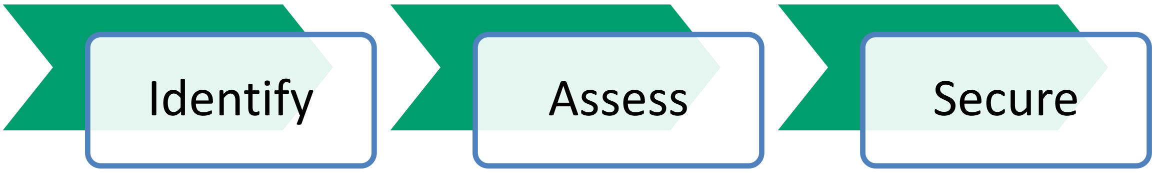
AppCheck and GDPR Compliance

CONTENTS

1. GDPR & APPCHECK AT A GLANCE

There is no doubt that the GDPR is serious business. AppCheck has noticed a significant shift in focus by company executives, taking a much more active interest in security matters since the GDPR, and specifically the fines were introduced. Naturally, with that comes a never-ending list of vendors claiming to solve the GDPR problem. In truth, no one product or service can achieve compliance, rather the GDPR requires a strategy that includes a thorough understanding of your responsibilities, exposure and requirements to demonstrate compliance with the six principals of the GDPR.

AppCheck has a significant part to play in your compliance strategy, this document highlights some existing and new features introduced to support compliance with the GDPR.



Identify

Assess

Secure

Identify website components that collect Personally Identifiable Information (PII).

Perform a security assessment to identify vulnerabilities that could lead to a data breach. Identify website components that are not GDPR compliant.

Provide a detailed remediation plan to resolve vulnerabilities and compliancy failings. Rescan and track remediation efforts throughout the process

1.1. BRIEF INTRODUCTION TO THE GDPR

The General Data Protection Regulation (GDPR) is a replacement for the EU Data Protection Directive (DPD) and will replace the UK's Data Protection Act to provide a regulation which is used across all EU member states.

The GDPR is very similar in spirit to the existing DPA that has been in effect in the UK for some time, but with significant enhancements.

Perhaps the most well-known of these are the fines. Previously, fines under the DPA were capped at £500,00, however, with the introduction of the GDPR, Severe non-compliance penalties can hit €20m or 4% of the organisations global turnover, whichever is greater.

To compound this, the reach of the GDPR has increased both in terms of the geography and who can be held to account for non-compliance. The GDPR applies to all companies that offer goods and/or services to EU residents regardless of where they reside. Unlike the outgoing DPD, Data Processor* as well as a Data Controllers can be held liable for non-compliance.

Further information on the GDPR can be found at the official website https://www.eugdpr.org/ and also on the UK's Information Commissioners Office website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

* A Data Controller is the person or business who determines the purpose and method for processing personal data. The Data Processor is anyone who processes (and/or stores) personal data on behalf of the controller.

1.1.1. BREXIT

When the UK leaves the EU, the new UK Data Protection Bill will adopt the GDPR in its entirety. Therefore, you should consider Brexit as making no difference to your GDPR compliance strategy.

2. OVERVIEW OF APPCHECK AND GDPR

2.1. IDENTIFY

One of the initial challenges facing organisations when preparing for GDPR is identifying and documenting all the places Personally Identifiable information (PII) is captured and stored.

To assist with this, AppCheck has introduced several new features.

