Audit report

27 July 2015, 12:03:51 - UTC

Tool version	5.6
Number of scanned websites	4
Number of identified vulnerabilities	82

Table of contents

Introduction

The audit tool DenyAll Vulnerability Manager Enterprise Edition enhances the identification of potential IT security vulnerabilities and the risk they could generate if they were exploited by an evil attacker.

The first part of this report brings a brief and executive summary of the security vulnerabilities identified. The second part lists all these vulnerabilities coupled with an assessment of their potential risks and a disclosure to help you understand and remediate them. Finally, the first appendix lists all the servers and services discovered during the scan.

Methodology

This report is not meant to be exhaustive and thus, does not replace the analysis an expert in pentesting could make. Moreover, all the information contained in this report should be validated by the administrator of the system targeted by the audit, in order to avoid any vulnerability mistakenly identified by the tool ("false positive").

Risk assessment

The risk assessment used in this report for rating each vulnerability relies on the Common Vulnerability Scoring System (CVSS) which considers two factors:

- the potential impact of an attack exploiting this vulnerability, in terms of availability of the application, confidentiality and integrity of the information,
- the exploitability of the vulnerability, as an easy-to-exploit vulnerability increases the number of potential attackers and thus, the likelihood of an attack.

The CVSS ratings (base rating, impact and exploitability) spread between 0 and 10.

Priorization of vulnerabilities

The priority suggested for each vulnerability falls into five levels: critical priority (CVSS base score equals 10), major (base score between 8 and 10), high (base score between 7 and 8), major (base score between 4 and 7) and low (base score lower than 4).

In order to determine the real risk induced by each vulnerability, the potential impact must be weighted by the asset value (for instance, the operational criticality of an application or the value of the information that could be compromised), and the exploitability, by the company exposure (for instance, financial activities motivate more attacks than others).

Finally, these risks may be mitigated by specific controls, either perventive, dissuasive or palliative.

Management Report

Summary

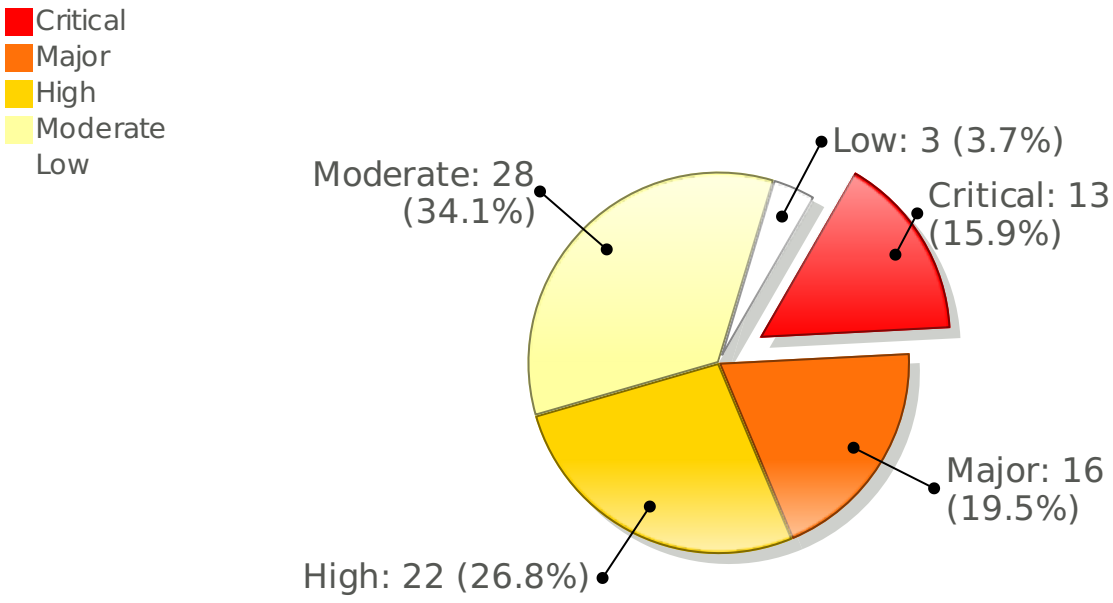
The websites which have been tested show up 82 vulnerabilities, including **13 critical priority vulnerabilities**.

These vulnerabilities are graphically presented below and detailed in the technical report.

	Risques					
	Critical	Major	High	Moderate	Low	**TOTAL**
AutoComplete enabled	0	0	0	0	3	3
Command injection	0	1	0	0	0	1
Cross-Site Request Forgery	0	0	10	0	0	10
Cross-Site Scripting	0	14	0	0	0	14
Database fingerprint	0	0	3	0	0	3
Fuzzing	0	0	0	1	0	1
Information leakage	0	0	0	11	0	11
Insecure HTTP method - listed	0	0	0	1	0	1
Local file inclusion	0	0	9	0	0	9
Password Capture	0	0	0	12	0	12
Remote administration interface	0	0	0	1	0	1
Remote file inclusion	0	1	0	0	0	1
Session fixation	0	0	0	1	0	1
SQL injection	10	0	0	0	0	10
TRACE HTTP method enabled	0	0	0	1	0	1
Trivial authentication account	3	0	0	0	0	3
TOTAL	13	16	22	28	3	82

