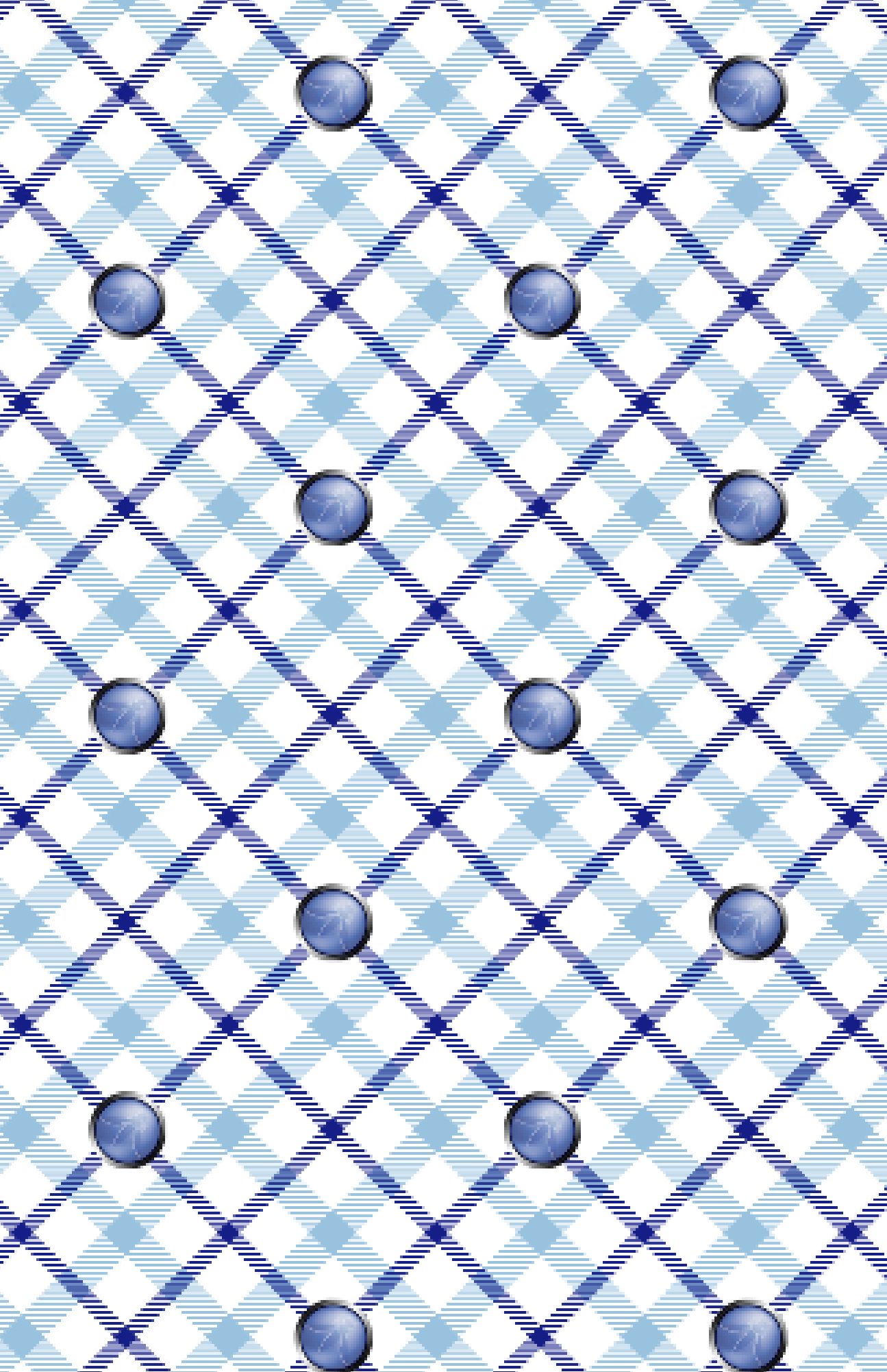
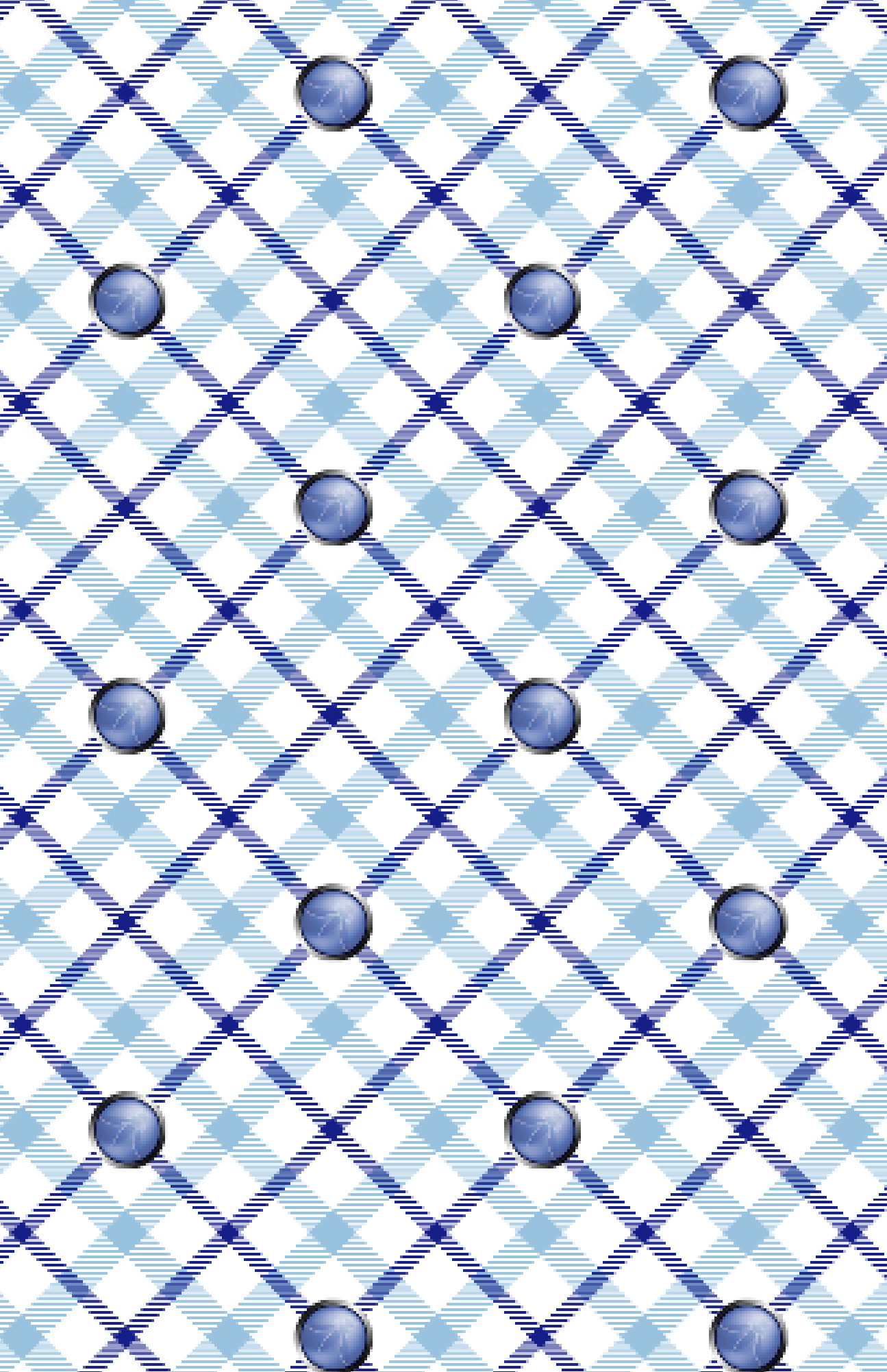


CORNUCOPIA

A

You have invented a new attack of any type

Read more about application security in OWASP's free Guides on Requirements, Development, Code Review and Testing, the Cheat Sheet series, and the Open Software Assurance Maturity Model

