



MAGNIFICENT IDENTITIES

**Magento Ecommerce Website  
Audit Sample Report  
XXXX Client**



## Summary

We have inspected the site, codebase and to certain degree the server as well. We have checked the backend code as well as the frontend code, with a full analysis on all the extensions used and the current database.

We also checked all the configuration settings and customer journey on different resolutions.

Based on this we can say that fixes, improvements and cleanup is necessary especially on the backend code, extension integration area - where high priority steps need to be done to ensure stability and maintainability. These steps we can carry out as a matter of urgency, and also on the server part we can work with Magento Hosting Company. We would be also happy to discuss some content related issues we found on the site!

More importantly unfortunately it seems that your site has been hacked, still infected and customer card details were stolen possibly, please see blocker issue below.

## Server and Security **BLOCKER**

We ran different scanning tools on the site and server and we identified different malicious code on the server. Magento's own scanning tool identified alterations in the Amazon Payment module, but also malicious card stealing script was planted on the site to steal card details.

Unfortunately we cant exactly see when these alterations were made, or how many card details were stolen but this definitely happened and the site is still infected!

Steps:

- Add version control (git) to make sure we can track additional alterations
- Clean and upgrade the Amazon Payments module to the latest
- Clean database from card stealing scripts
- Add missing security patches (see below) to block this and further strengthen security

**Estimation: 15**

## Backend code **HIGH**

The site has ~80 extensions - majority of these are installed and performing fine. But in many cases the code is full of unused or unnecessary file, or multiple versions of the same extension! These issues are causing instability and making the maintainability of the site difficult and time consuming.

Additionally many core files were overwritten making the upgrades really difficult, and also causing extra issues when the site is running.

The log files are full of different issues - clearly showing that the site is running into issues on different pages which further results in sub-optimal performance and reliability. Important to mention that these issues can grow bigger and can cause further issues going forward. Based on this we definitely recommend fixing these issues as a very first step. .

Steps:

- Code cleanup, removing unnecessary extension, extension upgrades to latest versions
- Fixing of wrong rewrites (conflicts with stock management, Core file rewrites)
- Working with simple servers to remove TLSv1.0
- Fixing issues identified in system logs (issues with stock handling, with tracking import, and in some cases issues with email sending based on the logs among other smaller ones)
- Adding missing security patches:  
**Security patch 10752, Security patch 10570, SUPEE-5994**
- <https://www.xxxxxx.com/calculators/page> fix as it generates errors
- In regards to **M2EPro** we believe that the memory settings are still misconfigured as it runs into memory limit **around 1GB only despite the memory limit being configured at 5GB**. This can be an other extension - or the issue is that currently a Beta version non public released is used in production environment, we will need to debug and add fixes accordingly.

**Estimation: 25-30h**

## Database **MEDIUM**

Based on our testing it seems that the database is performing fine, the server configuration seems fine as well, so that is good news! Although we noticed that the memory usage of the mysql server is pretty high - so this is something we should investigate with Magento Hosting Company. But as you have a 32GB memory server and based on our profiling there are still enough free memory left this is only a medium priority.

Steps:

- Consult with Magento Hosting Company to add mysql tuning configurations to improve memory usage

**Estimation: 2-4**

## Frontend Code **MEDIUM**

The frontend code is ok quality, but it has not been optimized for speed, and due to this Google PageSpeed and Gtmetrix are both downgrading the site performance which can result in poor SEO ranking as well (see screenshots attached at the end of this document). Also in some cases the customer experience and the mobile experience in general is not optimal.

Steps:

- Enable Javascript merging
- Enable CSS merging
- Full optimisation of images
- Serve media and static files through dedicated domain, or use a CDN solution (eg:media.XXX Client.com, static.XXX Client.com)
- Fix responsive issues

**Estimation: 12-16h**

## Configuration **MEDIUM / LOW**

The site is configured generally ok, but there are a few best practices that are missing, so we list them  here for sake of completeness:

- Sitemap: not configured
- Cookie Law: cookie restriction mode for asking permission for customers is not enabled  
Not complying with GDPR policies!
- SEO: Canonical tag not found - Google might see some content as duplication resulting in poor ranking
- SEO: Title and Description are not seo optimized
- SEO: Robots txt is missing - again site is not SEO optimised
- Product pages are not that user friendly, missing reviews, current content could be better displayed - would be happy to discuss possible update options

