Pure AppSec, No Fillers or Preservatives
OWASP Cheat Sheet Series

Michael Coates - Mozilla

September, 2011

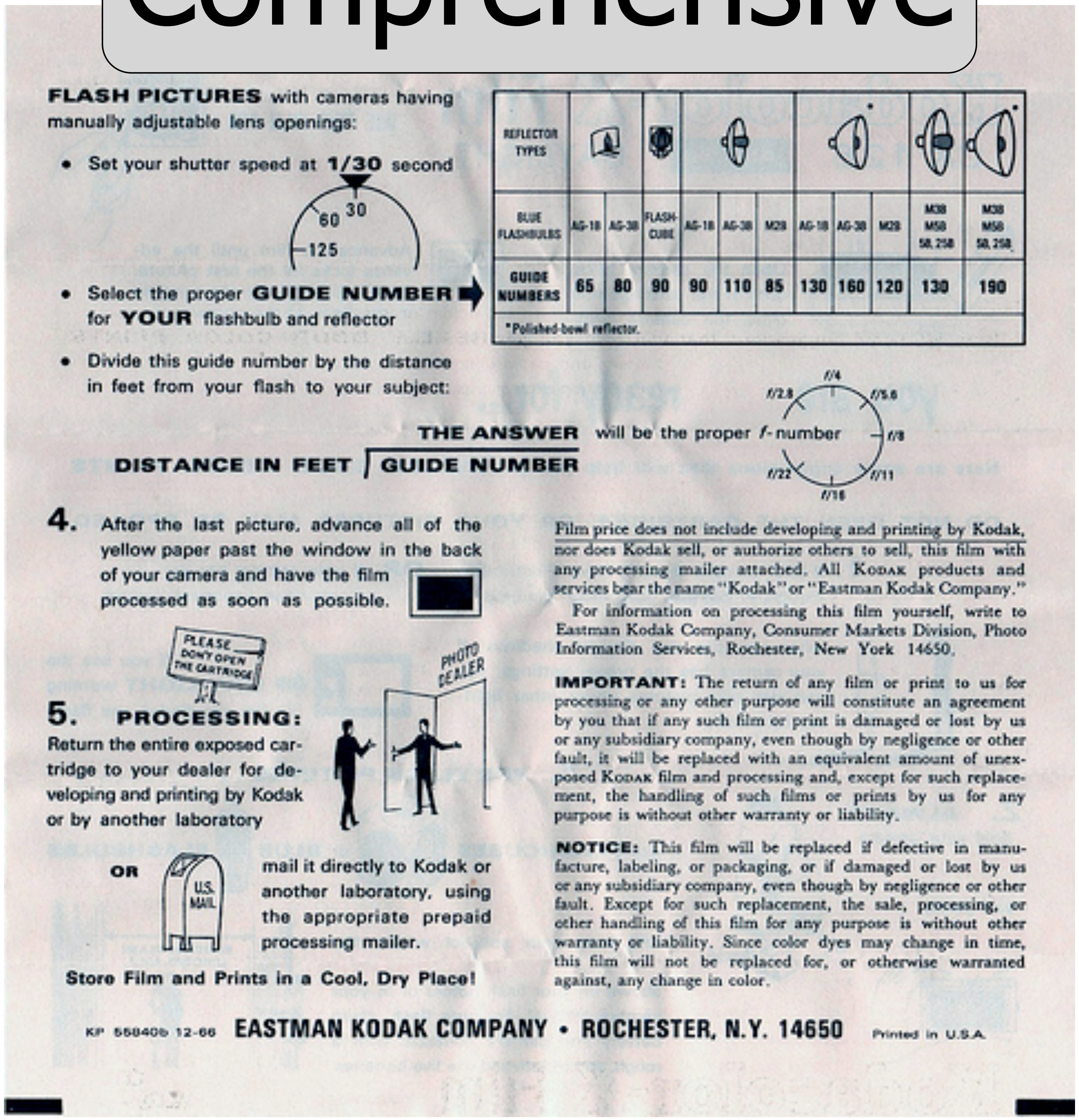
OWASP

The OWASP Foundation
http://www.owasp.org

Compact

http://www.flickr.com/photos/eprater/6043906778

Comprehensive


30
60
125
f/4
f/5.6
f/8
f/11
f/16
f/22
f/2.8
PLEASE DON'T OPEN THE CARTRIDGE
PHOTO DEALER
U.S. MAIL

FLASH PICTURES with cameras having manually adjustable lens openings:

- Set your shutter speed at **1/30** second
- Select the proper **GUIDE NUMBER** for **YOUR** flashbulb and reflector
- Divide this guide number by the distance in feet from your flash to your subject:

REFLECTOR TYPES								*			*
BLUE FLASHBULBS	AG-1B	AG-3B	FLASH-CUBE	AG-1B	AG-3B	M2B	AG-1B	AG-3B	M2B	M3B M5B 5B, 25B	M3B M5B 5B, 25B
GUIDE NUMBERS	65	80	90	90	110	85	130	160	120	130	190

*Polished-bowl reflector.

THE ANSWER will be the proper *f*-number

DISTANCE IN FEET ⟌ GUIDE NUMBER

4. After the last picture, advance all of the yellow paper past the window in the back of your camera and have the film processed as soon as possible.

5. PROCESSING: Return the entire exposed cartridge to your dealer for developing and printing by Kodak or by another laboratory

OR mail it directly to Kodak or another laboratory, using the appropriate prepaid processing mailer.

Store Film and Prints in a Cool, Dry Place!

Film price does not include developing and printing by Kodak, nor does Kodak sell, or authorize others to sell, this film with any processing mailer attached. All Kodak products and services bear the name "Kodak" or "Eastman Kodak Company."

For information on processing this film yourself, write to Eastman Kodak Company, Consumer Markets Division, Photo Information Services, Rochester, New York 14650.

IMPORTANT: The return of any film or print to us for processing or any other purpose will constitute an agreement by you that if any such film or print is damaged or lost by us or any subsidiary company, even though by negligence or other fault, it will be replaced with an equivalent amount of unexposed Kodak film and processing and, except for such replacement, the handling of such films or prints by us for any purpose is without other warranty or liability.

NOTICE: This film will be replaced if defective in manufacture, labeling, or packaging, or if damaged or lost by us or any subsidiary company, even though by negligence or other fault. Except for such replacement, the sale, processing, or other handling of this film for any purpose is without other warranty or liability. Since color dyes may change in time, this film will not be replaced for, or otherwise warranted against, any change in color.

KP 558406 12-66 **EASTMAN KODAK COMPANY • ROCHESTER, N.Y. 14650** Printed in U.S.A.

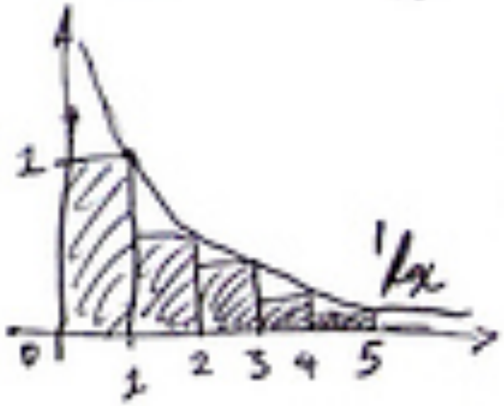
http://www.flickr.com/photos/southbeachcars/5394835890

Correct

$$P_{failure} = \sum_{c=k+1}^{2k} P_{\text{loop of size c exists}} = \frac{\sum_{c=k+1}^{2k} \text{number of permutations with loop of size c}}{2k!}$$

$$= \frac{\sum_{c=k+1}^{2k} \frac{2k!}{(2k-c)!\ c} (2k-c)!}{2k!} = \sum_{c=k+1}^{2k} \frac{1}{c} = H_{2k} - H_{k}$$

