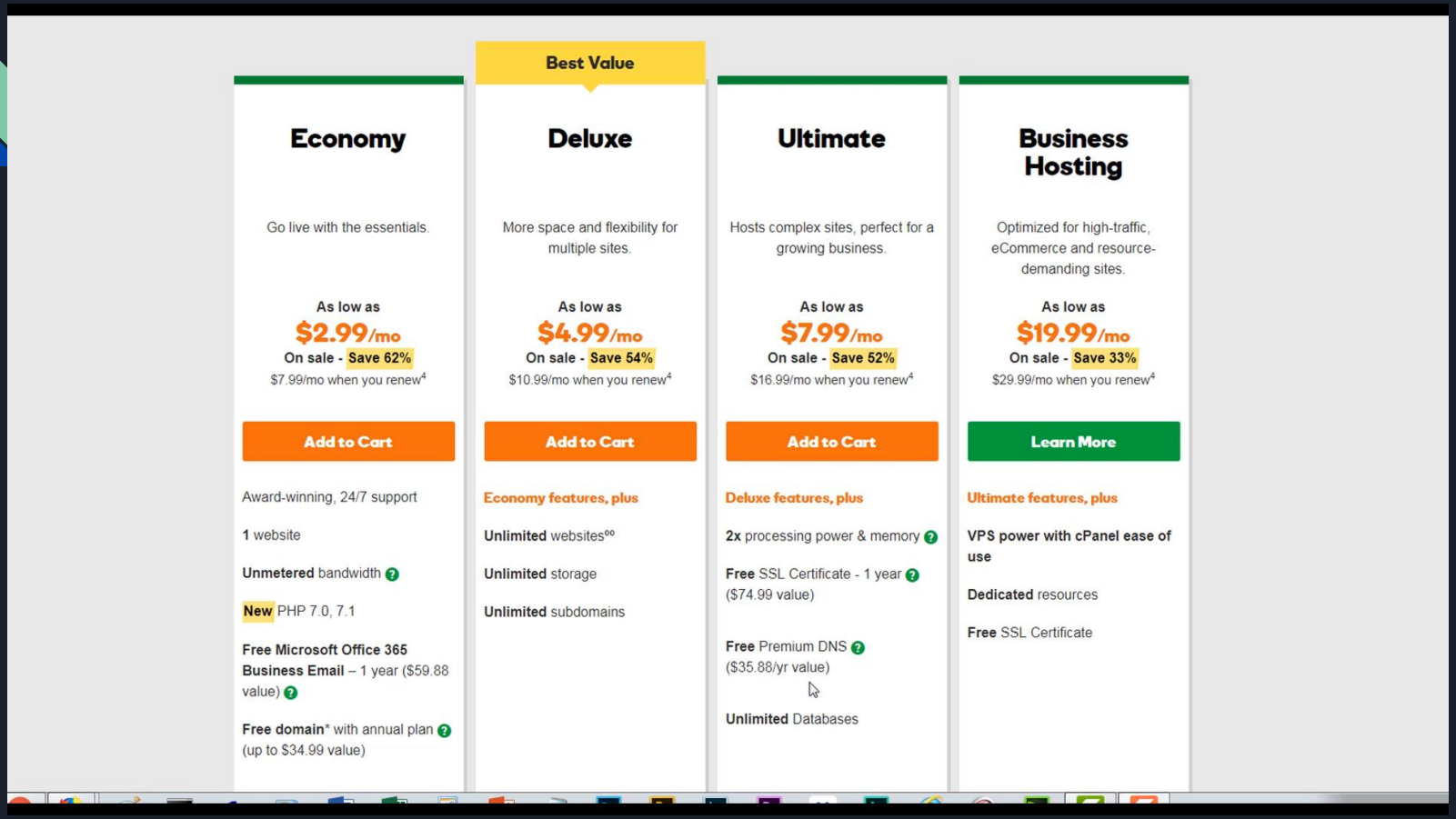
define(‘FORCE_SSL_ADMIN’, true);

Meet Thrifty Theo

Always wanting to save a buck, Theo opted for shared hosting for his company website.



