A Website on Web Application Security

University of Southampton, ECS, INFO2009 Academic Year 11-12

Group 13 (mixed): `'DROP TABLE groups;`

Keywords: Security, Web Development, Hacking, Passwords.

Resource: http://info2009.thomas-cairns.co.uk/

EdShare: http://www.edshare.soton.ac.uk/8199/

Left to Right: Sam Bull, Jordan Milton, Tom Cairns, Patrick Naish, Donglin Pu, Dan Palmer

Sam Bull: swb1g10@ecs.soton.ac.uk
Tom Cairns: tc14g10@ecs.soton.ac.uk
Jordan Milton: jksm1g10@ecs.soton.ac.uk
Patrick Naish: pn3g10@ecs.soton.ac.uk
Dan Palmer: djp3g10@ecs.soton.ac.uk
Donglin Pu: dp1e10@ecs.soton.ac.uk

Tutors: Richard A. Watson (raw); Klaus-Peter Zauner (kpz); Michael J. Butler (mjb); R. I. “Bob” Damper (rid)

Abstract

Security on the internet is becoming more and more of a concern as the internet becomes increasingly integral in our daily lives. If the security system of a website is not implemented correctly or thoroughly enough, personal and private details could be stolen, sensitive corporate information could be leaked, or the site or business could be sabotaged. As this is a serious concern, we created a website to act as an easy-to-use and informative resource for learning about how vulnerabilities and weaknesses can be exploited, some basic steps that can be taken to ensure that a website can be secured against the most common attacks, and how to find and secure other potential vulnerabilities in the website. Ultimately our resource is a starting point, but should convey the importance of internet security as well as setting users in the right direction when designing sites.

Introduction

Most people take internet security for granted, or are unaware of the risks of using the internet. They do not think twice about who signed the SSL certificate the site their user uses, or are not concerned about using a 6-letter all lowercase password. However, any system should be designed with the least proficient users in mind, and the internet is no exception. Developing and integrating security into websites is vastly important to ensure as many people as possible that they are not susceptible to risk. Unfortunately many websites are built by individuals who have no formal training or education in website security, or are simply unaware of the risks and exploits they are working into their product. To remedy this, we have created a website which educates about security issues, teaching why internet security is important, how hackers find and use exploits, how to fix said exploits and find others that need fixing, and other advice. The purpose of this website is to provide a solid, general base to work off of, and to point the user in the right direction to find more information.

Background

As an increasing number of people gain access to the internet, websites and our interaction with them become an ever more important aspect of daily life. This has led to an increase in the number of people with the ability to exploit security flaws in websites, and also makes them a more attractive target for illegal activity. As website owners have a legal and ethical responsibility to protect themselves and their users from illegal access to information, being able to create secure websites is a very important skill to have as a website developer. To be able to create a secure website however, it is also important to know the techniques employed by those trying to gain illegal access to a site.

Method

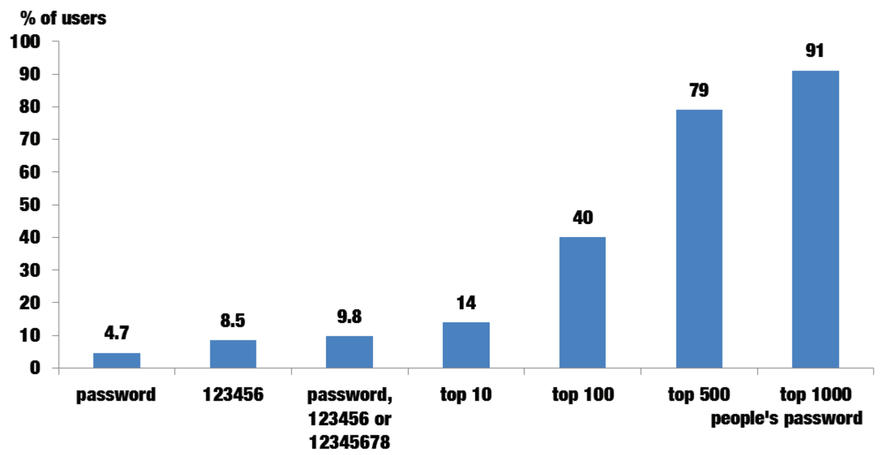
To create the artefact we first researched the different techniques and tactics that hackers will employ to gain access to information they are not legally allowed to have. Much of the information came from internet sources, but also from information learnt by mobile and secure systems students. This information formed the basis of our website aimed at teaching people how to block these attempts at illegal access to information on their sites or that of their users. We then researched the techniques employed by web site designers to protect themselves against these attacks, again through web sites and lecture slides. With this information we decided to lay out our website as a tutorial for creating a secure website while illustrating the risks of not keeping active content secure. We included sections where the reader can attempt common techniques employed by hackers to highlight how easy it is for unsecured or lazily secured sites to have information accessed illegally.