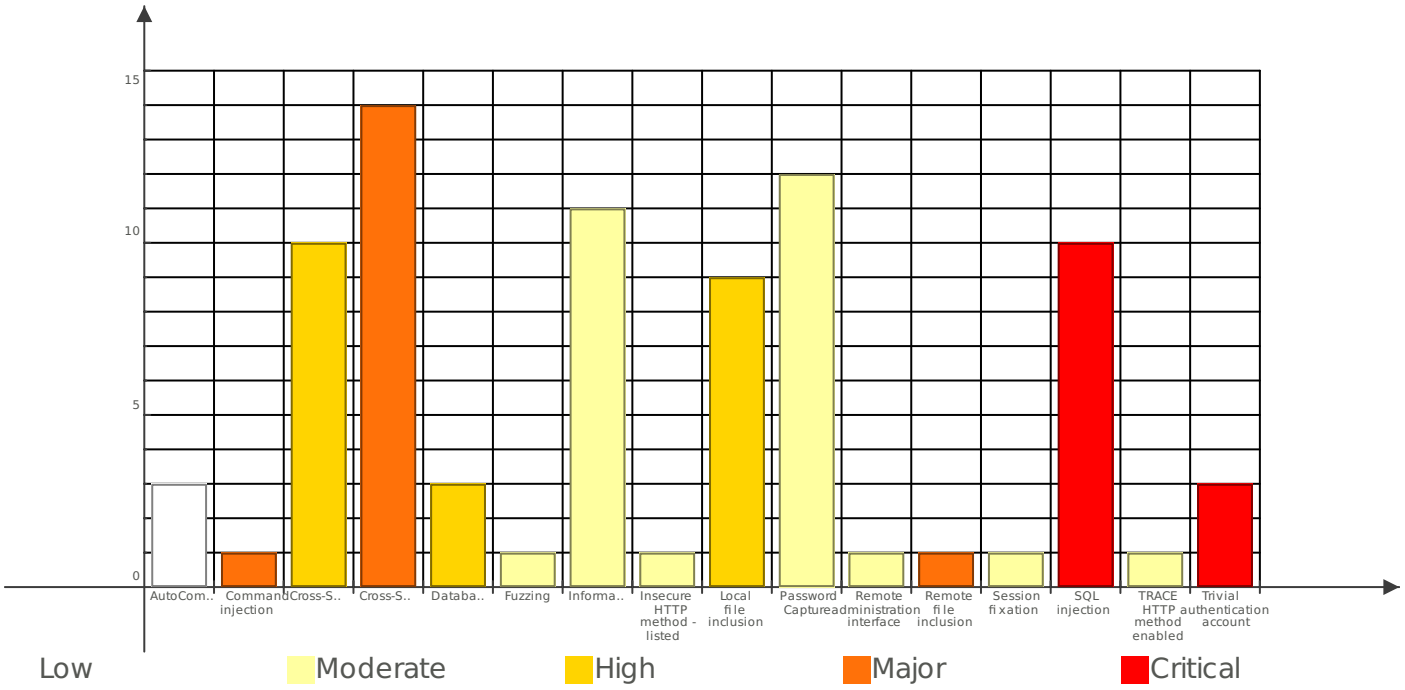
Vulnerabilities ordered by priority

This chart shows the number of identified vulnerabilities ordered by priority.



Web Vulnerabilities

This chart shows the number of vulnerabilities grouped by Type.



Technical report

Inventory

DVWA

Informations on website:

- HTTPSERVER : Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1
- XPOWEREDBY : PHP/5.3.2-1ubuntu4.5

Number of vulnerabilites:

- Critical: 3
- Major: 6
- High: 13
- Moderate: 16
- Low: 0

http://192.168.1.21/mutillidae

Informations on website:

- HTTPSERVER : Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1
- XPOWEREDBY : PHP/5.3.2-1ubuntu4.5

Number of vulnerabilites:

- Critical: 7
- Major: 6
- High: 6
- Moderate: 1
- Low: 0

http://192.168.1.21/WackoPicko

Informations on website:

- XPOWEREDBY : PHP/5.3.2-1ubuntu4.5
- HTTPSERVER : Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1

Number of vulnerabilites:

- Critical: 2
- Major: 3
- High: 0
- Moderate: 7
- Low: 0

http://192.168.56.30/bodgeit/

Informations on website:

- HTTPSERVER : Apache-Coyote/1.1

Number of vulnerabilites:

- Critical: 1
- Major: 1
- High: 3
- Moderate: 4
- Low: 3

Summary

- DVWA - Development / SQL injection - Critical
- DVWA - Development / Command injection - Major
- DVWA - Development / Remote file inclusion - Major
- DVWA - Development / Cross-Site Scripting - Major
- DVWA - Development / Local file inclusion - High
- DVWA - Development / Cross-Site Request Forgery - High
- DVWA - Configuration / Password Capture - Moderate
- DVWA - Development / Session fixation - Moderate
- DVWA - Configuration / Remote administration interface - Moderate
- DVWA - Configuration / Fuzzing - Moderate
- DVWA - Configuration / TRACE HTTP method enabled - Moderate
- DVWA - Configuration / Information leakage - Moderate
- http://192.168.1.21/mutillidae - Access control / Trivial authentication account - Critical
- http://192.168.1.21/mutillidae - Development / SQL injection - Critical
- http://192.168.1.21/mutillidae - Development / Cross-Site Scripting - Major
- http://192.168.1.21/mutillidae - Configuration / Database fingerprint - High
- http://192.168.1.21/mutillidae - Development / Local file inclusion - High
- http://192.168.1.21/mutillidae - Configuration / Password Capture - Moderate
- http://192.168.1.21/WackoPicko - Access control / Trivial authentication account - Critical
- http://192.168.1.21/WackoPicko - Development / SQL injection - Critical
- http://192.168.1.21/WackoPicko - Development / Cross-Site Scripting - Major
- http://192.168.1.21/WackoPicko - Configuration / Password Capture - Moderate
- http://192.168.1.21/WackoPicko - Configuration / Information leakage - Moderate
- http://192.168.56.30/bodgeit/ - Access control / Trivial authentication account - Critical
- http://192.168.56.30/bodgeit/ - Development / Cross-Site Scripting - Major
- http://192.168.56.30/bodgeit/ - Configuration / Database fingerprint - High
- http://192.168.56.30/bodgeit/ - Development / Cross-Site Request Forgery - High
- http://192.168.56.30/bodgeit/ - Configuration / Insecure HTTP method - listed - Moderate
- http://192.168.56.30/bodgeit/ - Configuration / Password Capture - Moderate
- http://192.168.56.30/bodgeit/ - Configuration / AutoComplete enabled - Low

DVWA

Development / SQL injection — Critical

Description: A SQL injection attack consists of insertion or injection of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Remediation: Primary Defenses: use of Prepared Statements (Parameterized Queries), use of Stored Procedures, escaping all user-supplied input. Additional Defenses: enforce least privilege and perform white list input validation.

