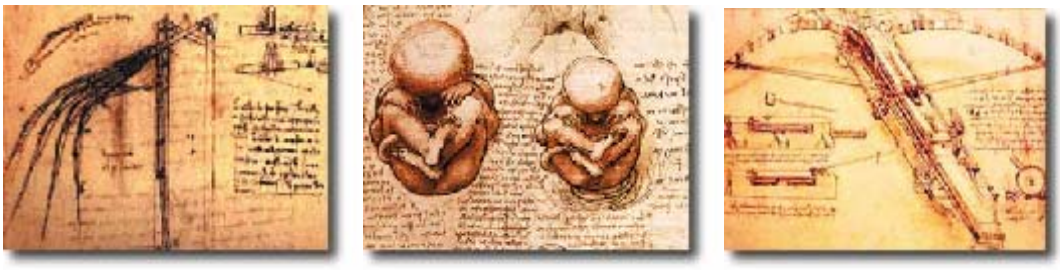
CORSAIRE

The natural choice for information security solutions



A Corsaire White Paper:
Cookie Path Best Practice

Author	Martin O'Neal
Document Reference	Cookie Path Best Practice.doc
Document Revision	V1.0 Released
Date	05 April 2004

Table of Contents

TABLE OF CONTENTS 2

1. INTRODUCTION 3

2. THE PROBLEM 3

3. THE SOLUTION 3

REFERENCES 3

ACKNOWLEDGEMENT 4

About The Author 4

About Corsaire 4

A Corsaire White Paper:
Cookie Path Best Practice

1. Introduction

Cookies provide a method for creating a stateful HTTP session and their recommended use is formally defined within RFC2965 and BCP44.

Although they are used for many purposes, they are often used to maintain a Session ID (SID), through which an individual user can be identified throughout their interaction with the site. For a site that requires authentication, this SID is typically passed to the user after they have authenticated and effectively maintains the authentication state. If an attacker can use a mechanism (such as sniffing or cross site scripting) to gain access to the SID, then potentially they can incorporate it within their own session to successfully assume the users identity.

The cookie specifications provide arguments for restricting the domain and path for which the user agent (browser) will supply the cookie. Both of these should be matched by the request before the user agent sends the cookie data to the server.

It is common for the path argument to be specified as the root of the origin server; a practise that can expose the application cookies to unnecessary additional scrutiny.

It is worth noting however, that whilst the various “same origin” security issues still afflict the browser vendors, the specification of the cookie path argument is somewhat of a moot point.

2. The Problem

The cookie standard is formally defined in RFC2965 [1]. This makes reference to the optional path argument that allows a cookie originator to specify “the subset of URLs on the origin server to which this cookie applies” [1].

The vast majority of web based applications simply set this argument to the root “/” of the origin server, either for simplicity or merely for lack of knowing any better. Where this oversight becomes useful is in conducting attacks against the session cookies of an application that does not suffer from any exploitable validation flaws, but that shares the same server environment with one that does.

As an example we shall imagine that a secure application shares a host with some sample files that were installed at the same time as the web server. Obviously, this would never happen in a live production environment (pauses to insert tongue firmly in cheek).

The secure application is located within the “/secure” folder but sets the cookie path argument to the root “/”. An attacker knows that the secure application has no useable vulnerabilities in itself. However, they also know that the sample files have an exploitable cross-site scripting (XSS) flaw that would give them access to the all-important session cookies. All they now need is a method to get a valid user to access the sample files (a completely different problem to solve).

The secure application vendor might have otherwise followed all the best practise recommendations when developing their application, but they could still be exposing sensitive information through the loosely specified path argument.

3. The Solution

Fortunately the solution to this issue is a straightforward one. By simply specifying the cookie path argument accurately, an application can take measures to protect itself from flawed products that share the same hosting environment.

References

[1] http://www.faqs.org/rfcs/rfc2965.html

Acknowledgement

This White Paper was written by Martin O'Neal, Technical Director of Corsaire.

About The Author

Martin O'Neal has spent a lifetime in the field of information technology. From an early start writing computer games during the home PC boom of the 1980's, he has been actively contributing to software development in a professional capacity for well over 20 years. He has gained a wide variety of skills across diverse platforms and system environments by working his way up through well-respected system integrators and consultancies. Having chosen to specialise in information security, Martin has spent the past 15 years working as an entrepreneur, writer, speaker, technologist and business strategist.

In 1997, Martin founded Corsaire Limited, a service-orientated information security consultancy. As Corsaire's Technical Director, he has helped establish the company as a world-class information security provider and assessor, and has pioneered the creation of a research and development function that is second to none.

Considered a serious individual by the leading security vendors, he has been called to provide a number with independent, confidential architecture and code review prior to product release. In addition, he regularly contributes to the alerting advisories – CERT, SANS, BugTraq, NISCC etc. with vulnerability identification, flaws and remedies.

Martin has established Corsaire's professional service delivery and founded the methodologies, policies and procedures developed within the department. Taking a hands-on leadership style, he enjoys direct involvement with customers particularly where information security strategy and implementation, and software development best practice are the key drivers.

Due to his breadth of experience and ability to explain technical issues in straightforward terms, he is regularly called upon to lecture on a variety of business and technical subjects. Furthermore, he has authored several articles and opinion-pieces for a wide variety of leading publications.

Undoubtedly recognised as an expert in his field, Martin holds numerous vendor accreditations and is highly certified as a CISSP, CISA, and CISM professional. He has also been cleared by GCHQ to provide InfoSec advice under the CESG Listed Advisor Scheme (CLAS) and has achieved an INFOSEC Professional certificate from Cisco that enables him to provide services to the US Government departments and agencies.

About Corsaire

Corsaire are experts at securing information systems. Through our commitment to excellence we help organisations protect their information assets, whilst communicating more effectively. Whether they are interacting with customers, employees, business partners or shareholders, our sound advice can help our clients reduce corporate risk and achieve tangible value from their investments.

Privately founded in 1997 and with offices in the UK and Australia, Corsaire are known for our personable service delivery and an ability to combine both technical and commercial aspects into a single business solution. With over eight years experience in providing information security solutions to the UK Government's National Security Agencies, Government departments and major private and non-profit sectors, we are considered a leading specialist in the delivery of information security planning, assessment, implementation and management.

Corsaire take a holistic view to information security. We view both business and security objectives as inseparable and work in partnership with our clients to achieve a cost-effective balance between the two. Through our consultative, vendor-neutral methods we ensure that whatever solution is recommended, an organisation will never be overexposed, nor carry the burden of unnecessary technical measures.

Corsaire have one of the most respected and experienced teams of principal consultants available in the industry and have consistently brought fresh ideas and innovation to the information security arena. We take pride in being a knowledge-based organisation, but we don't just stop there. Through a culture of knowledge-share, we are also committed to improving our client's internal understanding of security principles.

It is this approach to knowledge that differentiates us from most other information security consultancies. As a mark of this, we are known globally through our active contribution to the security research community, publishing papers and advisories on a regular basis. These we share freely with our clients, providing them with immediate access to the most up-to-date information risk management advice available, allowing them to minimize their exposure and gain an instant competitive advantage.

Whilst it is imperative for us to offer a high level of security to our clients, we believe that it is of equal bearing to provide a high level of service. At Corsaire our clients are not only protected but valued too. We work hard at building strong relationships that are founded on the cornerstones of respect and trust. With 80% of our customer base deriving from referrals we are certain that our clients value the quality, flexibility and integrity that partnering with Corsaire brings.

For more information contact us at **info@corsaire.com** or visit our website at **www.corsaire.com**