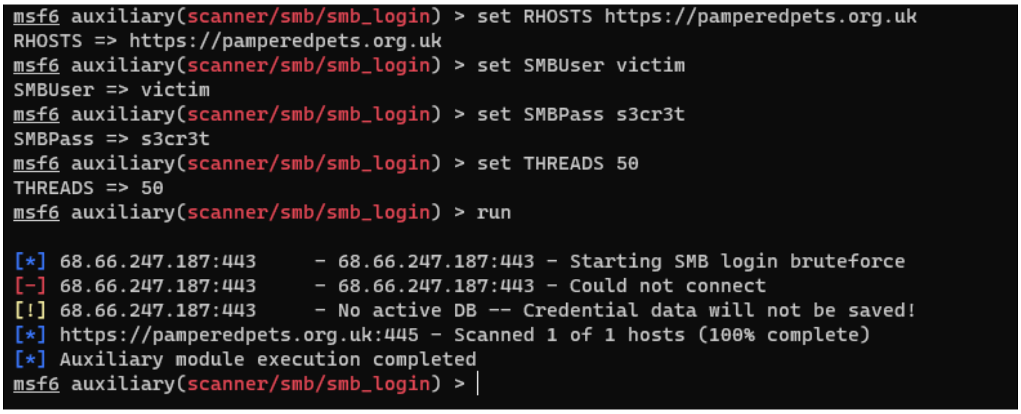
Website Choice Activity

In cybersecurity, a vulnerability is a weakness within an organisation's system that malicious hackers can exploit to gain illicit access. Various tools can be used to identify vulnerabilities on a website, including web application scanners, network scanners, and protocol scanners. To stay ahead of the curve and ensure top-notch security, it's wise to consult OWASP's web application security issues and take proactive measures accordingly (Varghese, 2021).

According to OWASP (2022), automated web application vulnerability scanners are designed to identify security vulnerabilities within web applications. These tools conduct an external scan of web applications to uncover weaknesses such as Cross-site scripting, SQL Injection, Command Injection, Path Traversal, and insecure server configuration. While numerous commercial and open-source options exist, it's important to note that OWASP does not officially endorse any particular tool. If you're curious about the efficacy of DAST tools, the OWASP Benchmark project is an excellent resource to explore.

I chose pamperedpets.org.uk as my website and attempted to use Metasploit for vulnerability testing. Unfortunately, I faced difficulties getting the desired results and used an online tool to evaluate the website's vulnerabilities, which I found at https://beaglesecurity.com. I have documented my findings and the consequences of my testing below.



```
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS https://pamperedpets.org.uk
RHOSTS => https://pamperedpets.org.uk
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser victim
SMBUser => victim
msf6 auxiliary(scanner/smb/smb_login) > set SMBPass s3cr3t
SMBPass => s3cr3t
msf6 auxiliary(scanner/smb/smb_login) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 68.66.247.187:443     - 68.66.247.187:443 - Starting SMB login bruteforce
[-] 68.66.247.187:443     - 68.66.247.187:443 - Could not connect
[!] 68.66.247.187:443     - No active DB -- Credential data will not be saved!
[*] https://pamperedpets.org.uk:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

The score for the Content Security Policy is -25, indicating that the CSP header has not been implemented. Content Security Policy (CSP) is an added security layer that detects and prevents attacks such as XSS and data injection (ScanRepeat, N.D.). To address the CSP Header Not Set issue, you need to configure your web server to return the Content-Security-Policy HTTP Header and define the appropriate values to control which resources the browser can load.

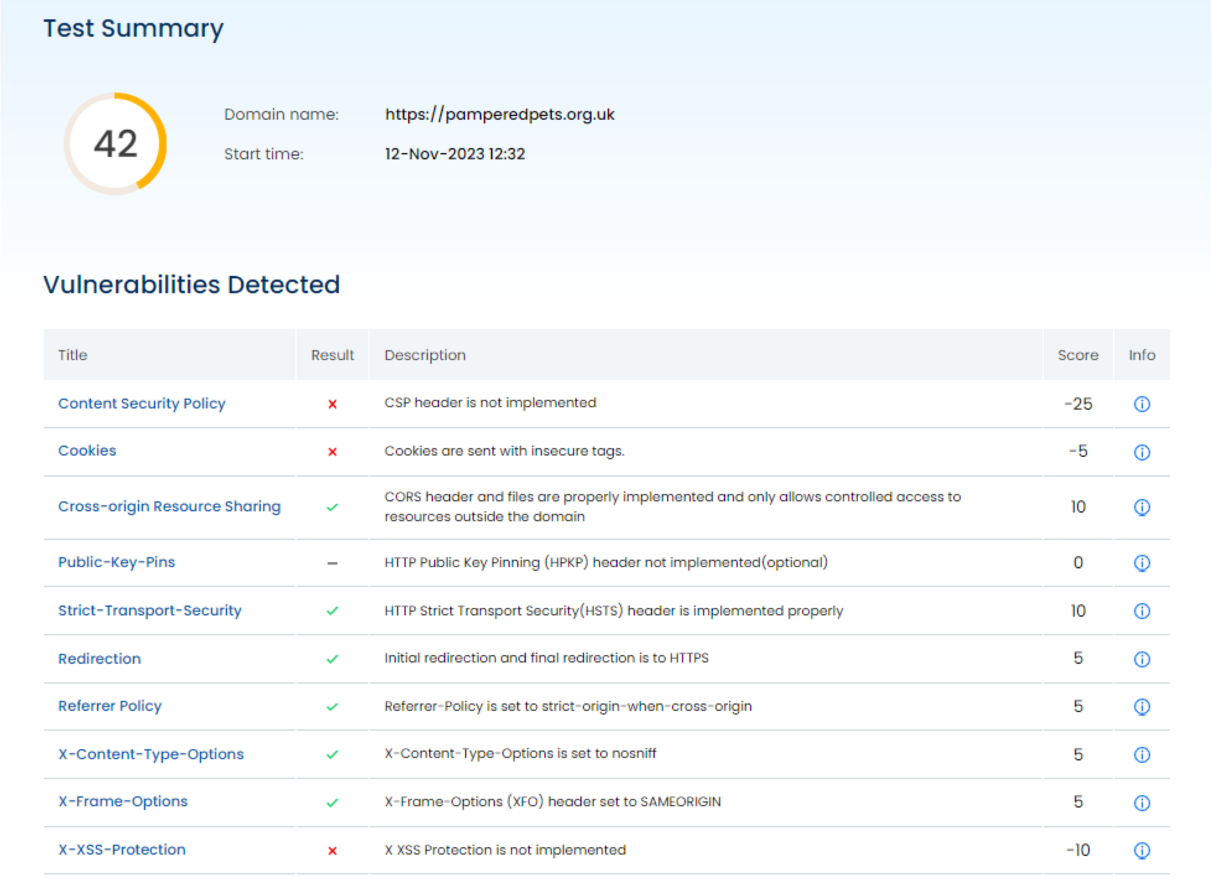
It is essential to ensure the security of data transmission when using cookies. The score for Cookies is -5, indicating that cookies are sent with insecure tags. The Secure Attribute can be set differently depending on the technology used to avoid this. For ASP.NET, it can use `requireSSL="true"` in the web.config file. PHP can set it in php.ini or during the script via the session_set_cookie_params or setcookie method. By selecting the Secure Attribute appropriately, you can guarantee that data transmission is secure (Coates, N.D.).

The website's X-XSS-Protection feature is currently not implemented, as indicated by the low score of -10. According to Tenable (2018), modern browsers allow websites to manage their XSS auditors through the HTTP 'X-XSS-Protection' response header. Unfortunately, the server doesn't return this header, making all website pages vulnerable to Cross-Site Scripting (XSS) attacks. This specific URL has been flagged as an example.

To prevent XSS attacks, one solution is to use Content-Security-Policy, which is recommended as long as legacy browser support isn't needed. Additionally, it's recommended to disallow unsafe inline scripts.

To fix this issue, the web server should be configured to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages.

Rastogi (2023) states that conducting a Website Penetration Test is crucial in detecting and resolving any security vulnerabilities on your website. This proactive approach helps mitigate risks, ensures compliance with regulatory requirements, uncovers potential vulnerabilities, and prepares your security team to respond to a real-life cyber-attack. Despite the size of your website, as research shows that almost 60% of cyberattacks target small businesses, conducting a Vulnerability Assessment and Penetration Testing is imperative.



Test Summary

Domain name: https://pamperedpets.org.uk

Start time: 12-Nov-2023 12:32

Vulnerabilities Detected

Title	Result	Description	Score	Info
Content Security Policy	✗	CSP header is not implemented	-25	ⓘ
Cookies	✗	Cookies are sent with insecure tags.	-5	ⓘ
Cross-origin Resource Sharing	✓	CORS header and files are properly implemented and only allows controlled access to resources outside the domain	10	ⓘ
Public-Key-Pins	–	HTTP Public Key Pinning (HPKP) header not implemented(optional)	0	ⓘ
Strict-Transport-Security	✓	HTTP Strict Transport Security(HSTS) header is implemented properly	10	ⓘ
Redirection	✓	Initial redirection and final redirection is to HTTPS	5	ⓘ
Referrer Policy	✓	Referrer-Policy is set to strict-origin-when-cross-origin	5	ⓘ
X-Content-Type-Options	✓	X-Content-Type-Options is set to nosniff	5	ⓘ
X-Frame-Options	✓	X-Frame-Options (XFO) header set to SAMEORIGIN	5	ⓘ
X-XSS-Protection	✗	X XSS Protection is not implemented	-10	ⓘ

References:

- Varghese, J. (2021). *Website Vulnerability Testing - Everything You Need to Know*. [online] Available at: https://www.getastra.com/blog/security-audit/website-vulnerability-testing/ [Accessed 12 Nov. 2023].
- OWASP (2022). *Vulnerability Scanning Tools | OWASP*. [online] owasp.org. Available at: https://owasp.org/www-community/Vulnerability_Scanning_Tools.
- ScanRepeat (N.D.). *Content Security Policy (CSP) Header Not Set*. [online] Available at: https://scanrepeat.com/web-security-knowledge-base/content-security-policy-csp-header-not-set.
- Coates, M. (N.D.). *Secure Cookie Attribute | OWASP*. [online] Available at: https://owasp.org/www-community/controls/SecureCookieAttribute.
- Tenable (2018). *Missing 'X-XSS-Protection' Header.* Available at: https://www.tenable.com/plugins/was/112526.
- Rastogi, N. (2023). *Guide On Website Penetration Testing and Vulnerability Scan*. [online] www.getastra.com. Available at: https://www.getastra.com/blog/security-audit/website-penetration-testing/.