Best Practices for Mitigating Risks of a Digital Experience Platform

KEYS CONFERENCE

smoothfusion

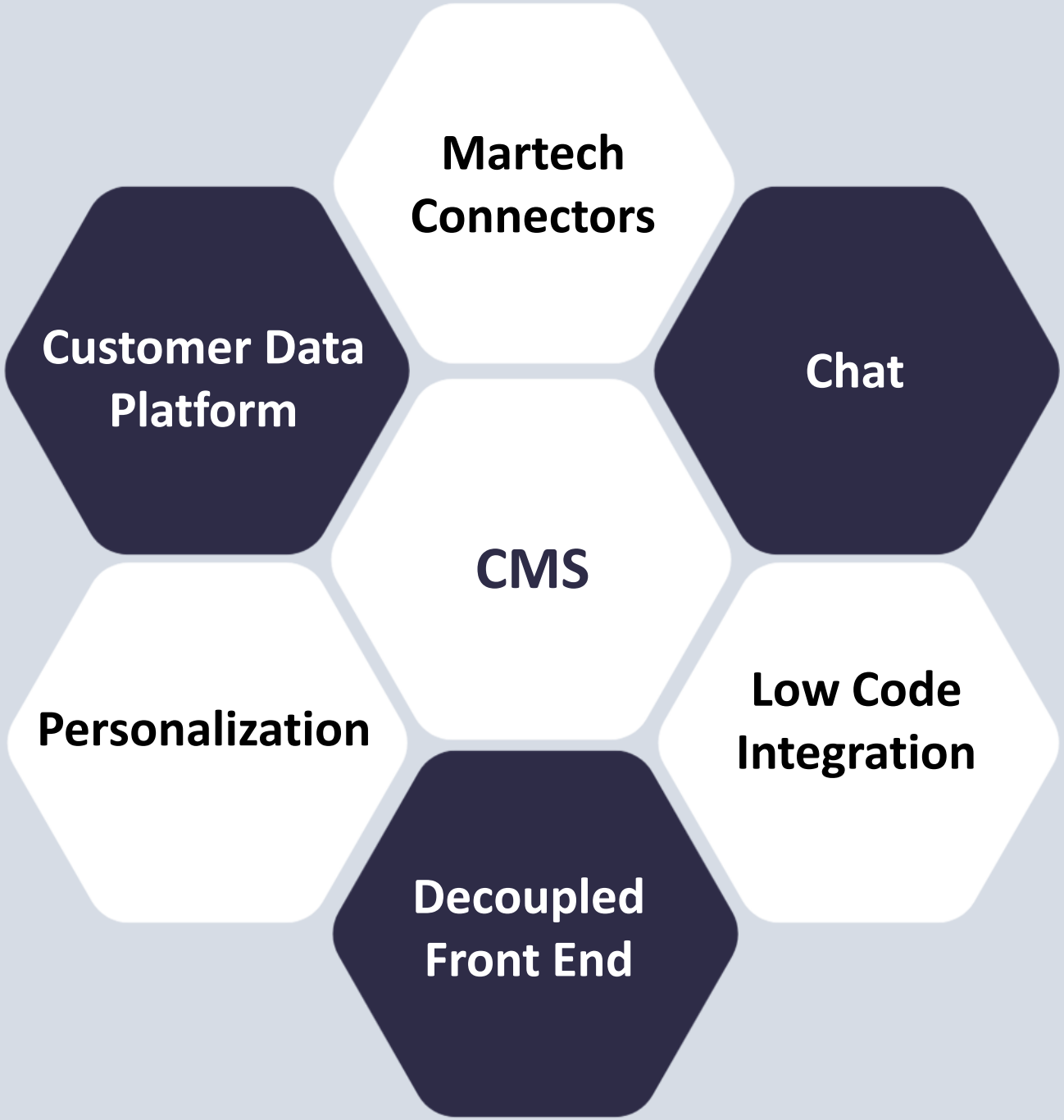
Agenda

- Define Digital Experience Platform (DXP)
- Discuss types of risks
- Explore risk mitigation
- Develop an action plan

What is a DXP?

