

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
- 
- A decorative graphic on the right side of the slide, consisting of a series of dark gray, 3D-style rectangular blocks arranged in a descending staircase pattern. Two blocks are highlighted: one in a light green color and one in a bright blue color, positioned at different levels of the staircase.

The stories you are about to hear
are mostly true...



Names have been changed to
protect the innocent.



Meet Mary



facebook





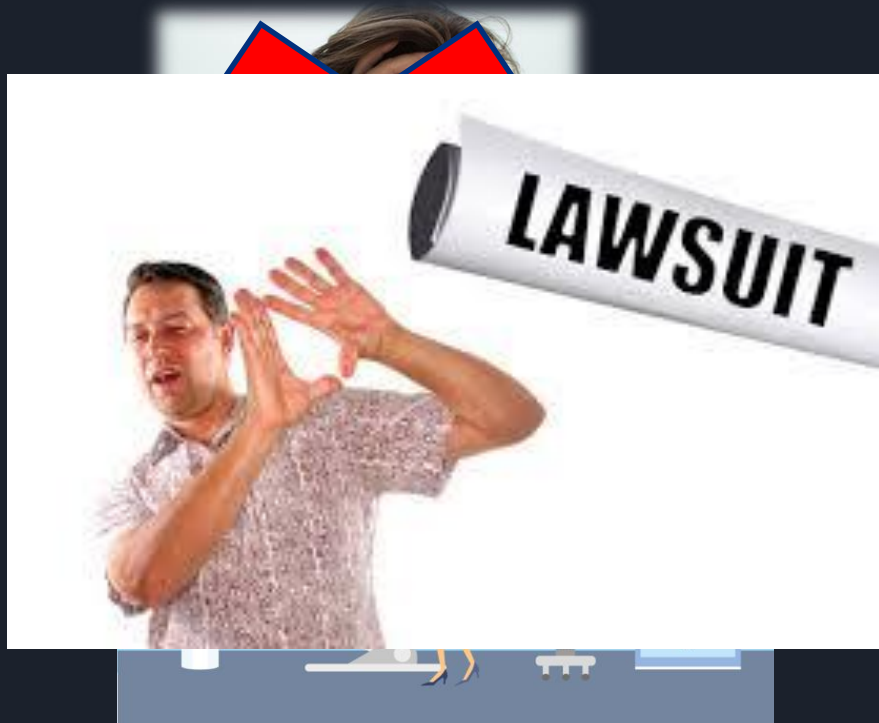
starbucks



starbucks1



So What Happened?



What The Hacker Saw

The image shows a Wireshark network traffic capture. The top pane displays a list of 27 packets. The bottom pane shows a detailed view of packet 27, which is an ICMPv6 Neighbor Solicitation message.

No.	Time	Source	Destination	Protocol	Length	Info
16	1.945988643	192.168.0.9	178.255.82.21	TCP	60	61556 → 2118 [ACK] Seq=1 Ack=2 Win=262144 Len=0
17	1.945995241	192.168.0.9	178.255.82.21	TCP	60	61556 → 2118 [FIN, ACK] Seq=1 Ack=2 Win=262144 Len=0
18	1.956626678	192.168.0.9	178.255.82.21	TCP	66	61557 → 2118 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8
19	1.991390741	178.255.82.21	192.168.0.9	TCP	60	2118 → 61556 [ACK] Seq=2 Ack=2 Win=29696 Len=0
20	2.001430634	178.255.82.21	192.168.0.9	TCP	66	2118 → 61557 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=
21	2.001461237	192.168.0.9	178.255.82.21	TCP	60	61557 → 2118 [ACK] Seq=1 Ack=1 Win=262144 Len=0
22	2.047866469	178.255.82.21	192.168.0.9	TCP	60	2118 → 61557 [FIN, ACK] Seq=1 Ack=1 Win=29696 Len=0
23	2.047877574	192.168.0.9	178.255.82.21	TCP	60	61557 → 2118 [ACK] Seq=1 Ack=2 Win=262144 Len=0
24	2.047878575	192.168.0.9	178.255.82.21	TCP	60	61557 → 2118 [FIN, ACK] Seq=1 Ack=2 Win=262144 Len=0
25	2.090958794	178.255.82.21	192.168.0.9	TCP	60	2118 → 61557 [ACK] Seq=2 Ack=2 Win=29696 Len=0
26	2.490393258	fe80::3e7a:8aff:feeb:a...	ff02::1	ICMPv6	110	Router Advertisement from 3c:7a:8a:eb:a1:27
27	2.601354843	fe80::3e7a:8aff:feeb:a...	ff02::1:ff33:7770	ICMPv6	86	Neighbor Solicitation for ::21d:d0ff:fe33:7770 from 3c:

▶ Frame 28: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▶ Ethernet II, Src: Vmware_a9:94:29 (00:0c:29:a9:94:29), Dst: ArrisGro_eb:a1:27 (3c:7a:8a:eb:a1:27)
▶ Internet Protocol Version 4, Src: 192.168.0.18, Dst: 91.189.91.157
▶ User Datagram Protocol, Src Port: 33933, Dst Port: 123
▶ Network Time Protocol (NTP Version 4, client)

```
0000  3c 7a 8a eb a1 27 00 0c 29 a9 94 29 08 00 45 10  <...'. .)..E.
0010  00 4c 59 e5 40 00 40 11 68 97 c0 a8 00 12 5b bd  .LY.@. h....[.
0020  5b 9d 84 8d 00 7b 00 38 38 3b 23 00 00 00 00 00  [...{.8 #;.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0050  00 00 dd 59 54 50 2f 26 46 55  ...YTP/& FU
```




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);
```

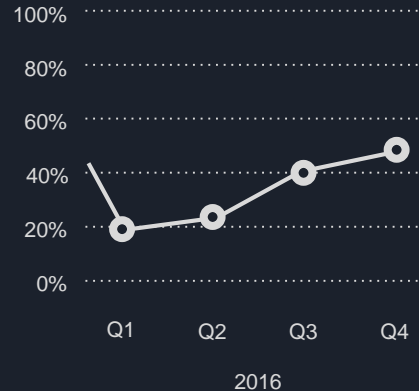
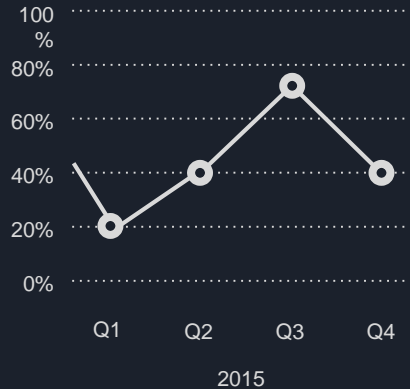
```
define('FORCE_SSL_ADMIN', true);
```





Meet Thrifty Theo

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



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)

Best 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 websites⁵⁰

