CYBER PATH™
POLICE & ACADEMIA
TALENT HORIZONS

First Step Web Assessment

Website Assessed: http://plemetal.co.uk/

Created For: PLE Metalworks

Report Submitted: 10/03/2023

Student Assessor: Joe Bloggs

NATIONAL CYBER RESILIENCE CENTRE GROUP

Contents

Overview – Your First Step Web Assessment

Thank you for entrusting our team at the Cyber Resilience Centre to help you. Our unique partnership between Policing, Business and Academia strives to support organisations like yours on their journey to Cyber Resilience. We recognise that this may be the first time you have considered contracting a cyber service and you might be unsure what to expect or how to act on these findings. Our team are dedicated to making the process as simple and transparent as possible, to help you understand the risks highlighted in this report and how to improve on them. Please raise any questions at all with us. We are here to help you learn as much as possible – there are no silly questions here!

Our 'First Step Web Assessment' has been designed by our private-sector experienced security team to provide you with an initial assessment of your website while allowing our cadre of cyber students an opportunity to further develop their skills under the strict management of our supervising team. Whilst this service is not a full penetration test or vulnerability test, it does offer an invaluable view on your website risk.

Your Assessment

Assessment Information	
Website Assessed	http://plemetal.co.uk
Assessment Completed By	Joe Bloggs
Date Completed	10/3/23
Methodology	Our students delivered this assessment using mainstream assessment tools and carefully following our considered first step web assessment methodology.
Overseen By	Cyber PATH Student Supervisors.

Our Findings

Following completion of the assessment, our team evaluated the findings which we list for you below.

Later in this report, we explain what we recommend that you do about these findings. We use a red, amber, and green reporting system to help you prioritise findings by risk - high risk (red), medium risk (amber) and low risk/positive findings (green). We also offer you a virtual meeting with our team to discuss these for further support (details below).

The Positive Elements of Your Website (Low Risk)	
1	**Domain Renewal date:** The date for the renewal of the domain is 21-10-23. Having more than six months left is normal, but attention should be given to ensure that the domain will renew when your domain expires on 21-10-23
2	**Monitor Policy configured DMARC (Domain Message Authentication, Reporting & Conformance):** DMARC is a security protocol that helps prevent email spoofing. DMARC is used to authenticate emails and set what should happen to an email if it does not pass authentication. DMARC has been partially implemented for your domain, which means that it may not prohibit the spoofing of emails from your domain. Currently, you have a 'Monitor' policy, which provides data that allows analysis on who might be abusing your domain using email - but does not prohibit this from happening.

Elements That May Require Further Investigation (Medium Risk)	
3	**Discovered Subdomain:** A subdomain is part of the main website (domain name), which has its own unique content and address. It allows the main website to have multiple sections with different addresses under the same main domain name. An example is the domain “example.com”, which could have subdomains of “blog.example.com”, “shop.example.com”, and “test.example.com”. There were no forgotten or concerning subdomains found within the assessment. Though may be worth obfuscating/disguising the ‘staging.plemetal.com’ domain name as it can identify the possible testing environment.
4	**Insecure SSL Encryption protocols used:** Having an SSL Certificate also requires that communication between a user’s web browser and the server is strong. The recommended protocols for encryption, in this case, are TLS versions 1.2 and 1.3. Versions before 1.2 are considered end-of-life and insecure. The site supports TLS version 1.1 and does not support version securer 1.3

Elements That May Require Immediate Attention (High Risk)	
5	**Vulnerabilities identified with outdated components:** Significant CVEs (Common Vulnerabilities & Exposures) have been identified on the web server due to running outdated components.

What We Recommend You Do Next

We may have shared a few points from our assessment that would benefit from further investigation. This is all part of the journey to greater Cyber Resilience! But what should you do next?

Having now completed the assessment, our team remain focused on helping you further, and the next step is to arrange an assessment meeting with you where we can talk through our findings and help you make an informed decision on how to proceed. You may need the help of your web developers or your IT managed service provider but rest assured that our team at CRC are always on hand to collaborate as we all now strive to improve the resilience of your website.

Finally, we have added a 'Technical Findings' section at the end of this report if you simply want to hand it to your developer or IT service provider. They will be familiar with the language and understand the recommendations in that section so this will inform them for you.

Let's Talk This Through

When you've had time to review our findings, please contact CRC on sample.report who will gladly make the meeting arrangements for a time and date that works for you. We look forward to speaking with you.

Technical Findings

This section is intended for your web developer or IT managed service provider and provides more technical detail related to the findings that we have presented to you. They may be able to use this to determine the correct mitigations based on additional information they may have.

