Vulnerability Audit and Assessment for ‘www.pamperedpets.org.uk’

Results and Executive Summary

Bradley Graham, 2024

Contents

I. Executive Summary

This report includes the executive summary and results of the vulnerability audit and assessment for the site ‘www.pamperedpets.org.uk’, complemented by the baseline analysis and plan previously provided.

A total of 11 unique vulnerabilities were found for the small website using a suite of open-source Dynamic Application Security Testing (DAST) tools which have been mapped to existing records in cyber-intelligence knowledge bases for reference. Vulnerabilities consisted of 10 technical vulnerabilities, and 1 human vulnerability; ranging from low to high impact, and low to medium likelihood of being exploited.

4 unique vulnerabilities stemmed from the outdated third-party Content Management System (CMS) software Joomla that should be updated. 1 unique vulnerability was due to a nearby service expiration date that should be renewed. 4 unique vulnerabilities were identified using a combination of skipfish and OWASP Zed Attack Proxy automated scans, that should be addressed by adjusting system configurations to employ safer protocols. 1 unique vulnerability arose through the identification of personal social media accounts associated with the site, and should be cleaned by wiping associations to the non-business accounts. The last vulnerability was a file exposure found through manual testing that should require privilege to access. It’s my recommendation that immediate action is taken. The site was found to be GDPR compliant pending mitigations of the highest priority vulnerabilities.

II. Identified Security Issues

ID	*Vulnerability*	*Aliases*	*Impact Score*	*Exploitation Likelihood*
1	Domain Name Hijacking	SSAC 007	High	Low
2	Vulnerable Third-Party Component	CWE-1395	High	Low
3	Improper Restriction of Excessive Authentication Attempts (MFA)	CVE-2023-23755, CWE-307	Moderate	Low
4	Improper Input Validation (MFA)	CVE-2023-23754, CWE-20, CWE-601	Moderate	Low
5	Exposure of Environment Variables (File Parsing)	CVE-2023-40626, CWE-200	High	Low
6	Files or Directories Accessible to External Parties	CWE-552	High	Medium
7	Impersonation	T1656	Moderate	Medium
8	MIME Type Mismatch	CAPEC-209	Low	Low
9	Improper Neutralization of Special Elements used in an SQL command	CWE-89	Moderate	Low
10	Missing CSRF tokens	CWE-352	Moderate	Low
11	Content Security Policy (CSP) Header Not Set	CWE-693	Low	Low

Figure 1. Security Issues of www.pamperedpets.org.uk

III. Risk Assessment

III. a. Impact, Likelihood and Priority Scores

The impact and likelihood scoring system used in section II is based upon Garvey's (2001) template. It consists of four impact categories: low, moderate, high and critical; and three likelihood categories: low, medium and high. Most security issues identified in this report would have a moderate impact on a business if they were exploited, but have a low likelihood of being exploited.

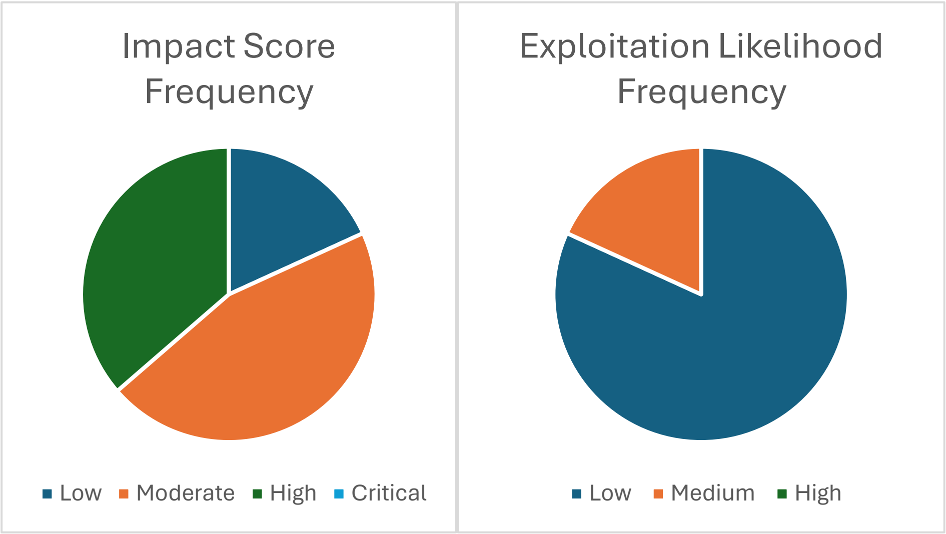


Figure 2. Impact and Exploitation Score Frequencies for the reported Security Issues of www.pamperedpets.org.

For each security issue, a priority is determined from combining the impact and likelihood scores using a risk matrix, as described by Dujim (2015). There are three bands of risk mitigation priority represented in this risk matrix: low priority, high priority, and urgent priority. These categories are represented from lightest grey to darkest grey respectively on the risk matrix below.

		Impact Scores			
		Low	Moderate	High	Critical
Likelihood Scores	High	▒	▒	▓	▓
	Medium	░	▒	▒	▓
	Low	░	░	▒	▒

Figure 3. A Risk Matrix portraying the range of Impact and Likelihood Scores associated with the identified Security Issues of www.pamperedpets.org.uk, with a Priority Score allocated to each combination.

There's an almost equal split of identified security issues, reported in section II, that have been given low and high priority for mitigating. Recommendations are given in section IV on how to remove this symmetry, and effectively reduce security risks.

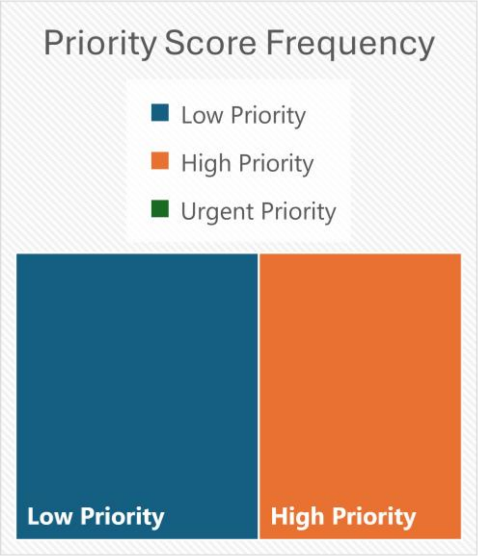


Figure 4. Priority Score Frequencies for the reported Security Issues of www.pamperedpets.org.uk

Priority	*Security Issue (ID)*
High	1, 2, 5, 6, 7
Low	3, 4, 8, 9, 10, 11

Figure 5. Map of Security Issues of www.pamperedpets.org.uk to Priority Band

III. b. Security Standards

An investigation into the legal and ethical compliance of 'www.pamperedpets.org.uk' was conducted regarding the newly found security issues. To ensure compliance with the General Data Protection Regulation (GDPR) each item on Proton AG's (2024) GDPR checklist was considered, which is a checklist co-founded by the Horizon 2020 Framework Programme of the European Union. The results of the consideration are summarised below:

GDPR: Lawful basis and transparency – The security issues have no impact on the lawful basis and transparency of the business' data processing activities.

GDPR: Data security – There is no evidence that the business is neglecting data security.

GDPR: Accountability and governance – The security issues have no impact on accountability and governance of the business.

GDPR: Privacy rights – There is no evidence that privacy rights are being neglected.

The degree of compliance to GDPR, of the business that owns www.pamperedpets.org.uk, is largely based on organisational factors. There was no evidence of personal information being utilised by the business. If personal information is being stored, then mitigations against the high priority security issues reported in section III.b must be adopted as is appropriate to the risks presented and the costs of implementation (ICO, n.d.). The continued investigation of low priority security vulnerabilities is necessary to maintain intelligence, and not ignore the possibility of surprise (Willis, 2007).

Discovery revealed there were no payment services being used at 'www.pamperedpet.org.uk', therefore PCI DSS compliance checks are not currently necessary. Discovery also didn't reveal anything about the information security management system (ISMS) of 'www.pamperedpets.org.uk' so an ISO 27001 compliance check was not possible too.

III. c. Methodology Limitations

The following tools were used to identify security issues at 'www.pamperedpets.org.uk':

Tool	*Function*
nikto	Web Server Scanning
skipfish	Active Web Application Scanning
WHOIS	Domain Name Registration Scanning
OWASP Zed Attack Proxy (ZAP)	Manual and Automated Web Application Scanning
Nmap	Network Discovery
theHarvester	OSINT Reconnaissance
hydra	Password Brute Forcing
sqlmap	Database Scanning

Figure 6. Vulnerability Assessment Tools used to identify Security Issues for www.pamperedpets.org.uk

Automated scanning sometimes produces observations being misclassified as security issues, also known as false-positives (Alavi et al, 2018). To compensate for this, manual verification was required before including security issues that were found using automated scanning tools. Unfortunately, this can lead to the under reporting of vulnerabilities, also known as false-negatives (Alavi et al, 2018).

The complete assessment was performed under black box conditions i.e. with a limit on the initial information available beforehand. Initial reconnaissance scanning included open-source intelligence (OSINT) gathering, yet did not provide enough intelligence to identify the legal business entity, or any media connected to 'www.pamperedpets.org.uk'. No economic, governance, management, or cyber-intelligence vulnerabilities could be identified due to this anonymity, although vulnerabilities of these types are reported to be likely (Johns & Ell, 2023).

Scanning revealed the following software is being used for 'www.pamperedpets.org.uk':

Software	*Version*	*Function*	*Latest Version*
Joomla	4.3.0	Content Management System	5.0.3
Apache	2.4.x	Web Server	2.4.58
PHP	8.0.30	Server-side Programming	8.3.3

Figure 7. Third Party Software that composes www.pamperedpets.org.uk

Software missing part of the version number could not be fully fingerprinted; therefore, the current version of those software must be treated as a range of version numbers. This report does not include an enumeration of vulnerabilities for ranges of version numbers due to the sheer amount of them. An assumption has been made that a software update is possible. Latest version security issues have been reported.

Scanning also revealed the following services are being used for 'www.pamperedpets.org.uk':

Services	*Function*
Enom	Domain Name Registrar
A2 Hosting	Website Hosting
cPanel	Website Hosting Control Panel

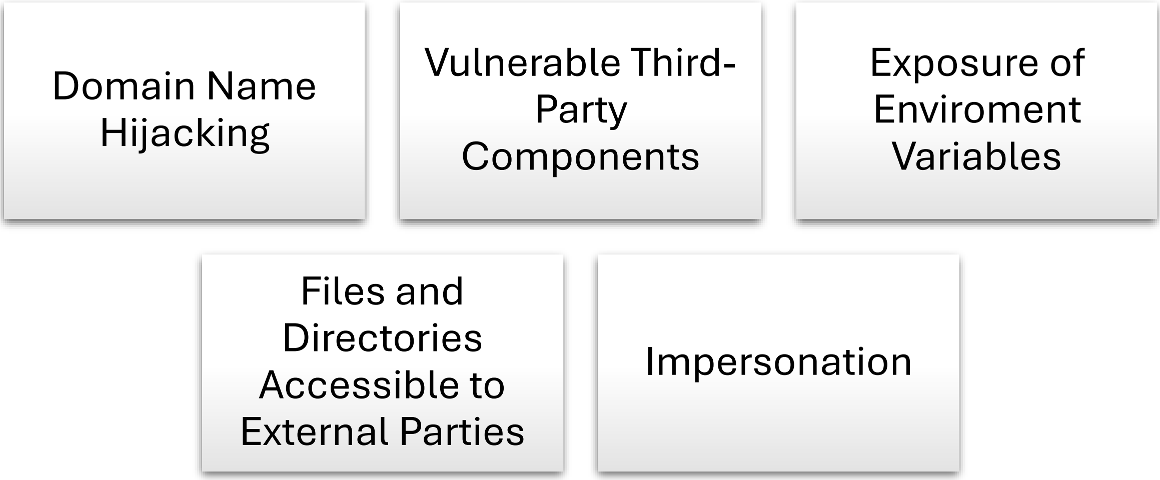
Figure 8. Third Party Services that are used by www.pamperedpets.org.uk

The list of services above is deemed important due to the possibility of impersonation, which is a growing security issue (Campobasso & Allodi, 2020). However, scanning did not reveal any specific human vulnerabilities for ‘www.pamperedpets.org.uk’.

Social media accounts were found for one person connected to ‘www.pamperedpets.org.uk’, whose name has not been included in this report for privacy reasons. The person had ‘www.pamperedpets.org.uk’ on their social media profile pages, as well as other information such as a telephone number, email address, and business address that appears to be active. There are clues suggesting this person is the previous domain name owner of ‘www.pamperedpets.org.uk’, not an active associate; so, with this possibility, no phishing attempts were conducted against them.

III. d. Risk Summary

The risk assessment of the reported security issues of ‘www.pamperedpets.org.uk’ reveals the five most urgent security issues to mitigate. The urgency is based on careful analysis of impact, likelihood, and compliance of the found security issues. It’s been noted that certain types of vulnerabilities were not identifiable through limitations of the penetration test, so a human-cantered security audit and assessment is recommended, but the following security issues are able to be addressed with significant reduction in business risk:



Domain Name Hijacking

Vulnerable Third-Party Components

Exposure of Enviroment Variables

Files and Directories Accessible to External Parties

Impersonation

Figure 8. The highest priority Security Issues to be mitigated on www.pamperedpets.org.uk

IV. Recommendations

The first recommended mitigation of this report is the prevention of domain name hijacking. The renewing of the nameserver service would be a form of prevention for ‘www.pamperedpets.org.uk’ as the domain name is set to expire on the 25th April, 2024, making it an attractive target. Domain name hijacking can lead to the capitalisation of residual trust (Vissers et al, 2017) which is the trust built from a previous owner’s success. Residual trust can be exploited to hide malicious activity such as malware hosting and spear phishing against the previous owner’s customers. Loss of a domain name can have high impact on a business too when it prevents web operations.

The second recommendation of this report is to update Joomla 4.3.0 to version 5.0.3. Today, Joomla version 4.3.0 is known to have at least three vulnerabilities including the exposure of environment variables through the manipulation of the language file parsing process. The exposure of environment variables can have a high impact on an IT system as they can safeguard sensitive information such as database credentials, API keys and authentication tokens, leading to larger business problems.

The third recommendation of this report is to make sure files and directories are inaccessible to nonauthorized actors. Files like the joomla.xml file allow external users to quickly learn possible attack vectors against the site. The URL ‘https://www.pamperedpets.org.uk/administrator/manifests/files/joomla.xml’ reveals to anybody: the outdated Joomla version, the database query language, and folders that might be of interest in crafting attacks.

The final recommended mitigation of this report is the adoption of information and event management platforms (IEMP) to specifically safeguard against impersonation, both the impersonation of users, and the impersonation of services. It’s inadvisable to allow personal, social media accounts to be connected to the business as it enables spear phishing through impersonation. A simple IEMP would protect against illegitimate associations, and the provision of false credentials to nonauthorized people. Human factors are the weakest link in secure systems (Jeong et al, 2019).

V. References

Alavi, S., Bessler, M. & Massoth, M. (2018) 'A Comparative Evaluation of Automated Vulnerability Scans versus Manual Penetration Tests on False-negative Errors', *CYBER 2018: The Third International Conference on Cyber-Technologies and Cyber-Systems*. Athens, Greece, 18-22 November. New York, Unite States: IARIA Press. 1-6. Available from: https://thinkmind.org/index.php?view=article&articleid=cyber_2018_1_10_80034 [Accessed 10 March 2024].