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

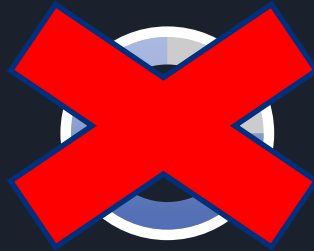
Dedicated resources

Free SSL Certificate

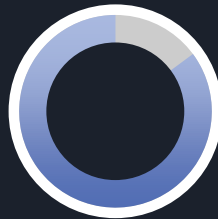
VPS / Dedicated / WP Managed

Every Host Nowadays has tiered options to choose from.

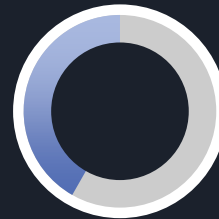
DON'T Choose Shared for your business or your clients



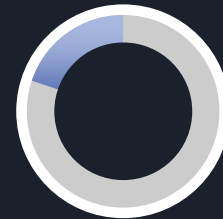
Shared



Managed



VPS



Dedicated



http://www.whatsmyip.org/



Community Ce... Awesome Screensho... Dave Ramsey Radio ... Gmail Hotmail eBay FedEx | Track UPS Package Tracking Kill That Debt.org | ... CCIE Vo



Your IP Address is 207.119.43.248

Network Troubleshooting Data capture, forensic analysis & intrusion detection on one platform www.Niksun.com

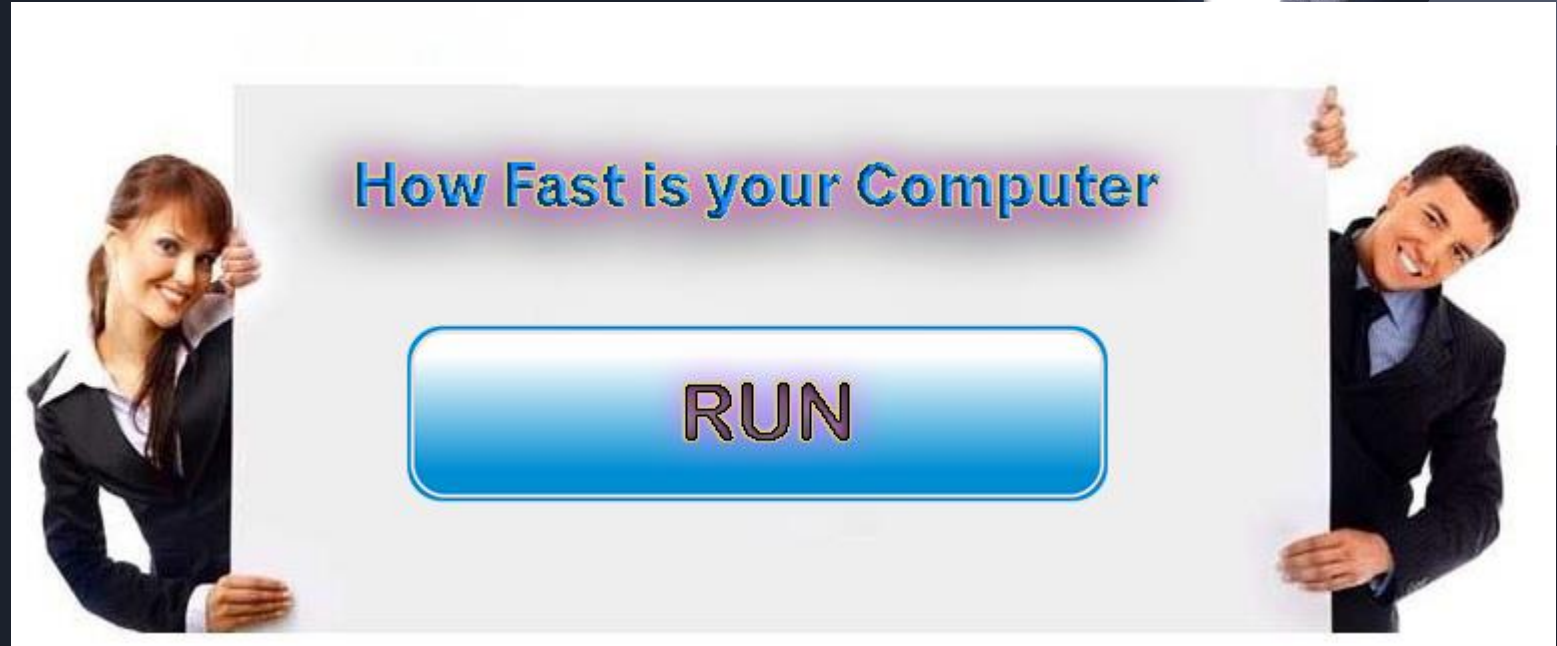
Springfield Coupons 1 ridiculously huge coupon a day. Like doing Springfield at 90% off! www.Groupon.com/Spr



Ads by Google

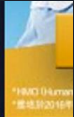
PLEASE do not use *automated* software or scripts to load this site