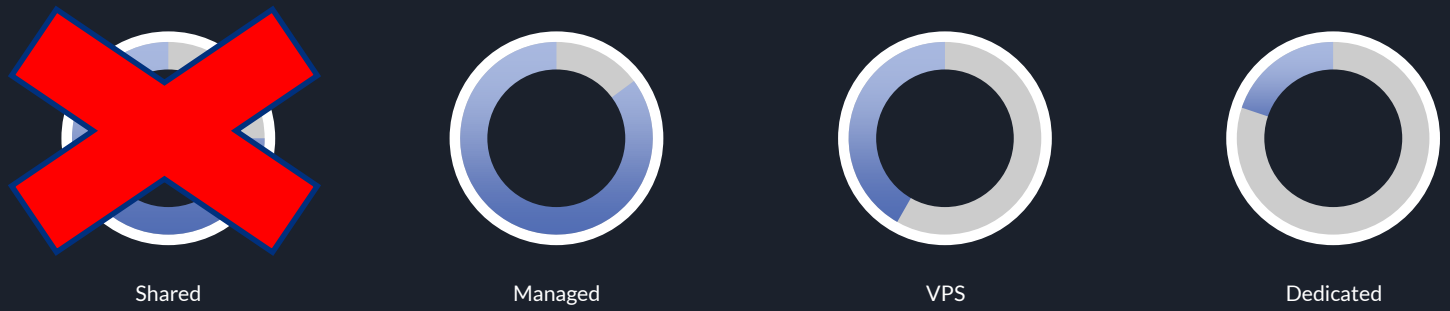



Best Value
Economy
Go live with the essentials.
As low as
$2.99/mo
On sale - Save 62%
$7.99/mo when you renew4
Add to Cart
Award-winning, 24/7 support
1 website
Unmetered bandwidth
New PHP 7.0, 7.1
Free Microsoft Office 365 Business Email – 1 year ($59.88 value)
Free domain* with annual plan (up to $34.99 value)
Deluxe
More space and flexibility for multiple sites.
As low as
$4.99/mo
On sale - Save 54%
$10.99/mo when you renew4
Add to Cart
Economy features, plus
Unlimited websites00
Unlimited storage
Unlimited subdomains
Ultimate
Hosts complex sites, perfect for a growing business.
As low as
$7.99/mo
On sale - Save 52%
$16.99/mo when you renew4
Add to Cart
Deluxe features, plus
2x processing power & memory
Free SSL Certificate - 1 year ($74.99 value)
Free Premium DNS ($35.88/yr value)
Unlimited Databases
Business Hosting
Optimized for high-traffic, eCommerce and resource-demanding sites.
As low as
$19.99/mo
On sale - Save 33%
$29.99/mo when you renew4
Learn More
Ultimate features, plus
VPS power with cPanel ease of use
Dedicated resources
Free SSL Certificate

VPS / Dedicated / WP Managed

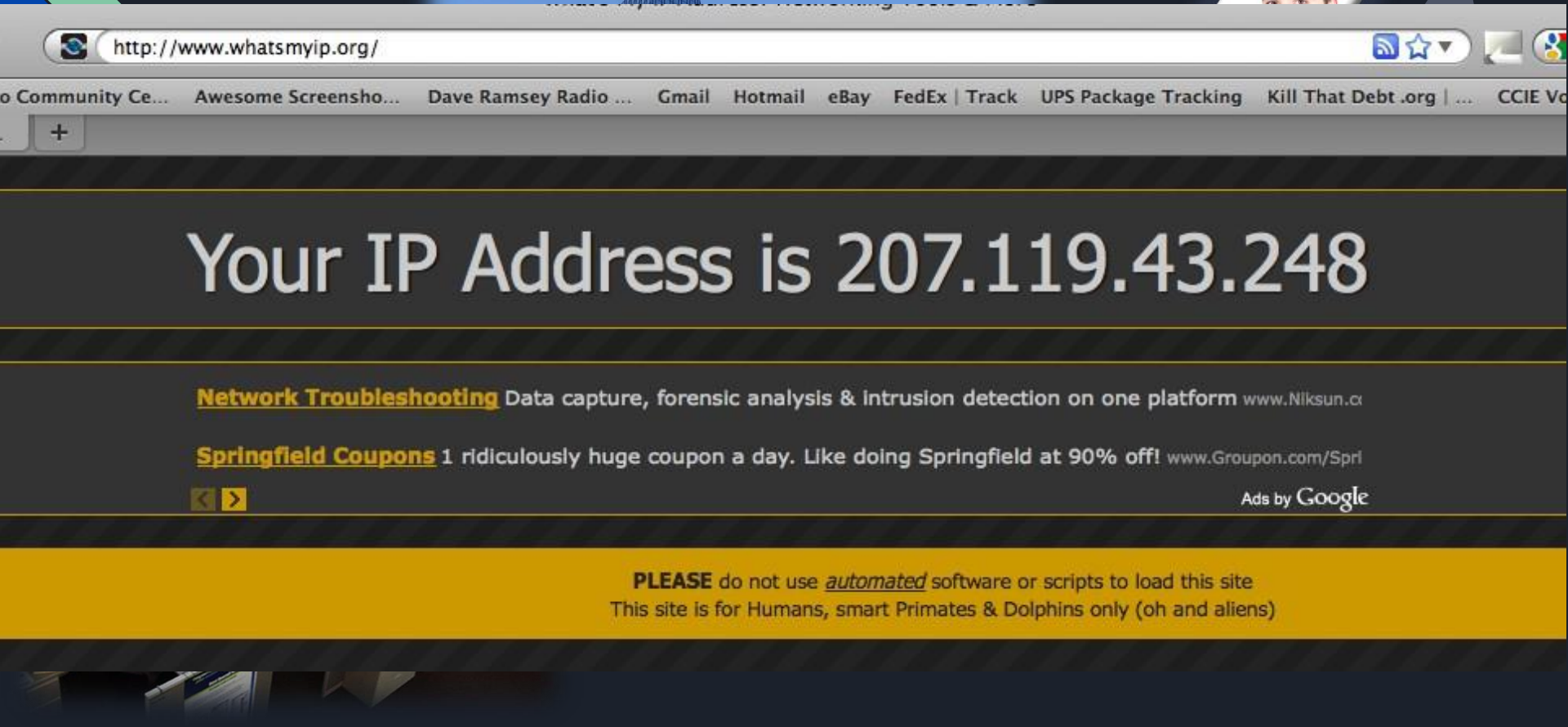
Every Host Nowadays has tiered options to choose from.