**Estimation: 8**



## Appendix A: Installed Extensions

	Extension	Feature	Action
1	Amazon_Diagnostics	Diagnostics for AMazon Payments	OK
2	Amazon_Payments	Amazon Payments	Infected, clean and upgrade
3	Aoe_Scheduler.xml	Utility to monitor cron jobs	OK
4	AW_Advancedreports.xml	Report creator	OK
5	BalkeTechnologies_StoreMaintenance.xml	Maintenance page, not used	Remove
6	BL_CustomGrid.xml	Admin Grid customizer	OK
7	Cm_RedisSession.xml	RedisCache extension	OK
8	Cmsmart_AjaxCart.xml	Theme extension for ajax cart, not used	Remove
9	Cmsmart_Ajaxsearch.xml	Theme extension for ajax search, not used	Remove
10	Cmsmart_CloudZoom.xml	Theme extension for product Zoom, not used	Remove
11	Cmsmart_CustomAttribute.xml	Theme extension for extra attributes, not used	Remove
12	Cmsmart_Qty.xml	Theme extension for extra attributes, not used	Remove



# Appendix B: Site screenshots

SECURITY issues:

## MAGENTO Security Scan Results



Tech Resources [Go to Magento.com](#)

[My Account](#)

[RESOURCES](#)

[SECURITY](#)

[DOWNLOAD](#)

### Security Report for **XXX CLIENT**

[Download PDF](#)

#### Failed Scans

Your site has failed a scan. This means it is vulnerable to attack or already a victim of malicious software.

Status	Group	Scan Name	Scan Details	Actions
<b>FAIL</b>	Compromise	Magento Compromise Injection	Your site is compromised with injected JavaScript. (81) The malicious code signature(s) has been found on the page. The malicious code signature(s) has been found in resources: <a href="https://furnishedukmagento-amclightingdirec.netdna-ssl.com/js/creativestyle/amazonpayments.min.js">https://furnishedukmagento-amclightingdirec.netdna-ssl.com/js/creativestyle/amazonpayments.min.js</a>	Review your site for signs of compromise. Find more information about <a href="#">How to Detect Malware</a> and apply <a href="#">security best practices</a> .
<b>FAIL</b>	Patch	Magento SUPEE 5994	SUPEE-5994 - Failed. HTTP 301, 302 or 404 expected (APPSEC-965), got '200'. HTTP 301, 302 or 404 expected (APPSEC-965), got '200'.	Apply the patch immediately. Review your site for signs of compromise. Find more information about <a href="#">SUPEE-5994 patch</a> and <a href="#">Security Best Practices</a> .
<b>FAIL</b>	Vulnerability	SSL TLS	Your server supports TLSv1.0. Please update your configuration to discontinue TLSv1.0 support	

#### Unidentified Results



# MAGEREPORT Security Scan Results

Enter shop or backend URL  **Go** >

**Rescan all** ↻

1 **www.XXXCLIENT.com** ⓧ

**Reports**

**HIGH Risk** for **www.XXXCLIENT.com** site is infected missing patches **Rescan** ↻

**Credit Card Hijack detected?** **hacked**

Magento 1 & 2 Risk rating **High**

This Credit Card Hijack check detects whether there is malicious javascript code injected into Magento shops that allows hackers to intercept credit card data. It also detects the malware signatures related with the MagentoCore and MageCart skimmer.

> [Read more about this check](#)

Malicious code found, you are vulnerable [How do I fix it?](#)

**Security patch 10752** **unknown**

Magento 1

SUPEE-10752 was released June 27th, 2018. This patch fixes several security issues.

> [More about applying Magento patches](#)

This patch cannot be detected from the outside of your store. [How do I verify that I am protected?](#)

**Security patch 10570** **unknown**

Magento 1

SUPEE-10570 was released February 27th, 2018. This patch fixes several security issues.

