Deloitte.

COMPANY X Services Inc.

Draft Report for Client Web Portal

February 27, 2018

Statement of Responsibility

The Report is being prepared solely for COMPANY X Services Inc. (hereafter also referred to as "COMPANY X" or the "company"). The use may not meet the requirements or objectives of any other party.

Our work is carried out under a Statement of Work with reference TS/suh/18-1234 from January 16, 2018 between Deloitte Risk Advisory B.V. (hereafter also referred to as "Deloitte") and COMPANY X. The scope and objectives of this review are summarised in the Management Summary. The matters raised in this report are only those which came to our attention during our review and are not necessarily a comprehensive statement of all weaknesses that exist or all actions that might be taken.

No other party is entitled to rely upon the report for any purpose whatsoever and if they do choose to rely upon the report, it will be at their own risk and without recourse to Deloitte. Should others choose to place reliance upon any matters which we have reported they are responsible for carrying out their own independent investigations. Accordingly, to the fullest extent permitted by law, readers agree that Deloitte will have no duty or liability to them in any way in connection with or arising from the report.

This work was performed under limitations of time and scope that are not potentially relevant to the actions of a malicious attack. Our work is based at a specific point in time, in an environment where both the systems and the threat profiles are dynamically evolving. It is therefore possible that vulnerabilities exist or will arise that were not identified during our review and there may or will have been events, developments and changes in circumstances subsequent to its issue which are likely to render the report's contents wholly or partly misleading or inaccurate.

Private and confidential

This document is provided solely for Company X informational purposes and internal use, and is not intended to be and should not be used by any person or entity other than Company X without the written permission of Deloitte.

This document does not in any way contain an expression of an opinion or any other form of assurance on Company X financial statements or any part thereof, nor an opinion or any other form of assurance on Company X internal control systems or its compliance with laws, regulations, or other matters.

This report is confidential. It includes technical details of security weaknesses that if available to untrusted parties could facilitate the execution of a breach against Company X. For that reason, access to this report should be restricted, and the report should not be published.

Table of contents

Management Summary

COMPANY X Services Inc. (hereafter also referred to as "COMPANY X" or the "company") engaged Deloitte Risk Advisory B.V. (hereafter also referred to as "Deloitte") to perform a time limited security assessment of the Client Web Portal application and its underlying host in a production environment. Our testing approach combines the use of automated scanning tools and manual techniques. This assists with the identification of physical and logical security vulnerabilities, patching deficiencies and misconfigurations, in order to make mitigation recommendations.

The results in this report are based on the analysis we performed remotely via the Internet from February 16 to February 27, 2018. This report provides an indication of the security posture of the in-scope systems as of the last day of the testing period.

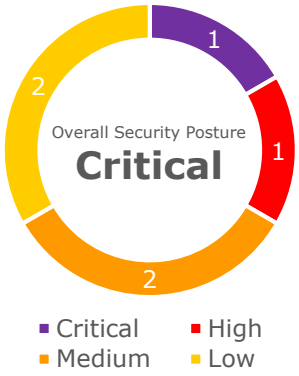
Assessment Scope

The scope of the assessment is defined below; please see appendix for a more detailed scope:

Target	Description
https://www.example.com	Client Web Portal provides a business social network platform for an organisation to engage collaboratively.

Table 1: Scope of the assessment

During this assessment, 1 critical, 1 high and 2 medium risk vulnerabilities were identified. 2 low risk vulnerabilities were also identified. These vulnerabilities could lead to compromise of the confidentiality, integrity and availability of the data held within the Client Web Portal application.



The security posture of the Client Web Portal identified during this assessment is illustrated on the figure shown on the left. Based on the highest identified risk rating, the exposure level at the time of testing of Client Web Portal is considered **Critical**

For further details and a more technical description of all identified observations and our recommendations, please refer to the Detailed Observations section and the appendix of this report, which also details Deloitte's methodology.

Figure 1: Overall Security State

Key observations and recommendations

A summary of the key observations identified and actions to mitigate or to reduce the risks can be seen below:

- **Outdated and vulnerable software version identified** - Outdated software containing known security vulnerabilities is used on the web server which allow an attacker to gain unauthorized access to confidential data stored on the server such as credit card information. Moreover, once the server has been taken over it can be used to perform further attacks on the network and against other companies
  Recommendation: Update the software to the latest stable release that includes all security updates. We also recommend implementing a patch process in order to identify vulnerable software versions in a timely manner.
- **Stored cross-site-scripting** - In the Client Web Portal a vulnerability known as XSS allows an attacker to inject malicious code into the website. This can lead to a take-over of the user session which can be used to perform unauthorized data alterations on behalf of a legitimate user;

Recommendation: We recommend applying input filtering to all input fields and URL parameters in the entire application to assure that only valid input is processed.

- **Cross-Site Request Forgery (CSRF):** An existing session can be abused by a malicious user using a technique known as CSRF. This allows a malicious user to perform actions using the permissions of the currently logged in user and could lead to unauthorized payments.
  Recommendation: We recommend including an additional unpredictable token in every function that performs sensitive actions. The unpredictable token should be unique (i.e. should change) per user session or per request.
- **Mail server can be abused for sending spam:** The mail service hosted on the same server as the Client Web Portal can be used for sending spam. This can cause the mail server to be put on a blacklist of mail servers which prevents mail from being delivered. Furthermore, server performance can be degraded.
  Recommendation: Disable the open relay functionality on the mail server.

Although the vulnerabilities identified above pose a greater risk to Client Web Portal, there are other vulnerabilities detailed in this report that Company X should consider remediating before performing a re-test to validate whether applied fixes are effective. We estimate the effort for the re-test of the vulnerabilities identified in this report at approximately 2 days.

Root Cause Analysis

Based on the identified vulnerabilities, Deloitte analysed the root cause of the vulnerabilities and categorised the root cause into the following:

Root Cause	Description
Security Misconfiguration	Security misconfigurations can occur at many levels of the application stack, including but not limited to, web server, database and utilised frameworks, where configuration settings have not been adequately hardened.
Insecure Programming	Without including a security by design principle in each stage of the software development lifecycle, secure coding principles may not be considered when implementing controls. This may result in vulnerabilities that when remediated outside of the software development lifecycle, become extremely costly.
Insufficient Patch Management	An undefined process to patch business critical infrastructure/ application/ third party software may result in the organisations threat landscape posing additional risk outside of the organisations risk appetite. This may result in publically exploitable vulnerabilities being present on the organisations perimeter that could lead to loss of data, resulting in reputational damage and/or hefty fines.

Table 2: Identified root causes derived from our observations

The root cause of the identified issues can be detailed below. We recommend that COMPANY X reviews this to identify if their current processes can be improved upon.

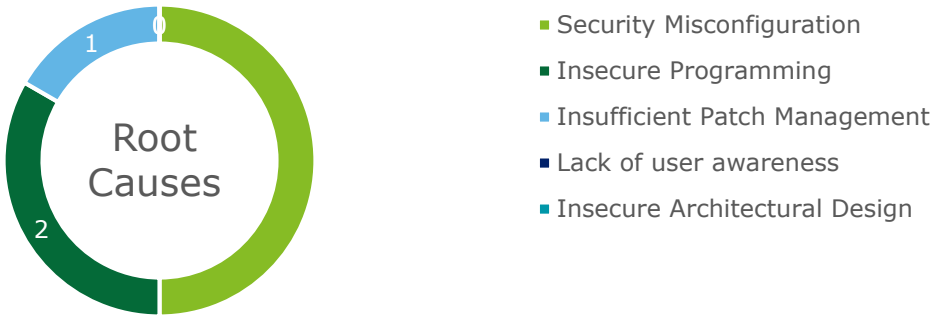


Figure 2: Root Cause Overview

It should be noted that testing was performed against a UAT environment. Based the information provided, the UAT environment was identical to the production environment at the time of testing. Our report assumes that all observations also apply to the production environment of Client Web Portal*. However, the observations identified were not verified in production. Our experience tells us that there may be slight configuration deviations between UAT and production environments. Therefore, additional or slight variations of these security observations might exist in the production environment. We recommend COMPANY X perform a full setup and configuration comparison between the tested UAT and the production environment to verify their setup. Further testing conditions and limitations of the testing can be found in the appendix of this report.*

Observations

The following table gives an overview of our observations from the security assessment. For detailed descriptions of each observation, please refer to the Detailed Observations section of this document.

ID	Name	Area Identified	Root Cause	Risk	Target
PT-1	Outdated and vulnerable software versions identified	Infrastructure	Insufficient Patch Management	Critical	www.example.com
PT-2	Stored cross-site scripting (XSS)	Application	Insecure Programming	High	www.example.com
PT-3	Cross-Site Request Forgery (CSRF)	Application	Insecure Programming)	Medium	www.example.com
PT-4	Mail server can be abused for sending spam	Infrastructure	Security Misconfiguration	Medium	www.example.com
PT-5	Insecure SSL configuration	Infrastructure	Security Misconfiguration	Low	www.example.com
PT-6	Version information disclosure	Infrastructure	Security Misconfiguration	Low	www.example.com

Table 3: Observations of the assessment

Detailed Observations

The following pages contain the detailed observations

PT-1: Outdated and vulnerable software versions identified

Target(s)	Root Cause	Insecure Configuration	Risk	• Critical
www.example.com	Reference	OWASP - A9 Using Components with Known Vulnerabilities	Impact	• High
			Likelihood	• High

Description

We noticed that outdated and vulnerable software versions are in use. The following outdated software was identified:

```
www.example.com is running Apache 0.0.1 released October 2001
```

Apache 9.0.6 was released in March 2018. Apache 0.0.1 contains the following known vulnerabilities:
- Arbitrary code execution;
- DoS issues;
- Privilege escalation weakness.

Impact

If an attacker is able to compromise the software, the attacker can gain complete access to the Client Web Portal, including all data on the system like account details and financial information. Moreover it is possible to cause availability issues on the affected systems.

Likelihood

This issue can be abused by anyone on the Internet. Exploit code is readily available.

Recommendation

We recommend disabling the open relay functionality on the mail server. Mail should only be accepted in case it is intended for a domain for which the server is handling incoming e-mail. In case the server is not handling incoming e-mail the SMTP port should only be accessible from systems which use the server to send mail.

Reference

The following CVEs are connected to the observation mentioned above:

Apache 0.0.1 Top 5 CVEs:

CVE Identifier	Vulnerability Type(s)	Publish Date	CVS Score	Access	Complexity
CVE-2012-1182	Exec Code	2012-04-10	10.0	Remote	Low
CVE-2013-4408	Exec Code Overflow	2013-12-10	8.3	Local Network	Low
CVE-2010-2063	DoS Exec Code Overflow Mem. Corr.	2010-06-17	7.5	Remote	Low
CVE-2010-3069	DoS Exec Code Overflow	2010-09-15	7.5	Remote	Low
CVE-2011-2522	CSRF	2011-07-29	6.8	Remote	Medium

Table 4: CVE ID and CVS Score

PT-2: Stored cross-site scripting (XSS)

Target(s)	Root Cause	Insecure Programming	Risk	• High
www.example.com	Reference	OWASP - A7 Cross-Site Scripting (XSS)	Impact	• Medium
			Likelihood	• High

Description

We noticed that the X-Application is vulnerable to 'stored cross-site scripting' (XSS). It is possible to inject JavaScript code into the database due to a lack of sufficient input filtering. This allows an attacker to inject code that will later be executed by legitimate users when the affected database content is retrieved and displayed in the browser of that user. This would allow an attacker to perform unauthorized actions in the application on behalf of legitimate users or spread malware via the application.

Examples of locations where stored XSS is possible are:

```
http://www.example.com/xapplication/profile.php in the "Voornaam" field.
```

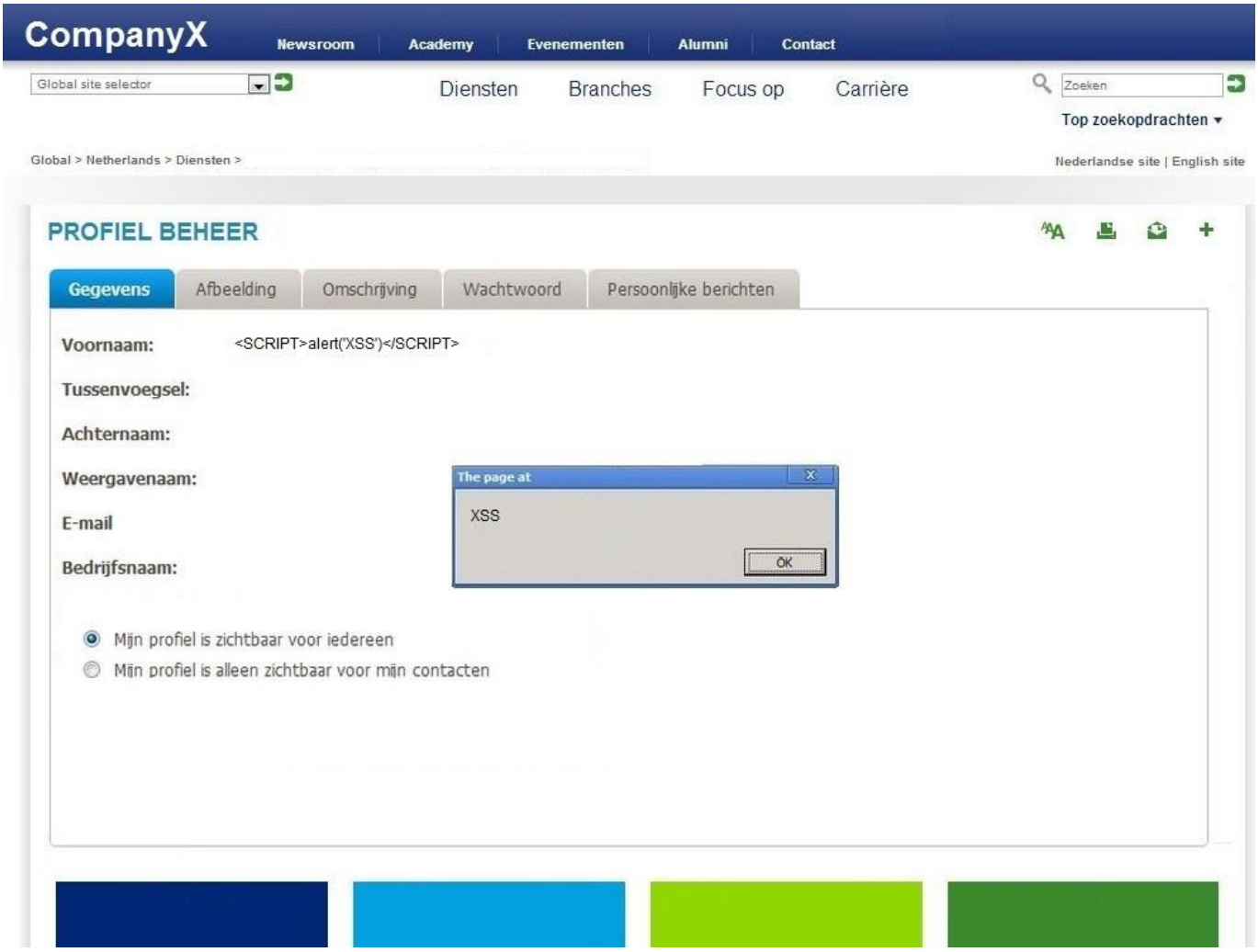


Figure 3: This is a descriptive caption of what can be seen

Impact

It is possible to store code in the 'Voornaam' field of the profile page which is accessible by anyone. Opening the page results in execution of the code injected by the attacker. Successful exploitation could allow an attacker to

make payments on behalf of legitimate users or spread malware via the application.

Likelihood
This attack can be performed by anyone from the Internet. Moderate technical skills are required to perform a successful XSS attack.

Recommendation
We recommend applying input filtering to all input fields and URL parameters in the entire application to assure that only valid input is processed. In case the input field should only contain numbers, the filter should reject all other types of input without sending the input to the database. In case special characters should be allowed into an input field, the application should use a standard function to "escape" the special characters.

Moreover, we recommend apply similar filtering to dynamic output shown by the application to the end user ("output sanitation").

PT-3: Cross-Site Request Forgery (CSRF)

Target(s)	Root Cause	Insecure Programming	Risk	Medium
www.example.com	Reference	-	Impact	High
			Likelihood	Low

Description
We noticed that the Client Web Portal is vulnerable to CSRF (Cross Site Request Forgery) attacks. A CSRF attack consists of an attacker providing a malicious link to a valid application user. If a user is tricked into clicking the link, the user will carry out the action specified by the attacker if logged into the application.

An example of a request that is vulnerable to CSRF:

```
http://www.example.com/forum/movemoney.php
```

Impact
Successful exploitation could lead to unauthorized actions carried out by individual user accounts. An attacker can gain access to the MoveMoney function and use this to transfer money to arbitrary accounts leading to large financial losses.

Likelihood
Exploitation of CSRF requires advanced technical skills. The attacker would need to lure a victim to visit a malicious page while the victim is logged in to the application or trick the user into logging in to the application.

Recommendation
We recommend applying input filtering to all input fields and URL parameters in the entire application to assure that only valid input is processed. In case the input field should only contain numbers, the filter should reject all other types of input without sending the input to the database. In case special characters should be allowed into an input field, the application should use a standard function to "escape" the special characters.

Moreover, we recommend apply similar filtering to dynamic output shown by the application to the end user ("output sanitation").

Reference

Refer to https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF) for more background information regarding CSRF.

PT-4: Mail server can be abused for sending spam

Target(s)	Root Cause	Security Misconfiguration	Risk	Medium
www.example.com	Reference	OWASP – A6 Security Misconfiguration	Impact	Medium
			Likelihood	High

Description
We noticed that a mail server is running which allows sending mail to any domain on the Internet, a so called open relay server.

We identified the following open relay mail servers:

```
www.example.com is accepting mail via port 25 (SMTP)
```

Open relay servers are often used by spammers to send large amounts of unsolicited e-mail.

Impact
In case the open relay mail server is abused by spammers, the domain is likely to become black-listed meaning that email will no longer be accepted from that domain. This could have a severe impact on the ability of Company X to send any e-mail. In addition there can be a reputational impact since end-users can identify Company X as the origin of the unsolicited mails.

Likelihood
Limited technical skills are required to identify the open relay server. Spammers are actively scanning the Internet to identify open relay servers to be used for sending out unsolicited e-mail.

Recommendation
We recommend disabling the open relay functionality on the mail server. Mail should only be accepted in case it is intended for a domain for which the server is handling incoming e-mail. In case the server is not handling incoming e-mail the SMTP port should only be accessible from systems which use the server to send mail.

PT-5: Insecure SSL/TLS configuration

Target(s)	**Root Cause**	Security Misconfiguration	**Risk**	Low
www.example.com	**Reference**	OWASP – A6 Security Misconfiguration	**Impact**	Low
			Likelihood	Medium

Description

We identified the following potentially insecure SSL/TLS configurations on the servers:

IP address	Port	SSLv2 disabled	POODLE	HSTS enabled	RC4 disabled	BEAST	BREACH	MD5 disabled	PFS	TLS > 1.0 Supported
www.example.com	443	OK	X	OK	OK	X	OK	OK	OPT	OK

Table 5: SSL misconfiguration I

IP address	Port	SSL Renegotiation	SWEET32	Logjam	Heartbleed	FREAK	TLS_FALLBACK_SCSV supported	CRIME
www.example.com	443	OK	X	OK	OK	X	OK	OK

Table 6: SSL misconfiguration II

Mark	Description
OK	No risk identified
X	The service is vulnerable to this attack
OPT	PFS cipher suites are optional

Table 7: SSL misconfiguration

Note: Disabling old and insecure SSL version (such as SSL v3) will improve security, however older browsers do not support new versions such as TLS 1.2. This could mean that users of the application are unable connect to the application. Therefore we recommend researching whether users are still using the older versions before disabling them.

```
Testing vulnerabilities

Heartbleed (CVE-2014-0160)                not vulnerable (OK), timed out
CCS (CVE-2014-0224)                       not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
Secure Renegotiation (CVE-2009-3555)      not vulnerable (OK)
Secure Client-Initiated Renegotiation     not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
BREACH (CVE-2013-3587)                    potentially NOT ok, uses gzip HTTP compression. - only supplied "/" tested
                                          Can be ignored for static pages or if no secrets in the page
POODLE, SSL (CVE-2014-3566)               VULNERABLE (NOT ok), uses SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention supported (OK)
SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers
FREAK (CVE-2015-0204)                     not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                          make sure you don't use this certificate elsewhere with SSLv2 enabled services
                                          https://censys.io/ipv4?q=9E9EA0B4416EE4B2B8C2FB7918A312DB28A1CA83B160BF44E17DB219F974B574 could help you to find out
LOGJAM (CVE-2015-4000), experimental      VULNERABLE (NOT ok): common prime nginx/1024-bit MODP group with safe prime modulus detected (1024 bits),
                                          but no DH EXPORT ciphers
BEAST (CVE-2011-3389)                     SSL3: ECDHE-RSA-AES256-SHA
                                                DHE-RSA-AES256-SHA
                                                DHE-RSA-CAMELLIA256-SHA
                                                AES256-SHA CAMELLIA256-SHA
                                                ECDHE-RSA-AES128-SHA
                                                DHE-RSA-AES128-SHA
                                                DHE-RSA-CAMELLIA128-SHA
                                                AES128-SHA CAMELLIA128-SHA
                                                DHE-RSA-SEED-SHA SEED-SHA
                                                IDEA-CBC-SHA
                                                ECDHE-RSA-DES-CBC3-SHA
                                                EDH-RSA-DES-CBC3-SHA
                                                DES-CBC3-SHA
                                          TLS1: ECDHE-RSA-AES256-SHA
                                                DHE-RSA-AES256-SHA
                                                DHE-RSA-CAMELLIA256-SHA
                                                AES256-SHA CAMELLIA256-SHA
                                                ECDHE-RSA-AES128-SHA
                                                DHE-RSA-AES128-SHA
                                                DHE-RSA-CAMELLIA128-SHA
                                                AES128-SHA CAMELLIA128-SHA
                                                ECDHE-RSA-DES-CBC3-SHA
                                                EDH-RSA-DES-CBC3-SHA
                                                DES-CBC3-SHA DHE-RSA-SEED-SHA
                                                SEED-SHA IDEA-CBC-SHA
                                          VULNERABLE -- but also supports higher protocols (possible mitigation): TLSv1.1 TLSv1.2
LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS
RC4 (CVE-2013-2566, CVE-2015-2808)        VULNERABLE (NOT ok): ECDHE-RSA-RC4-SHA
                                                               C4-SHA RC4-MD5
```

Table 8: Insecure SSL/TLS configuration identified by the tool "TestSSL" (https://testssl.sh/)

Impact
Successful exploitation could allow an attacker to decrypt intercepted traffic data, which may hold sensitive data such as a user's login password or other personal data. However, the vulnerability only affects users for which the attacker can intercept SSL traffic.

Likelihood
The attacker would need to be on designated networks (i.e. on the path between the user and the server) to abuse these SSL issues. Advanced technical skills are required to intercept, manipulate and decrypt SSL traffic.

Recommendation
We recommend improving the TLS/SSL configuration of the affected systems:

- Disable support for the SSL version 2 protocol.
- Investigate whether SSL version 3 is required by application users. If possible, disable support for the SSL version 3 protocol because it exposes users to the POODLE attack.
- Investigate whether TLS version 1.0 is required by application users. If possible, disable support for the TLS version 1.0 protocol because it exposes users to the BEAST attack.
- Enable support for the TLS version 1.2 protocol.
- Enable Forward Secrecy ciphers using the DHE/ECDHE algorithm to support Forward Secrecy in modern browsers.

Note: Disabling old and insecure SSL versions (such as SSL v3) will improve security, however older browsers might have issues with new versions such as TLS 1.1 or 1.2. Users may not be able to connect to the application. Therefore we recommend researching whether users are still using older browser versions before disabling them.

Reference
Also refer to https://www.ssllabs.com/projects/best-practices/index.html for a detailed guide on how to configure SSL in a secure manner.

PT-6: Version information disclosure

Target(s)	Root Cause	Security Misconfiguration	Risk	Low
www.example.com	Reference	OWASP – A6 Security Misconfiguration	Impact	Low
			Likelihood	High

Description
We noticed that the server used to serve the Client Web Portal discloses technical and detailed version information in HTTP response headers. The information disclosed contains:

```
• Microsoft IIS version: Microsoft-IIS/7.5
• X-AspNet version: 2.0.50727
• X-AspNet Version: 4.0.0319
```

This information may help an attacker in further attacks.

Impact
The header contents allow an attacker to obtain technical information which could be used as a platform for further attack.

Likelihood
This issue can be abused by anyone on the Internet. The HTTP headers can be viewed using freely available tools.

Recommendation
We recommend removing technical and detailed version information from HTTP headers.
• X-AspNet-Version header can be removed by adding following parameter to the IIS web.config file within corresponding section;
• X-AspNetMvc-Version header can be removed by adding following parameter to the global.asax configuration file within the Application Start section: MvcHandler.DisableMvcResponseHeader = true
• X-Powered-By header can be removed by adding following parameter to the IIS web.config file within corresponding section;
• Server header can be removed by programming a module, see
http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwantedhttp-response-headers.aspx

Appendix A – Detailed Scope

The detailed scope of this security assessment was the following:

Target	Assessment Testing Type	Approach	Environment	Name and Version
www.example.com	Web	Grey box	UAT	Client Web Portal
www.example.com	Infra	Black box	UAT	Client Web Portal

Table 9: Detailed Scope

The following test users and assigned roles were provided:

User	Role
Admin	Adminstrator
Testuser1	Super User
Testuser2	Normal User

Table 10: Provided Test User Accounts

Appendix B - Methodology

Deloitte has developed its own penetration testing methodology inspired by the OWASP, WASC and OSSTM standards and has it customized in order to deliver a consistent and high-quality service. This methodology follows the steps described below, and is regularly updated based on new attack techniques and vulnerabilities that are discovered. More details on the specific security assessment activities performed during our engagement can be found in our proposal.

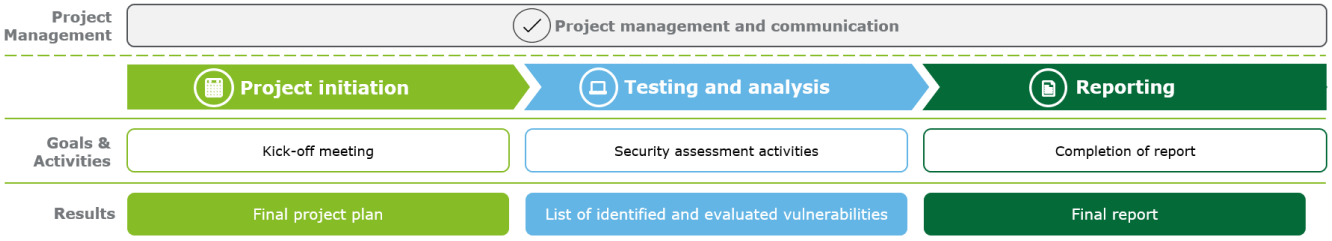


Figure 4: Deloitte's Security Assessment Services Methodology

Appendix C – Limitations

Deloitte's consultants work under limitations of time and scope that may not apply to the activities of a malicious user or an attacker. They also work at a specific point in time, in an environment where both the systems tested and the threat profiles are dynamically evolving. It is therefore possible that vulnerabilities exist, or will arise, that were not identified during the test.

Deloitte's observations are representative of the environment in scope at the time of the test. If the environment is modified through changes in configuration, installed software packages, or application code, then additional vulnerabilities may be introduced that the test did not identify.

The test was limited to a reasonable efforts basis and limited sample functionality on what could be achieved within the requested test window; hence, there may be vulnerabilities that were not identified during the test. Likewise, vulnerabilities that have been identified above may be present in other parts of the environment than those noted.

Appendix D – Risk Rating Methodology

This overview describes the attributes of the observations discussed in this report. In our rating we take into account the following aspects: financial impact, performance, reputation, regulatory violation, environmental and safety.

Impact

- **High:** Events that would pose a direct threat to the confidentiality and integrity of very sensitive information or availability of critical systems. The issue identified could harm the organisation either financially or legally, and could potentially create a loss of image.
- **Medium:** Events that pose a direct threat to the confidentiality and integrity of (a subset of) sensitive information or availability of non-critical systems; or the issue gives an attacker access to systems or other means that provide an advanced platform for further attack.
- **Low:** The issue leads to technical information disclosure or increases the chance of successful attacks. This issue does not directly lead to unauthorised access, nor poses a direct threat to the confidentiality and integrity of sensitive information.

Likelihood

- **High:** The vulnerability is easy to exploit. Little information is required to exploit the issue, or an exploit kit is easy to obtain and use. No effective measures have been taken to prevent the issue from occurring.
- **Medium:** The vulnerability is harder to exploit. More information is required, or exploit tools require knowledge, to take advantage of it. Some effective measures have been taken to prevent the issue from occurring. However, the level of measures taken leaves room for improvement.
- **Low:** The vulnerability is difficult to exploit. Exploitation requires specialist knowledge or detailed knowledge of the specific technical implementation. Alternatively, effective measures have been taken to prevent the issue from occurring.

Calculating the Risk

The advice for further action for observations made is based on the likelihood and impact rating of the particular observation. The table below describes the way the advice for further action is derived from Likelihood and Impact in general.

Impact	Likelihood: Low	Likelihood: Medium	Likelihood: High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Low

Figure 5: Risk Assessment

Deloitte Risk Rating

Critical/High: Management is informed on the same day the security issue is identified. Medium/Low: Management is informed as part of the full report of the security test.

Deloitte.