A **digital experience platform** (DXP) is an integrated set of core technologies that support the composition, management, delivery and optimization of contextualized digital experiences.[1]

1. https://www.gartner.com/en/marketing/glossary/digital-experience-platform-dxp-



What makes up a DXP?

Types of Risk

Compliance

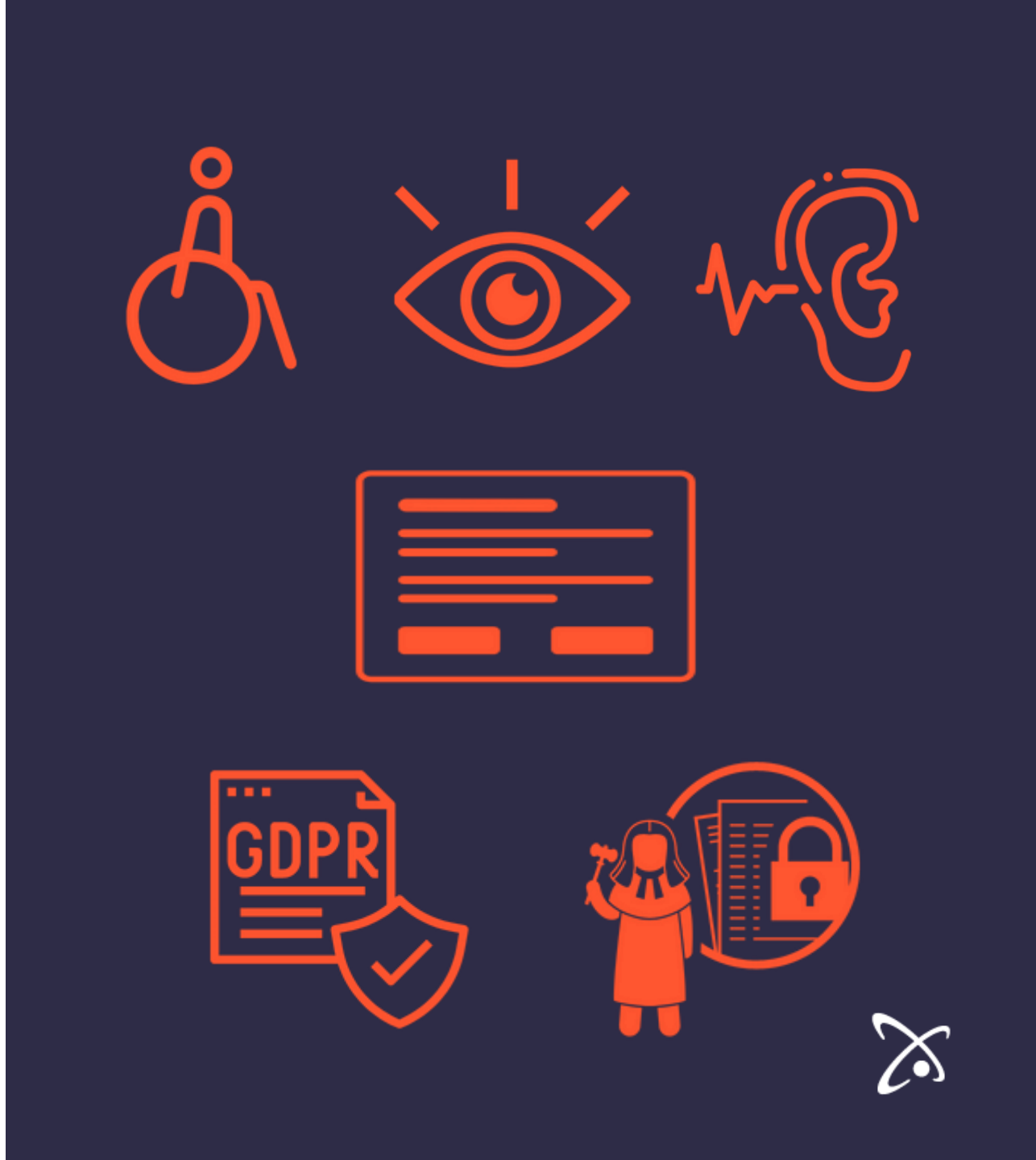
Availability

Security

Compliance

Compliance

- ADA
- Speedbumps
- Privacy Laws



WCAG/ADA/508

WCAG
Web Content Accessibility Guidelines

ADA

SECTION
508
GUIDELINES

How to Mitigate the Risk?