This site is for Humans, smart Primates & Dolphins only (oh and aliens)

Gullible Gary





外毀

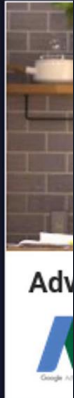


Connecting

OppoBox LLC
104.207.83.25



CSL
Kwai Chung



url: KKAQh*E05BME06G*WOC*GW*kuB*Y1E*P1*7*W*F*LLG*it*DYOX*mmati*8/20*hu*8*utw*compaign_*Cinile_*0/20/HMOX/20201894

RAT

You've Been



RATted

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

Phone Calls

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



In Person

Hacker pretends to be someone he is not

Other

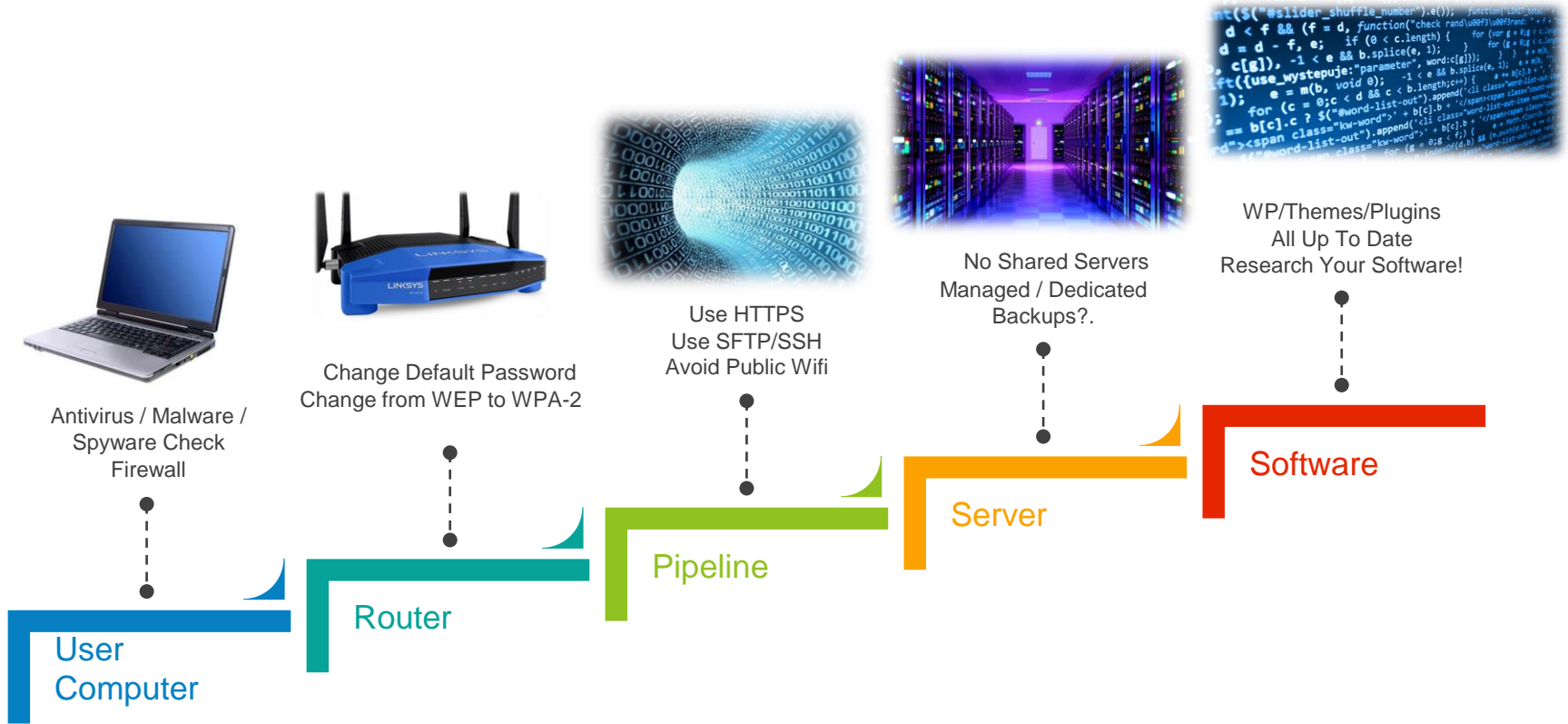
USB / Freeware offers / Free Games /



I love fixing hacked sites on holidays!

Said NO ONE ... EVER!

Educate Your Clients On Security From Their Fingertips to the Server





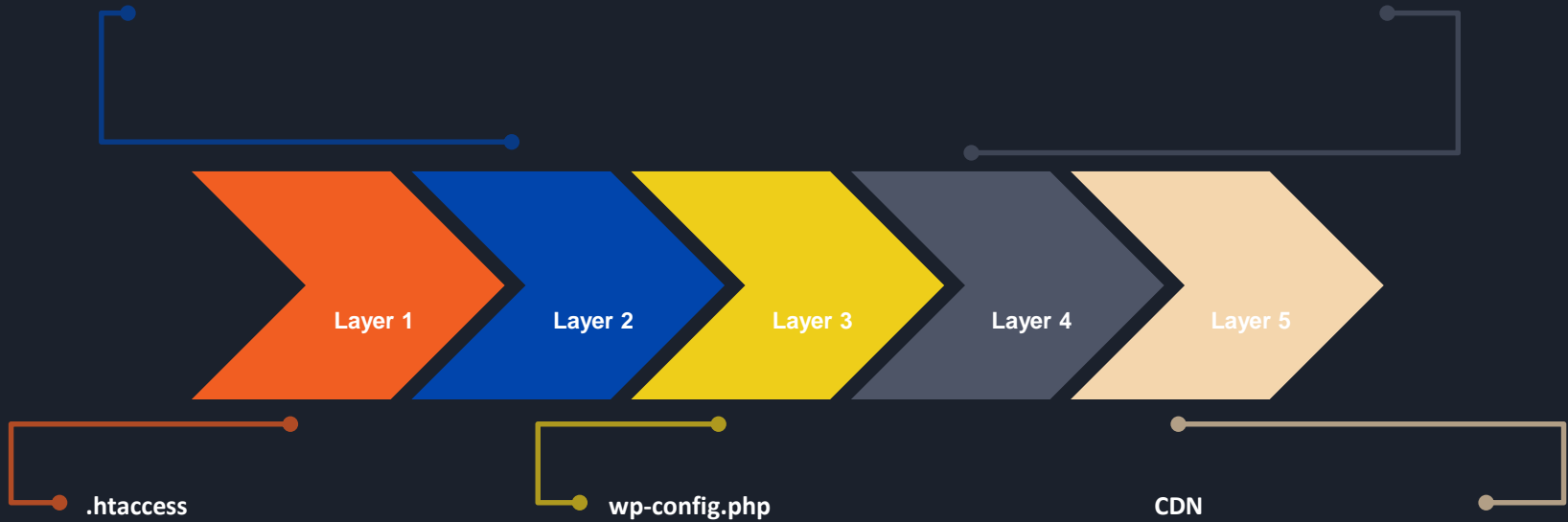
A Nod to Plugins

A Brute Force Attack Plugin –
Such as WordFence

A Backup Plugin –
Such as BackupBuddy



BEYOND: Hardening WordPress



Server Software

php7



THE
APACHE[®]
SOFTWARE FOUNDATION

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');
```