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

References: OWASP 2013 A1, OWASP prevention sheet, CWE-89 , PCI DSS 6.5.1

- Page: http://10.1.5.38/dvwa/vulnerabilities/sqli_blind/?id=-6922%27+OR+4082%3DSLEEP%286%29+AND+%27DENYALLnvcv%27%3D%27DENYALLnvcv&Submit=Submit
  Action: http://10.1.5.38/dvwa/vulnerabilities/sqli_blind/
  Parameter type: GET
  Attacked parameter: id
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: id=-6922' OR 4082=SLEEP(6) AND 'DENYALLnvcv'='DENYALLnvcv
- Page: http://10.1.5.38/dvwa/vulnerabilities/brute/?username=-1962%27+OR+1248%3DSLEEP%286%29+AND+%27DENYALLYYWu%27%3D%27DENYALLYYWu&password=denyall&Login=Login
  Action: http://10.1.5.38/dvwa/vulnerabilities/brute/
  Parameter type: GET
  Attacked parameter: username
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: username=-1962' OR 1248=SLEEP(6) AND 'DENYALLYYWu'='DENYALLYYWu
- Page: http://10.1.5.38/dvwa/vulnerabilities/sqli/?id=-7272%27+OR+3294%3DSLEEP%286%29+AND+%27DENYALLASpB%27%3D%27DENYALLASpB&Submit=Submit
  Action: http://10.1.5.38/dvwa/vulnerabilities/sqli/
  Parameter type: GET
  Attacked parameter: id
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: id=-7272' OR 3294=SLEEP(6) AND 'DENYALLASpB'='DENYALLASpB

Development / Command injection — Major

Description: An attacker can exploit this vulnerability to take control of the system.

Remediation: Control and protect commands by escaping all user-supplied input.

Priority: Major

Methodology: black box

Risk: 9.3 (Impact: 10.0, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:C/).

References: OWASP 2013 A1,OWASP Command injection, CWE-77 , PCI DSS 6.5.1

- Page: http://10.1.5.38/dvwa/vulnerabilities/exec/
  Action: http://10.1.5.38/dvwa/vulnerabilities/exec/
  Parameter type: POST
  Attacked parameter: ip
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: ip=;sleep 6;

Development / Remote file inclusion — Major

Description: Remote file inclusion allows an attacker to send a malicious program on the application server and to execute it.

Remediation: File inclusion can be avoided by protecting the objects parameters references (internal or external). It may also be restricted by appropriate server configurations.

Priority: Major

Methodology: black box

Risk: 9.0 (Impact: 9.5, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:C/A:P/).

References: OWASP 2007 A3, CWE-98 , PCI DSS 6.5.1

- Page: http://10.1.5.38/dvwa/vulnerabilities/fi/?page=https%3A%2F%2Fedge.denyall.com%2F
  Action: http://10.1.5.38/dvwa/vulnerabilities/fi/
  Parameter type: GET
  Attacked parameter: page
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: page=https://edge.denyall.com/

Development / Cross-Site Scripting — Major

Description: Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

Remediation: Output Encoding: a technique used to ensure that characters are treated as data, not as characters that are relevant to the interpreter\'s parser. There are lots of different types of escaping, sometimes confusingly called output encoding. Some of these techniques define a special escape character, and other techniques have a more sophisticated syntax that involves several characters.

Priority: Major

Methodology: black box

Risk: 8.3 (Impact: 8.5, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:C/A:P/).

References: OWASP 2013 A3, OWASP prevention sheet, CWE-79 , PCI DSS 6.5.7

- Page: http://10.1.5.38/dvwa/vulnerabilities/view_source.php?id=%27%3Balert%28%27DenyAll1362668949696%27%29%3B%27&security=low
  Action: http://10.1.5.38/dvwa/vulnerabilities/view_source.php
  Parameter type: GET
  Attacked parameter: id
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: id=';alert('DenyAll1362668949696');'

- Page: http://10.1.5.38/dvwa/vulnerabilities/xss_s/
  Action: http://10.1.5.38/dvwa/vulnerabilities/xss_s/
  Parameter type: POST
  Attacked parameter: mtxMessage
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: mtxMessage=<script>alert(313371362668948181)</script>
- Page: http://10.1.5.38/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28313371362668947773%29%3C%2Fscript%3E
  Action: http://10.1.5.38/dvwa/vulnerabilities/xss_r/
  Parameter type: GET
  Attacked parameter: name
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: name=<script>alert(313371362668947773)</script>
- Page: http://10.1.5.38/dvwa/vulnerabilities/xss_s/
  Action: http://10.1.5.38/dvwa/vulnerabilities/xss_s/
  Parameter type: POST
  Attacked parameter: txtName
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: txtName=<script>alert(313371362668948152)</script>

Development / Local file inclusion — High

Description: Local file inclusion allows an attacker disclose information from the application server.

Remediation: File inclusion can be avoided by protecting the objects parameters references (internal or external). It may also be restricted by appropriate server configurations.

Priority: High

Methodology: black box

Risk: 7.8 (Impact: 7.8, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:N/A:P/).

References: OWASP 2007 A3, CWE-98 , PCI DSS 6.5.1

- Page: http://10.1.5.38/dvwa/vulnerabilities/view_source.php?id=exec&security=%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd%2500
  Action: http://10.1.5.38/dvwa/vulnerabilities/view_source.php
  Parameter type: GET
  Attacked parameter: security
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: security=/../../../../../../../../../../../../../../etc/passwd%00
  security=/../../../../../../../../../../../../../../..//etc/passwd%00
- Page: http://10.1.5.38/dvwa/vulnerabilities/view_source_all.php?id=%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd%2500
  Action: http://10.1.5.38/dvwa/vulnerabilities/view_source_all.php
  Parameter type: GET
  Attacked parameter: id
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: id=/../../../../../../../../../../../../../../etc/passwd%00
  id=/../../../../../../../../../../../../../../..//etc/passwd%00
- Page: http://10.1.5.38/dvwa/vulnerabilities/view_help.php?id=%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd%2500&security=low
  Action: http://10.1.5.38/dvwa/vulnerabilities/view_help.php
  Parameter type: GET
  Attacked parameter: id
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: id=/../../../../../../../../../../../../../../etc/passwd%00
  id=/../../../../../../../../../../../../../../..//etc/passwd%00
- Page: http://10.1.5.38/dvwa/vulnerabilities/view_source.php?id=%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fet

c%2Fpasswd%2500&security=low
Action: http://10.1.5.38/dvwa/vulnerabilities/view_source.php
Parameter type: GET
Attacked parameter: id
Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
Informations: id=/../../../../../../../../../../../../../../etc/passwd%00
id=/../../../../../../../../../../../../../..//etc/passwd%00

- Page: http://10.1.5.38/dvwa/vulnerabilities/fi/?page=%2Fetc%2Fpasswd
  Action: http://10.1.5.38/dvwa/vulnerabilities/fi/
  Parameter type: GET
  Attacked parameter: page
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
  Informations: page=/etc/passwd
  page=/etc/passwd
  page=php://input

Development / Cross-Site Request Forgery — High

Description: CSRF (or XSRF) attacks help an attacker to make the user performs requests without his consent

Remediation: Protect forms by adding a token with an unpredictable value and by checking this value when forms data are received

Priority: High

Methodology: black box

Risk: 7.1 (Impact: 6.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:M/A:N/).