- Start with a design system

Overview

Components

+ Accordion
Alert
Badge
Blockquote
Breadcrumb
+ Buttons
+ Cards
Checkbox
+ Counter
Filter
+ Icons
+ Links
+ Lists
Location
+ Pagination
Paragraph
Radio
Range Input
Select
Step
Switch
Table

Buttons

Rounded

Ensure the `btn-round` class is on any buttons used.

Solid | Outlined | Gradient X | Gradient Y

Solid

Primary | Secondary | Success | Danger | Warning | Info | Light | Dark | Link

Gradient

Colors for the gradients are pulled from the `$primary` and `$secondary` color choices.

Gradient X | Gradient Y

Outlined

Solid | Secondary | Tertiary

Disabled

How to Mitigate the Risk?

- Start with a design system
- Use Browser Plug-Ins when Developing
- Use Automated Scanning Tools
- Use Workflow

Speed Bumps

Leaving Our Website

- By continuing to this link, you will be leaving our website and entering the Wild West of the internet.
- Some other legal stuff we have to say because you are leaving the comfort and security of our website to another website that we have no control over.

Stay on This Page

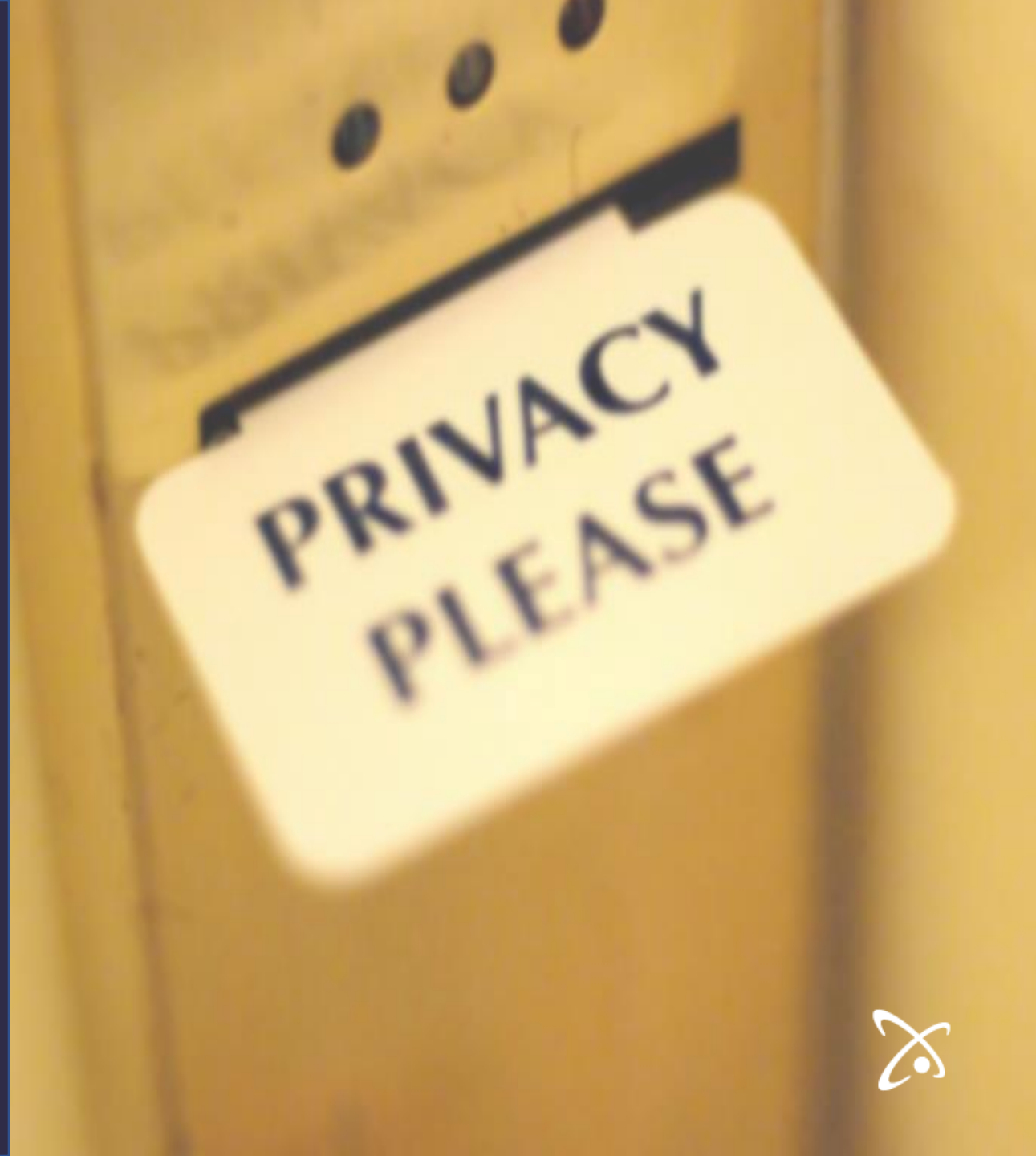
Continue

Speed Bumps

- Disclosure statements on links to third-party sites
- Reduce user confusion about ownership of sites
- Can be difficult to manage the URLs that don’t need the speed bump
- Manage a whitelist in the DXP

Privacy Laws

- Laws are changing
- Some requirements like GDPR and state specific laws are being rolled out more nationally
- Cookie acceptance banners
- Site privacy policies



Availability

DDOS

- Distributed Denial of Service
- Availability issue
- Use Cloudflare

Security

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

smoothfusion.com

Overview
Analytics
DNS
Email Beta
Spectrum
SSL/TLS
Security
Overview
WAF New
Managed Rules Moved
Firewall Rules Moved
Page Shield
Bots
DDoS
Tools Moved
Settings
Access
Speed
Collapse sidebar