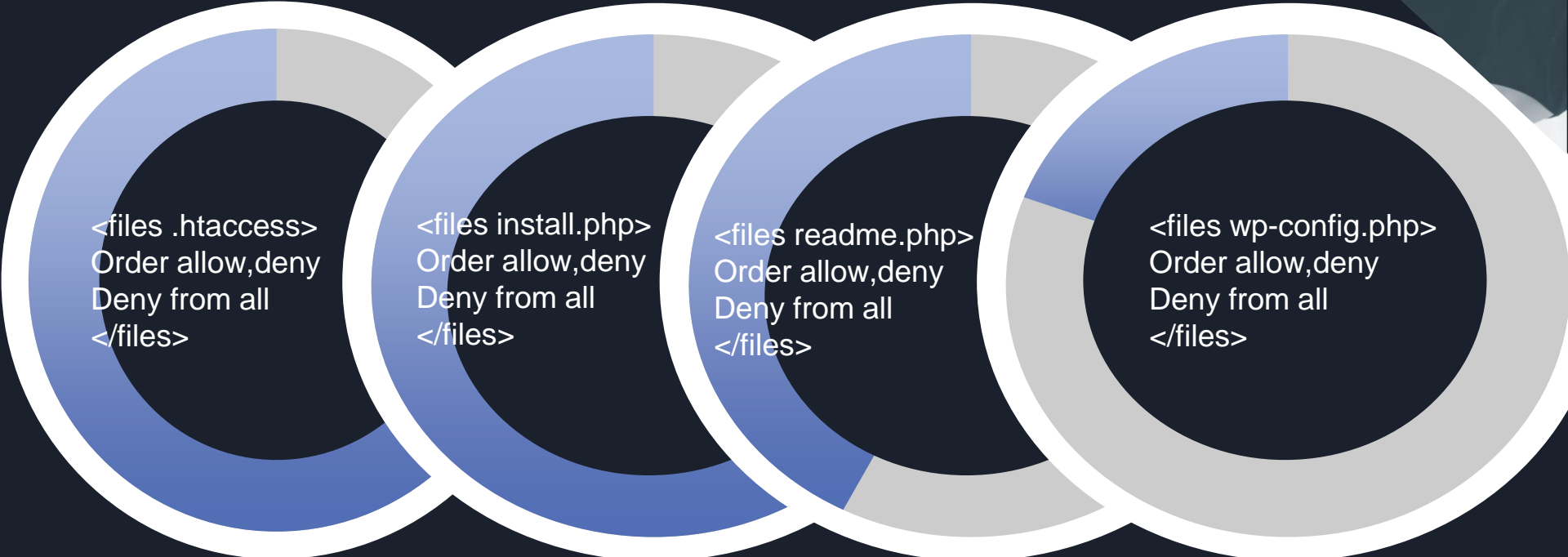
```
define('AUTH_KEY', '*@9?)my;-f>}PX]d*z1h0uyee1j|]]W*kjh$}FpKmM-r8jC}S`j4Sq4khU}8O.`);  
define('SECURE_AUTH_KEY', 'xUR:ph.ndpz+_M(&skfA,u63@.qt2A!5rT=iG6m1pn.B)w-  
*+kX!c4M]u(`.W$7z'); define('LOGGED_IN_KEY', '(+IEG|cay>H[N-g=RA3,C0i$0CM)V?1  
Cm,KB=W8Bv*dFZ-A2yBw%BM}Kf:{:bm}'); define('NONCE_KEY', 'r)w5~WA|{=r+fJ02ei>IToW7j-  
OeO!T~FO #Mf5pkYc*TX@&U%~RiCL:t&3;<ePS'); define('AUTH_SALT', ' 006c>Ht1Fs-.bjA-  
es0Pv0PoIlC***HT!aV+|#4q,i:Pg1c+qGF2FwRpqoC eF0'); define('SECURE_AUTH_SALT',  
'UyR(:vRo=-SG-yjF92t#`p)Rx|8IQJ7_V1)HrRMt4DcNM0UB@r9?RzOiU(=5HU &');  
define('LOGGED_IN_SALT', 'ix|#E-qTj+x%&0*ArU$W*~@~wvcuR?wA!#/#17`Pd_Z$-SJ vj8rl]w:&5/G&-  
HhgJ'); define('NONCE_SALT', 'I)VWFg+$v.3o=P*rH,Tt~Mc 4YW^BP9oX-r.Z.y}>}r];jWN1W43g4kdje  
&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:



```
<files .htaccess>  
Order allow,deny  
Deny from all  
</files>
```

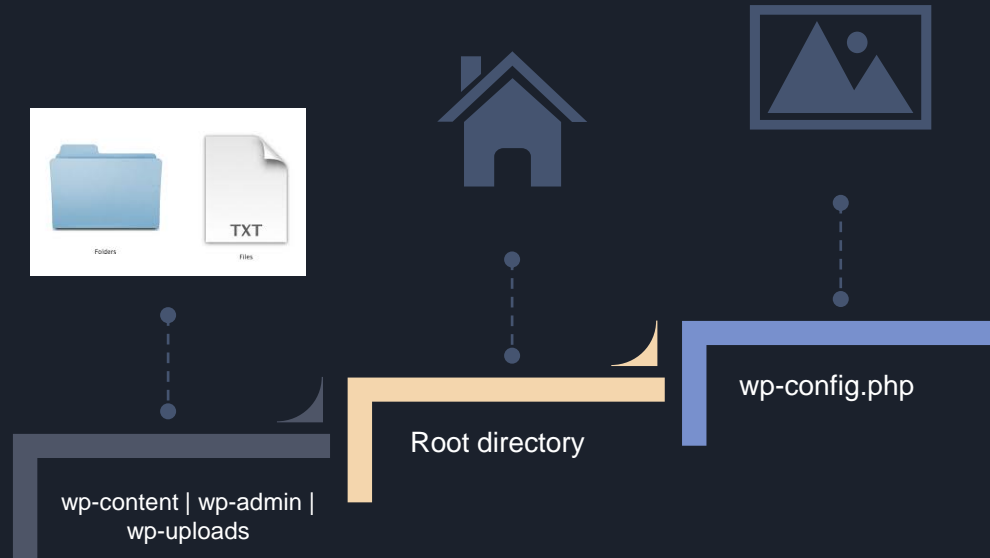
```
<files install.php>  
Order allow,deny  
Deny from all  
</files>
```