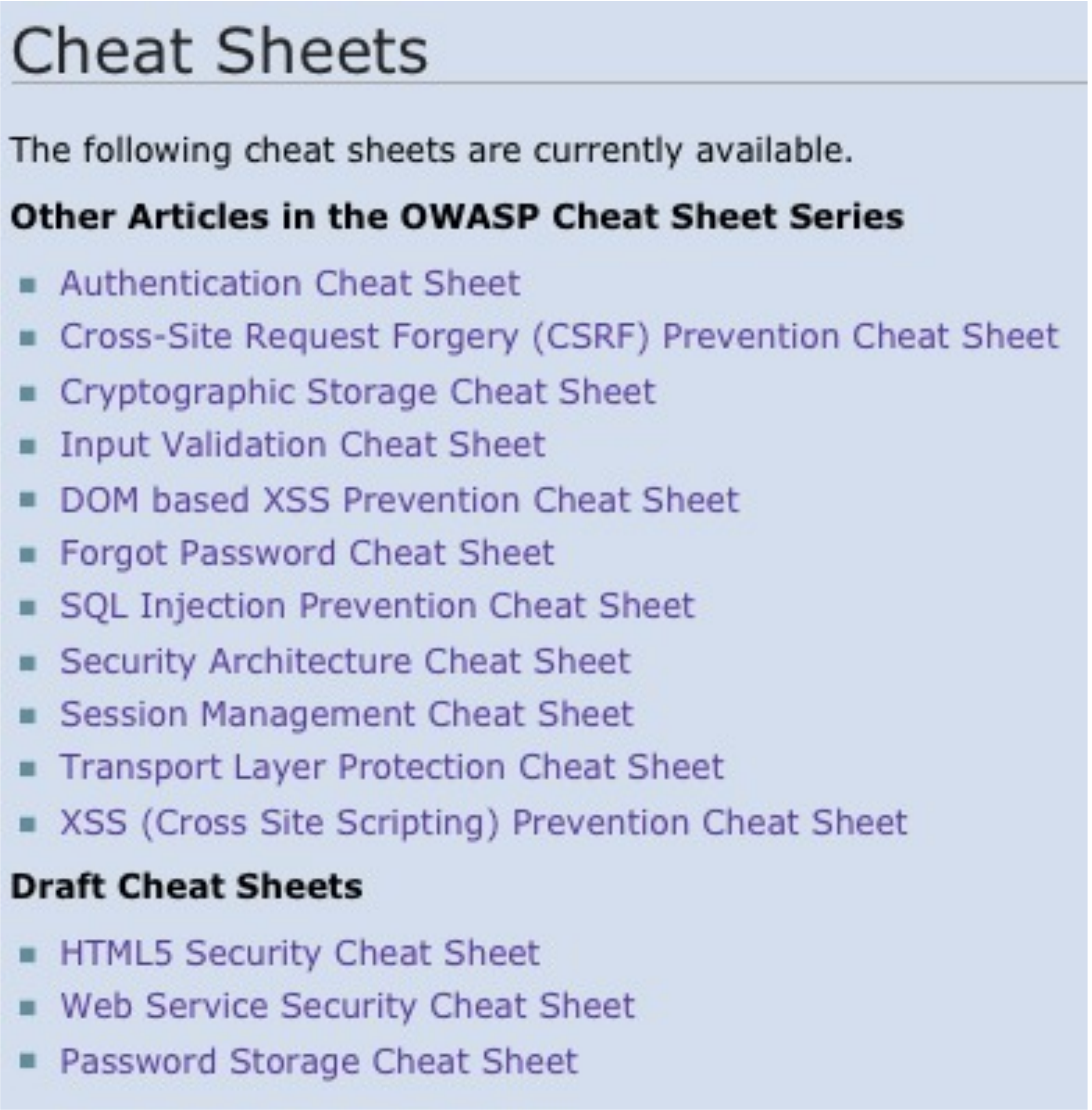
$$\leq \int_{k}^{2k} \frac{1}{x} dx = \ln 2k - \ln k = \ln 2 .$$



$$P_{success} = 1 - P_{failure} \geq 1 - \ln 2 \simeq 0.30 \qquad \square$$

http://www.flickr.com/photos/behdad/526904677

The Cheat Sheets



Cheat Sheets

The following cheat sheets are currently available.

Other Articles in the OWASP Cheat Sheet Series

- Authentication Cheat Sheet
- Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet
- Cryptographic Storage Cheat Sheet
- Input Validation Cheat Sheet
- DOM based XSS Prevention Cheat Sheet
- Forgot Password Cheat Sheet
- SQL Injection Prevention Cheat Sheet
- Security Architecture Cheat Sheet
- Session Management Cheat Sheet
- Transport Layer Protection Cheat Sheet
- XSS (Cross Site Scripting) Prevention Cheat Sheet

Draft Cheat Sheets

- HTML5 Security Cheat Sheet
- Web Service Security Cheat Sheet
- Password Storage Cheat Sheet