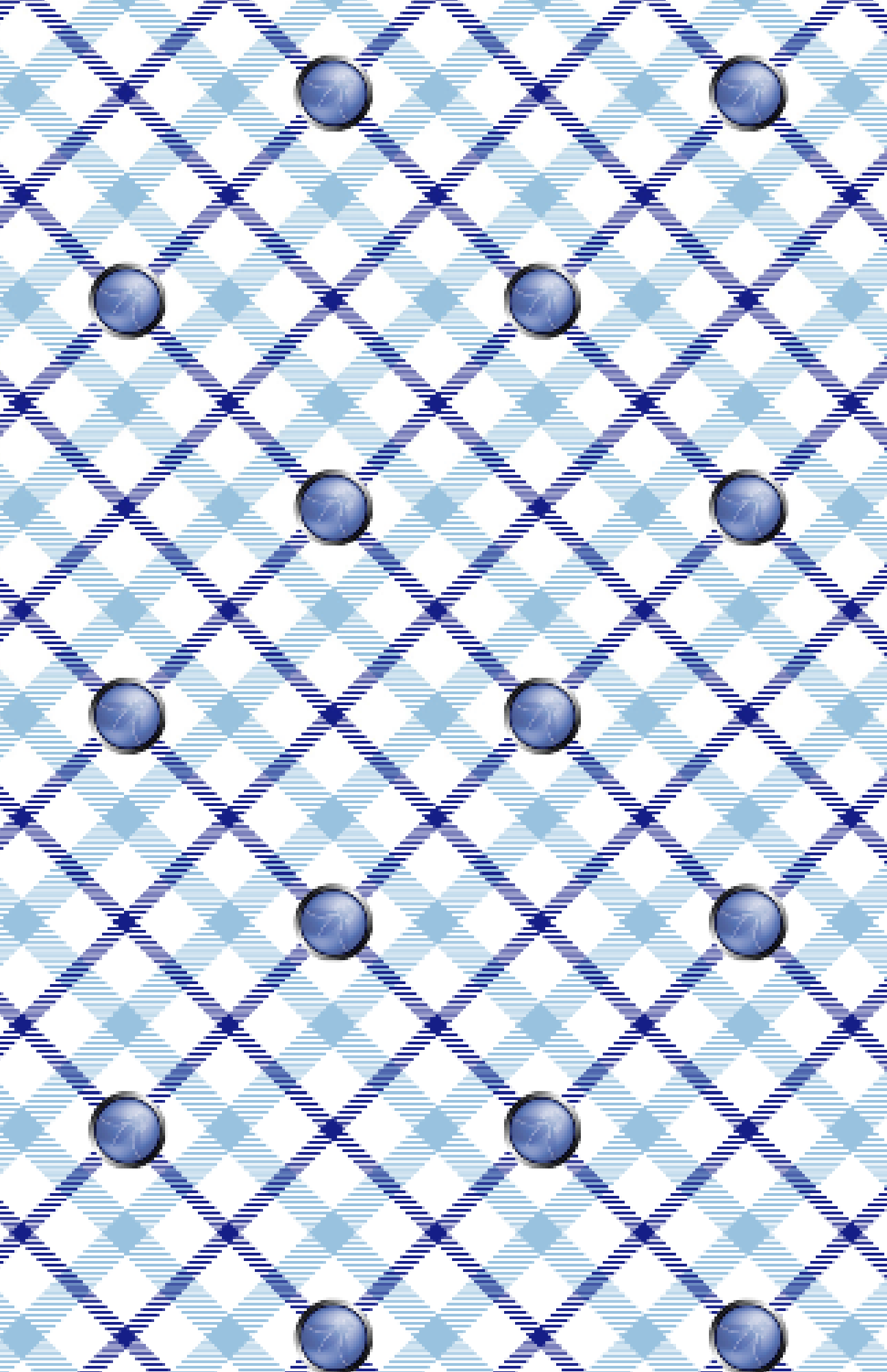


CORNUCOPIA

2

Lee can bypass application controls because dangerous/risky programming language functions have been used instead of safer alternatives, or there are type conversion errors, or because the application is unreliable when an external resource is unavailable, or there are race conditions, or there are resource initialization or allocation issues, or overflows can occur

OWASP SCP 194-202, 205-209
OWASP ASVS 5.1
OWASP AppSensor -
CAPEC 25, 26, 29, 96, 123-4, 128-9, 264-5
SAFECODE 3, 5-7, 9, 22, 25-26, 34



CORNUCOPIA

3

Andrew can access source code, or decompile, or otherwise access business logic to understand how the application works and any secrets contained