```
<files readme.php>  
Order allow,deny  
Deny from all  
</files>
```

```
<files wp-config.php>  
Order allow,deny  
Deny from all  
</files>
```

Move wp-config up 1 folder above root

Out of sight, out of mind



Set file permissions at 644 and 755 for folders.



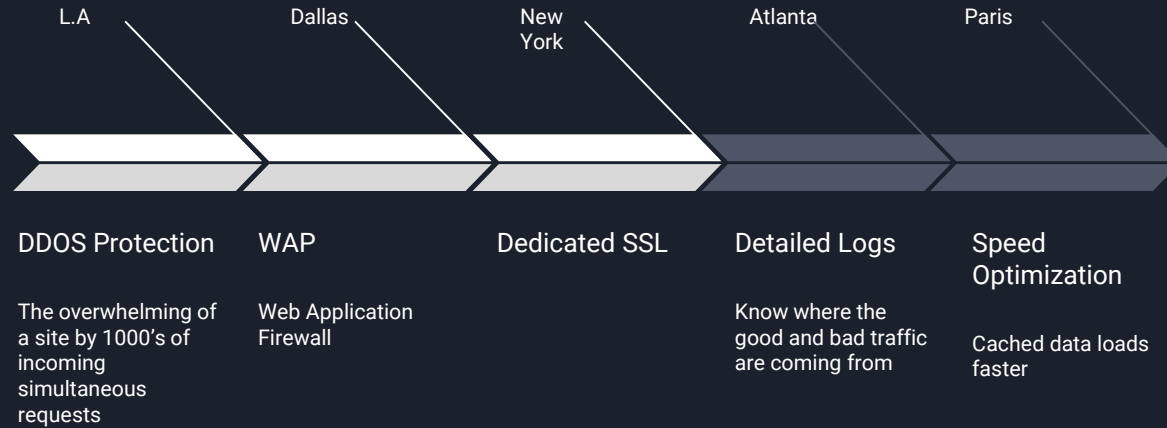
Folders



files



CDN



Content Delivery Network

`SELECT * FROM Users WHERE UserId = 0 'OR' 1='1`

LOGIN TO YOUR ACCOUNT

LOGIN

Remember Me [Forgot Password?](#)



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