The Authors

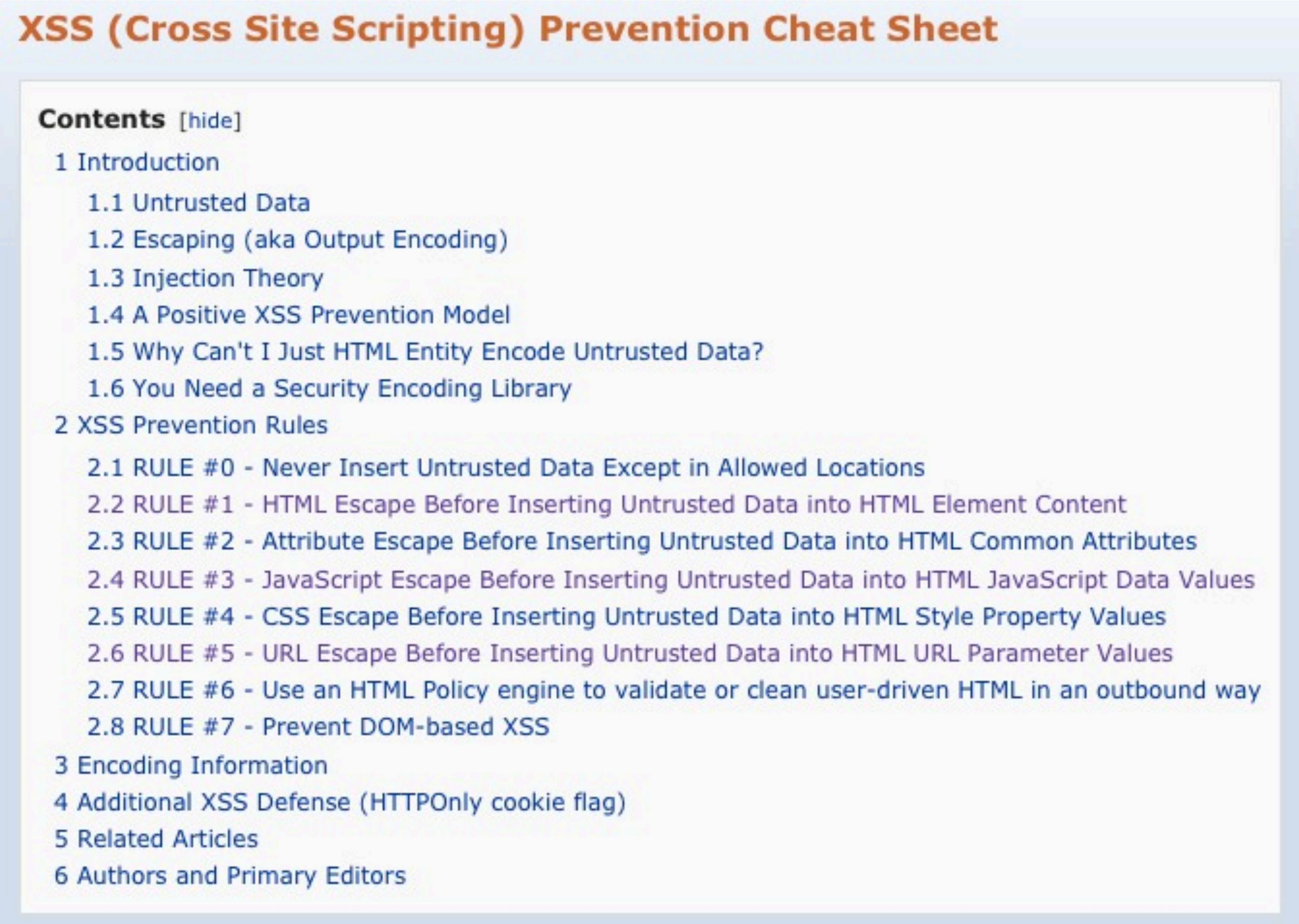
Abraham Kang
Achim Hoffmann
Chris Schmidt
Dave Ferguson
Dave Wichers
David Rook
Edwardo Alberto Vela Nava
Eoin Keary
Eric Sheridan
Erlend Oftedal
Fred Donovan
Gareth Heyes
Jeff Williams
Jeremy Long

Jim Manico
John Steven
Kevin Kenan
Kevin Wall
Lenny Zeltser
Mario Heiderich
Michael Boberski
Michael Coates
Mike Samuel
Paul Petefish
Raul Siles
Robert Hansen
Stefano Di Paola
Tyler Reguly

Most Visited Cheat Sheets

XSS (Cross Site Scripting) Prevention Cheat Sheet	354,208
SQL Injection Prevention Cheat Sheet	180,011
Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet	78,086
Transport Layer Protection Cheat Sheet	46,343
Authentication Cheat Sheet	28,074

Total Cheat Sheet Views : 740,000



XSS (Cross Site Scripting) Prevention Cheat Sheet

Contents [hide]

1 Introduction
- 1.1 Untrusted Data
- 1.2 Escaping (aka Output Encoding)
- 1.3 Injection Theory
- 1.4 A Positive XSS Prevention Model
- 1.5 Why Can't I Just HTML Entity Encode Untrusted Data?
- 1.6 You Need a Security Encoding Library

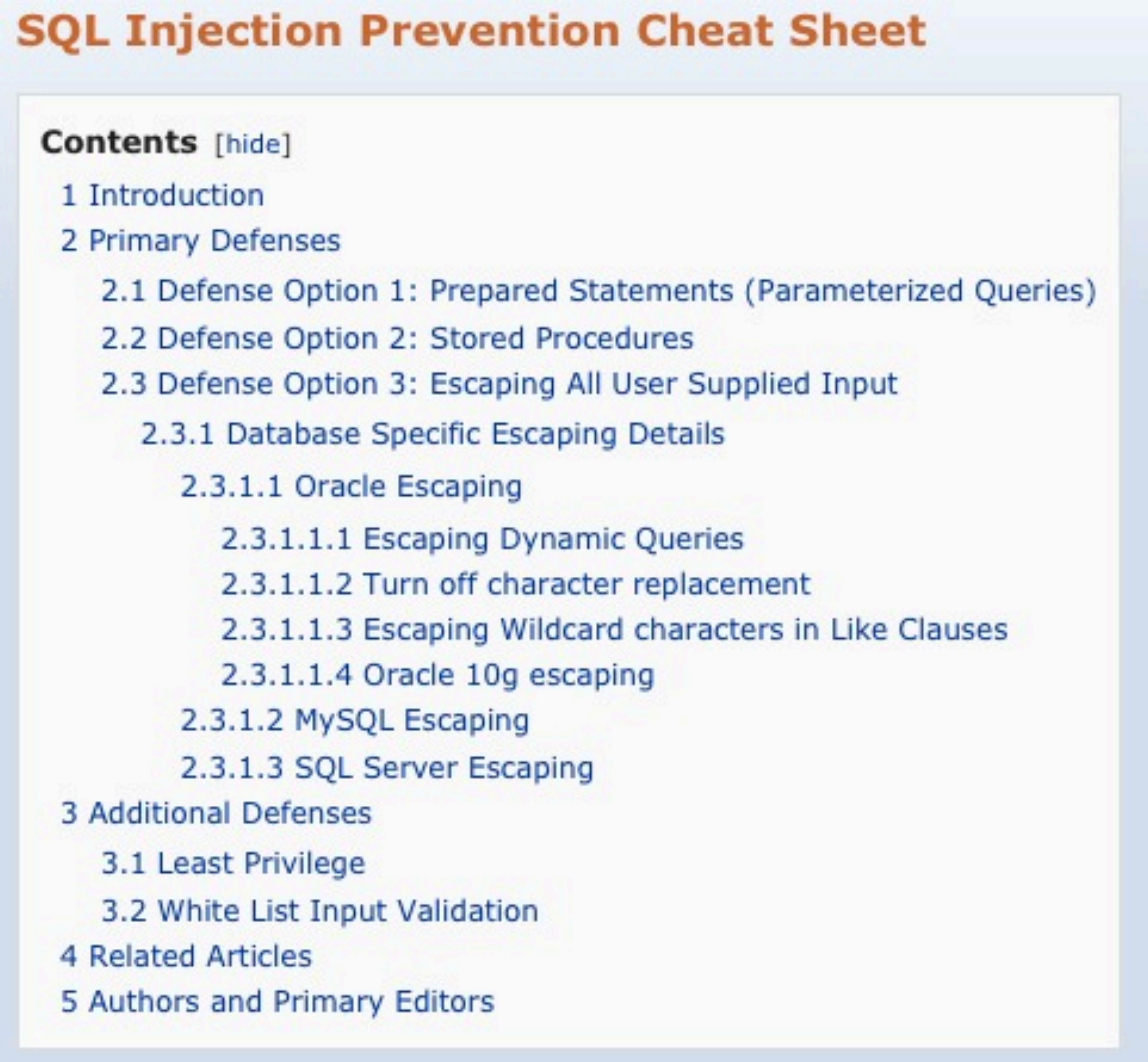
2 XSS Prevention Rules
- 2.1 RULE #0 - Never Insert Untrusted Data Except in Allowed Locations
- 2.2 RULE #1 - HTML Escape Before Inserting Untrusted Data into HTML Element Content
- 2.3 RULE #2 - Attribute Escape Before Inserting Untrusted Data into HTML Common Attributes
- 2.4 RULE #3 - JavaScript Escape Before Inserting Untrusted Data into HTML JavaScript Data Values
- 2.5 RULE #4 - CSS Escape Before Inserting Untrusted Data into HTML Style Property Values
- 2.6 RULE #5 - URL Escape Before Inserting Untrusted Data into HTML URL Parameter Values
- 2.7 RULE #6 - Use an HTML Policy engine to validate or clean user-driven HTML in an outbound way
- 2.8 RULE #7 - Prevent DOM-based XSS

