



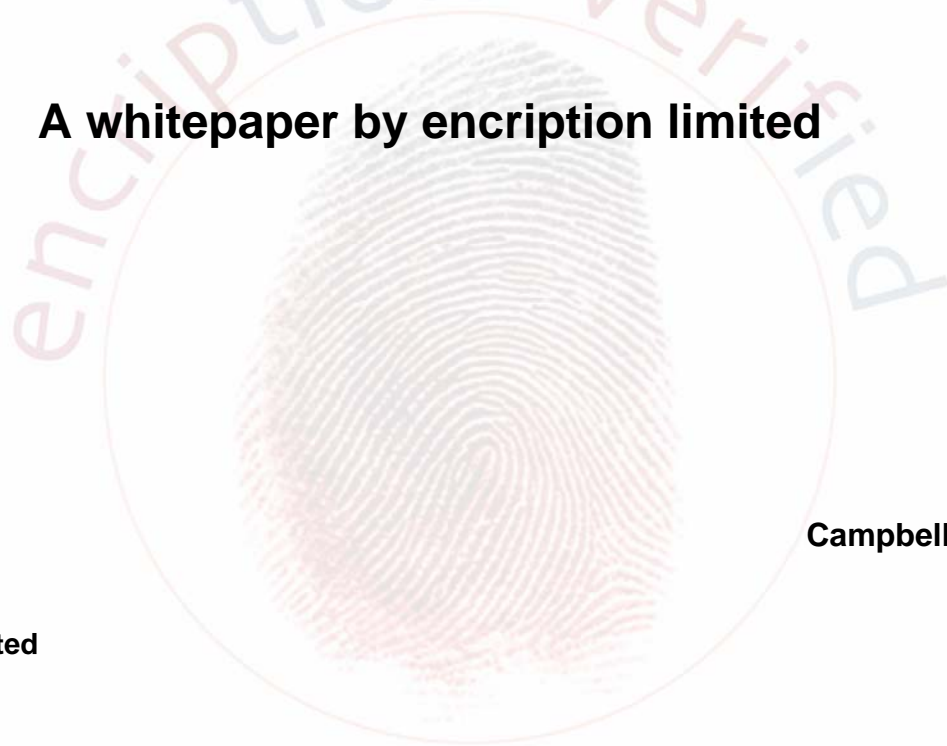
encription

ethical hacking services

www.encription.co.uk

The need for secure web development

A whitepaper by encription limited



Campbell Murray

encription limited
The Stables
White Lodge
Bevere
Worcester
WR3 7RQ
www.encription.co.uk

The need for secure web development



Introduction

Having an interactive web site has become almost compulsory in business today. Gone are the days of the 'poster' or 'banner' website providing a description of what a company does and how to contact it. Even the governments of the world are piloting projects to encourage businesses to adopt online practices so they don't fall behind in a globally changing economy. And everyone knows you need a website, don't you? Today's websites increasingly form part of business management systems, from handling orders and enquiries to processing payroll and credit cards. To get your website seen by the search engines it is accepted that you must update the content regularly to keep it "fresh", hence content management systems, which allow you to interact with your website and change it, abound.

This is all well and good for business and your search engine rankings but how well has the web site been written? Is it fast? Has it been developed to recognized standards? Web programming languages and database technologies have never been easier to learn and use, bespoke solutions can be created quickly and cost effectively, but cost is still the greatest discussion point regardless of the business sector.

It's not easy for the web development companies, and the issues they face are multiple. It is a cut throat [read 'buyers'] market with often as many as a dozen agencies tendering for the same job at any given time. The proliferation of web developers is in part due to supply and demand, but also largely down to the ease with which a web application can be created, it is not difficult.

In their effort to win contracts the focus of web developers is naturally drawn towards design, budget, return on investment and time scales. Compound this with a lack of security awareness in the web development sector and it is hardly surprising that according to *Gartner Group*:

"75 percent of security breaches now occur at the application level, and 3 out of 4 business websites are vulnerable to attack".

This document intends to highlight why and how application developers across all industry sectors should be reviewing their production and training processes in order to place an emphasis on security at the design stage.

Legislation surrounding web sites is changing at a rapid pace to include accessibility and privacy law, whilst web design agencies are doing a great job in keeping abreast of these and other developments, they fail to even consider the security of the web site or software application.

A good web site can give a high return on investment (ROI) making it appear very cost effective. It may also be well marketed and easy to use, but if an attacker can change the price on all your items, deface your website with unsavoury material and/or take it out of action altogether, then you could see not only a downturn in online sales and lead generation, you may turn customers away from you altogether and suffer considerable financial losses. Restoring damage to your reputation is far more difficult than repairing a defaced web site; it is often impossible.



The need for secure web development



What's it all about?

To build and deploy secure web applications, you need to create 'hacker resistant' code and business logic into the development environment. Quality in the staging environment needs to be thoroughly tested; security and compliance should be enforced through internal and external audits. In order to do this you have to have an understanding of what attacks are commonly leveled at web applications and how they work, this is where web design and development agencies are currently lacking. Furthermore it will push the price of the final product up and that is why this industry change has been resisted for so long.

More serious threats are ignored

Many systems administrators are quite clued up on security issues these days, and the advent of secure automatic software updates for the vast range of generic operating systems and software is taken for granted. Little is done to protect against the more serious technical attacks, including hacking.

You can be given a false sense of security

On the other hand security systems such as firewall log analysis using IDS [Intrusion Detection System] can, and will, give a false sense of security to the Systems Administrators, because all too often they do not examine what is happening at the HTTP [Hyper Text Transfer Protocol] or web layer; the web site.

More functionality means more threats

As a result of the development of server technologies web applications can now interact with a server operating system like never before. You can upload or download files, create, modify or delete entries in databases, read files off the hard drive, even generate on demand files such as PDF's and executables (.exe). However with this level of control a web application, without proper user security administration, can expose not only the web site, but also the server it resides on, to the danger of attack and being compromised. With servers becoming more secure, the web application itself is now a far softer target for the attacker.



Common web application attacks

Exploiting input areas

By far the most common error made by web developers surrounds input validation. That is anywhere on a web site where the user, or visitor, inputs information. This doesn't necessarily have to be via a form, it can be through the URL [Uniform Resource Locator] i.e. the website address which you may see in the address bar of your web browser. By inputting special characters into these areas the attacker may be able to modify content on your page, access restricted areas which you thought were password protected, modify the server logs and even redirect visitors to other websites, including their own. The two most common injection attacks are SQL [Structured Query Language] injection and XSS [Cross Site Scripting].

Exploiting SQL code

SQL is the language of all common databases and it is this which allows the use of content management systems. If the web developer does not filter out this language from web input, then your database can be modified. If the developer allows his web application to connect to the database with high privileges then the database may be deleted altogether.

Cross site scripting

XSS [Cross Site Scripting] is again an injection technique but this time using a different language altogether. Take the scenario where you permit your site visitors to create their own profiles for other visitors to see. This may be a blog or a client area on your site. The web design agency's marketing specialists will probably see this is an opportunity to encourage visitors to come back often and to update their profiles. This will add value to the site and your search engine rankings. However if this type of input is not validated and stripped of certain special characters, then the attacker can use it to redirect visitors to another website altogether, often their own. If your site is an online store where orders are taken and credit cards processed, the attacker could redirect your visitors to a clone of your shop, processing the transactions into his own bank account. The first you may know is when customers ring to ask where their order is. You will be even more surprised when you find that the order was not placed on your website!

XSS can also be achieved as a result of SQL injection if your website reads its content out of a database.

Always validate at server level

Input validation has to occur at the web server level. Client side, i.e. via your web browser, validation of your input is easily defeated by the average attacker. Server side validation of input must be used at all times.



The need for secure web development



Think about file names

Not only is the web application at risk of compromise from insufficient input validation, the database itself is at risk. Web developers may be great designers but they are largely unimaginative when it comes to naming conventions and passwords. A content management system in a folder called 'admin' on the same web URL will be easily found. If predictable passwords are used then it's game over for your website.

Cheap can be expensive

Furthermore in the cost cutting culture of web design cheap to implement database technologies such as Access are commonplace. If the path to the database is predictable then the attacker may easily download the file and read all content.

Think about passwords

Passwords should be strong, at least 8 characters in length and contain a mixture of upper and lower case letter with some numbers too. But if the database is obtained then no matter how strong the password is it will be no barrier to the attacker if they can read it straight out of the file. Passwords should be hashed [encrypted] at all times.

Drop the commentary

Other common mistakes include leaving critical information regarding the structure of the website hidden within the pages of the website itself. These are called HTML comments and are identified by the <!--and --> delimiters in HTML [Hypertext Markup Language, the defacto language of all web browsers]. Next time you visit a web page view the 'page source'. You will almost certainly see that there is a lot more to the web page than meets the eye with often lines of code hidden from the visitor but easily read by the attacker.

Watch out for cookies

Session and Cookie management within applications is an area of security which is without fail left to the web server itself, but common information hijacking techniques abound. Vulnerability in this area can lead to sites and your visitor's confidentiality being compromised.

These are just a few of the most common vulnerabilities unwittingly built into web applications by web design agencies and developers.



The need for secure web development



What is the solution?

I'm not a target so I am OK!

