Content Urgent Care

TICKER CONTENT (just the recent WordPress hack feeds, find a up to date site):

WP prior to 5.2.3 allows XSS in post previews by authenticated users.

In 2018 90% of Content Management Systems hacked were WordPress.

WordPress before 5.2.3 has an issue with URL sanitization in wp\_kses\_bad\_protocol\_once in wp-includes/kses.php that can lead to cross-site scripting (XSS) attacks.

50% of hacked WordPress sites in 2018 were due to outdated software, themes and plug-ins.

WordPress before 5.2.3 allows reflected XSS in the dashboard.

50% of WordPress vulnerabilities are related to plug-ins.

In WordPress before 5.2.3, validation and sanitization of a URL in wp\_validate\_redirect in wp-includes/pluggable.php could lead to an open redirect.

84% of all security vulnerabilities are the result of cross-site scripting or XSS attacks.

WordPress before 5.2.3 allows XSS in shortcode previews.

39% of WordPress Vulnerabilities are because of cross-site scripting (XSS).

WordPress before 5.2.3 allows XSS in stored comments.

11% of attacks are caused by WordPress themes.

WordPress before 5.2.3 allows XSS in media uploads because wp\_ajax\_upload\_attachment is mishandled.

44% of WordPress hacking was caused by outdated WordPress sites.

WordPress before 5.1.1 does not properly filter comment content, leading to Remote Code Execution by unauthenticated users in a default configuration.

CAROUSEL: already updated

Slide 1

Slide 2

Slide 3

Slide 4

INFO SECTIONS:

Info1:

Header: URGENT ALERT

Content: Roughly 90% of all Content Management Systems (CMS) that were hacked in 2018 were WordPress sites. Hackers gained access to most of the sites through vulnerabilities in themes and plug-ins, lack of proper configuration, and poor website maintenance by webmasters. Over 50% of sites that were hacked, were due to outdated core software, themes and plug-ins. Are your themes, plug-ins and WordPress core software up to date? Find out now, before it is too late.

Info2

Header: E-COMMERCE ATTACKS

Content: Hackers use and deploy backdoor vulnerabilities to gain access to sites and use the site to deploy additional malware operations. Once a site is infected, the site will either redirect users to a spam-specific pages or unwanted content. Often this will include injected content on popular industry sites such as fashion and entertainment with the goal of monetizing on affiliate marketing. Often the

EMERGENCY ROOM:

Is your WordPress site currently down? Do you believe your site may be affected by a virus, vulnerability or under attack from a hacker? Does your organization want to know how secure your site currently is? Choose the option below that is most fitting, fill out the form with the required information and we will perform an assessment on your site and contact you with a path forward.

EXTENDED CARE:

After your initial assessment, review and if necessary, recovery of your site, you can choose an Extended Care program that fits your company or organizations needs to help prevent malicious attacks on your site. We offer security assessments and provide preventative measures to thwart future attacks. Select an option below for more information or speak with one of our expert advisors.

FOOTER:

For alerts and updates, be sure to follow WordPress Urgent Care on your choice of social media:

Powerpoint?

Non formal at this point, informational Q&A

If face to face- collateral

Leave behinds, slide decks

If into more formal arrangement for sales

What is your elevator pitch for this client? 2 minutes quick fire to explain your product

Ways to promote

Less time with sales, more click to buy the better

Online white label

Wpbuffs.com security white label and partnerships

Depending on development time, white label it initially and build on it while ramping up on it.

Run a package to increase price point, white label products, intel,

White labels package and deliver product and reach out in extenuating circumstance

Example white label 50 + intel and review 25 + markup for services +25

Be pitch ready:

Company name, value of service, how is delivered, how do you let client sleep at night

Nobody like to pay, everyone needs

Security is about mitigation, not about paying fines. Pay for security reduce the damages

Strategy, go to market

Who are, what provides, what solution?

Show the customer what out there and how it can hurt them

10 recommended and only spending 3%

What is your advantage over competition? People, Subject Matter Experts, tech

Some people are numbers, some are story, what type of person are you dealing with.

With your pitch, address the pain point. That’s when they buy. (compliance, retailer losing money, WP is lifeblood and getting spammed accounts) What’s keeping you up at night

Reinforce solution with data and facts credible sources.

Gardner, web content management, magic quadrant

Niche, vision, challenge, leaders

Automatic or WordPress if a challenger

Key points, not me telling you, it’s the top analysts, use credible source industry leaders.

Reverse engineer gardner and businesses to see how they work. “According to Gardner…”

Analysts, only, don’t use competitor.

OWASP

Sponsor and partnerships with data leaders in the industry

Sponsor OWASP meetings, and associate with them

Were asking design studios if they offer security, to prevent client compromise

What happens if client hacked

Do they handle it

Outsource

Customers on their own or we handle it in house

What is the market going to sustain in regard to price.

Consumer market

Business to business partnership or alliances

Less money more clients

Intentions at start?

Initially, hands on, over time develop tools. Use white label, resale, as develop tools. Tools to automate, setup on maint contract.

Fix and maintain or just care per incident

Depends on customer, small vs large companies.

75-85 per hour for initial

Proactive assets 150

Recovery 85-125 ball park

Hacked site full bore 350

Avg incident 60-80 hours

Propose monthly fee flat rate based on services offered

Avg contract with client monitoring 3yr discounted

Sm company 250K a year to large 1.5 mill a year

Resell our services, maybe use credits for multiple hosted sites

Netcraft or netnames taking down malicious domains, legal contracted they will use “credit or coins” to give client to give them times they can use the service.

Don’t overlook opportunity for education, certification, training. WordPress Urgent Care training class?

WordPress security experts class, WordPress user class, WordPress, admin class.

WordPress certifications? Two day curriculum for $3500 to be certified.