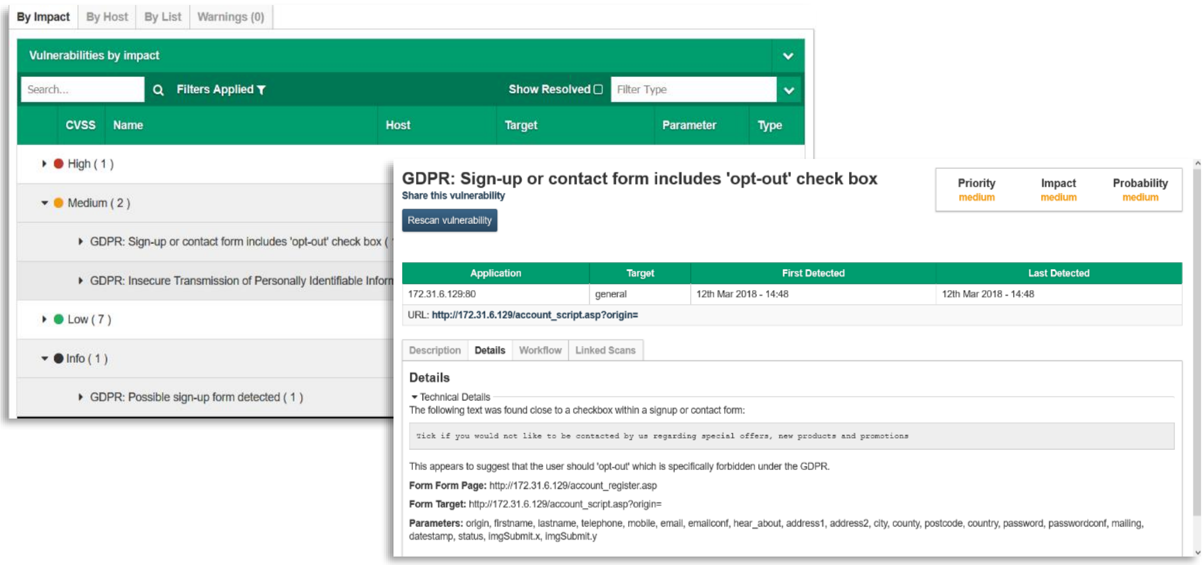
2.1.1. PII Data Collection identification.

AppCheck has added a new module that identifies any form that requests PII data from the user. Whilst in many cases forms of this nature are well known to the organisation, there may be some that are overlooked. For example, signup forms to receive a newsletter may not be at the forefront of your GDPR strategy, yet they could still be accumulating PII data which gets overlooked.

2.1.2. Non-compliant consent collection.

Obtaining clear consent for the collection, storing or processing of PII data is a key requirement of the GDPR. The previous DPD was a little ambiguous when it came to what is and what isn't deemed consent. This ambiguity meant that many organisations implemented a "opt-out" checkbox or implied consent through the act of registering (with the terms of that consent buried away in the T&C's). The GDPR has cleared up this ambiguity and states that Consent requires a positive opt-in. The use or pre-ticked boxes or any other method of default consent is specifically forbidden under the GDPR.

AppCheck includes a new module to flag forms collecting PII data that appear to be non-compliant. Opt-out check boxes, forms that appear to apply default consent and pre-checked acceptance tick boxes are reported.



GDPR: Sign-up or contact form includes 'opt-out' check box

Priority	Impact	Probability
medium	medium	medium

Application	Target	First Detected	Last Detected
172.31.6.129:80	general	12th Mar 2018 - 14:48	12th Mar 2018 - 14:48

URL: **http://172.31.6.129/account_script.asp?origin=**

Details

Technical Details

The following text was found close to a checkbox within a signup or contact form:

```
Tick if you would not like to be contacted by us regarding special offers, new products and promotions
```

This appears to suggest that the user should 'opt-out' which is specifically forbidden under the GDPR.

Form Form Page: http://172.31.6.129/account_register.asp

Form Target: http://172.31.6.129/account_script.asp?origin=

Parameters: origin, firstname, lastname, telephone, mobile, email, emailconf, hear_about, address1, address2, city, county, postcode, country, password, passwordconf, mailing, datestamp, status, imgSubmit.x, imgSubmit.y

2.1.1. INSECURE DATA CONNECTION

Any component that collects PII data is examined weaknesses within transport security such as transmission of user credentials over clear-text and insecure data caching.

2.2. ASSESS

The real strength of AppCheck lies within its ability to detect critical impact vulnerabilities that could lead to a data breach. Whilst it is important that all security vulnerabilities within your web applications be addressed, some pose a more immediate threat than others. The GDPR Scan profile focuses on vulnerabilities that when exploited provide unauthorised access to databases and hosted systems. The table below highlight some of the checks performed by AppCheck, note these are some examples from thousands of checks performed during an AppCheck scan.

Component	Detail
Critical Impact Vulnerabilities.	2.2.1. Injection Vulnerabilities The *Injection* class of vulnerabilities has remained at the number one spot in the OWASP Top 10 since 2010 and remains so in the most recent release in late 2017. Injection flaws, such as *SQL*, *NoSQL*, *OS*, and *LDAP* injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. AppCheck performs comprehensive checks for a wide range of injection vulnerabilities including; *SQL, NoSQL, XPath, Code, Command Injection, LDAP* Injection and Expression Language Injection The AppCheck Vulnerability Analysis Engine provides detailed rationale behind each finding including a custom narrative to explain the detection methodology, verbose technical detail and proof of concept evidence through safe exploitation. 2.2.2. Broken Access Control Vulnerabilities While crawling an application, AppCheck analyses session tokens to identify security flaws such as insufficient entropy and other common session management flaws that could permit session token prediction. AppCheck also includes configurable password guessing modules to identify weak account credentials within systems such as; HTML Form Authentication, Outlook Web Access (OWA), Content Management Systems (e.g. WordPress), NTLM/Basic Authentication, Management systems and SSL VPN gateways.