References: OWASP 2013 A8, OWASP Prevention sheet, CWE-352 , PCI DSS 6.5.9

- Page: http://10.1.5.38/dvwa/vulnerabilities/sqli_blind/
  Informations: Form: '<form action="#" method="GET"></form>' is vulnerable
- Page: http://10.1.5.38/dvwa/vulnerabilities/captcha/
  Informations: Form: '<form action="#" method="POST"></form>' may be vulnerable (no anti-csrf token found)
- Page: http://10.1.5.38/dvwa/vulnerabilities/brute/
  Informations: Form: '<form action="#" method="GET"></form>' may be vulnerable (no anti-csrf token found)
- Page: http://10.1.5.38/dvwa/vulnerabilities/csrf/
  Informations: Form: '<form action="#" method="GET"></form>' may be vulnerable (no anti-csrf token found)
- Page: http://10.1.5.38/dvwa/vulnerabilities/exec/
  Informations: Form: '<form action="#" method="post" name="ping"></form>' is vulnerable
- Page: http://10.1.5.38/dvwa/vulnerabilities/xss_s/
  Informations: Form: '<form method="post" name="guestform" onsubmit="return validate_form(this)"></form>' is vulnerable
- Page: http://10.1.5.38/dvwa/vulnerabilities/xss_r/
  Informations: Form: '<form action="#" method="GET" name="XSS"></form>' is vulnerable
- Page: http://10.1.5.38/dvwa/vulnerabilities/sqli/
  Informations: Form: '<form action="#" method="GET"></form>' is vulnerable

Configuration / Password Capture — Moderate

Description: An form authentication password is sent over HTTP, which enables interception or spoofing.

Remediation: Encrypt the communication (using HTTPS).

Priority: Moderate

Methodology: black box

Risk: 6.4 (Impact: 7.8, Exploitability: 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:N/A:P/).

References: OWASP 2013 A6, OWASP Prevention sheet, CWE-319 , PCI DSS 6.5.4

- Page: http://10.1.5.38/dvwa/vulnerabilities/brute/
  Action: http://10.1.5.38/dvwa/vulnerabilities/brute/
  Parameter type: GET
  Attacked parameter: password
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
- Page: http://10.1.5.38/dvwa/vulnerabilities/csrf/
  Action: http://10.1.5.38/dvwa/vulnerabilities/csrf/
  Parameter type: GET
  Attacked parameter: password_new
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
- Page: http://10.1.5.38/dvwa/vulnerabilities/captcha/
  Action: http://10.1.5.38/dvwa/vulnerabilities/captcha/
  Parameter type: POST
  Attacked parameter: password_new
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low
- Page: http://10.1.5.38/dvwa/login.php
  Action: http://10.1.5.38/dvwa/login.php
  Parameter type: POST
  Attacked parameter: password
  Cookie: PHPSESSID=g4eur49fvr58n4jt1k1nbfvfm1;security=low

Development / Session fixation — Moderate

Description: Keeping the same session ID when a user log-in can help a "session fixation" attack.

Remediation: Change session id when authenticating

Priority: Moderate

Methodology: white box

Risk: 5.8 (Impact: 4.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:P/A:N/).

References: OWASP 2013 A2, OWASP session management sheet, CWE-384

- Page: http://10.1.5.38/dvwa/login.php

Configuration / Remote administration interface — Moderate

Description: We found an administration interface with remote access

Remediation: Disable it

Priority: Moderate

Methodology: black box

Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).

- Page: http://10.1.5.38/dvwa/config/

Configuration / Fuzzing — Moderate

Description: The web server configuration allows an attacker to retrieve architecture information, allowing him to completely crawl the website.

Remediation: Modify the server configuration to correct the flaws listed below, or remove the file that facilitates crawling the website (they should not be found on a production server).

Priority: Moderate

Methodology: black box

Risk: 5.0 (Impact: 2.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:P/I:N/A:N/).

- Page: http://10.1.5.38/dvwa/robots.txt

Configuration / TRACE HTTP method enabled — Moderate

Description: Trace http method is active

Remediation: Disable it

Priority: Moderate

Methodology: black box

Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).

References: OWASP Cross Site Tracing

- Page: http://10.1.5.38/dvwa/
  Parameter type: HTTP
  Attacked parameter: TRACE

Configuration / Information leakage — Moderate

Description: The web server configuration allows retrieving architecture information which could be useful to execute a malicious attack.

Remediation: Modify the server configuration to correct the flaws listed below.

Priority: Moderate

Methodology: black box

Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).

- Page: http://10.1.5.38/dvwa/dvwa/css/
  Informations: Directory indexing: http://10.1.5.38/dvwa/dvwa/css/
- Page: http://10.1.5.38/dvwa/dvwa/
  Informations: Directory indexing: http://10.1.5.38/dvwa/dvwa/
- Page: http://10.1.5.38/dvwa/dvwa/js/
  Informations: Directory indexing: http://10.1.5.38/dvwa/dvwa/js/
- Page: http://10.1.5.38/dvwa/dvwa/includes/
  Informations: Directory indexing: http://10.1.5.38/dvwa/dvwa/includes/
- Page: http://10.1.5.38/dvwa/vulnerabilities/
  Informations: Directory indexing: http://10.1.5.38/dvwa/vulnerabilities/
- Page: http://10.1.5.38/dvwa/dvwa/includes/DBMS/
  Informations: Directory indexing: http://10.1.5.38/dvwa/dvwa/includes/DBMS/
- Page: http://10.1.5.38/dvwa/config/
  Informations: Directory indexing: http://10.1.5.38/dvwa/config/
- Page: http://10.1.5.38/dvwa/dvwa/images/
  Informations: Directory indexing: http://10.1.5.38/dvwa/dvwa/images/

http://192.168.1.21/mutillidae

Access control / Trivial authentication account — Critical

Description: A trivial authentication account was found on this page of the website

Remediation: Change the password of the account to a more complicated one

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

References: OWASP 2013 A2, OWASP prevention sheet, CWE-521

- Page: http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Action: http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Informations: [POST(Fuzz) - http://192.168.1.21/mutillidae/index.php?page=user-info.php Params:{#view_user_name:admin#password:admin#Submit_button:Submit}]

Development / SQL injection — Critical

Description: A SQL injection attack consists of insertion or injection of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Remediation: Primary Defenses: use of Prepared Statements (Parameterized Queries), use of Stored Procedures, escaping all user-supplied input. Additional Defenses: enforce least privilege and perform white list input validation.

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

References: OWASP 2013 A1, OWASP prevention sheet, CWE-89 , PCI DSS 6.5.1

- Page: http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php
  Action: http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php
  Parameter type: POST
  Attacked parameter: uid
  Cookie: uid=1
  Informations: [Cookie -> -9448' OR 9272=SLEEP(6) AND 'VULNITsVtDw'='VULNITsVtDw]
- Page: http://192.168.1.21/mutillidae/index.php?page=login.php
  Action: http://192.168.1.21/mutillidae/index.php
  Parameter type: GET
  Attacked parameter: uid
  Cookie: uid=1
  Informations: [Cookie -> -4093' OR 6668=SLEEP(6) AND 'VULNITslKow'='VULNITslKow]
- Page: http://192.168.1.21/mutillidae/redirectandlog.php?forwardurl=-6036%27%20OR%207735%3DSLEEP%286%29%20AND%20%27VULNITsatyf%27%3D%27VULNITsatyf
  Action: http://192.168.1.21/mutillidae/redirectandlog.php
  Parameter type: GET
  Attacked parameter: forwardurl
  Informations: forwardurl=-6036' OR 7735=SLEEP(6) AND 'VULNITsatyf'='VULNITsatyf
- Page: http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php

Action: http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php
Parameter type: POST
Attacked parameter: show_only_user
Informations: show_only_user=-6360' OR
5524=BENCHMARK(6000000,MD5(CHAR(109,100,77,67))) AND 'VULNITsuxPd'='VULNITsuxPd

- Page: http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Action: http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Parameter type: POST
  Attacked parameter: view_user_name
  Informations: view_user_name=-1165' OR
  2626=BENCHMARK(6000000,MD5(CHAR(116,109,65,77))) AND 'VULNITsyayF'='VULNITsyayF
- Page: http://192.168.1.21/mutillidae/index.php?page=register.php
  Action: http://192.168.1.21/mutillidae/index.php?page=register.php
  Parameter type: POST
  Attacked parameter: user_name
  Informations: user_name=-6715' OR
  1607=BENCHMARK(6000000,MD5(CHAR(100,73,81,119))) AND
  'VULNITsaqnA'='VULNITsaqnA

Development / Cross-Site Scripting — Major

Description: Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

Remediation: Output Encoding: a technique used to ensure that characters are treated as data, not as characters that are relevant to the interpreter\'s parser. There are lots of different types of escaping, sometimes confusingly called output encoding. Some of these techniques define a special escape character, and other techniques have a more sophisticated syntax that involves several characters.

Priority: Major

Methodology: black box

Risk: 8.3 (Impact: 8.5, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:C/A:P/).

References: OWASP 2013 A3, OWASP prevention sheet, CWE-79 , PCI DSS 6.5.7

- Page: http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Action: http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Parameter type: POST
  Attacked parameter: view_user_name
  Informations: view_user_name=<script>alert(33155949271132212779038 3)</script>
- Page: http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php
  Action: http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php
  Parameter type: POST
  Attacked parameter: input_from_form
  Informations: input_from_form=<script>alert(33155949271132212779195 6)</script>
- Page: http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php
  Action: http://192.168.1.21/mutillidae/index.php?page=view-someones-blog.php
  Parameter type: POST
  Attacked parameter: show_only_user
  Informations: show_only_user=<script>alert(33155949271132212779252 1)</script>
- Page: http://192.168.1.21/mutillidae/index.php?submit=Submit&page=source-viewer.php&php_file_name=%3Cscript%3Ealert%28331559492711322127793620%29%3C%2Fscript%3E
  Action: http://192.168.1.21/mutillidae/index.php
  Parameter type: GET
  Attacked parameter: php_file_name
  Informations: php_file_name=<script>alert(33155949271132212779362 0)</script>
- Page: http://192.168.1.21/mutillidae/index.php?page=login.php

Action: http://192.168.1.21/mutillidae/index.php?page=login.php
Parameter type: POST
Attacked parameter: user_name
Informations: user_name=<script>alert(331559492711322127789288)</script>

- Page: http://192.168.1.21/mutillidae/index.php?page=register.php
  Action: http://192.168.1.21/mutillidae/index.php?page=register.php
  Parameter type: POST
  Attacked parameter: password
  Informations: password=<script>alert(331559492711322127788820)</script>

Configuration / Database fingerprint — High

Description: Giving information on the database system used mays help an attacker (error messages...)

Remediation: Do not display error messages giving information on the database used

Priority: High

Methodology: black box

Risk: 7.8 (Impact: 6.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N/).

References: PCI DSS 6.5.5

- Page: http://192.168.1.21/mutillidae/?page=register.php
  Action: http://192.168.1.21/mutillidae/
  Informations: An error showed that the DBMS could be MySQL
- Page: http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php
  Action: http://192.168.1.21/mutillidae/index.php?page=add-to-your-blog.php
  Informations: An error showed that the DBMS could be MySQL

Development / Local file inclusion — High

Description: Local file inclusion allows an attacker disclose information from the application server.

Remediation: File inclusion can be avoided by protecting the objects parameters references (internal or external). It may also be restricted by appropriate server configurations.

Priority: High

Methodology: black box

Risk: 7.8 (Impact: 7.8, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:C/I:N/A:P/).

References: OWASP 2007 A3, CWE-98 , PCI DSS 6.5.1

- Page: http://192.168.1.21/mutillidae/index.php?submit=Submit&page=%2Fetc%2Fpasswd&php_file_name=vulnit-0.01902171156707999
  Action: http://192.168.1.21/mutillidae/index.php?submit=Submit&page=/etc/passwd&php_file_name=vulnit-0.01902171156707999
  Parameter type: GET
  Attacked parameter: page
- Page: http://192.168.1.21/mutillidae/?page=%2Fetc%2Fpasswd
  Action: http://192.168.1.21/mutillidae/?page=/etc/passwd
  Parameter type: GET
  Attacked parameter: page
- Page: http://192.168.1.21/mutillidae/index.php?submit=Submit&page=source-viewer.php&php_file_name=%2Fetc%2Fpasswd
  Action: http://192.168.1.21/mutillidae/index.php?submit=Submit&page=source-viewer.php&php_file_name=/etc/passwd

Parameter type: GET
Attacked parameter: php_file_name

- Page: http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php&text_file_name=http%3A%2F%2Fwww.phpbb.de%2Findex.php&B1=Submit
  Action: http://192.168.1.21/mutillidae/index.php?page=text-file-viewer.php
  Parameter type: GET
  Attacked parameter: text_file_name

Configuration / Password Capture	Moderate

Description: An form authentication password is sent over HTTP, which enables interception or spoofing.

Remediation: Encrypt the communication (using HTTPS).

Priority: Moderate

Methodology: black box

Risk: 6.4 (Impact: 7.8, Exploitability: 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:N/A:P/).

References: OWASP 2013 A6, OWASP Prevention sheet, CWE-319 , PCI DSS 6.5.4

- Page: http://192.168.1.21/mutillidae/?page=user-info.php
  Action: http://192.168.1.21/mutillidae/index.php?page=user-info.php
  Parameter type: GET
  Attacked parameter: password

http://192.168.1.21/WackoPicko

Access control / Trivial authentication account — Critical

Description: A trivial authentication account was found on this page of the website

Remediation: Change the password of the account to a more complicated one

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

References: OWASP 2013 A2, OWASP prevention sheet, CWE-521

- Page: http://192.168.1.21/WackoPicko/admin/index.php?page=login
  Action: http://192.168.1.21/WackoPicko/admin/index.php?page=login
  Informations: [POST(Fuzz) - http://192.168.1.21/WackoPicko/admin/index.php?page=login
  Params:{#adminname:admin#password:admin}
  Cookies:{%PHPSESSID:k56vbc1uf3dnabf5kcdbcecoc5}]

Development / SQL injection — Critical

Description: A SQL injection attack consists of insertion or injection of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Remediation: Primary Defenses: use of Prepared Statements (Parameterized Queries), use of Stored Procedures, escaping all user-supplied input. Additional Defenses: enforce least privilege and perform white list input validation.

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

References: OWASP 2013 A1, OWASP prevention sheet, CWE-89 , PCI DSS 6.5.1

- Page: http://192.168.1.21/WackoPicko/users/login.php
  Action: http://192.168.1.21/WackoPicko/users/login.php
  Parameter type: POST
  Attacked parameter: username
  Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
  Informations: username=-8709' OR 7409=SLEEP(6) AND 'VULNITsUMlJ'='VULNITsUMlJ

Development / Cross-Site Scripting — Major

Description: Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

Remediation: Output Encoding: a technique used to ensure that characters are treated as data, not as characters that are relevant to the interpreter\'s parser. There are lots of different types of escaping, sometimes confusingly called output encoding. Some of these techniques define a special escape character, and other techniques have a more sophisticated syntax that involves several characters.

Priority: Major

Methodology: black box

Risk: 8.3 (Impact: 8.5, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:C/A:P/).

References: OWASP 2013 A3, OWASP prevention sheet, CWE-79 , PCI DSS 6.5.7

- Page: http://192.168.1.21/WackoPicko/piccheck.php
  Action: http://192.168.1.21/WackoPicko/piccheck.php
  Parameter type: POST
  Attacked parameter: name
  Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
  Informations: name=<script>alert(331559492711322129319722)</script>
- Page: http://192.168.1.21/WackoPicko/pictures/search.php?query=%3Cscript%3Ealert%28331559492711322129318918%29%3C%2Fscript%3E&y=0&x=0
  Action: http://192.168.1.21/WackoPicko/pictures/search.php
  Parameter type: GET
  Attacked parameter: query
  Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
  Informations: query=<script>alert(331559492711322129318918)</script>
- Page: http://192.168.1.21/WackoPicko/guestbook.php
  Action: http://192.168.1.21/WackoPicko/guestbook.php
  Parameter type: POST
  Attacked parameter: comment
  Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
  Informations: comment=<script>alert(331559492711322129321736)</script>

Configuration / Password Capture — Moderate

Description: An form authentication password is sent over HTTP, which enables interception or spoofing.

Remediation: Encrypt the communication (using HTTPS).

Priority: Moderate

Methodology: black box

Risk: 6.4 (Impact: 7.8, Exploitability: 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:N/A:P/).

References: OWASP 2013 A6, OWASP Prevention sheet, CWE-319 , PCI DSS 6.5.4

- Page: http://192.168.1.21/WackoPicko/users/login.php
  Action: http://192.168.1.21/WackoPicko/users/login.php
  Parameter type: GET
  Attacked parameter: password
  Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
- Page: http://192.168.1.21/WackoPicko/passcheck.php
  Action: http://192.168.1.21/WackoPicko/passcheck.php
  Parameter type: GET
  Attacked parameter: password
  Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
- Page: http://192.168.1.21/WackoPicko/admin/index.php?page=login
  Action: http://192.168.1.21/WackoPicko/admin/index.php?page=login
  Parameter type: GET
  Attacked parameter: password
  Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5
- Page: http://192.168.1.21/WackoPicko/users/register.php

Action: http://192.168.1.21/WackoPicko/users/register.php
Parameter type: GET
Attacked parameter: password
Cookie: PHPSESSID=k56vbc1uf3dnabf5kcdbcecoc5

Configuration / Information leakage	Moderate

Description: The web server configuration allows retrieving architecture information which could be useful to execute a malicious attack.

Remediation: Modify the server configuration to correct the flaws listed below.

Priority: Moderate

Methodology: black box

Risk: 4.3 (Impact: 2.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:N/A:N/).

- Page: http://192.168.1.21/WackoPicko/
  Action: http://192.168.1.21/WackoPicko/
  Informations: mailto:contact@wackopicko.com
- Page: http://192.168.1.21/WackoPicko/pictures/
  Action: http://192.168.1.21/WackoPicko/pictures/
  Informations: Directory indexing: http://192.168.1.21/WackoPicko/pictures/
- Page: http://192.168.1.21/WackoPicko/users/
  Action: http://192.168.1.21/WackoPicko/users/
  Informations: Directory indexing: http://192.168.1.21/WackoPicko/users/

http://192.168.56.30/bodgeit/

Access control / Trivial authentication account — Critical

Description: A trivial authentication account was found on this page of the website

Remediation: Change the password of the account to a more complicated one

Priority: Critical

Methodology: black box

Risk: 10.0 (Impact: 10.0, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:C/A:C/).

References: OWASP 2013 A2, OWASP prevention sheet, CWE-521

- Page: http://192.168.56.30/bodgeit/login.jsp
  Informations: [test@thebodgeitstore.com:password]

Development / Cross-Site Scripting — Major

Description: Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

Remediation: Output Encoding: a technique used to ensure that characters are treated as data, not as characters that are relevant to the interpreter\'s parser. There are lots of different types of escaping, sometimes confusingly called output encoding. Some of these techniques define a special escape character, and other techniques have a more sophisticated syntax that involves several characters.

Priority: Major

Methodology: black box

Risk: 8.3 (Impact: 8.5, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:P/I:C/A:P/).

References: OWASP 2013 A3, OWASP prevention sheet, CWE-79 , PCI DSS 6.5.7

- Page: http://192.168.56.30/bodgeit/search.jsp?q=%3Cscript%3Ealert%2831337137635400324 3%29%3C%2Fscript%3E
  Action: http://192.168.56.30/bodgeit/search.jsp
  Parameter type: GET
  Attacked parameter: q
  Cookie: JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
  Informations: q=<script>alert(313371376354003243)</script>

Configuration / Database fingerprint — High

Description: Giving information on the database system used mays help an attacker (error messages...)

Remediation: Do not display error messages giving information on the database used

Priority: High

Methodology: black box

Risk: 7.8 (Impact: 6.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:C/I:N/A:N/).

References: PCI DSS 6.5.5

- Page: http://192.168.56.30/bodgeit/basket.jsp
  Action: http://192.168.56.30/bodgeit/basket.jsp
  Cookie: JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
  Informations: Some errors found during SQL injection test: SQLException: Unexpected end of command in statement [UPDATE BasketContents SET quantity = 1 WHERE basketid=-5059
  SQLException: Unexpected end of command in statement [UPDATE BasketContents SET quantity = 1 WHERE basketid=-6530
  SQLException: Unexpected end of command in statement [UPDATE BasketContents SET quantity = 1 WHERE basketid=-7338
  SQLException: Unexpected end of command in statement [UPDATE BasketContents SET quantity = 1 WHERE basketid=-7914
  SQLException: Unexpected end of command in statement [UPDATE BasketContents SET quantity = 1 WHERE basketid=2

Development / Cross-Site Request Forgery — High

Description: CSRF (or XSRF) attacks help an attacker to make the user performs requests without his consent

Remediation: Protect forms by adding a token with an unpredictable value and by checking this value when forms data are received

Priority: High

Methodology: black box

Risk: 7.1 (Impact: 6.9, Exploitability: 8.6) CVSS : (AV:N/AC:M/AU:N/C:N/I:M/A:N/).

References: OWASP 2013 A8, OWASP Prevention sheet, CWE-352 , PCI DSS 6.5.9

- Page: http://192.168.56.30/bodgeit/contact.jsp
  Informations: Form: '<form method="POST"></form>' may be vulnerable (no anti-csrf token found)
- Page: http://192.168.56.30/bodgeit/basket.jsp
  Informations: Form: '<form action="basket.jsp" method="post"></form>' is vulnerable

Configuration / Insecure HTTP method - listed — Moderate

Description: Some insecure methods have been found using the method OPTIONS. These methods may allow a user to modify the content of the website (eg: DELETE, MKCOL, PUT)

Remediation: Disable insecure HTTP methods or restrict them to some authenticated users.

Priority: Moderate

Methodology: black box

Risk: 6.4 (Impact: 4.9, Exploitability: 10.0) CVSS : (AV:N/AC:L/AU:N/C:N/I:P/A:P/).

- Page: http://192.168.56.30/bodgeit/
  Parameter type: HTTP
  Informations: PUT, DELETE: http://192.168.56.30/bodgeit/js/
  PUT, DELETE: http://192.168.56.30/bodgeit/images/

Configuration / Password Capture	Moderate

Description: An form authentication password is sent over HTTP, which enables interception or spoofing.

Remediation: Encrypt the communication (using HTTPS).

Priority: Moderate

Methodology: black box

Risk: 6.4 (Impact: 7.8, Exploitability: 5.5) CVSS : (AV:A/AC:M/AU:N/C:C/I:N/A:P/).

References: OWASP 2013 A6, OWASP Prevention sheet, CWE-319 , PCI DSS 6.5.4

- Page: http://192.168.56.30/bodgeit/login.jsp
  Action: http://192.168.56.30/bodgeit/login.jsp
  Parameter type: POST
  Attacked parameter: password
  Cookie: JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
- Page: http://192.168.56.30/bodgeit/register.jsp
  Action: http://192.168.56.30/bodgeit/register.jsp
  Parameter type: POST
  Attacked parameter: password1
  Cookie: JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
- Page: http://192.168.56.30/bodgeit/password.jsp
  Action: http://192.168.56.30/bodgeit/password.jsp
  Parameter type: POST
  Attacked parameter: password1
  Cookie: JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2

Configuration / AutoComplete enabled	Low

Description: The attribute autocomplete allows the browser to keep entered value to permit autocompletion of forms. Disabling this function increase the sercurity when other users have access to the browser.

Remediation: Add attribute autocomplete=off to form or input tags.

Priority: Low

Methodology: black box

Risk: 3.3 (Impact: 4.9, Exploitability: 3.4) CVSS : (AV:L/AC:M/AU:N/C:P/I:P/A:N/).

References: OWASP Session management

- Page: http://192.168.56.30/bodgeit/password.jsp
  Action: http://192.168.56.30/bodgeit/password.jsp
  Parameter type: POST
  Attacked parameter: password1
  Cookie: JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
- Page: http://192.168.56.30/bodgeit/register.jsp
  Action: http://192.168.56.30/bodgeit/register.jsp
  Parameter type: POST
  Attacked parameter: password1
  Cookie: JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2
- Page: http://192.168.56.30/bodgeit/login.jsp
  Action: http://192.168.56.30/bodgeit/login.jsp
  Parameter type: POST
  Attacked parameter: password
  Cookie: JSESSIONID=5B9F09C337431A1CF53D75067A0C5664;b_id=2

Appendices

Appendix A: Website pages & forms

The following URLs and forms have been crawled and tested:

http://192.168.56.30/bodgeit/

- /
- /about.jsp
- /admin.jsp
- /advanced.jsp
- /basket.jsp
  - /basket.jsp (POST)
- /contact.jsp
  - /contact.jsp (POST)
- /home.jsp
- /images/
- /js/
- /login.jsp
  - /login.jsp (POST)
- /password.jsp
  - /password.jsp (POST)
- /product.jsp
  - /basket.jsp (POST)
- /register.jsp
  - /register.jsp (POST)
- /score.jsp
- /search.jsp
  - /search.jsp (GET)

Appendix B: Glossary

- **Target** - generic term which means server, desktop, workstation, printer, router or any other device accessible on the network.
- **Patch** - update fixing one or more vulnerabilities. Patches concern operating systems, databases, softwares, or packets (Unix).
- **CVSS** - Common Vulnerability Scoring System. This is an assessment standard of the severity of computer system security vulnerabilities. The Base metric is displayed as a 6-letter vector following each risk.
- **DBMS** - DataBase Management System.
- **Exploitability** - easiness to exploit a vulnerability. A higher exploitability indicates that the vulnerability requires less skills to be exploited, so a threat may more likely occur.
- **Function** - the control function determines the roots of a vulnerability. For instance, an SQL injection is caused by a development mistake. A trivial password comes from a wrong access control parameterization. The configuration of a service may also lead to information leakage.
- **Impact** - potential effect on the service availability, the confidentiality or the integrity of the data stored on a target.
- **DNS name** - Domaine Name Server. A name obtained by reverse resolution from the DNS server.
- **Netbios name** - Name of a target belonging to a Windows domain or workgroup.
- **Object** - the system concerned by the vulnerability: operating system (including the applications installed on the OS), DBMS, web servers/sites or network.
- **Priority** - The 3 levels (Critical, Major and High) suggested in this report facilitate the identification of the most critical vulnerabilities in order to address them first.
  Note: all the vulnerabilities mentioned in this report are high-risk issues (CVSS greater than 7) and thus, should all be addressed.
- **Risk** - potentiel risk of a threat exploiting the vulnerability. The final risk of a vulnerability should also consider the value of the targeted asset (i.e. the criticity of the information stored in this target or the operational dependancy to the services provided by this target) and the controls that could mitigate the risk (audit logs, contingency plan, etc).
  The risk computation is explained in this document (in the Base metric chapter).
- **Vulnerability** - weakness which allows an attacker to reduce a system's information assurance (in terms of service availability, integrity or confidentiality of the information stored on the targeted device).

Appendix C: Auditing tools

- **Aircrack** is a set of auditing tools allowing to analyse the security of wifi access points. Author and maintainer: Thomas d'Otreppe.
- **db2getprofile** (part of the db2utils suite) gets the access profile to DB2 database and particularly lists the instances and databases. Author and maintainer: Patrik Karlsson.
- **dhcping** is a DHCP and BOOTP scanner. Author et maintainer: Edwin Groothuis.
- **dig** - provided within the dnsutils package - allows to request a DNS server to get the list of the nameservers by DNS zone transfer. Author and maintainer: Internet Systems Consortium, Inc (ISC).
- **fimap** is an open source penetration testing tool that automates the process of detecting file inclusion flaws. Author and maintainer: Iman Karim.
- **flasm** disassembles SWF menus in order to extract the links redirecting to other webpages. Author and maintainer: Ben Schleimer.
- **git** is a distributed version control system Author and maintainer: Linus Torvalds.
- **Medusa** allows to test connexion ID on lots of services (FTP, SSH, SNMP, SMTP...). Author and maintainer: JoMo-Kun.
- **mit-krb5** implements under unix the kerberos protocol used for the domain authentication (when the domain is managed by an Active Directory starting from Windows 2003). Author and maintainer: Massachusetts Institute of Technology.
- **MSSQLScan** allows to get some informations on Microsoft SQL Server database. Author and maintainer: Patrik Karlsson.
- **nbtscan** includes the same features as windows 'nststat' command (listing all open Netbios services). Author and maintainer: Stephen Friedl.
- **Nmap**, the famous ports scanner used to detect running services on targets. Author and maintainer: Gordon Lyon.
- **OpenVAS** integrates several thousands of tests upon patch management: OS, applications, DBMS, etc. Author and maintainer: OpenVAS team.
- **rpcclient** allows to acces to "named pipe" and to execute MS RPC commands. It's part of the Samba suite. Author and maintainer: Samba team.
- **SidGuesser** allows to discover Oracle instances when they are transmitted by listener (attacking using a dictionary). Author and maintainer: Patrik Karlsson.
- **snmpwalk** provided within the net-snmp package allows to browse informations given by SNMP protocol. Author and maintainer: Net-SNMP.
- **SMBAT**(SaMBa Auditing Tools) includes smbdumpusers tool allowing to list the users of Windows NT/2000. Author and maintainer: Patrik Karlsson.
- **samba** is the standard Windows interoperability suite of programs for Linux and Unix. Author and maintainer: Samba team.
- **sqlmap** is an open source penetration testing tool that automates the process of detecting SQL injection flaws. Author and maintainer: Bernardo Damele.
- **sslscan** determines which cryptographic algorithms is in use on a SSL server (basically in the case of an https webapplication). Author and maintainer: Ian Ventura-Whiting.
- **Tiger** is a Unix security audit and intrusion detection tool. Author and maintainer: Tiger.
- **tnscmd10g** allows to list the instances of the Oracle database (including 10g and 11g versions). Author: James W. Abendschan, Maintainer: Saez Scheihing.
- **WhatWeb** identifies content management systems (CMS), blogging platforms, stats/analytics packages, javascript libraries, servers and more. Author and maintainer: Brendan Coles.
- **wdiff** is a front end to diff for comparing files on a word per word basis. Author and maintainer: Denver Gingerich.

Appendix D: Report generation

- **The eZ Components library** allows to generate all the figures inside this report. Author and maintainer: eZ Systems.
- **PostgreSQL** is a relational database management system (RDBMS). Author and maintainer: PostgreSQL Global Development Group.
- **wkhtmltopdf** (read: WebKit HTML to PDF) combines the strength of the XHTML/CSS Webkit engine (used by Chrome and Safari for example) and its PDF library. Author and maintainer: Jakob Truelsen.

Legal notice

In accordance with the LCEN Act of 22 June 2004, the DenyAll product is exclusively made available for legitimate users and businesses whom their mission is to perform security audits.
By accepting the DenyAll agreement license, the user agrees to abide by the Godfrain act of January 6, 1988 punishing unauthorized intrusions into a computer system.

Copyright statement