Addendum: Site Security

Transcript of Report from Kenny Purdie, IT Security Consultant and Ex Resident on Pound Hill.

Good Evening David,

Firstly, my apologies for taking so long to get back to you.

With regards the overall security of the site, I have to say I do not specialise in Website security but there are a few things I can call out here from what you have provided. Firstly, there is a legal requirement to protect any Personally Identifiable Information supplied by either contributors or users of your website; this is probably your primary concern when discussing with the PCC who I believe have their own Data Protection Officer nominated who should support this position.

DM: I need to make the PCC aware of the issue; I am sure they have this in hand anyway.

Secondly, where you have fee paying members you will no doubt be processing their financial information; hopefully you will be achieving this through leveraging the security available through your payment scheme provider, however if the website is saving any payment details in itself, I would urge you to modify the design to ensure the burden for protecting financial information remains with the service provider.

DM: Yes, all financial data is kept off site by the payment suite (Woo Commerce). This is one of the reasons for my recommending this payment route. Woo Commerce (through their app) take all the pressure off the site managers to process and store such data.

In terms of general security and from your original mail I quote: -

'My vision is to have a secure site, with separate access by users (both free and paid for) by editors to control the content, membership secretary to control the members and social media, and administrators(s) to control the site.'

This logical separation of duties is known as a Role Based Access Control model and is an excellent model to deploy. However, it does come with a management overhead in terms of people forgetting passwords and needing them reset. I mean this in terms of the people who are administering the site rather than your users or paid members which we will cover later. The concept of separation of duties enable those administrators to have more than one function; for example where you have an editor who requires a password reset, you could enable both an administrator and the membership secretary to approve the reset request. Having two people make a joint decision prevents anyone fraudulently escalating their privilege, however I am not sure that this is a risk you are really carrying in such a small group of admins, rather you would most likely rely on the ethics of those volunteering to support the site, but it is worth bearing in mind as the site transitions to another team. It would also be a step in the direction of answering the question raised by the PCC 'who polices the police' although I have always preferred 'Quis custodiet ipsos custodes?' myself.

DM: Worth bearing in mind if, for instance, we went for a fully managed multi-editor solution which is at least possible but not in the current plan.

I am also assuming that your users and members have an automated mechanism by which they can request a password reset again leveraging your service provider (WordPress in this instance) functionality? Assuming there is an automated mechanism by which to reset a password, you could consider making this available to all users regardless of role; this is

Addendum: Site Security

slightly less secure but again weighed against the burden of management versus the sensitivity of the information available will be a business decision.

DM: This is part of the Ultimate Member (UM) suite. In addition, individual members can see their own stored data at any stage by looking at their Membership pages. It is available to all roles that are logged into (ie admissible to) the site.

You may also find that you have the ability to enforce what is known as 'password complexity' e.g. a certain length of password which must contain a mix of letters, numbers, upper and lower case and special characters; I would counsel against this as it generally leads to users being forced to create a password which they subsequently forget, increasing any management overhead with password resets (assuming there is any in this group). Additionally I would counsel against enforcing password resets after a given period of time. The latest guidance on passwords from the National Cyber Security Centre is to use 3 random words (google NCSC 3 random words). Research has shown this to be easier for users to remember and results in less password reset requests.

DM: This is useful information, Kenny. UM allows options for passwords to be set by the administrator including many of the ones that you mention.

With regards the assertion that 'not everything behind a paywall cannot be found by a search engine' I would be tempted to test this against your own site by doing a search from a popular search engine for a piece of data very specific to your site; you will probably find the search engine will not find it.

DM: I think this double negative could be restated: everything behind a paywall can be found by a search engine.

As you say, this should not be possible.

I have done some testing, last summer, using our search feature and having tweaked some settings, I am now sure that the site is secure. The Search Feature is currently disabled for non-logged in users.

The issue here is that as far as our Pages are concerned, individual Pages need to be secured appropriately, not simply the menu that finds them.

Newspapers have different paywalls which let searchers view a subset of available information in the hope it will generate the sale of a subscription. Standard search engines cannot access data which is hidden in an access controlled area; otherwise all sorts of government information which partially be available for reading on the internet, rather than just that information we wish to be published and even where information is published it is still possible to secure an area with access controls. Google is not as powerful as some of the PCC seem to think. As a counter to this argument however, it is probably best to test against a unique image also; whilst the search engine should not be able to see anything within a partitioned area, images can occasionally behave slightly differently to other pieces of data due to the meta data which can be attached to them e.g. it might look like it comes from your site but the meta data could actually tell you that the image is available somewhere else on the internet, should you decide to decode it and find out.

DM: As you say, 'images' are different, without a secure setting per image, so their access can only normally be controlled via a call from an appropriately secure Page.

I have not yet explored the meta data per image options. WIP.

Note for all; Images are managed in the Media Library in WordPress along with documents and videos.

Addendum: Site Security

I am not really privy to the security functions within WordPress but the last control I would mention is Data Loss Prevention tools; these could be adopted to notify you if and when an authorised users access data or images and copies them outside of the website. This is where you are most at risk of breaching the confidence of someone who has submitted data and wishes it to remain within the site only. Again, not being ofay with the software and subscription you are using I cannot really provide any more detailed advice without a lot of further research which due to work commitments I just cannot do at the moment.

DM: I interpret this as akin to data protection tools to protect the copyright of images. Plug-ins are available to do this and I would like to consider these along with your point raised here regarding the data protection of submission providers, myself included. WIP.

In closing, I would support your thinking on the PCC embracing the opportunity to manage this resource and the attendant security presented by the current design; it is clear a lot of thought has gone into the structure and its security thus far and I applaud your efforts to date. Unfortunately, whilst you may be able to lead a horse to water, to the best of my knowledge it is still a criminal offence to drown the animal despite its contemptuous behaviour.....

I hope this is helpful and apologise again it has taken so long for me to respond. If there is anything I can do in the future to support this or any other village initiative, I would be more than happy to help where time allows.

Wishing you good luck with your future meeting,

Kind regards,

Kenny

DM: I have asked some supplementary questions on security including, my concern about Ransome Ware demands to the site and whether or not our security arrangements were, in his view proportionate.