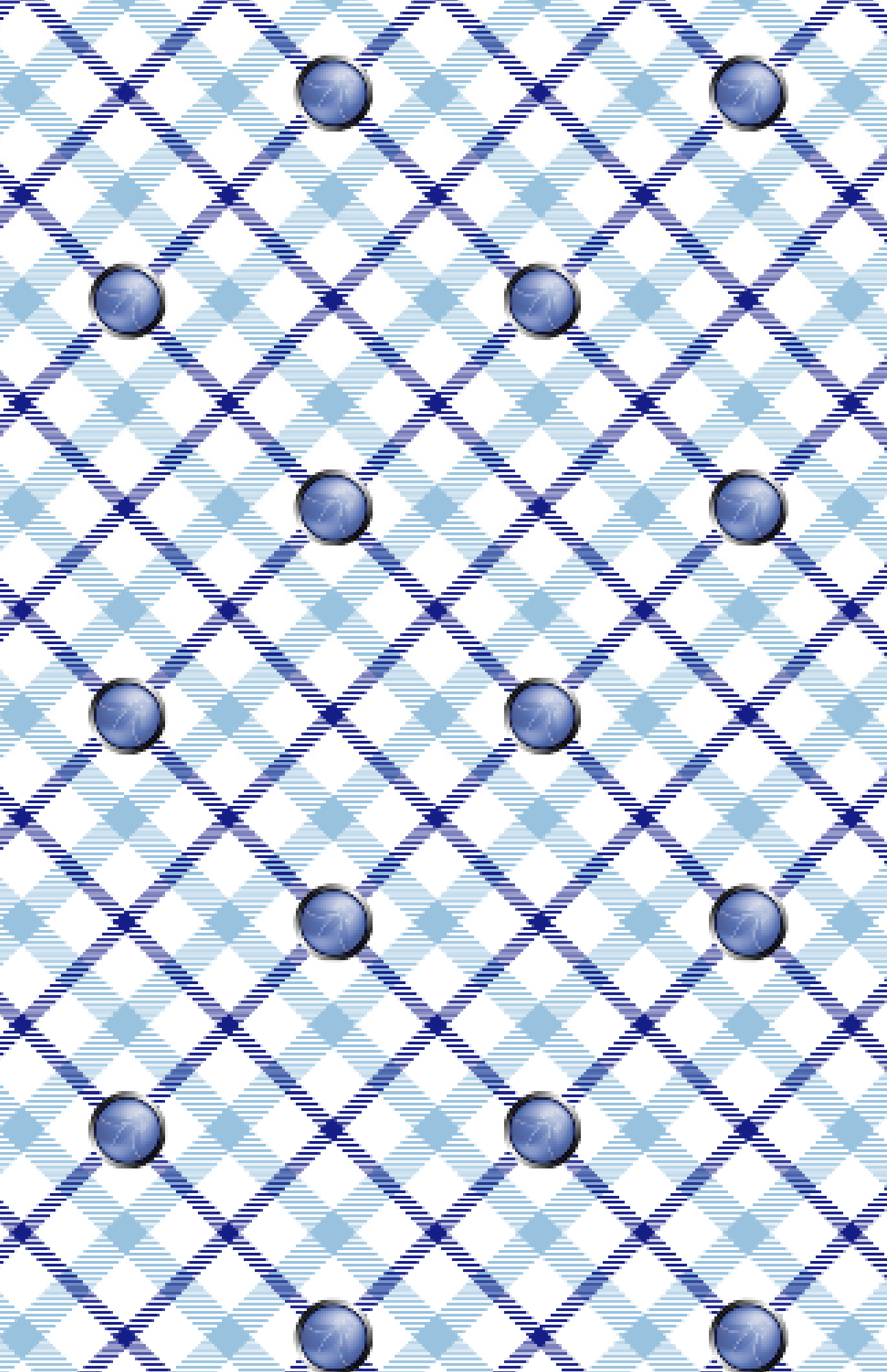
OWASP SCP
134

OWASP ASVS
-

OWASP AppSensor
-

CAPEC
56, 189, 207, 211

SAFECODE
-



CORNUCOPIA

4

Keith can perform an action and it is not possible to attribute it to him

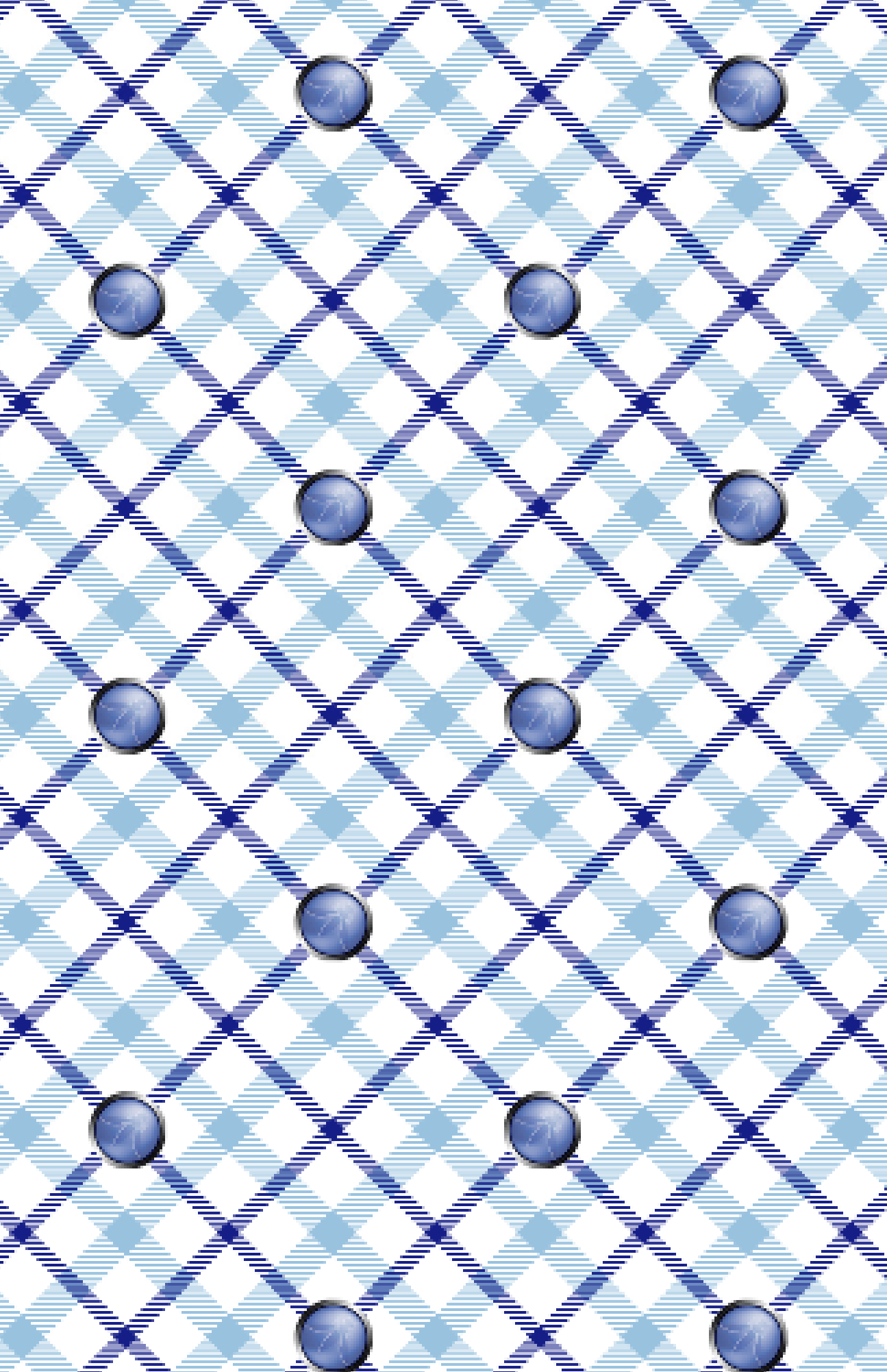
OWASP SCP
181

OWASP ASVS
-

OWASP AppSensor
-

CAPEC
-

SAFECODE
-



CORNUCOPIA

5

Larry can influence the trust other parties including users have in the application, or abuse that trust elsewhere (e.g. in another application)

OWASP SCP

-

OWASP ASVS

-

OWASP AppSensor

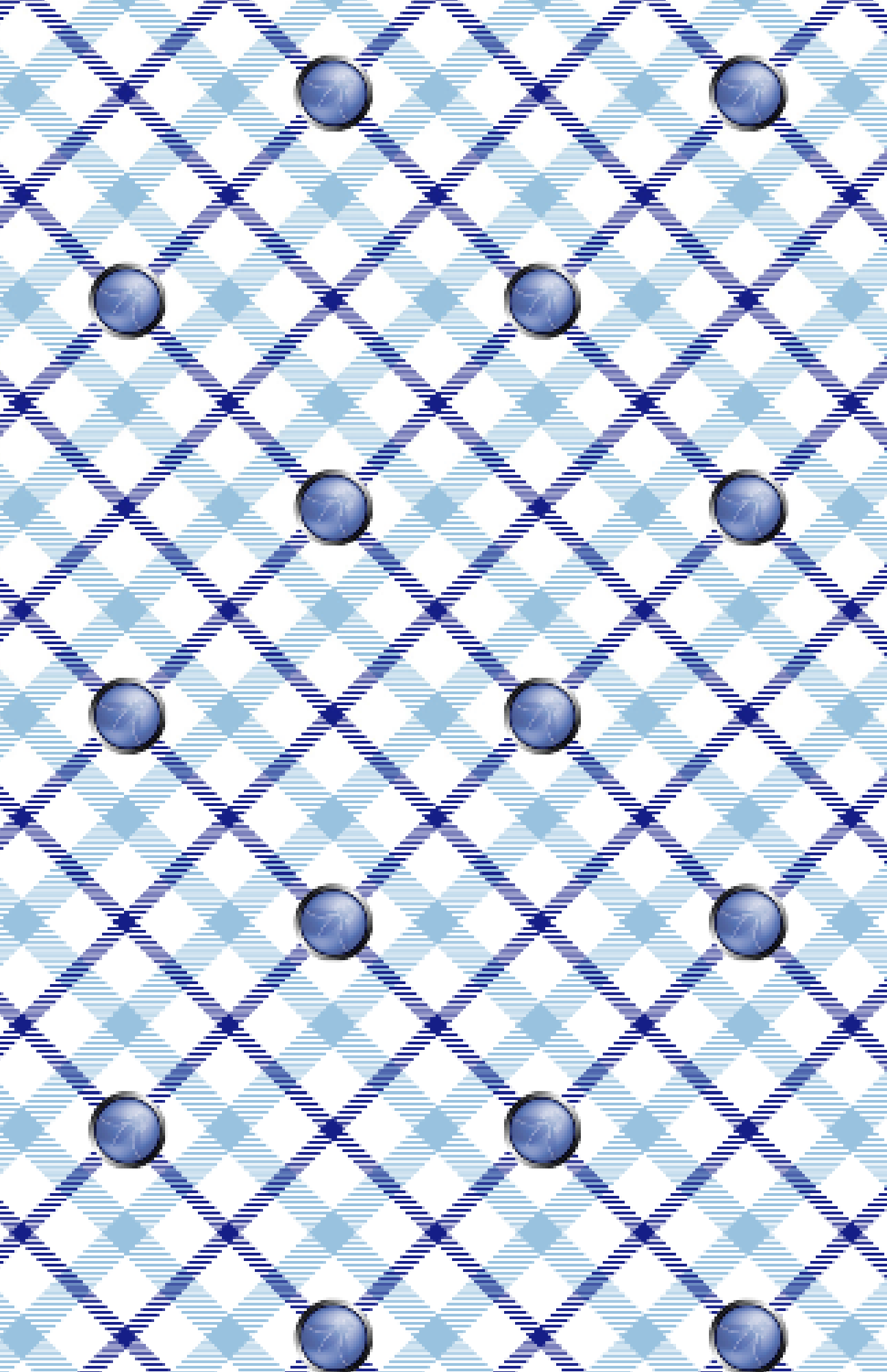
-

CAPEC

89, 103, 181, 459

SAFECODE

-

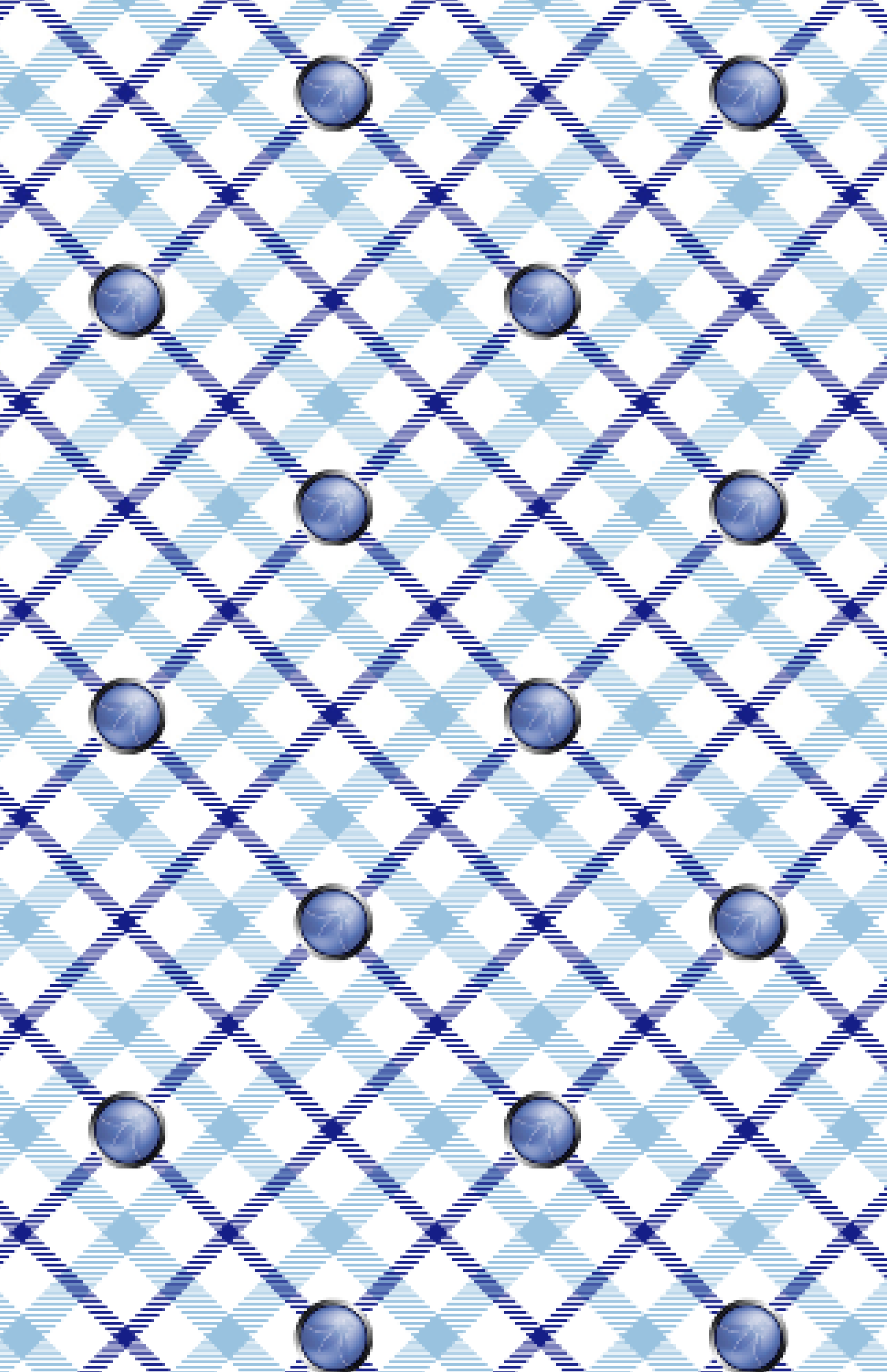


CORNUCOPIA

6

Aaron can bypass controls because error/exception handling is missing, or is implemented inconsistently, or is partially implemented, or does not deny access by default (i.e. errors terminate access/execution), or relies on handling by some other service or system

OWASP SCP 109, 110, 111, 112, 155
OWASP ASVS 8.4
OWASP AppSensor -
CAPEC 54, 98, 164
SAFECODE 4, 11, 23



CORNUCOPIA

7

Mwengu's actions cannot be investigated because there is not an adequate accurately time-stamped record of security events, or there is not a full audit trail, or these can be altered or deleted by Mwengu, or there is no centralized logging service

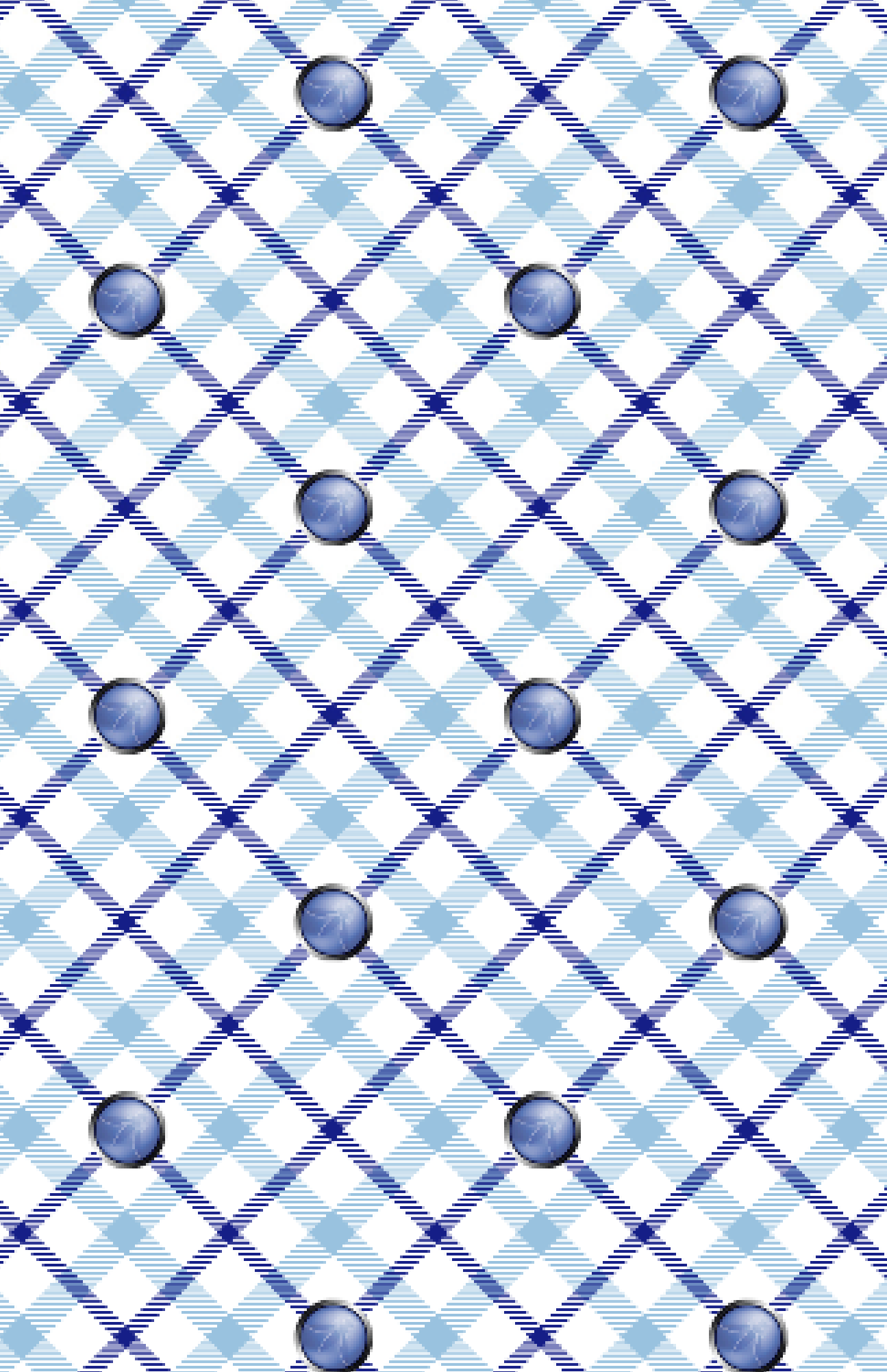
OWASP SCP
113-115, 117, 118, 121-130

OWASP ASVS
2.12, 4.15, 5.7,7.5,8.3,8.5-6,8.8,8.9,10.4,12.3

OWASP AppSensor
-

CAPEC
93

SAFECODE
4



CORNUCOPIA

8

David can bypass the application to gain access to data because the network and host infrastructure, and supporting services/applications, have not been securely configured, the configuration rechecked periodically and security patches applied, or the data is stored locally, or the data is not physically protected

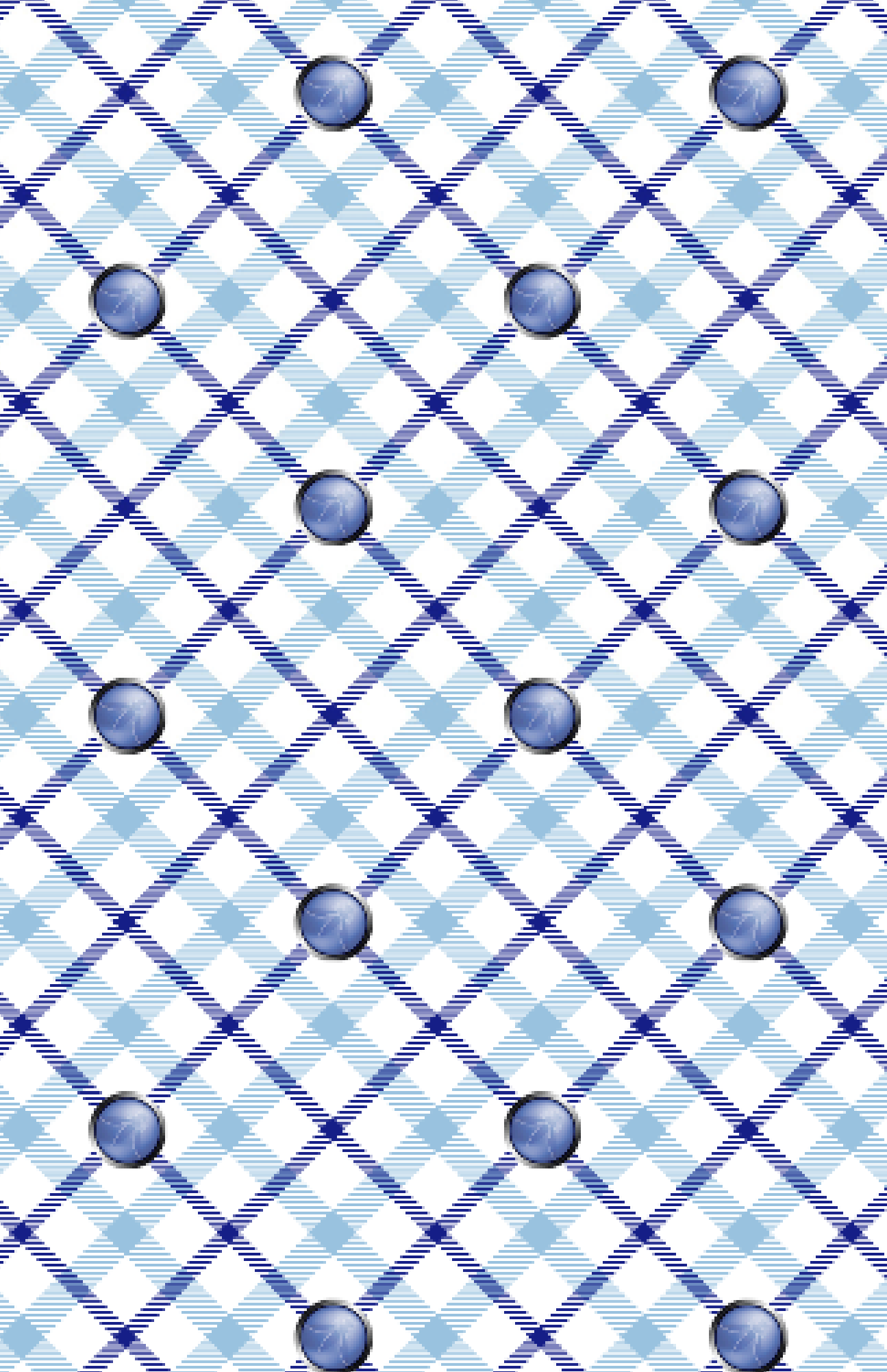
OWASP SCP
151, 152, 156, 160, 161, 173-177

OWASP ASVS
11.2, 11.3, 11.6

OWASP AppSensor
RE1, RE2

CAPEC
37, 220, 289, 310, 436

SAFECODE
-



CORNUCOPIA

9

Michael can bypass the application to gain access to data because administrative tools or administrative interfaces are not secured adequately

OWASP SCP

-

OWASP ASVS

-

OWASP AppSensor

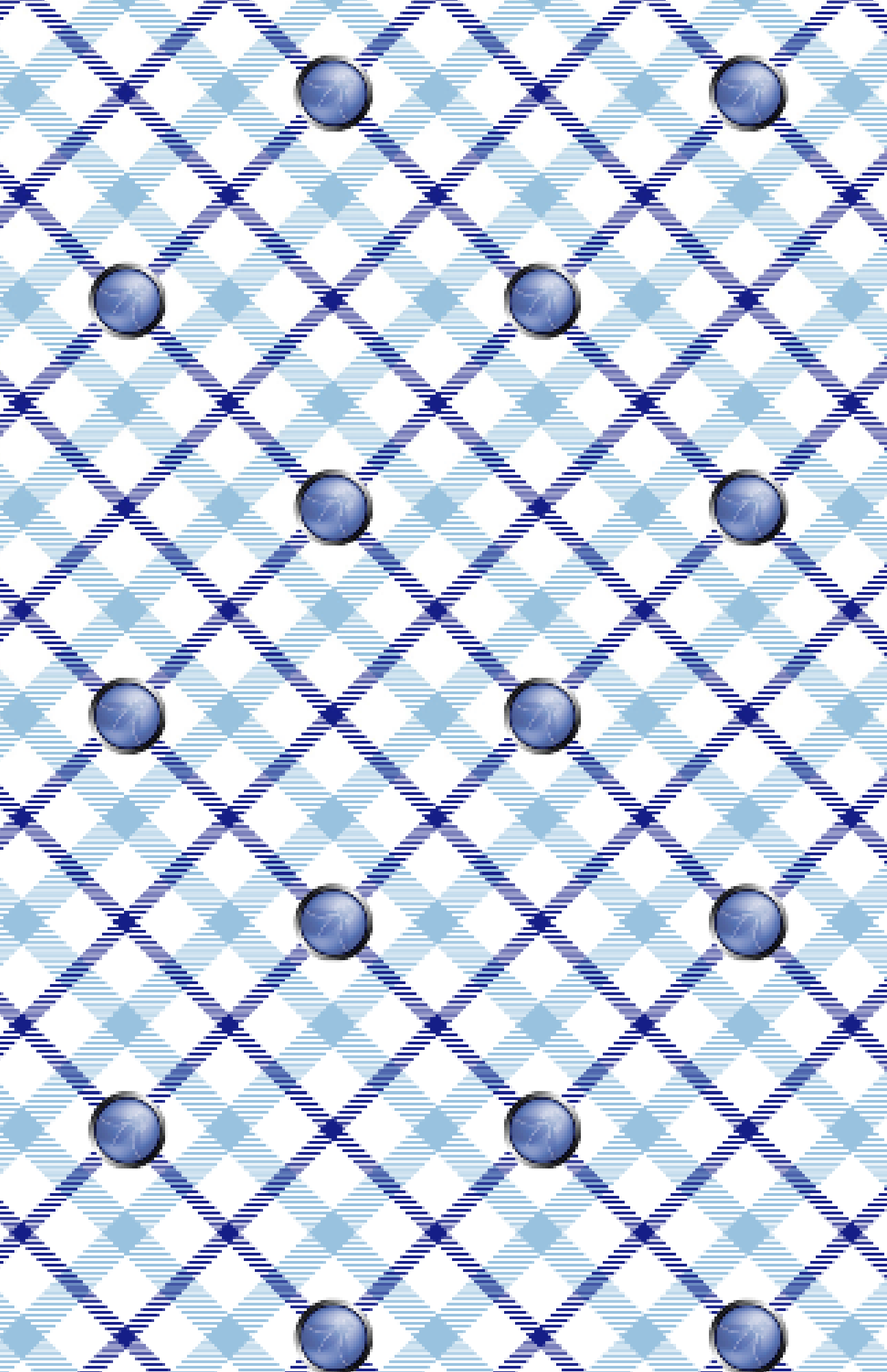
-

CAPEC

225, 122

SAFECODE

-



CORNUCOPIA

10

Xavier can circumvent the application's controls because code frameworks, libraries and components contain malicious code or vulnerabilities (e.g. in-house, commercial off the shelf, outsourced, open source, externally-located)

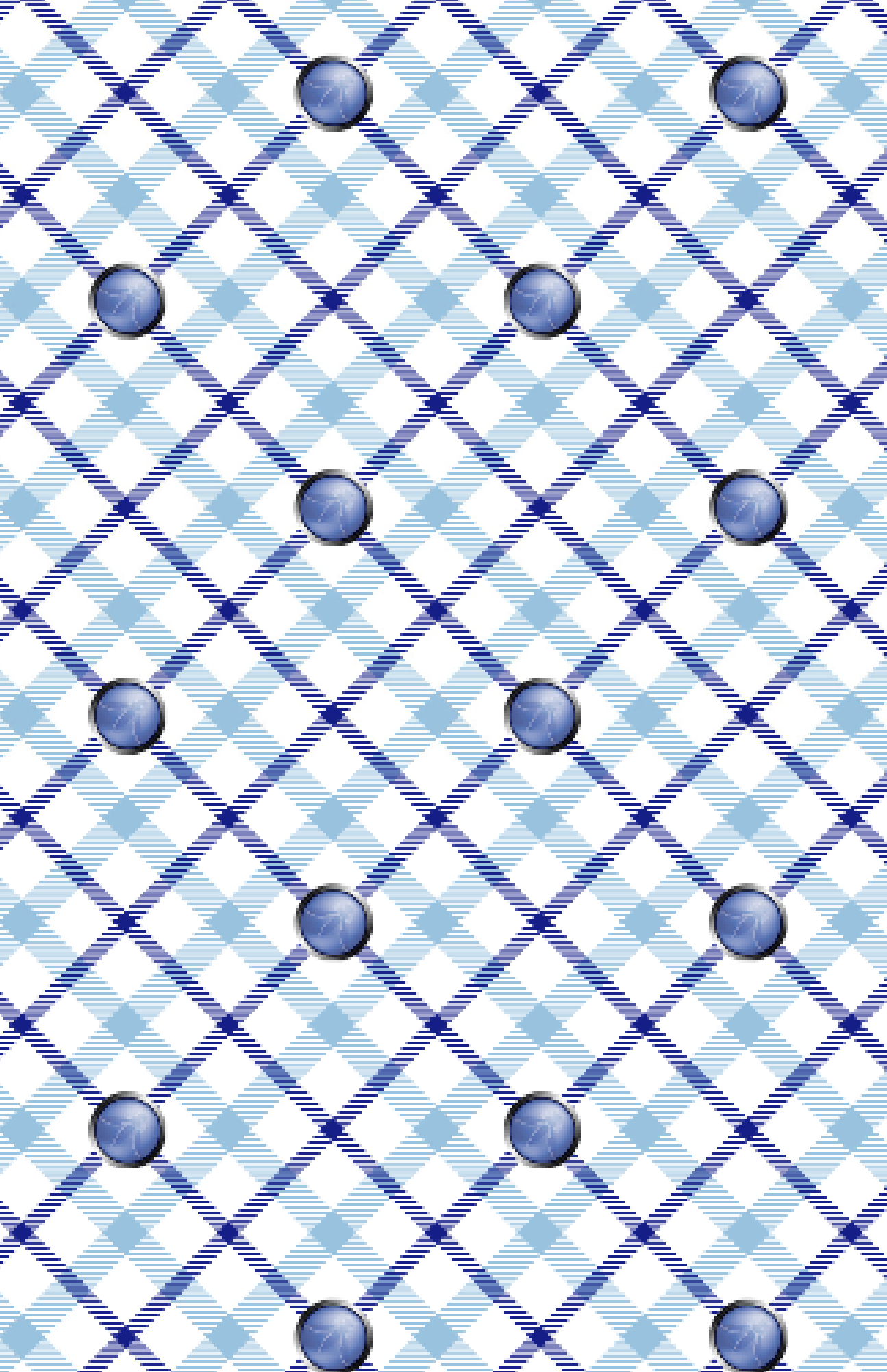
OWASP SCP
57, 151, 152, 204, 212

OWASP ASVS
2.15, 3.13, 4.16, 5.9, 6.10, 7.10, 8.12, 13.1

OWASP AppSensor
-

CAPEC
68, 438, 439, 442

SAFECODE
15



CORNUCOPIA

J

Roman can exploit the application because it was compiled using out-of-date tools, or its configuration is not secure by default, or security information was not documented and passed on to operational teams

OWASP SCP

-

OWASP ASVS

-

OWASP AppSensor

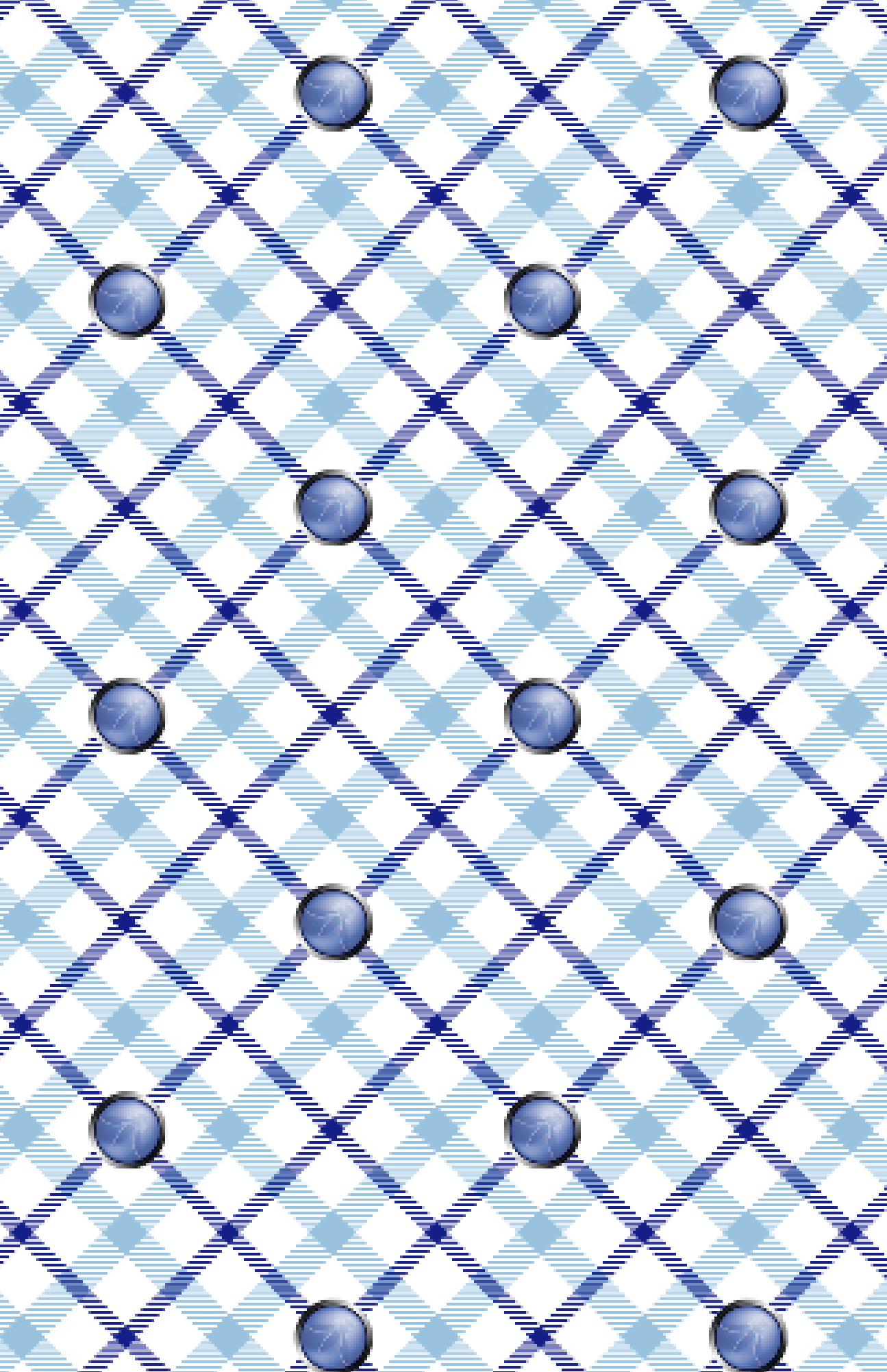
-

CAPEC

-

SAFECODE

4



CORNUCOPIA

Q

Jim can undertake malicious, non-normal, actions without real-time detection and response by the application

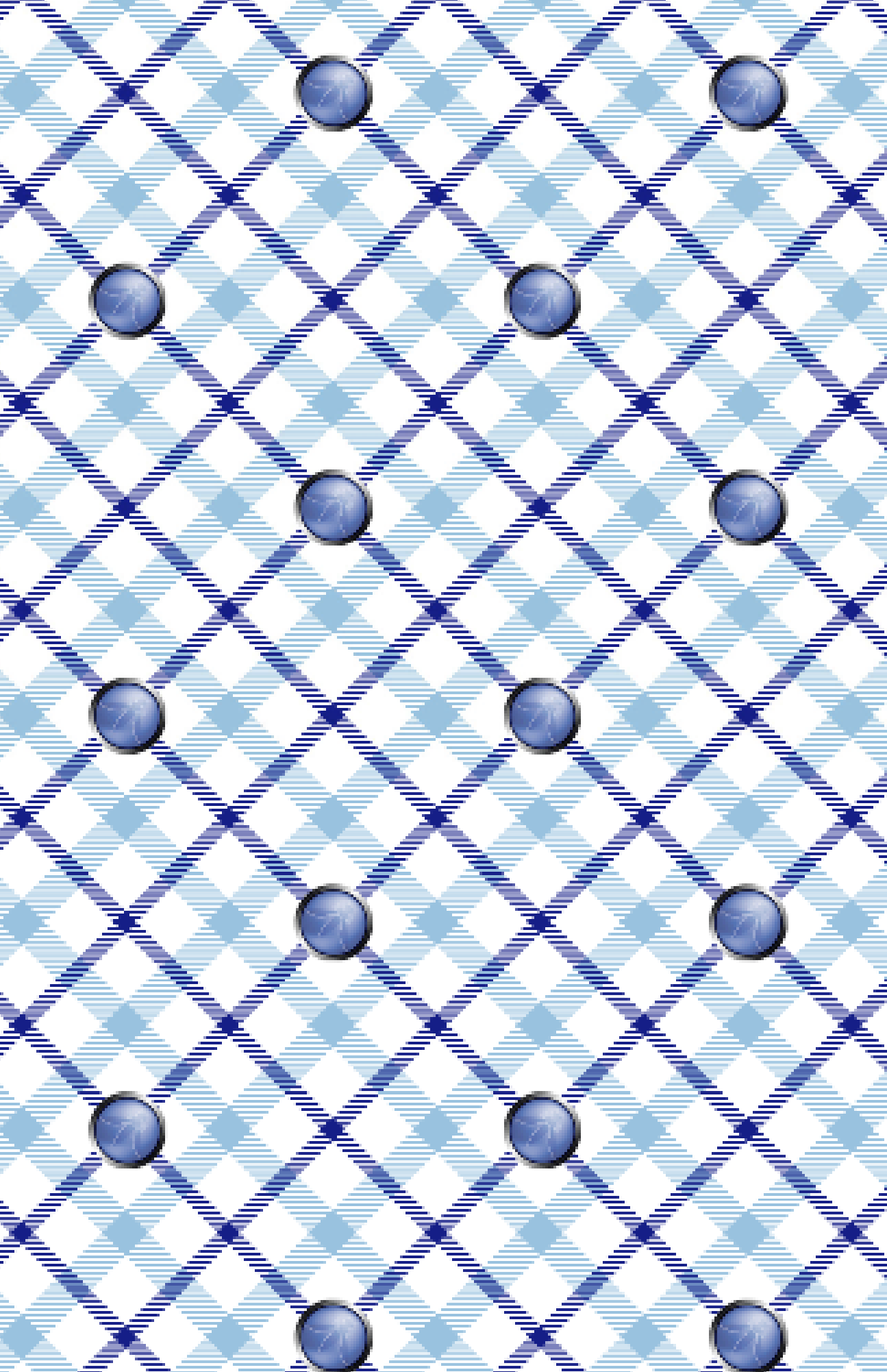
OWASP SCP
-

OWASP ASVS
-

OWASP AppSensor
(All)

CAPEC
(All)