Package: OWASP ModSecurity Core Rule Set

Covers OWASP Top 10 vulnerabilities, and more.

Sensitivity: Low

Action: Legacy CAPTCHA

Group	Description	Mode
OWASP Bad Robots	Detection of bad web robots that are not from search engines but perform malicious searching and spidering of web sites.	On
OWASP Common Exceptions	Special rules to reduce false positives.	On
OWASP Generic Attacks	Detection of generic attacks against web-based applications without specific knowledge of the application. Detects things like attempting to access an LDAP directory, inject shell commands, and attacks against PHP.	On
OWASP HTTP Policy	Enforcement of policies around the HTTP protocol such as methods that are supported and headers that are allowed.	On
OWASP Protocol Anomalies	Detection of unusual use of the HTTP protocol that may indicate an attack, but that may also be legitimate.	On
OWASP Protocol Violations	Detection of violations of the HTTP protocol that often indicate an attacker attempting to penetrate a site.	On
OWASP Request Limits	Detection of excessively large numbers of HTTP headers, HTTP arguments or files.	On
OWASP Slr Et Joomla Attacks	Rules to detect attacks on Joomla.	Off
OWASP Slr Et Lfi Attacks	Rules to detect LFI attacks.	On
OWASP Slr Et PhpBB Attacks	Rules to detect attacks on PHPBB.	Off

1 to 10 of 20 items

Advanced

How to Mitigate the Risk?

1 Broken Access Control

- Use the roles, permissions, groups built into the DXP

Permissions

by Section | by User | by Role

Select a section

- Global Permissions
- Classification of content
- Workflow
- Multisite management
- News
- Blogs
- Events
- Libraries
- Forms
- Lists
- Content blocks
- Pages and templates
- Module builder
- Feeds & Notifications
- Search and Indexes
- Translations
- A/B testing
- Dashboard
- Forums
- Site Sync
- Alerts
- Careers
- Locations
- People
- Positions
- Products
- Rates

Forms

Who can...