Discussion

Security is a growing issue, as more people than ever before are connected to the internet also the amount of people with the ability and motive to attempt to illegally access information is increasing. The site covers the importance of web site security, as well as looking at recent attacks highlighting the potential severity of problems caused by gaps in security and that as owners or administrators of a website you can’t be complacent.

Password Security

The first important issue is password security from the perspective of someone maintaining or creating a website. It is important to begin with to have secure administrator passwords to many systems including web application administrator page, database root password and database password for web application access. The site discusses these, and goes into more detail about their complexity and the responsibilities of those creating or maintaining a site. You also need to be secure in the way in which passwords are stored on your site, so that if someone manages to access the databases in some way they still can’t see the passwords. The most important thing is to not store the passwords themselves as plain text. The site looks into the different methods for securely storing the passwords and why secure storage of passwords is important. You need to also consider the ways in which a hacker will attempt to gain access to the password, the site looks into brute-force attacks and then includes an interactive page allowing them to test their own password for safety in the case of someone attempting to brute-force their password. Lastly with respect to password security, the site looks into alternative authentication methods.



Type of attacks

The site then discusses the two main types of attack on a site, Cross-Site Scripting and SQL injection. It is important to understand these attacks to aid your ability to defend your site against them. Cross-Site Scripting involves injecting malicious code into a web page that gives the attacker either heightened privileges on the user’s information, or redirects them to a malicious page that has the look of an authentic site. SQL injection is when the attacker ‘injects’ SQL commands into forms and gets the server to execute them, often with the intention of getting increased privileges, creating long term errors in a database or data loss. These are described in more detail with interactive examples allowing the user to see how the attack works, raising their awareness. It also discusses how to defend the site against these attacks.

Other security considerations and Security Checklist

The last section of our site looks at other security considerations, and specific advice for when the user creates or edits a website. We discuss what is HTTPS, what it means and why it is more secured. Then, becasue this system is based on trust, we discuss what security certificates you should trust and therefore which you should acquire for your site if you want to implement it. CAPTCHAs are also covered, explaining their use and good design practices. The site also covers how as a creator or maintainer, you would test your own system for security to make sure that you are not putting users at risk. For general security tips, the site covers three popular languages used to create languages and give advice specific to those languages as well as tips that are relevant for all site administrators.

Conclusion

By following the tutorial, the reader should have learnt a lot about security and have a good introduction to the issues surrounding it. They should also be able to use what they have learnt from this tutorial to create a secure site, and have a good understanding of the techniques employed and why they are important. While this is the case, we realise there are issues that we weren’t able to cover and our site should therefore be seen as a solid foundation to understanding security. If a reader is interested in security then we advise moving on to more advanced resources, of which there are an increasing amount as site security becomes more relevant to everyday life.

References

AWS, A. (n.d.), ‘Amazon ec2 instance types’.
URL: http://aws.amazon.com/ec2/instance-types/
Bevand, M. (2010), ‘Whitepixel breaks 28.6 billion password/sec’.
URL: http://blog.zorinaq.com/
Burnett, M. (2011), ‘More top worst passwords’.
URL: http://xato.net/security/passwords
Foundation, T. A. (2011), ‘Security tips’.
URL: http://httpd.apache.org/docs/2.0/misc/security_tips.html
Letzing, J. (2011), ‘Facebook flaw exposes its ceo’.
URL: http://online.wsj.com/article/SB10001424052970204083204577082732651078156.html?mod=googlenews_wsj
P, M. (2011), ‘How to update to metasploit 4 and use autopwn in backtrack 5’.
URL: http://greyhat-security.com/how-update-metasploit-4-and-use-autopwn-backtrack-5
PHP Developers (2011), ‘Php: Security - manual’.
URL: http://php.net/manual/en/security.php
Pullicino, J. (2011), ‘Preventing xss attacks’.
URL: http://www.acunetix.com/blog/web-security-zone/articles/preventing-xss-attacks/
Ristic, I. (2005), Apache Security, O’Reilly Media. Rodriguez Valderrama, J. (2011), ‘cool-php-captcha’.
URL: http://code.google.com/p/cool-php-captcha/
Shiflett, C. (2005), Essential PHP Security, O’Reilly Media.
Stuart, K. & Arthur, C. (2011), ‘Playstation network hack: why it took sony seven days to tell the world’.
URL: http://www.guardian.co.uk/technology/gamesblog/2011/apr/27/playstation-network-hack-sony