SAFECODE
1, 27



CORNUCOPIA

K

Gareth can utilize the application to deny service to some or all of its users

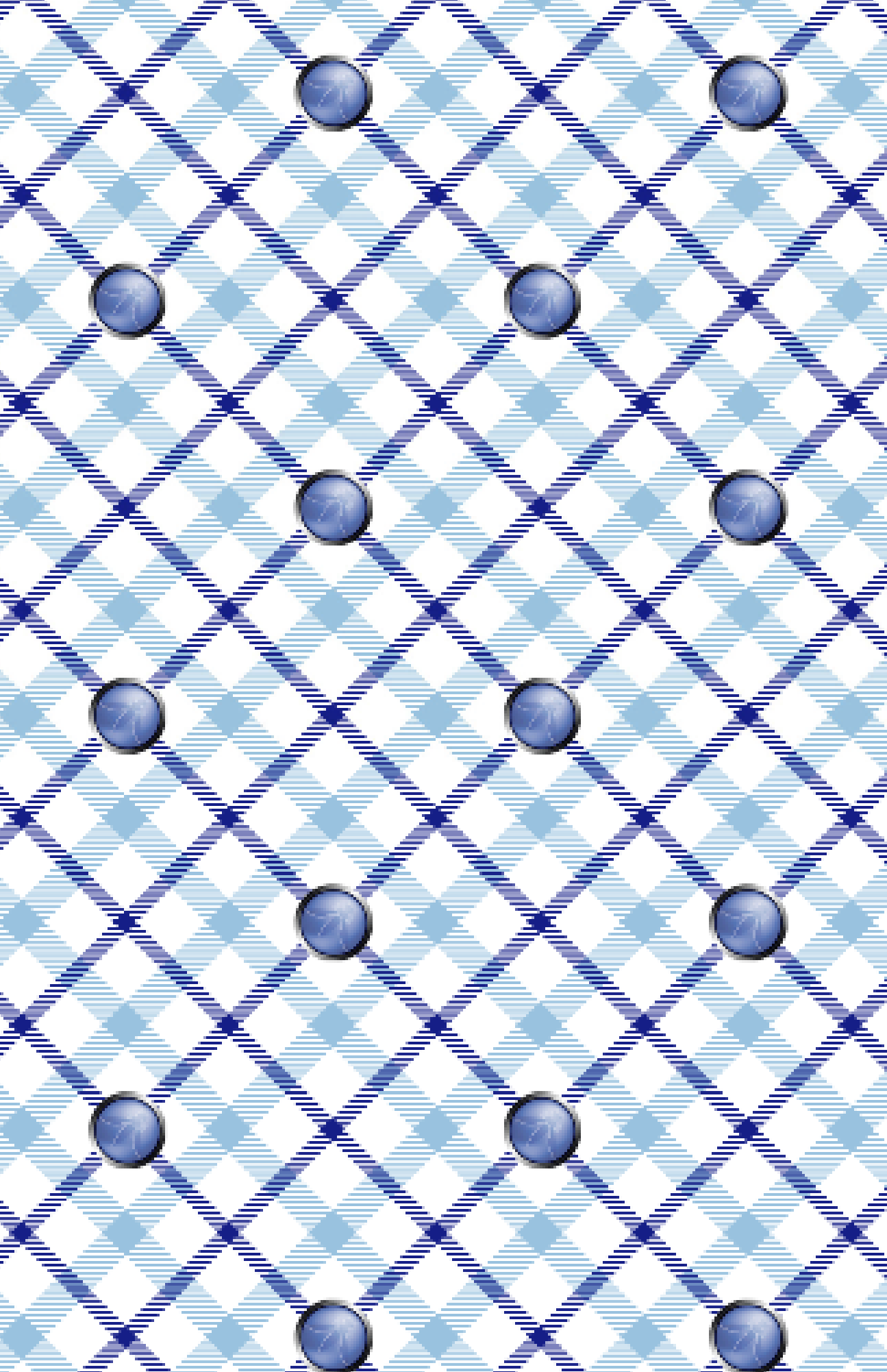
OWASP SCP
41

OWASP ASVS
-

OWASP AppSensor
UT1-4, STE3

CAPEC
2, 25, 119

SAFECODE
1

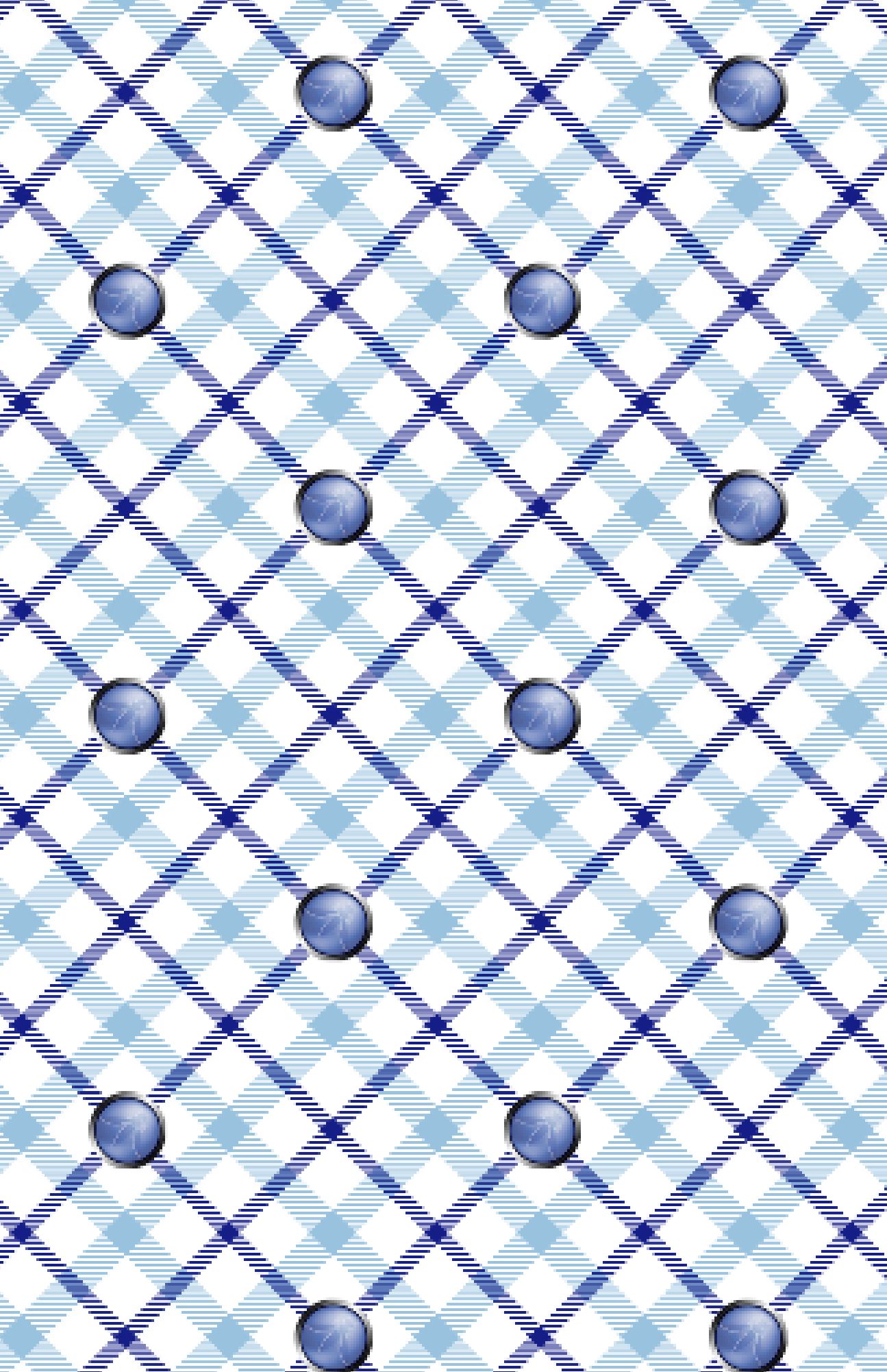


WILD CARD

Joker

Alice can utilize the application to attack users' systems and data

Have you thought about becoming an individual OWASP member? All tools, guidance and local meetings are free for everyone, but individual membership helps support OWASP's work



WILD CARD

Joker

Bob can influence, alter or affect the application so that it no longer complies with legal, regulatory, contractual or other organizational mandates

Examine vulnerabilities and discover how they can be fixed using training applications in the free OWASP Broken Web Applications VM, or using the online challenges in the free Hacking Lab