View form (?)
Everyone — Change

Create form (?)
Authors
Editors — Change

Modify form (?)
Editors
Owner — Change

Delete form (?)
Editors
Owner — Change

Change form owner (?)
Editors — Change

Change permissions (?)
Administrators only — Change

View responses (?)
Everyone — Change

How to Mitigate the Risk?

1 Broken Access Control

- Use the roles, permissions, groups built into the DXP
- Use roles, groups in CRM/External
- Protect API endpoints in Headless scenarios

CMS

API

Get, Post, Put

Mobile App/SPA

Back to Services

Edit a web service

Name

Default

URL name

default

Who can access the content by this service?

- Everyone
  Everyone can read, authenticated users can write (according to their permissions)
- Authenticated users
  Authenticated users can read and write (according to their permissions)
- Administrators only

Allow access from other domains

Allow HTTP access control (CORS) for specific domains.
Enter one domain per line.
Example:
http://www.mytrustedhost.com
https://www.mysecuredtrustedhost.com

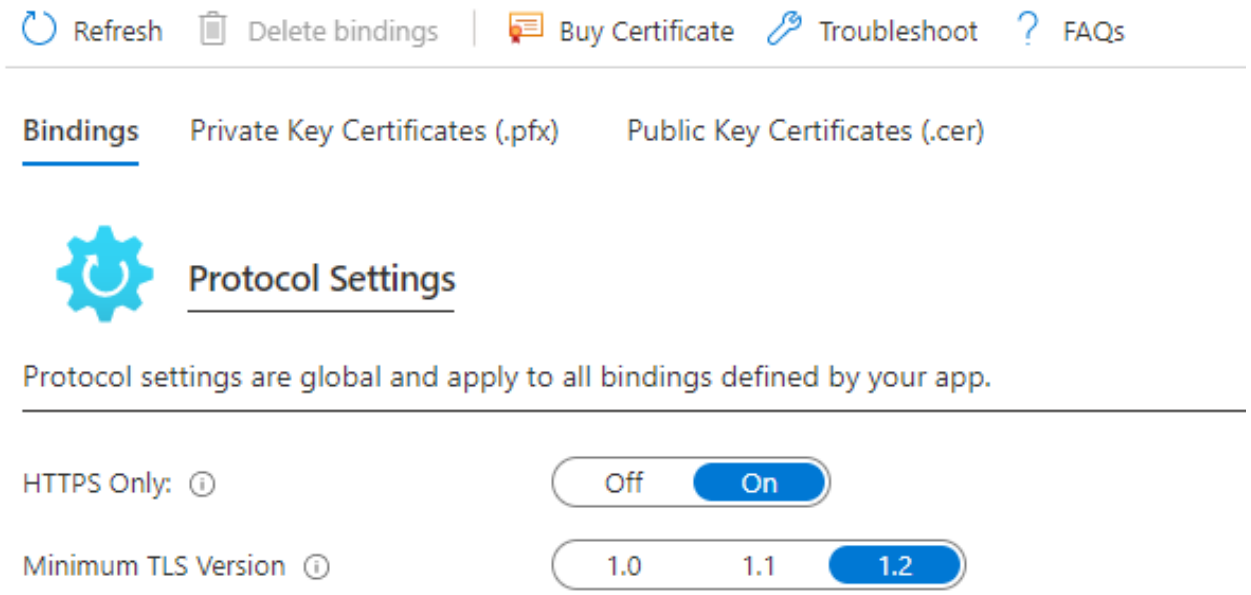
Access restriction

Create a combination of letters and numbers to restrict external calls to this service. Only users and applications providing this combination will be able to access the service.

How to Mitigate the Risk?

2 Cryptographic Failures

- Protect data in transit and at rest
- Turn off older, weaker TLS
- When sending data to other systems, use encryption



How to Mitigate the Risk?