The Positive Elements of Your Website (Low Risk)	
1	**Domain Renewal date:** Ensure that you have auto-renewal configured on your domain, with up-to-date payment details attached to the account.
2	**Partially configured DMARC (Domain Message Authentication, Reporting & Conformance):** DMARC is a security protocol that helps prevent email spoofing. DMARC is used to authenticate emails and set what should happen to an email if it does not pass authentication. DMARC has been partially implemented for your domain, which means that it may not prohibit the spoofing of emails from your domain. Proposed Mitigation: Fully Implementing DMARC will prevent email spoofing of the company's main domain, there are three policies that can be implemented. These are: • Monitor Policy – This does not prohibit or affect the sending and receiving of mail, but instead provides data that allows analysis who is sending emails using the domain. It is recommended that organisations move from this to a quarantine policy when they've collected enough information. • Quarantine Policy - This will put emails in a folder similar to the junk/spam folder but can check if someone is sending email on behalf of your domain with special permission. • Reject Policy – This will reject all emails that fail the DMARC check, causing them to bounce. This requires thorough configuration of all third parties that are authorised to send emails on your behalf (such as a CRM system or email service provider), or these emails will also be disregarded. Decide on a policy that matches with your current readiness – such as beginning with monitor, and then commence the process of configuring third-party software that may need authorisation to send your mail when you increase the policy strength to Quarantine or Reject. This conversation can be had with your service provider, and we can help facilitate it.

Elements That May Require Further Investigation (Medium Risk)	
3	**Discovered Subdomain:** Subdomains are created by allocating the name of the subdomain to a resource in your DNS records. Whilst the type of DNS record can differ (primarily depending on the type of resource one would assign), the common record used is the Canonical Name record (CNAME). It's important to understand what domains and subdomains may utilise your resources, and what could possibly provide an avenue for exploitation for a person with bad intent. The easiest pathway to understanding this is to look at the full DNS records as provided by your service provider. Up to date records will let you know the full extent of your reach, and what public facing URLs will point to your IP's. We can help facilitate this conversation with your service provider if you'd like.

4	The discovery of outdated TLS standards on the website increases the threat surface of the site and creates a possibility for exploitation by a person with malicious intent. The best course of action is to update the site to support TLS 1.3 and end support for TLS 1.1. This can be achieved with assistance from your website service provider.

Elements That May Require Immediate Attention (High Risk)	
5	**Vulnerabilities identified with outdated components:** Many of the vulnerabilities can be mitigated with regular patching schedules. The outdated components identified are: • Apache Web Server 2.4.50 serving content on (Port 80/http & 443/https) The continued use of outdated software may introduce a critical risk to the website. The risk lies that techniques could be developed to compromise the said outdated software. We recommend that the list of known vulnerabilities is reviewed until the software can be updated or this risk is accepted. **CVE-2021-42013** An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased paths, this could allow for remote code execution.

There's more to the Cyber Resilience Centres…

There are many additional ways to engage with CRC. If you haven't already, you can join the community, which is free of charge. This membership includes practical, government-approved guidance, as well as regular information updates to keep you informed of our other help and services on offer, including:

- **Educational Events** - we run regular webinars and events on a range of topics relevant to your small business or third sector organisation.
- **Affordable solutions** - we offer a range of paid services like this one which are designed to address the most pertinent risks affecting SMEs, as identified by policing and Government.
- **Cyber Essentials Certification** - we have a Trusted Partners forum, which is made up of IASME approved Cyber Essentials Certifiers. If you are planning on achieving Cyber Essentials or Cyber Essentials Plus certification, we can refer you to the Trusted Partners forum of local suppliers in the region that provide this.

About the Cyber Resilience Centre Network

The National Cyber Resilience Centre Group and Cyber Resilience Centres are funded and supported by the Home Office and policing in a not-for-profit partnership with the private sector and academia to strengthen our national cyber resilience across SMEs and the supply chain.

At a national level, NCRCG is building a coalition of police, government, large employers and organisations, and academia to ensure a collaborative and coherent approach to cyber resilience.

NCRCG and its National Ambassadors and the CRC network are committed to investing in the next generation of cyber experts. As such, NCRCG has launched Cyber PATH in partnership with the CRC network and over 45 universities.

The nine CRCs operate across England and Wales. They serve SMEs in their locality helping to build cyber resilience against threats that are specific to them. Cyber PATH empowers students to work with their regional CRC in meeting the requests brought to them by local businesses.

Each CRC retains the freedoms to deliver tailored, trusted and affordable support, with NCRCG providing insight and solutions at a macro level.

You can learn more about the work of the NCRCG here. We can help your own customers and suppliers too, so spread the word.

Help Bundles and Additional Services

If you are ready for more support, we offer a free community and a selection of Help Bundles which include paid services and 12 months of support. This includes:

- Full website vulnerability testing
- Policy Review
- Staff awareness training
- And more....

Visit our selection of Help Bundles and Services here.

You can also engage with us through our social media channels.

Get in touch with us at sample.report if there's anything else we can help you with.