Component	Detail
	2.2.3. Sensitive Data Exposure AppCheck includes multiple Modules to identify sensitive data disclosure vulnerabilities including: Insufficiently protected administrative interfaces, Publicly accessible source code repositories such as GIT and SVN, Hidden files and backups. A new module introduced in February 2018 will optionally identify misconfigured server-side caching systems that could disclose sensitive user information to other application users. 2.2.4. Insecure Components and Systems AppCheck includes a regularly updated database containing thousands of known vulnerabilities within content management systems, application frameworks, server and client-side components. If configured to do so, AppCheck will perform a comprehensive infrastructure assessment against all IP addresses and web applications defined within the scope. 2.2.5. Insecure File Upload Components Insecure file upload components could allow a malicious attacker to gain remote code execution on the affected Web Server and therefore gain access to sensitive data held on the server and on locally accessible systems. AppCheck audits the web application for vulnerabilities such as; Unrestricted upload and execution of server-side scripts (asp, aspx, jsp, php and cfm), Insecure unpacking of zip and tar based archives (path traversal), Insecure filename handling (path traversal and null truncation)
User Registration / Clear Text Password Storage	Storing passwords in clear-text or using reversible encryption could greatly increase the impact or a successful attack against the system, and could lead to a significant data breach that would otherwise be limited by secure password storage. The following statement is included with ICO guidelines: *“Secure handling of passwords is a final measure which reduces the adverse consequences of an otherwise successful attack which has defeated other security measures.”* 2.2.6. Detecting Clear Text password storage AppCheck attempts to automatically register an account on the system using an email address that is later received by the Sentinel out-of-band monitoring system. The same email address is used within password recovery forms to determine if the password submitted during registration is sent back to the user.

Component	Detail
	If Sentinel receives the registered password via email, then the application must either store the password in Clear Text or using reversible encryption. This presents significant vulnerability since any attacker who gains access to the user database and/or application is likely to also have access to users clear-text passwords. **References** https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf
Second Order Cross-Site Scripting (XSS)	Stored Cross-Site Scripting (XSS) vulnerabilities occur when data submitted to the application is not properly handled (filtered or sanitised) before being embedded pages rendered by other users. The malicious attacker could exploit this flaw to embed JavaScript code within the application that would then be executed by other users. It's common to find Personally Identifiable Information (PII) is accessible by exploiting Second Order XSS. Commonly vulnerable systems include; CRM systems, Newsletter management, Order Processing, Blogs, Analytics and other user feedback systems. 2.2.7. Delayed Execution Typically, application vulnerabilities are detected in-band by submitting specially crafted input to the application the vulnerability is then detected based upon the applications response. Common indicators include specific time delays, page response structure and data returned within the page. However, some vulnerabilities may only occur as the result of user interaction or processing that occurs outside of the scan window. This can also include other integrated systems that are not directly tested by AppCheck. For example, consider a CRM system used to manage user data submitted through a public facing website. If the CRM platform does not render data securely, it may be vulnerable to Cross-Site Scripting. The attacker could target this system by submitting a malicious JavaScript payload (via the public web site) designed to exfiltrate data from the CRM system when it is later executed. 2.2.8. Detecting Delayed Execution This module is designed to detect Second-Order Cross-Site Scripting (XSS) vulnerabilities by submitting payloads designed to trigger an Out-of-band connection to our Sentinel monitoring system. Upon execution, the injected payload reports (encrypted); the initial injection point, the page in which the payload renders and a copy of the current page so that it can be later reviewed.