DON'T Choose Shared for your business or your clients

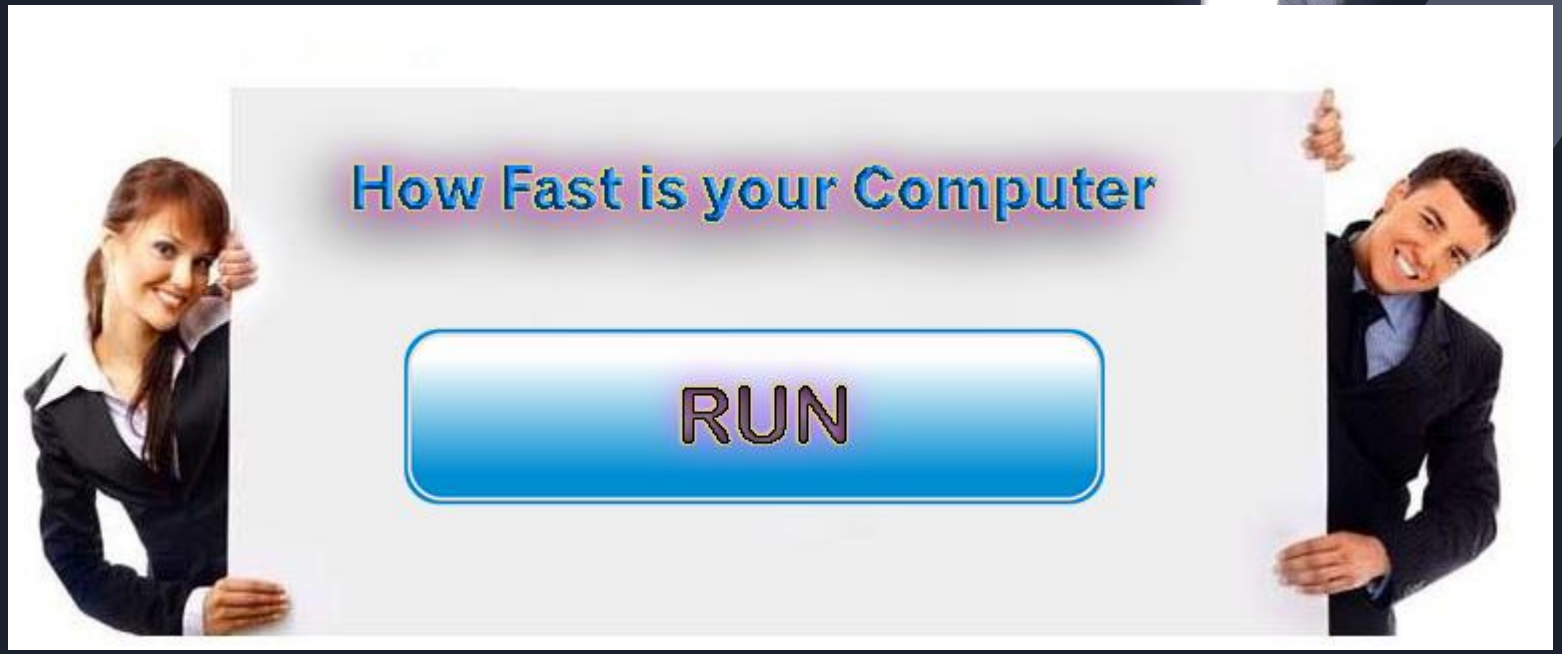


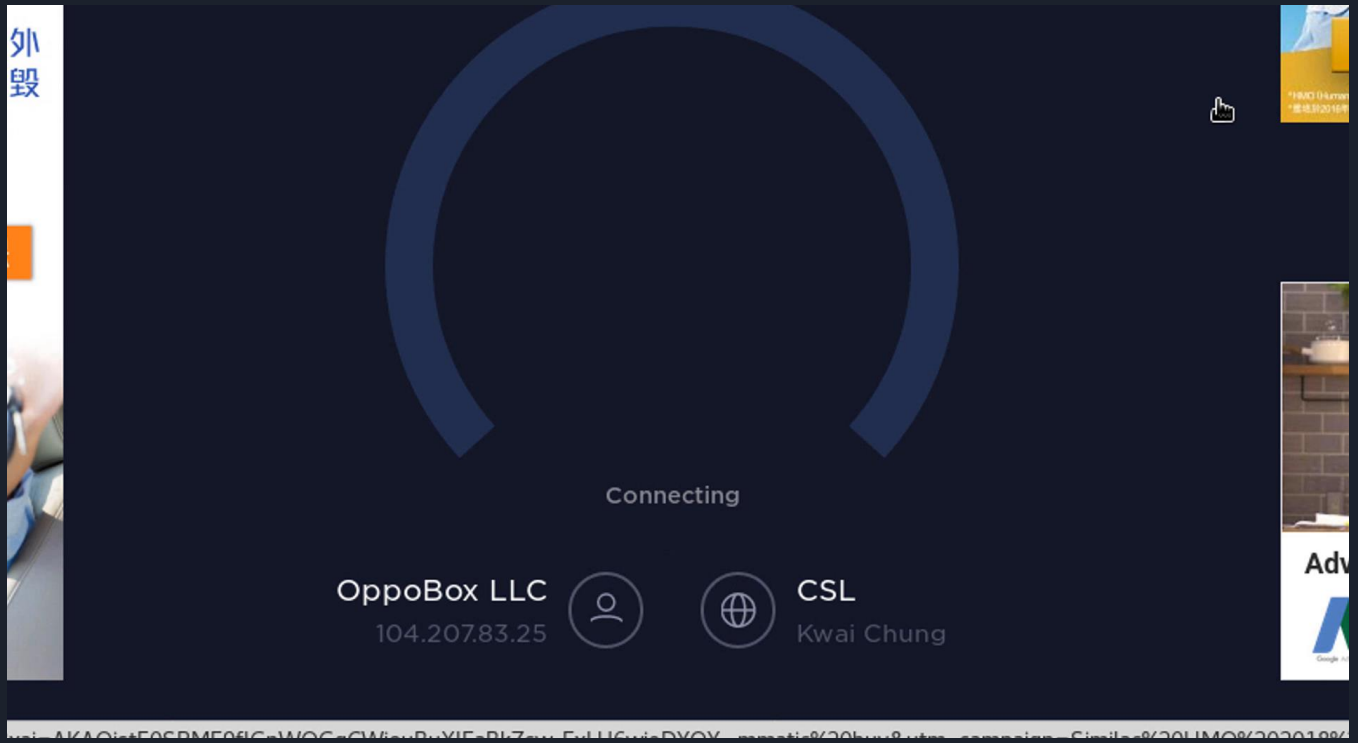
Shared Managed VPS Dedicated

Gullible Gary



Gullible Gary




Connecting
OppoBox LLC
104.207.83.25
CSL
Kwai Chung


YOU HAVE BEEN
HACKED!

RAT

Remote Access Trojan


I love fixing hacked sites on holidays!
We Need To Educate Our Clients
Who Gets Blamed?
The Developer!
Said NO ONE .... EVER!