3 Encoding Information

4 Additional XSS Defense (HTTPOnly cookie flag)

5 Related Articles

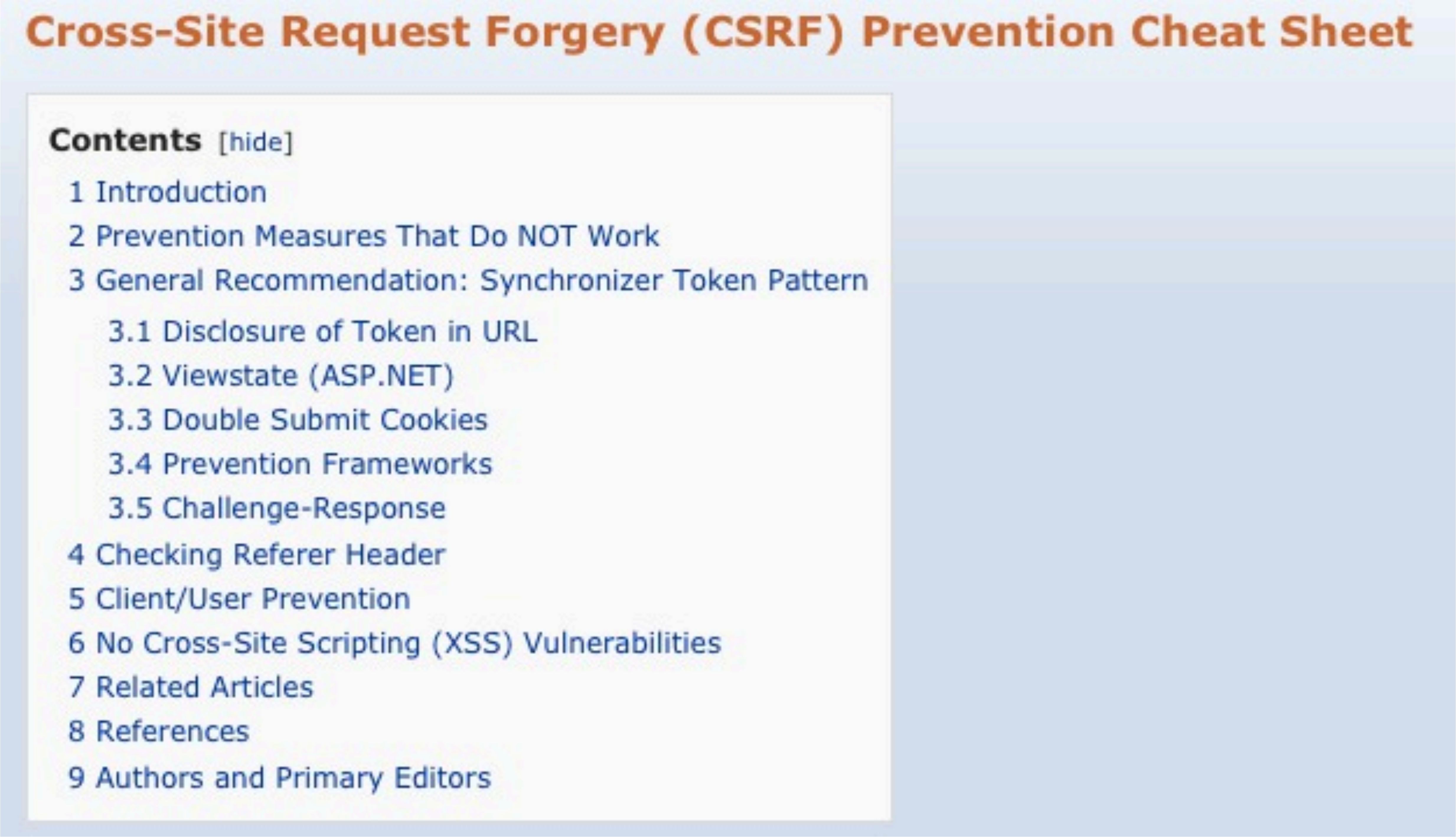
6 Authors and Primary Editors



SQL Injection Prevention Cheat Sheet

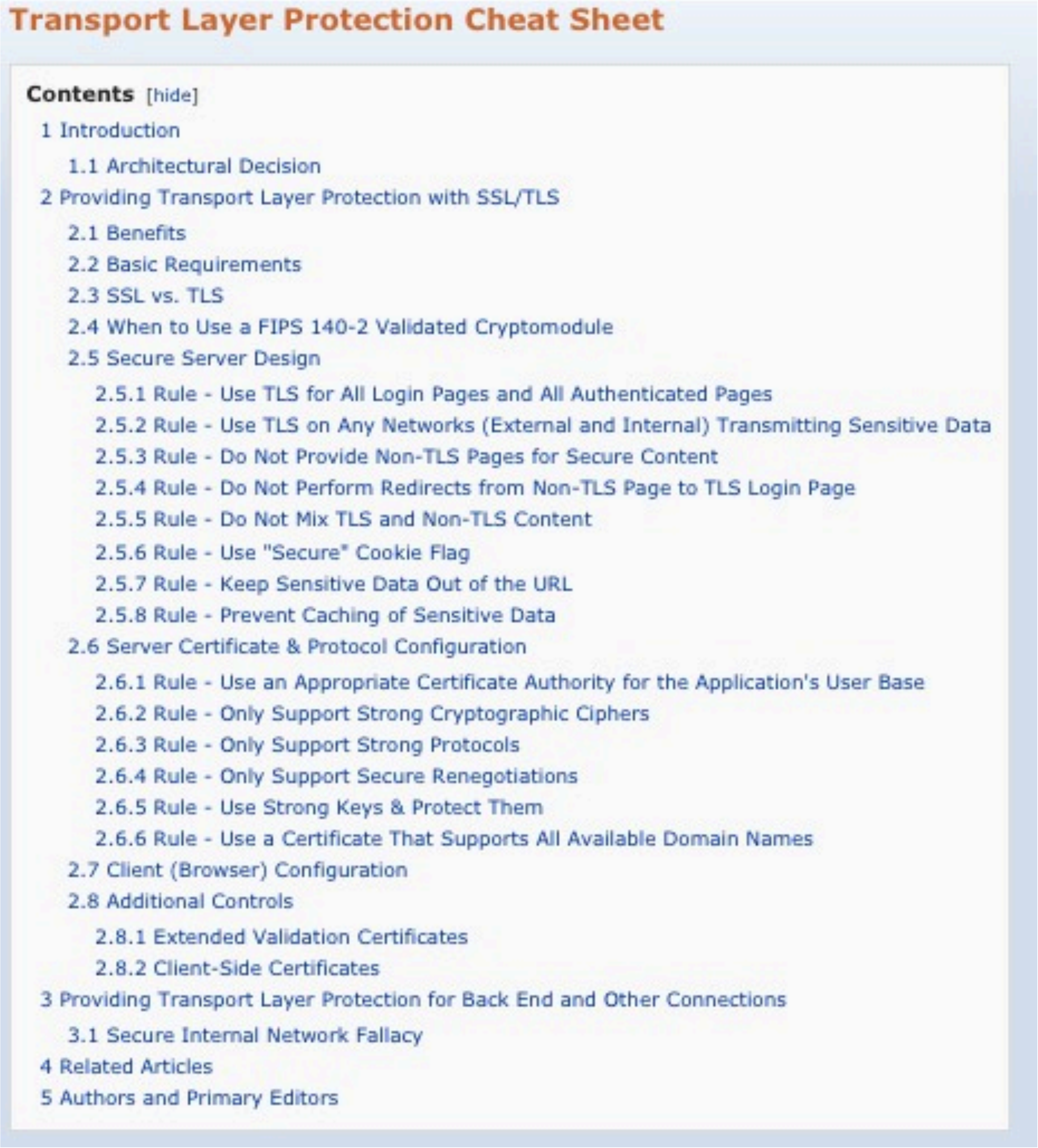
Contents [hide]

- 1 Introduction
- 2 Primary Defenses
  - 2.1 Defense Option 1: Prepared Statements (Parameterized Queries)
  - 2.2 Defense Option 2: Stored Procedures
  - 2.3 Defense Option 3: Escaping All User Supplied Input
    - 2.3.1 Database Specific Escaping Details
      - 2.3.1.1 Oracle Escaping
        - 2.3.1.1.1 Escaping Dynamic Queries
        - 2.3.1.1.2 Turn off character replacement
        - 2.3.1.1.3 Escaping Wildcard characters in Like Clauses
        - 2.3.1.1.4 Oracle 10g escaping
      - 2.3.1.2 MySQL Escaping
      - 2.3.1.3 SQL Server Escaping
- 3 Additional Defenses
  - 3.1 Least Privilege
  - 3.2 White List Input Validation
- 4 Related Articles
- 5 Authors and Primary Editors



Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

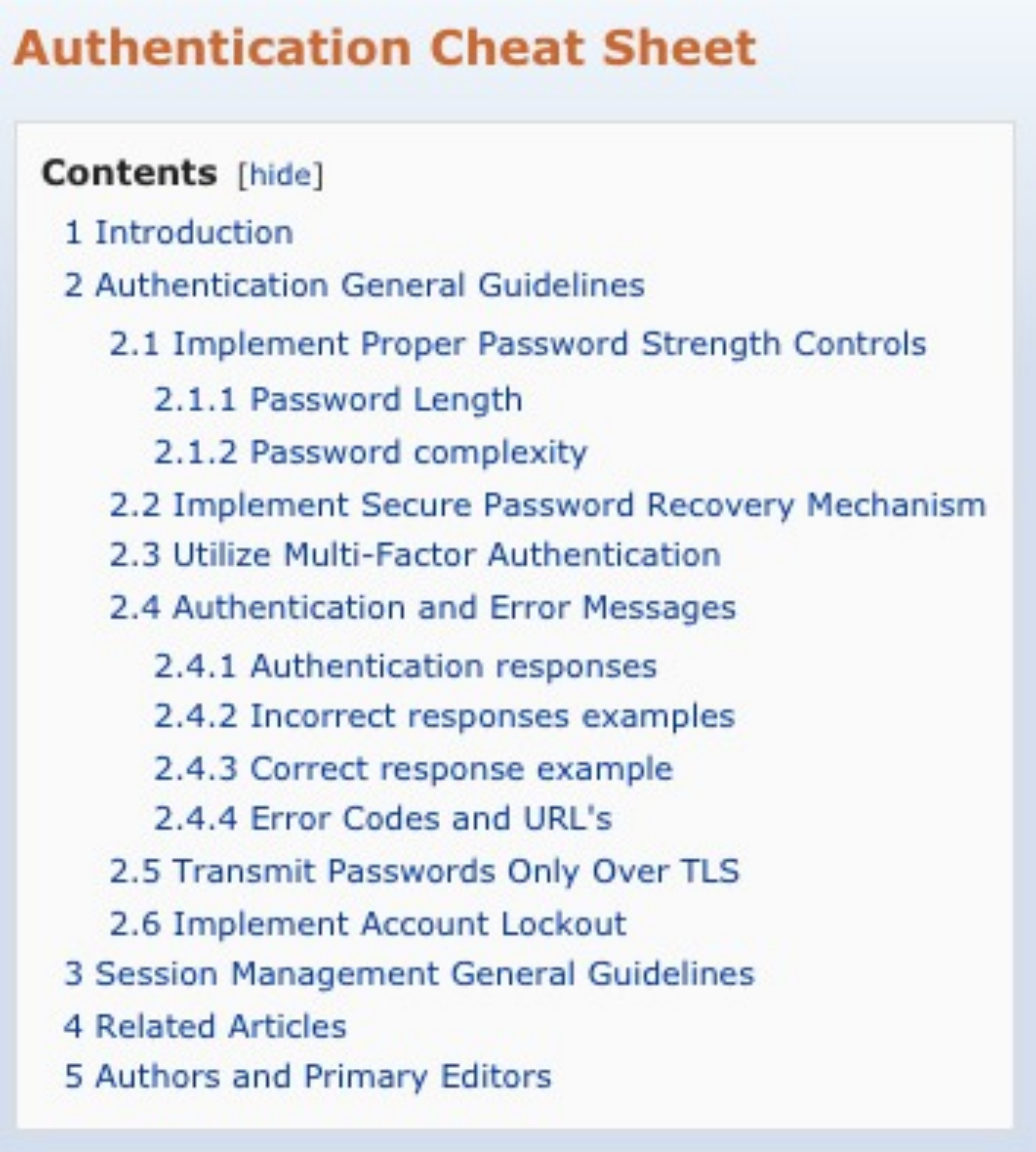
Contents [hide]



Transport Layer Protection Cheat Sheet

Contents [hide]

1 Introduction
  1.1 Architectural Decision
2 Providing Transport Layer Protection with SSL/TLS
  2.1 Benefits
  2.2 Basic Requirements
  2.3 SSL vs. TLS
  2.4 When to Use a FIPS 140-2 Validated Cryptomodule
  2.5 Secure Server Design
    2.5.1 Rule - Use TLS for All Login Pages and All Authenticated Pages
    2.5.2 Rule - Use TLS on Any Networks (External and Internal) Transmitting Sensitive Data
    2.5.3 Rule - Do Not Provide Non-TLS Pages for Secure Content
    2.5.4 Rule - Do Not Perform Redirects from Non-TLS Page to TLS Login Page
    2.5.5 Rule - Do Not Mix TLS and Non-TLS Content
    2.5.6 Rule - Use "Secure" Cookie Flag
    2.5.7 Rule - Keep Sensitive Data Out of the URL
    2.5.8 Rule - Prevent Caching of Sensitive Data
  2.6 Server Certificate & Protocol Configuration
    2.6.1 Rule - Use an Appropriate Certificate Authority for the Application's User Base
    2.6.2 Rule - Only Support Strong Cryptographic Ciphers
    2.6.3 Rule - Only Support Strong Protocols
    2.6.4 Rule - Only Support Secure Renegotiations
    2.6.5 Rule - Use Strong Keys & Protect Them
    2.6.6 Rule - Use a Certificate That Supports All Available Domain Names
  2.7 Client (Browser) Configuration
  2.8 Additional Controls
    2.8.1 Extended Validation Certificates
    2.8.2 Client-Side Certificates
3 Providing Transport Layer Protection for Back End and Other Connections
  3.1 Secure Internal Network Fallacy
4 Related Articles
5 Authors and Primary Editors



Authentication Cheat Sheet

Contents [hide]

1 Introduction
2 Authentication General Guidelines
  2.1 Implement Proper Password Strength Controls
    2.1.1 Password Length
    2.1.2 Password complexity
  2.2 Implement Secure Password Recovery Mechanism
  2.3 Utilize Multi-Factor Authentication
  2.4 Authentication and Error Messages
    2.4.1 Authentication responses
    2.4.2 Incorrect responses examples
    2.4.3 Correct response example
    2.4.4 Error Codes and URL's
  2.5 Transmit Passwords Only Over TLS
  2.6 Implement Account Lockout
3 Session Management General Guidelines
4 Related Articles
5 Authors and Primary Editors

What’s Next?

- Cheat sheet updates
- Single cheat sheet download
- Cheat sheet book

Questions?