3 Injection

- Use the API from the DXP, don’t write SQL queries
- Use a firewall to monitor the URLs

How to Mitigate the Risk?

4 Insecure Design

- Use a partner with a secure software development lifecycle
- Use a library of tested components/patterns
- Use a partner experienced in working with the DXP
- Use a partner experienced in working with FIs
- Ask for the due diligence packet
- Ask about code management and deployment
- Data in Zapier, power automate, etc. (PII In history logs)

← Zap Runs

Success

RUN ID: 00667427-b415-a786-82ab-f44807f45eb1

02. Form Submission -->Subscribe Mailchimp

February 01, 2022 - Run history for this Zap

This Zap run used the **America/Chicago** timezone - Edit Zap Details

1. Found 1 new request in Webhooks.

2022-02-01 16:03:50 - Edit This Step

Data out

Search


```
"IpAddress": "216.167.154.246",
"SubmissionTime": "2022-02-01T22:03:49.9377671Z",
"FormId": "0090dde6-0502-4c67-9f38-c2e2b46ea147",
"FormName": "sf_subscriberform",
"FormTitle": "Subscriber Form",
"FormSubscriptionListId": "00000000-0000-0000-0000-000000000000",
"SendConfirmationEmail": false,
"Controls": [
  {
    "FieldControlName": "Email",
    "Id": "0b30c80d-8ed5-4ea7-9b9b-c2ea0e567661",
    "SiblingId": "00000000-0000-0000-0000-000000000000",
    "Text": null,
    "Type": 0,
    "Title": "Email Address",
    "FieldName": "EmailTextFieldController",
    "Value": "bhunt@bhunt.com",
    "OldValue": null
  }
],
"NotificationEmails": [],
"Origin": null
```

How to Mitigate the Risk?

5 Security Misconfiguration

- Missing appropriate security hardening across any part of the application stack
- Unneeded features enabled
- Missing Security Headers
  - HTTP Strict Transport Security (HSTS)
  - Content Security Policy (CSP)
  - Cross Site Scripting Protection (X-XSS)
  - X-Frame-Options
  - X-Content-Type-Options

Web security

SECURITY POLICY	ENABLED	HTTP HEADER	
Trusted sources Load scripts, styles, fonts, videos, and so on from trusted sources only	✓	`Content-Security-Policy`	Edit
Public keys for web servers Associate a public key with a certain web server	✗	`Public-Key-Pins`	Edit
Referrer information Control which referrer information your pages send	✓	`Referrer-Policy`	Edit
HTTP strict transport security Allow access and send data only when using HTTPS, instead of HTTP	✓	`Strict-Transport-Security`	Edit
Prevention of styles and scripts sniffing Prevent browsers for MIME type content sniffing	✓	`X-Content-Type-Options`	Edit
Control of embeding your content Control the rendering of your pages in <iframe> or <object> on other sites	✓	`X-Frame-Options`	Edit
Prevention of cross-site scripting attack Stop pages from loading when cross-site scripting attacks are detected	✓	`X-XSS-Protection`	Edit

TRUSTED SOURCES

Enable trusted sources

Load scripts, styles, fonts, videos, and so on from trusted sources only

Removing any of the trusted sources from the lists below may cause serious problems with your sites or Sitefinity CMS.

Trusted sources for...

Syntax reference

Any content (?)

'self'

Scripts

www.google.com
*.google-analytics.com
*.googletagmanager.com
apis.google.com

Styles

platform.twitter.com/css/
*.twimg.com
*.typekit.net

Fonts, images, video and audio

Forms, frames, child sources, connect sources, plugins

Report URL (?)

Done or Cancel

How to Mitigate the Risk?

6 Vulnerable and Outdated Components

- Keep your CMS/DXP up to date
- Regular Vulnerability Scanning
- Microsoft Defender for Cloud
- Open-source vs Closed

How to Mitigate the Risk?