2.3. SECURE

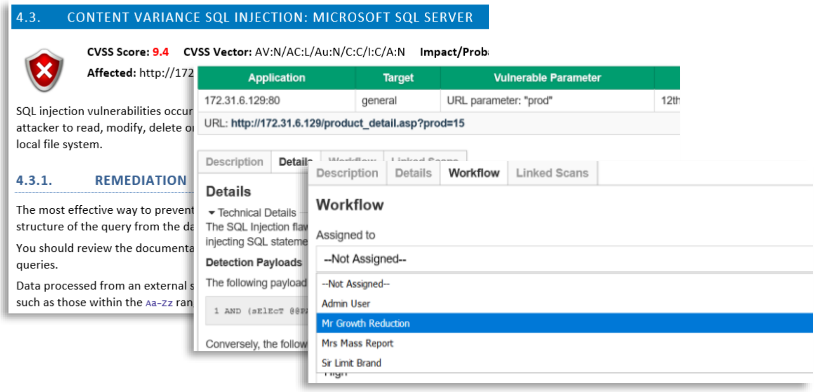
2.3.1. REPORTING & REMEDIATION

Each finding reported by AppCheck includes a detailed remediation steps backed by our workflow management system and the ability to rescan individual vulnerabilities. Critical impact vulnerabilities are safely exploited to provide proof of concept evidence to support remediation efforts and help demonstrate impact to the business.

Results Management

Each finding is backed by a detailed technical narrative with comprehensive remediation advice.

Findings can be assigned to members of your team and tracked through the remediation lifecycle. Rescanning of individual vulnerabilities, and integration with popular bug tracking systems such as Jira work to support your remediation and validation process.



4.3. CONTENT VARIANCE SQL INJECTION: MICROSOFT SQL SERVER

CVSS Score: 9.4 **CVSS Vector:** AV:N/AC:L/Au:N/C:C/I:C/A:N **Impact/Prob**

Affected: http://172

SQL injection vulnerabilities occur
attacker to read, modify, delete o
local file system.

4.3.1. REMEDIATION

The most effective way to prevent
structure of the query from the da

You should review the documenta
queries.

Data processed from an external s
such as those within the Aa-Zz ran

Application	Target	Vulnerable Parameter	
172.31.6.129:80	general	URL parameter: "prod"	12th

URL: **http://172.31.6.129/product_detail.asp?prod=15**

Details

Technical Details
The SQL Injection flaw
injecting SQL stateme

Detection Payloads

The following payload

```
1 AND (sElEcT @@P
```

Conversely, the follow

Workflow

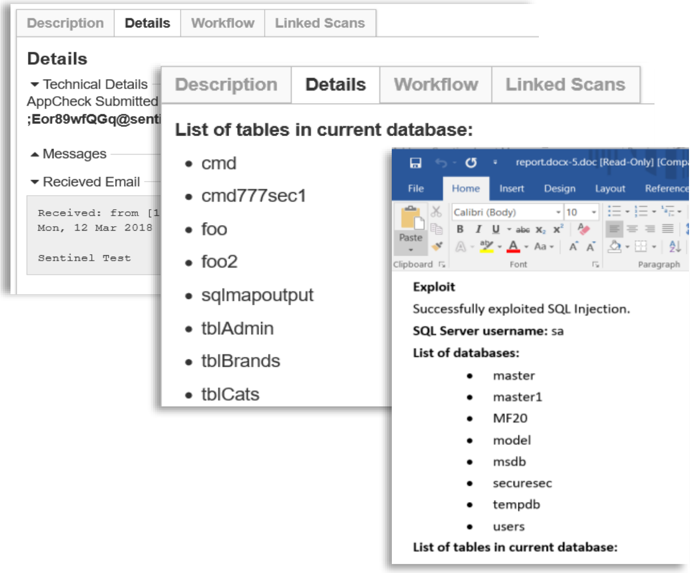
Assigned to

--Not Assigned--

- --Not Assigned--
- Admin User
- Mr Growth Reduction
- Mrs Mass Report
- Sir Limit Brand

Safe Exploitation

When safe to do so, vulnerabilities are safely exploited to demonstrate their impact. For example, SQL Injection vulnerabilities are exploited to list accessible tables, providing you with solid evidence to demonstrate vulnerability impact to the organisation.



Details

Technical Details
AppCheck Submitted
;Eor89wfQGq@senti

Messages

Recieved Email

```
Received: from [1
Mon, 12 Mar 2018

Sentinel Test
```

List of tables in current database:

- cmd
- cmd777sec1
- foo
- foo2
- sqlmapoutput
- tblAdmin
- tblBrands
- tblCats

report.docx-5.doc [Read-Only] [Compa

Exploit

Successfully exploited SQL Injection.

SQL Server username: sa

List of databases:

- master
- master1
- MF20
- model
- msdb
- securesec
- tempdb
- users

List of tables in current database: