Web Application Report

This report includes important security information about your Web Application.

The OWASP Ten Most Critical Web Application Security Vulnerabilities 2007 Update Report

This report was created by IBM Rational AppScan 7.8.0.2
18/07/2014 07:55:15 p.m.

The OWASP Ten Most Critical Web Application Security Vulnerabilities 2007 Update

Web Application Report

TextReportCreatedBy

Scanned Web Application: http://10.10.10.115/qbs
Scan Name: qbs

Content

This report contains the following sections:

- Description
- Compliance Scan Results
- Unique Compliance-related Issues Detected
- Compliance-Related Issues and Section References

IMPORTANT INFORMATION ABOUT THIS REPORT

This Compliance Scan Results Report is based on the results of an automated Web Application Security scan, performed by AppScan.

An AppScan scan attempts to uncover security-related issues in web applications, testing both the http frameworks (e.g. web servers) and the code of the application itself (e.g. dynamic pages). The testing is performed over HTTP, and is limited only to those issues that are specified for testing and identified in an automated fashion via the HTTP channel. The scan is also limited to those specific issues included in an automatic and/or manual explore performed during the scan. The security-related issues detected are compared to selected regulatory or industry standard requirements to produce this report. There may be areas of compliance risk associated with such regulation or standard that are not specified for testing by AppScan. This report will not detect any compliance-related issues in areas of compliance risk that are not tested by AppScan. The report identifies areas where there may be a compliance risk, but the exact impact of each uncovered issue type depends on the individual application, environment, and the subject regulation or standard. Regulations and standards are subject to change, and the scans performed by AppScan may not reflect all such changes. It is the user’s responsibility to interpret the results in this report for determination of impact, actual compliance violations, and appropriate remedial measures, if any.
Section references to regulations are provided for reference purposes only. The issues reported are general compliance-related risks and are not to be interpreted as excerpts from any regulation.

The information provided does not constitute legal advice. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Description

Summary Description

The OWASP Top Ten is a list of vulnerabilities that require immediate remediation. Existing code should be checked for these vulnerabilities, as these flaws are being actively targeted by attackers. Development projects should address these vulnerabilities in their requirements documents and design, build and test their applications to ensure that they have not been introduced. Project managers should include time and budget for application security activities including developer training, application security policy development, security mechanism design and development, penetration testing, and security code review.

Although setout as an education piece, rather than a standard or a regulation, it is important to note that several prominent industry and government regulators are referencing the OWASP top ten list as a list of vulnerabilities that must be periodically checked for and protected against. These bodies include among others VISA USA, MasterCard International and the American Federal Trade Commission (FTC).

However, according to the OWASP team the OWASP top ten first and foremost an education piece, not a standard. The OWASP team suggests to any organization about to adopt the Top Ten paper as a policy or standard to consult with the OWASP team first.

The OWASP Top Ten 2007 update is based on the results of the MITRE Vulnerability Trends for 2006. This means these are the latest most popular vulnerabilities categories. However, organization should still apply the necessary protections against the 2004 top ten vulnerabilities.

Covered Entities

All companies and other entities that develop any kind of web application code are encouraged to address the top ten list and start the process of ensuring their web applications do not contain any of the listed vulnerabilities. Adopting the OWASP Top Ten is an effective first step towards changing the software development culture within the organization into one that produces secure code.

For more information on OWASP Top Ten, please review the -The Ten Most Critical Web Application Security Vulnerabilities - 2007 Update document, that can be found at http://www.owasp.org

For more information on securing web applications, please visit http://www-01.ibm.com/software/rational/offerings/websecurity/.

(*) DISCLAIMER IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Compliance Scan Results

13 unique issues detected across 10 sections of the regulation:

Section	No. of Issues
1. Cross site scripting (XSS) flaws (A1)	-
2. Injection flaws (A2)	2
3. Malicious file execution (A3)	2
4. Insecure direct object reference (A4)	4
5. Cross site request forgery (CSRF) (A5)	-
6. Information leakage and improper error handling (A6)	5
7. Broken authentication and session management (A7)	6
8. Insecure cryptographic storage (A8)	7
9. Insecure communications (A9)	6
10. Failure to restrict URL access (A10)	-

Unique Compliance-related Issues Detected

13 unique issues detected across 10 sections of the regulation:

ID	URL	Parameter/Cookie	Test Name	Sections
1	http://10.10.10.115/		Error Page Path Disclosure	4, 6
2	http://10.10.10.115/		Microsoft IIS Non-Existent idq File Path Disclosure	4, 6
3	http://10.10.10.115/qbs/		Error Page Path Disclosure	4, 6
4	http://10.10.10.115/qbs/		Microsoft IIS Non-Existent idq File Path Disclosure	4, 6
5	http://10.10.10.115/qbs/login.cshtml	pwd	Unencrypted Login Request	7, 8, 9
6	http://10.10.10.115/qbs/newuser.cshtml	password	Unencrypted Login Request	7, 8, 9
7	http://10.10.10.115/qbs/newuser.cshtml	passwordConfirm	Unencrypted Login Request	7, 8, 9
8	http://10.10.10.115/qbs/js/jquery-ui.custom.js		Client-Side (JavaScript) Cookie References	6, 8
9	http://10.10.10.115/qbs/selfpwd.cshtml	passwordOld	Unencrypted Login Request	7, 8, 9
10	http://10.10.10.115/qbs/selfpwd.cshtml	password	Unencrypted Login Request	7, 8, 9
11	http://10.10.10.115/qbs/selfpwd.cshtml	passwordConfirm	Unencrypted Login Request	7, 8, 9
12	http://10.10.10.115/qbs/examimport.cshtml	uploadedLayout	Potential File Upload	2, 3
13	http://10.10.10.115/qbs/userimport.cshtml	uploadedLayout	Potential File Upload	2, 3

Compliance-Related Issues and Section References

1) Cross site scripting (XSS) flaws

(A1)

No issues.

2) Injection flaws

(A2)

2 Issues

Potential File Upload

Security Risks

- It is possible to run remote commands on the web server. This usually means complete compromise of the server and its contents
- It is possible to upload, modify or delete web pages, scripts and files on the web server

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Restrict user capabilities and permissions during the file upload process

Issues:

Issue ID	URL	Parameter/Cookie
12	http://10.10.10.115/qbs/examimport.cshtml	uploadedLayout
13	http://10.10.10.115/qbs/userimport.cshtml	uploadedLayout

3) Malicious file execution

(A3)

2 Issues

Potential File Upload

Security Risks

- It is possible to run remote commands on the web server. This usually means complete compromise of the server and its contents
- It is possible to upload, modify or delete web pages, scripts and files on the web server

Causes:

- Insecure web application programming or configuration

Remediation Tasks:

Restrict user capabilities and permissions during the file upload process

Issues:

Issue ID	URL	Parameter/Cookie
12	http://10.10.10.115/qbs/examimport.cshtml	uploadedLayout
13	http://10.10.10.115/qbs/userimport.cshtml	uploadedLayout

4) Insecure direct object reference

(A4)

4 Issues

Error Page Path Disclosure

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- The web server or application server are configured in an insecure way
- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Cancel output of debugging error messages and exceptions and contact vendor for a security patch.

Issues:

Issue ID	URL	Parameter/Cookie
1	http://10.10.10.115/	

Microsoft IIS Non-Existent idq File Path Disclosure

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Apply patches from Microsoft security bulletin MS00-006

Issues:

Issue ID	URL	Parameter/Cookie
2	http://10.10.10.115/	

Error Page Path Disclosure

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- The web server or application server are configured in an insecure way
- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Cancel output of debugging error messages and exceptions and contact vendor for a security patch.

Issues:

Issue ID	URL	Parameter/Cookie
3	http://10.10.10.115/qbs/	

Microsoft IIS Non-Existent idq File Path Disclosure

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Apply patches from Microsoft security bulletin MS00-006

Issues:

Issue ID	URL	Parameter/Cookie
4	http://10.10.10.115/qbs/	

5) Cross site request forgery (CSRF)

(A5)

No issues.

6) Information leakage and improper error handling

(A6)

5 Issues

Error Page Path Disclosure

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- The web server or application server are configured in an insecure way
- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Cancel output of debugging error messages and exceptions and contact vendor for a security patch.

Issues:

Issue ID	URL	Parameter/Cookie

1	http://10.10.10.115/	

Microsoft IIS Non-Existent idq File Path Disclosure

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Apply patches from Microsoft security bulletin MS00-006

Issues:

Issue ID	URL	Parameter/Cookie
2	http://10.10.10.115/	

Error Page Path Disclosure

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- The web server or application server are configured in an insecure way
- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Cancel output of debugging error messages and exceptions and contact vendor for a security patch.

Issues:

Issue ID	URL	Parameter/Cookie
3	http://10.10.10.115/qbs/	

Microsoft IIS Non-Existent idq File Path Disclosure

Security Risks

- It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Remediation Tasks:

Apply patches from Microsoft security bulletin MS00-006

Issues:

Issue ID	URL	Parameter/Cookie
4	http://10.10.10.115/qbs/	

Client-Side (JavaScript) Cookie References

Security Risks

- The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side

Causes:

- Cookies are created at the client side

Remediation Tasks:

Remove business and security logic from the client side

Issues:

Issue ID	URL	Parameter/Cookie
8	http://10.10.10.115/qbs/js/jquery-ui.custom.js	

7) Broken authentication and session management

(A7)

6 Issues

Unencrypted Login Request

Security Risks

- It may be possible to steal user login information such as usernames and passwords that are sent unencrypted

Causes:

- Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted

Remediation Tasks:

Always use the HTTP POST method when sending sensitive information

Issues:

Issue ID	URL	Parameter/Cookie
5	http://10.10.10.115/qbs/login.cshtml	pwd
6	http://10.10.10.115/qbs/newuser.cshtml	password
7	http://10.10.10.115/qbs/newuser.cshtml	passwordConfirm
9	http://10.10.10.115/qbs/selfpwd.cshtml	passwordOld
10	http://10.10.10.115/qbs/selfpwd.cshtml	password
11	http://10.10.10.115/qbs/selfpwd.cshtml	passwordConfirm

8) Insecure cryptographic storage

(A8)

7 Issues

Unencrypted Login Request

Security Risks

- It may be possible to steal user login information such as usernames and passwords that are sent unencrypted

Causes:

- Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted

Remediation Tasks:

Always use the HTTP POST method when sending sensitive information

Issues:

Issue ID	URL	Parameter/Cookie
5	http://10.10.10.115/qbs/login.cshtml	pwd

6	http://10.10.10.115/qbs/newuser.cshtml	password
7	http://10.10.10.115/qbs/newuser.cshtml	passwordConfirm

Client-Side (JavaScript) Cookie References

Security Risks

- The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side

Causes:

- Cookies are created at the client side

Remediation Tasks:

Remove business and security logic from the client side

Issues:

Issue ID	URL	Parameter/Cookie
8	http://10.10.10.115/qbs/js/jquery-ui.custom.js	

Unencrypted Login Request

Security Risks

- It may be possible to steal user login information such as usernames and passwords that are sent unencrypted

Causes:

- Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted

Remediation Tasks:

Always use the HTTP POST method when sending sensitive information

Issues:

Issue ID	URL	Parameter/Cookie
9	http://10.10.10.115/qbs/selfpwd.cshtml	passwordOld
10	http://10.10.10.115/qbs/selfpwd.cshtml	password
11	http://10.10.10.115/qbs/selfpwd.cshtml	passwordConfirm

9) Insecure communications

(A9)

6 Issues

Unencrypted Login Request

Security Risks

- It may be possible to steal user login information such as usernames and passwords that are sent unencrypted

Causes:

- Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted

Remediation Tasks:

Always use the HTTP POST method when sending sensitive information

Issues:

Issue ID	URL	Parameter/Cookie
5	http://10.10.10.115/qbs/login.cshtml	pwd
6	http://10.10.10.115/qbs/newuser.cshtml	password
7	http://10.10.10.115/qbs/newuser.cshtml	passwordConfirm
9	http://10.10.10.115/qbs/selfpwd.cshtml	passwordOld
10	http://10.10.10.115/qbs/selfpwd.cshtml	password
11	http://10.10.10.115/qbs/selfpwd.cshtml	passwordConfirm

10) Failure to restrict URL access

(A10)

No issues.