Social Engineering

*** Hacking the People – Not the Tech**

Phishing Emails

Email - Click on the wrong attachment and it's game over

In Person

Hacker pretends to be someone he is not

Phone Calls

Tricked into giving away info, going to a site, taking some action / IRS & Tech Support Scams

Other

USB / Freeware offers / Free Games /


I love fixing hacked sites on holidays!
Said NO ONE .... EVER!

Educate Your Clients On Security From Their Fingertips to the Server

Antivirus / Malware / Spyware Check
Firewall

User Computer

Change Default Password
Change from WEP to WPA-2

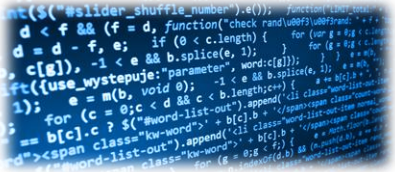
Router

Use HTTPS
Use SFTP/SSH
Avoid Public Wifi

Pipeline

No Shared Servers
Managed / Dedicated
Backups?.

Server



WP/Themes/Plugins
All Up To Date
Research Your Software!

Software

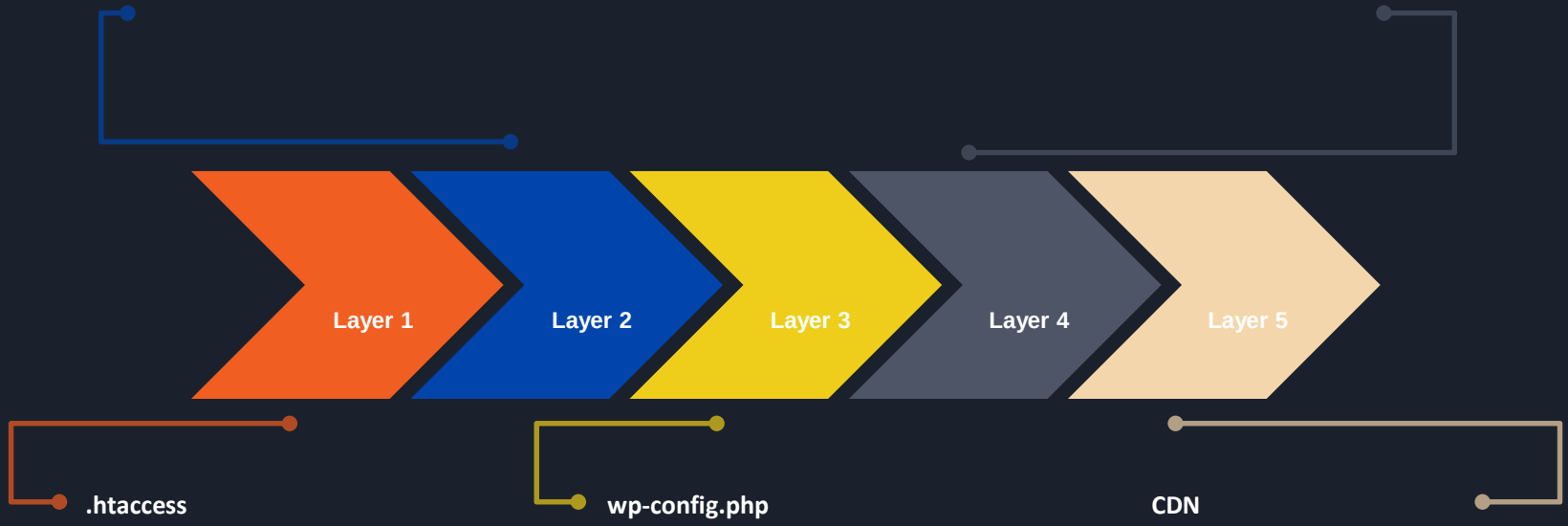
A Nod to Plugins

A Brute Force Attack Plugin –
Such as WordFence

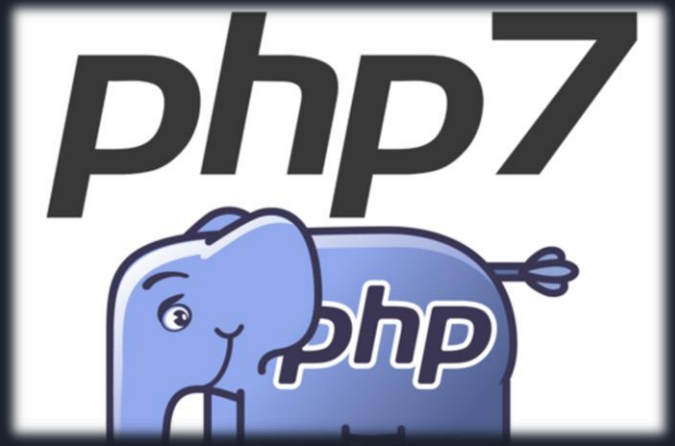
A Backup Plugin –

Such as BackupBuddy

BEYOND: Hardening WordPress



Server Software



Secret Keys - Authentication Unique Keys and Salts

Set of random variables that improve encryption of information stored in the user's cookies

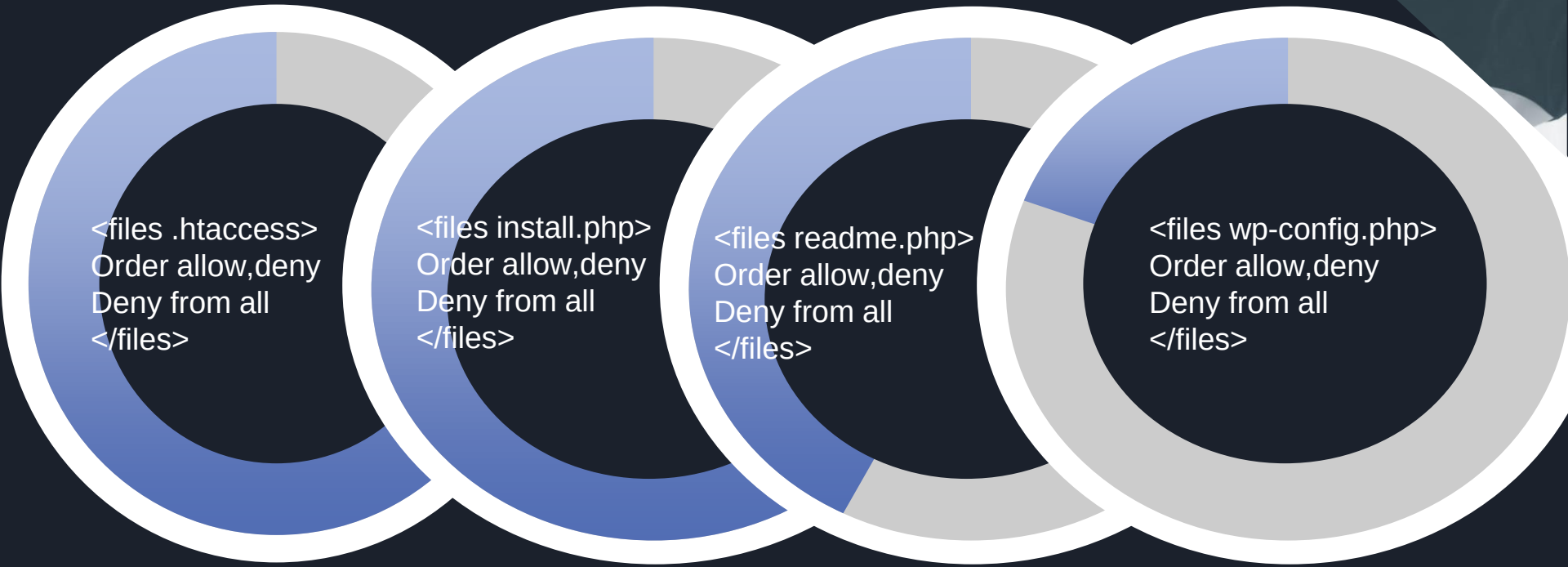
```
define('AUTH_KEY',         'put your unique phrase here');
define('SECURE_AUTH_KEY',  'put your unique phrase here');
define('LOGGED_IN_KEY',    'put your unique phrase here');
define('NONCE_KEY',        'put your unique phrase here');
define('AUTH_SALT',        'put your unique phrase here');
define('SECURE_AUTH_SALT', 'put your unique phrase here');
define('LOGGED_IN_SALT',   'put your unique phrase here');
define('NONCE_SALT',       'put your unique phrase here');
```

```
define('AUTH_KEY',  '*@9?))my;-f>}PX]d*z1h0uyee1j|]]]W*kjh$}FpKmM-r8jC}S`j4Sq4khU}8O.');
define('SECURE_AUTH_KEY',  'xUR:ph.ndpz+_M(&skfA,u63@.qt2A!5rT=iG6m1pn.B)w-*+kX!c4M]u(`.W$7z');
define('LOGGED_IN_KEY',  '(+IEG|cay>H[N-g=RA3,C0i$0CM)V?1Cm,KB=Wh8Bv*dFZ-A2yBw%BM}Kf:{:bm');
define('NONCE_KEY',  'r)w5~WA|{=r+fJ02ei>IToW7j-OeO!T~FO  #Mf5pkYc*TX@&U%~RICL:t&3:<ePS');
define('AUTH_SALT',  '  006c>Ht1Fs-.bjA-es0Pv0PoIIC***HT!aV+|#4q,i:Pg1c+qGF2FwRpqoC  eF0');
define('SECURE_AUTH_SALT',  'UyR(:vRo-=SG-yjF92t#`p)Rx|8IQJ7_V1)HrRMt4DcNM0UB@r9?RzOiU(=5HU  &');
define('LOGGED_IN_SALT',  'ix]#E-qTj+x%&0*ArU$W*@~wvcuR?wA!#/I7`Pd_Z$-SJ  v|8rI]w:&5/G&-HhgJ');
define('NONCE_SALT',  ')IVWFg+$v.3o=P*rH,Tt~Mc  4YW^BP9oX-rZ.y}>}r];jWN1W43g4kd|e&fG}1-');
```

https://api.wordpress.org/secret-key/1.1/salt

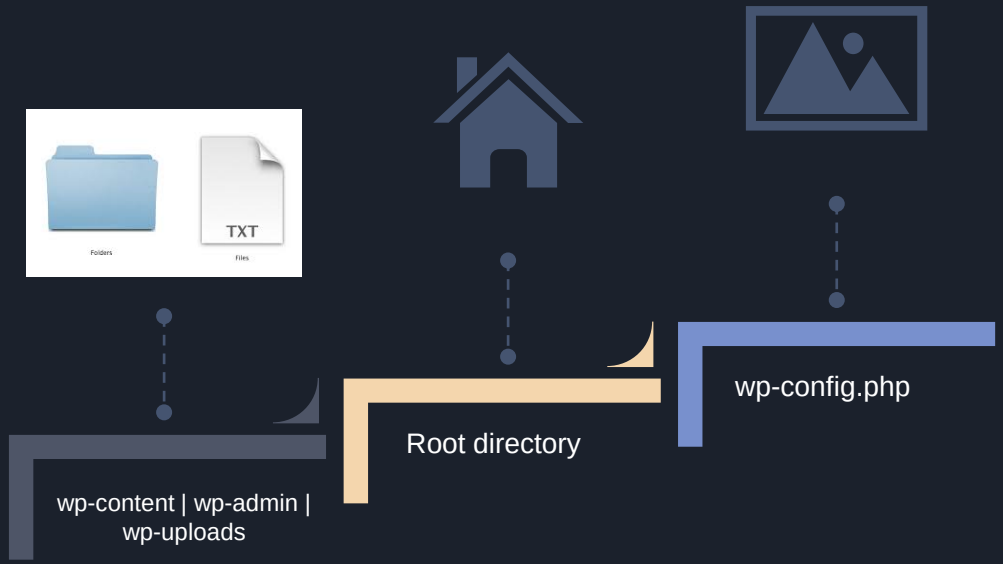
Get to Know Mr .htaccess

Deny Access to wp-config.php and important friends:



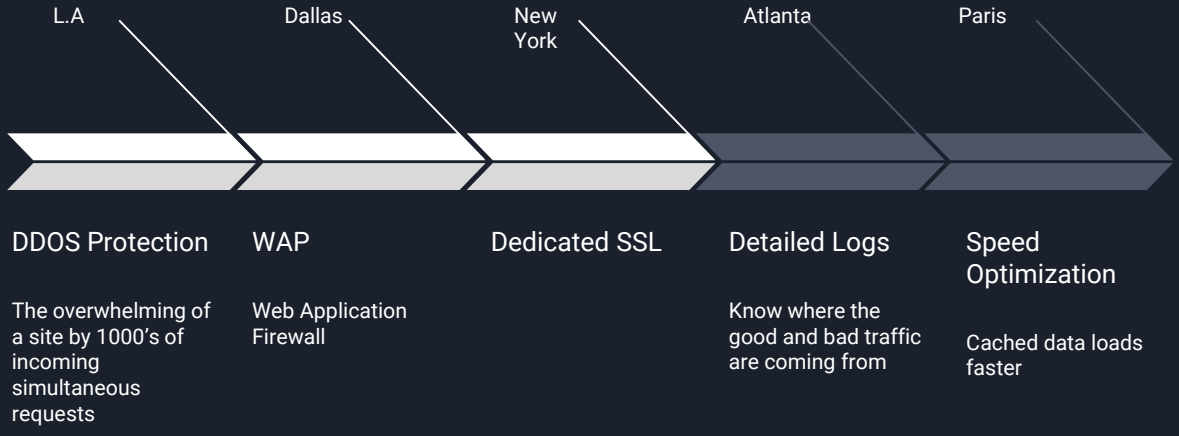
Move wp-config up 1 folder above root

Out of sight, out of mind



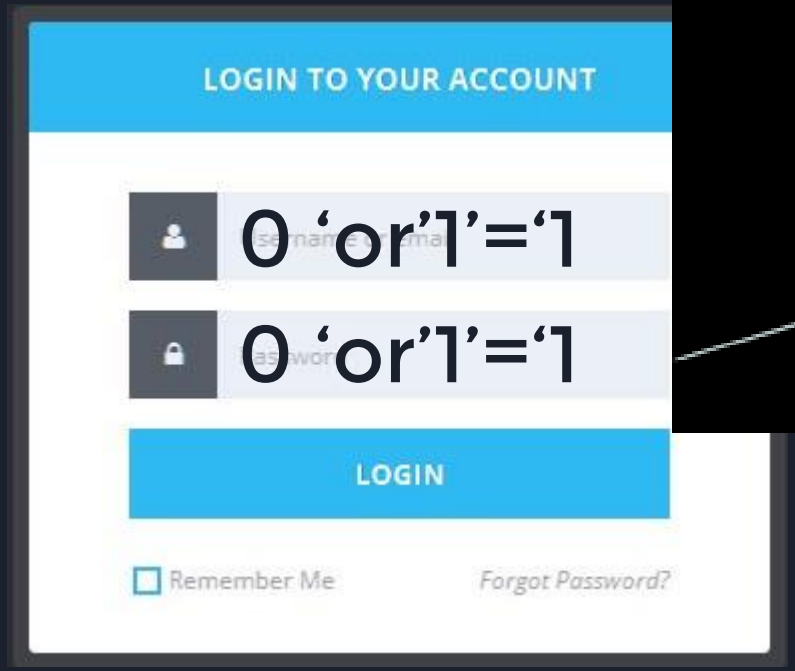
Set file permissions at 644 and 755 for folders.

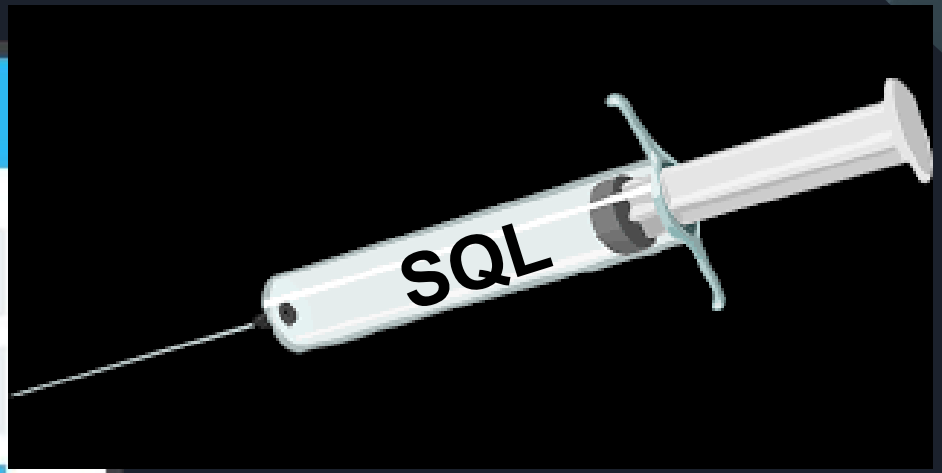
CDN



Content Delivery Network

SELECT * FROM Users WHERE UserId = 0 ‘OR’1’=‘1





SQL Injection

Cross Site Scripting XXS

- Client Side Code Injection Attack
- Attacker does not target a victim directly. Instead, an attacker would exploit a vulnerability within a website or web application that the victim would visit, essentially using the vulnerable website as a vehicle to deliver a malicious script to the victim’s browser.

WordPress Security – “Beyond The Plugins”

Steve Schwartz

AVT Marketing

Steve@AVTmarketing.com

704-288-5705