Security sounds expensive doesn't it? All that extra effort to protect your investment when you may not see yourself as a target any way. You haven't been attacked yet so why should you be worried? Well there are two very strong arguments for adopting security best practice in web development.

Hacking is a hobby for some

Firstly you are a target, there are no two ways about it. The increase in online hacking activity in the last four years has drawn me to coin the term 'recreational hacker'. Allow me to elucidate. In the late 1980's there were perhaps 20 hacking tools. Today estimates set them at over 100,000; the majority are free to download and require little technical knowledge to use. Marry this with the exponential growth of global internet access and you have a new breed of hacker, the hobbyist.

Your search rankings make you a target

Now consider the fact that large organisations and public sector bodies, whether they have been attacked or not, have done something about their web site security, you are left with a global network of recreational hackers just looking for a target to compromise. Of course with the excellent marketing and search engine optimisation your web design agency provided you with everyone can find you online. Now how long do you think you have before your next?

Web sites need to be written differently

Security practices can in fact save time and money if they are implemented correctly. To prevent input injection obviously we have to adopt a different approach to writing our website code. It may mean a little more effort, but to prevent against XSS and SQL injection it is essential.

Planning for security has hidden benefits

On the other hand creating an effective and detailed threat model from your application design will enable the developers to complete the build of the web application in a shorter time than before and particularly save time in quality assurance and staging, since the testing will be focused where it is needed. You will then be able to spend more time testing the site to ensure that it is really secure and performs as you want it to.

A grasp of the principles of least privilege will also empower the web developer to write smarter business logic speeding the development time without compromising security.



The need for secure web development



Conclusions

Web sites and staff are the most insecure part of any system and the main target for hackers. People can be trained, web sites can be developed more securely, the fact that they are not, is often due to ignorance on the part of the web developer and the pressure to deliver a web site quickly within a specific budget.

If a web site is developed securely and to pre-defined standards, then the time taken for development, and risk of attack, will reduce. Showing web site visitors that a site has been written securely and is regularly tested to make sure that it remains secure, will give them confidence in the company owning the web site the web site itself. Visits to the site should increase and with it the business it transacts.

Developing a secure web site is easy when you know how, it just requires the knowledge and the application of that knowledge in a disciplined way.

Selling the fact that a web site could cost more should not be difficult, when the client understands why, and can see that taking this approach will mean more revenue through the web site in the future, and a greatly reduced risk of attack, the business case becomes obvious.

It is very difficult to differentiate one web developer from another, the offerings are so similar. Including security as an integral part of the development is unusual and a great differentiator.

Not only do web developers need to start thinking about security, the purchaser has to start asking pertinent questions of any agency that approaches them, or they approach, to discuss the next great .com idea. .

IT security can be seen as a black art and an unnecessary expense, it is neither. So let's put IT security on the agenda.

I hope this paper has been useful and has at least made you think about your web site security.



The need for secure web development



ABOUT ENCRPTION LIMITED

encription limited is a UK based IT security company operating from a secure location in Worcestershire. From this central location we are able to deliver our services worldwide.

With highly experienced consultants at our disposal, encription limited is able to meet your IT security needs, no matter how simple or complex, including consultancy, penetration testing and staff training. All our consultants have extensive experience in IT security, forensic investigation and ethical hacking. We work to BS7799 (ISO27001) security standards and we are ISO 9001:2000 certified.

Our mission

Is to make IT systems and information, whether complex or not, more secure.

In doing so, we keep abreast of the latest IT security threats and work with appropriate organisations, professional bodies and the Police to develop and maintain IT security standards, defences and techniques that will reduce the risk of an attack on your IT systems. Our solutions are tailored to your specific needs, risk profile and budget.

Our Partners

We are commercial partners of the SMART governance network.

We are members of the National e-Crime prevention initiative steering committee.

We work closely with WARP groups nationwide.

We are working with the new public sector TIGER testing standards initiative.

We work with Police Crime Prevention Units providing training for crime reduction officers in IT security threats so that they can provide meaningful advice for business and the public alike.

We also collaborate with Police NHTCU's (National High Tech Crime Units).

Our Clients include

Building societies, professional service companies including solicitors, accountants, manufacturers, the public sector, Small to Medium Enterprises (SMEs).

About the author: Campbell Murray is the Technical Director of encription limited [www.encription.co.uk] and has many years experience in the building and penetration testing of web applications across a range of languages, server and database technologies.

LEGAL NOTICE

LIMITATION OF LIABILITY. THE AUTHOR WILL NOT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR PERSONAL INJURY, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS OR CONFIDENTIAL INFORMATION, LOSS OF PRIVACY, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE INFORMATION IN THIS DOCUMENT, EVEN IF THE AUTHOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Permission is hereby granted to freely distribute this document as long as it is not altered and the author is acknowledged.