7 Identification and Authentication Failures

- Use MFA everywhere
- Use password managers
- Don’t roll your own authentication, use Azure AD
- Remove access to CMS and all components for employees who depart

How to Mitigate the Risk?

8 Software and Data Integrity

- Vulnerabilities in npm packages
- Establish review process for code and config
- Ensure CI/CD pipeline has appropriate controls

How to Mitigate the Risk?

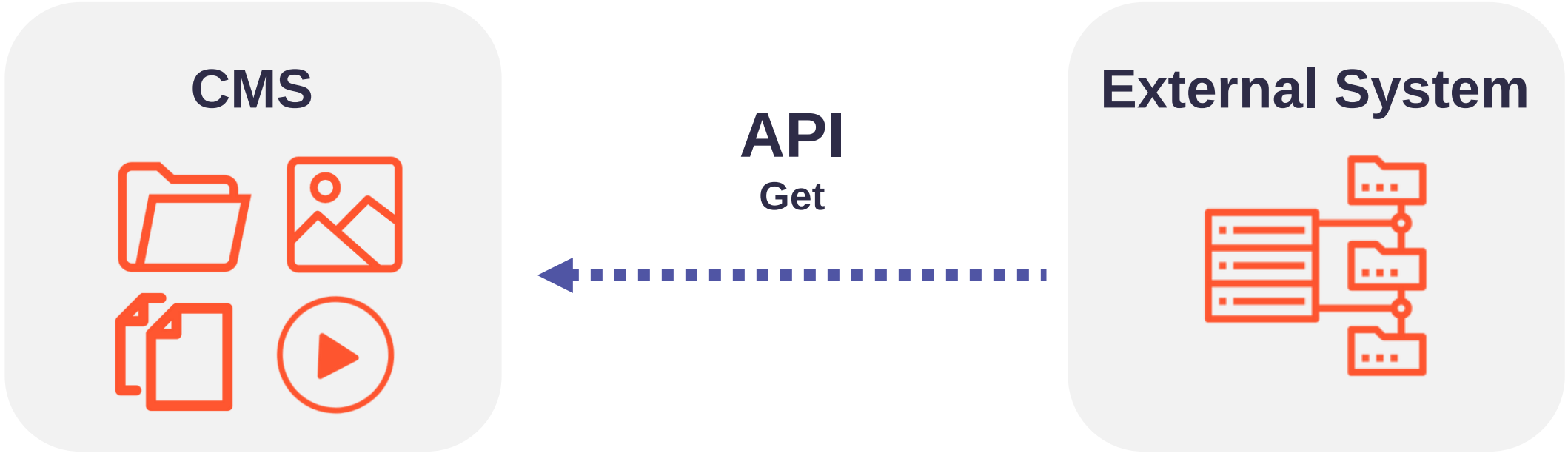
9 Security Monitoring and Logging

- Add audit logging to you DXP
- Log API events
- Review history logs from other systems, i.e. automation
- Use Cloudflare for monitoring

How to Mitigate the Risk?

10 Sever-Side Request Forgery

- SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL.
- It allows an attacker to coerce the application to send a crafted request to an unexpected destination.


CMS
API
Get
External System

Develop an Action Plan

- Be proactive in talking with marketing team
- Document the systems used including CMS/DXP and other components
- Document data flow
- Review OWASP Top 10 to see what is relevant
- Incorporate findings into incident response plan
- Test, improve, repeat

KEYS CONFERENCE

DON'T FORGET!

Fill out the survey to get your sticker!

Questions?

Upcoming Sessions

TANDEM

Creating an Effective Incident Response Plan

Lindsey McReynolds, Tandem

RISK & COMPLIANCE

CoNetrix Security Auditors: A Panel Discussion

Mark Faske, Bret Mills, Mark Riff, & Ty Purcell, CoNetrix Security

CYBERSECURITY

Understanding the Value of Your SIEM and SOC

Mike Richline, CoNetrix Technology

KEYS CONFERENCE

Thanks for joining!

Brad Hunt

President

Smooth Fusion

Dusty Ellis

Customer Success Manager

Smooth Fusion