> [More about applying Magento patches](#)

This patch cannot be detected from the outside of your store. [How do I verify that I am protected?](#)

**Security patch 6788 (secrets leak)** **installed**

Magento 1

Patch SUPEE-6788 fixes multiple issues: in some cases hackers can steal your passwords and customer data. Released October 27th, 2015

> [Read more](#)

Brought to you by the  
Magento hosting  
platform  
**HYPERNODE**  
by *byte*

- ✓ Save your site list.
- ✓ Get notified about new vulnerabilities.

H > [Register using Hypernode by Byte](#)

> [Register using Github](#)

> [Register using Google](#)

> [Register using LinkedIn](#)



## RESPONSIVE issues:

Length  
165cm (65in)

Unit Price: £16.99

[Edit](#)

Qty:  [↻](#)

Subtotal: £16.99

[✕ Remove](#)

Subtotal £72.96

Shipping & Handling (Free Standard Delivery (3-4 working days)) £0.00

Grand Total £72.96

Estimate Shipping and Tax [▼](#)

Discount Codes [▼](#)



**EBAY BUYER**

Excellent, thank you beautiful , super fast delivery.  
Quality Blackout Roller Blinds Thermal Fabric Metal  
Tube - FREE Cut Down Service.

● ○ ○

**XXX CLIENT**

**MENU**

[My Account](#) [Log In](#) [Sign Up](#)

[Contact Us](#)

Search our entire store... [Cart](#)

## Shopping Cart

**Proceed to Checkout**

[Pay with Amazon](#) or

[PayPal Check out](#)  
The safer, easier way to pay

Childrens Curtain Pole TweetyPie



## SPEED issues:

Speed Tools > Insights

GUIDES REFERENCE SUPPORT

## Speed Insights

www. XXX CLIENT.com/

Mobile Desktop

**Page Speed**  
Unavailable

**Optimization**  
**Medium**  
63 / 100



is currently showing a single-page report. Chrome User Experience Report [does not have sufficient real-world speed data](#) for this page, but was still able to analyze this page to identify potential optimizations that may improve the speed of this page. Please investigate the recommendations below. [Learn more.](#)

### Stats

Statistics show that the median page on the internet requires 4 render-blocking round trips and ~89 resources (1.3MB) to load. PSI estimates your page requires 5 render-blocking round trips and 85 resources (1.7MB) to load. Fewer round trips and bytes results in faster pages.

### Optimization Suggestions

- Optimize images  
[Learn how to fix](#)
- Defer render-blocking JavaScript and CSS in above-the-fold content  
[Learn how to fix](#)
- Minify JavaScript

## Gtmetrix rankings:

**GTmetrix** Features Resources Blog GTmetrix PRO Log In Sign Up

**Latest Performance Report for:**  
[https://www. XXXCLIENT .com/](https://www.XXXCLIENT.com/)

Report generated: Tue, Oct 23, 2018, 4:02 PM -0700  
Test Server Region: Vancouver, Canada  
Using: Chrome (Desktop) 62.0.3202.94, PageSpeed 1.15-gtI, YSlow 3.1.8

**Performance Scores**

PageSpeed Score <b>C (71%)</b>	YSlow Score <b>C (75%)</b>
-----------------------------------	-------------------------------

**Page Details**

Fully Loaded Time <b>3.5s</b>	Total Page Size <b>1.73MB</b>	Requests <b>83</b>
----------------------------------	----------------------------------	-----------------------

PageSpeed | YSlow | Waterfall | Timings | Video | History

RECOMMENDATION	GRADE	TYPE	PRIORITY
Optimize images	F (0)	IMAGES	HIGH
Serve scaled images	F (8)	IMAGES	HIGH
Defer parsing of JavaScript	F (22)	JS	HIGH
Minify JavaScript	B (80)	JS	HIGH
Leverage browser caching	B (89)	SERVER	HIGH
Minify CSS	A (92)	CSS	HIGH

**What do my scores mean?**

Rules are sorted in order of impact upon score. Optimizing rules at the top of the list can greatly improve your overall score.

**Not every recommendation will apply to your page.** The recommendations are meant to be generic, best practices, some things will be out of your control (eg. external resources) or may not apply to your page.

[Learn more about PageSpeed/YSlow scores and how they affect performance.](#)

Re-Test Compare Page Settings Monitor Set Up Alerts Download PDF

Share This Report