Data Protection Standards

Team 1: Chan KeiYiu Yvone, HungWei Lin, Thien Liu, Yusuf Fahry

Discussion

- Target
  - https://loadedwithstuff.co.uk
- Standards
  - ICO (2020) – General Data Protection Regulation (GDPR)
  - PCI Security Standards (2020)
  - HIPPA (2020)
- Which standards would apply to the target?
- How to evaluate if the target meets the standards
- Recommendation on the target to meet those standards

GDPR - Overview

- Introduced by Information Commissioner's Office (ICO) in the European Union (EU) in April 2016.
- Effective on 25 May 2018.
- Replaces the Data Protection Directive (DPA) of 1995.
- Applies to all entities that deal with the user data of EU residents.

GDPR – Commonly Used Terms

Data Subject	A natural person who can be identified by their personal data
Personal Data	Name, age, email, phone number, health, biometrics, etc
Controller	An entity that decides why and how to process the personal data
Processor	An entity that processes the data on behalf of the controller
Processing	Operations performed on data (collect, store, modify, erase, etc.)
Supervisory Authority	Public authority who monitors the exercise of data protection regulation
Pseudonymisation	A technique of data processing in a manner that the personal data can no longer be associated with a data subject without the use of additional data

GDPR Compliance checklist

- A privacy policy page should be accessible via a link on every page of the website
- Email marketing services will need users' permission before being sent
- Users should be able to opt out of emails at any time.
- Cookie banner is available
- Forms to collect user data should include a privacy statement and an opt-in option

GDPR - Recommendations

- Create an accessible privacy and policy page to inform site's visitors about how the webiste collect, use, store, and disclose their personal data.
- Users have to verify their email address after subcribing to newsletter.
- Allow users to unsubscribe from newsletter without any difficulty
- Use cookie banner to inform visitors about how the website uses cookies, what information will be stored, and user right to refuse the storage of cookies.
- Add privacy statement where user data will be collected and an opt-in option to get user consent to collect data

PCI DSS - Overview

- 1.Risk management
  - Your business identifies, assesses and manages information security risks.
- 2.Information security policy
  - Your business has an approved and published information security policy which provides direction and support for information security (in accordance with business needs and relevant laws and regulations) and is regularly reviewed.
- 3.Secure storage
  - Your business has secure storage arrangements to protect records and equipment in order to prevent loss, damage, theft or compromise of personal data.

PCI DSS – Overview (cont.)

- 4.Secure disposal
  - Your business has a process to securely dispose of records and equipment when no longer required.
- 5.User access controls
  - Your business assigns user accounts to authorised individuals, and manages user accounts effectively to provide the minimum access to information.
- 6.System password security
  - Your business has appropriate password security procedures and 'rules' for information systems and has a process in place to detect any unauthorised access or anomalous use.
- 7.Patch management
  - Your business keeps software up-to-date and applies the latest security patches in order to prevent the exploitation of technical vulnerabilities.
- 8.Boundary firewalls
  - Your business has boundary firewalls to protect computers from external attack and exploitation and help prevent data breaches.

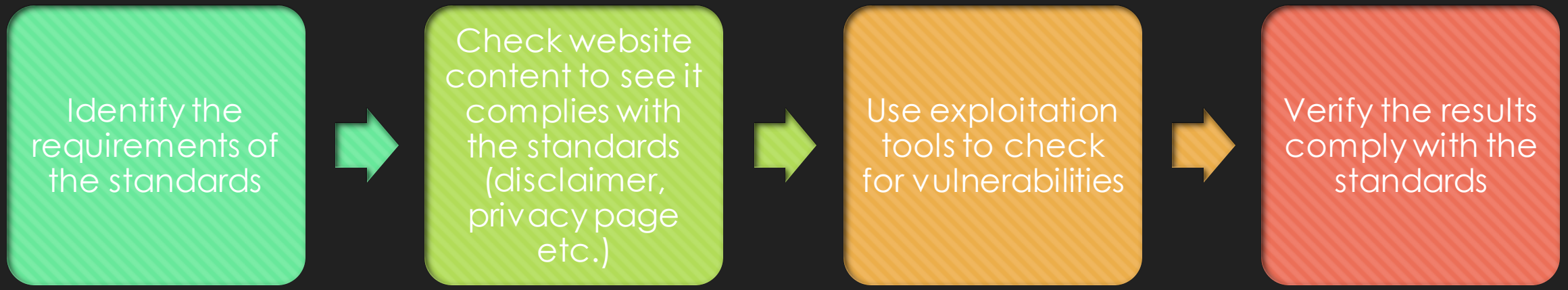
PCI DSS Checklist

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need to know
- Assign a unique ID to each person with computer access

PCI DSS Recommendations

- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for all personnel

Proposed checking workflow



Proposed tools and checking areas

Tool	Purposes	Checking points
The Harvester	• Accurately catalog the target's email addresses and subdomains (Martorella, 2019)	GDPR - User access controls PCI DSS - Restrict access to cardholder data by business need to know
NMAP	• Perform port scanning and network mapping to identify open ports • Determine the target's available services (nmap.org, 2022)	GDPR - User access controls PCI DSS - Restrict access to cardholder data by business need to know
Nessus and Nikto	• Automate the web scanning process for vulnerabilities, out-of-date and unpatched software • Search for dangerous files on web servers (Engebretson, 2013)	GDPR – Patch management PCI DSS - Use and regularly update anti-virus software or programs

Proposed tools and checking areas (cont.)

Tool	Purpose	Checking points
Metasploit framework	• Provides exploit management (lookup, update, documentation) and a plethora of payloads (tasks performed after successful target system exploitation) (Holik, 2014)	GDPR – Secure Storage
Burp Suite	• Actively or passively scan web applications' vulnerabilities • Intruder and sequencer options to perform brute force attacks or fuzz testing (PortSwigger, 2020)	OWASP Top Ten (refer to Potential Risks)

References

- Information Commissioner's Office. (N.D.) Data protection self assessment. Available from : https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/ [Accessed 29 Apr 2022]
- PCI Security Standards Council. (N.D.) Document Library. Available from: https://www.pcisecuritystandards.org/document_library [Accessed 29 Apr 2022]