Campobasso, M. & Allodi, L. (2020) 'Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale', *CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. United States, 9–13 November. New York, United States: Association for Computing Machinery. 1665-1680. DOI: https://doi.org/10.1145/3372297.3417892 [Accessed 09 March 2024].

Dujim, N. (2015) Recommendations on the use and design of risk matrices. *Safety Science* 76(1): 21-31. DOI: https://doi.org/10.1016/j.ssci.2015.02.014 [Accessed 10 March 2024]

Garvey, P. (2001) Implementing a Risk Management Process for a Large Scale Information System Upgrade – A Case Study. *INSIGHT* 4(1): 15-22. DOI: https://doi.org/10.1002/inst.20014115 [Accessed 09 March 2024].

ICO. (n.d.) Security outcomes. Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/security-outcomes/ [Accessed 10 March 2024].

Jeong, J., Mihelcic, J., Oliver, G. & Rudolph, C. (2019) 'Towards an Improved Understanding of Human Factors in Cybersecurity', *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC).* Los Angeles, United States, 12-14 December. New York, United States: IEEE. 383-345. DOI: https://doi.org/10.1109/CIC48465.2019.00047 [Accessed 10 March 2024].

Johns, E & Ell, M. (2023) *Official Statistics Cyber security breaches survey 2023*. UK: Department for Science, Innovation & Technology. Available from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023 [Accessed 09 March 2024].

Proton AG. (2024) GDPR checklist for data controllers. Available from: https://gdpr.eu/checklist/ [Accessed 10 March 2024].

Vissers, T., Barron, T., Goethem, T., Joosen, W. & Nikiforakis, N. (2017) 'The Wolf of Name Street: Hijacking Domains Through Their Nameservers', *CCS '17: Proceedings of* *the 2017 ACM SIGSAC Conference on Computer and Communications Security*. Texas, United States, 30 October – 3 November. New York, United States: Association for Computing Machinery. 957-970. DOI: https://doi.org/10.1145/3133956.3133988 [Accessed 10 March 2024].

Willis, H. (2007) *Using Risk Analysis to Inform Intelligence Analysis*. California, United States: RAND. Available from: https://www.rand.org/pubs/working_papers/WR464.html [Accessed 10 March 2024].

VI. Bibliography

A2 Hosting. (n.d.) Hosting in the Fast Lane. Available from: https://www.a2hosting.com/ [Accessed 09 March 2024].

The Apache Software Foundation. (2023) APACHE HTTP SERVER PROJECT. Available from: https://httpd.apache.org/ [Accessed 09 March 2024].

cPanel LLC. (n.d.) Simplify website & server management. Available from: https://cpanel.net/ [Accessed 10 March 2024].

Enom LLC. (2024) Start selling Domains, Email and SSL. Available from: https://www.enom.com/ [Accessed 09 March 2024].

ICANN. (2024) SSAC Publications. Available from: https://www.icann.org/fr/ssac/publications [Accessed 09 March 2024].

MITRE. (2023) CAPEC Common Attack Pattern Enumeration and Classification. Available from: https://capec.mitre.org/index.html [Accessed 10 March 2024].

MITRE. (2023) CVE Program Mission. Available from: https://www.cve.org/ [Accessed 09 March 2024].

MITRE. (2024) ATT&CK Enterprise Techniques. Available from: https://attack.mitre.org/techniques/enterprise/ [Accessed 09 March 2024].

MITRE. (2024) CWE Common Weakness Enumeration. Available from: https://cwe.mitre.org/index.html [Accessed 09 March 2024].

Open Source Matters, Inc. (2024) The Flexible Platform Empowering Website Creators. Available from: https://www.joomla.org/ [Accessed 10 March 2024].