1 Executive Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **axisvalue.com** using a Basic analysis type. The evaluation commenced on **March 15** at **03:00** and concluded within a timeframe of **00h:12m:28s**. The scope of the work included a comprehensive scan of the web application and infrastructure, focusing on identifying High and Medium-risk vulnerabilities as per OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **2 High-risk**, **2 Medium-risk**, and **14 informational**. Critical findings include High-risk shared hosting environments with over **100 domains** on the same IP, posing significant exposure to potential attacks. Additionally, unusual port assignments were detected, indicating possible evasion of security controls. Medium-risk issues include the absence of a Web Application Firewall (WAF) on **50%** of analyzed hosts, increasing vulnerability to injection attacks, and insecure open ports detected via Nmap. Immediate actions should focus on mitigating High-risk shared hosting and securing port configurations to prevent unauthorized access and potential data breaches.

1.3 Key Security Issues

Title	Risk
Shared Hosting Environment Analysis	High
Unusual Port Assignments Detected	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium

1.3.1 Shared Hosting Environment Analysis

Description:

The analysis identified that the domain **axisvalue.com** and its subdomain **www.axisvalue.com** are hosted in a shared environment with over **393 shared domains**. This configuration significantly increases the risk of cross-site contamination and potential data breaches due to the shared infrastructure.

Affected Assets:

- Hostnames: **axisvalue.com**, **www.axisvalue.com**

Recommendations:

Transition to a dedicated hosting environment to mitigate the risks associated with shared hosting. Implement strict access controls and monitoring to detect any unauthorized activities.

1.3.2 Unusual Port Assignments Detected

Description:

An unusual port assignment was detected on the host **www.axisvalue.com** with IP **208.68.246.151**, where non-standard services were observed running on expected ports. This may indicate attempts to evade detection or misconfigured applications.

Affected Assets:

- Host: **www.axisvalue.com** with IP **208.68.246.151**

Recommendations:
Conduct a thorough review of port configurations and ensure that services are running on standard ports as per best practices. Implement network segmentation and intrusion detection systems to monitor for unusual activities.

1.3.3 Absence of WAF

Description:
The absence of a Web Application Firewall (WAF) was noted on one of the two analyzed hosts, representing a **50% vulnerability rate**. This lack of protection increases susceptibility to injection attacks and unauthorized data access.

Affected Assets:
- Host without WAF protection: **www.axisvalue.com**

Recommendations:
Deploy a robust Web Application Firewall to shield web applications from common threats such as SQL injection and cross-site scripting. Regularly update WAF rules to adapt to emerging threats.

1.3.4 Nmap Port Scan Results Analysis

Description:
The scan revealed several open ports, including port **80/tcp**, running HTTP services without encryption on Microsoft IIS httpd 8.5. This poses a risk due to the lack of encryption for data in transit.

Affected Assets:
- IP Address: **208.68.246.151** - Ports: **80/tcp, 443/tcp**

Recommendations:
Ensure that HTTP traffic is redirected to HTTPS, and implement HTTP Strict Transport Security (HSTS) to enforce secure connections. Regularly review open ports and close any unnecessary ones to reduce the attack surface.

1.4 General Recommendations

To enhance the security posture of your web application and infrastructure, it is recommended to:

1. Transition critical assets from shared hosting environments to dedicated servers.
2. Regularly audit and secure all open ports, ensuring services run on standard configurations.
3. Implement a comprehensive Web Application Firewall solution across all hosts.
4. Enforce HTTPS with HSTS for all web traffic to ensure data integrity and confidentiality.
5. Conduct continuous monitoring and periodic security assessments for proactive threat detection and mitigation.

By addressing these High and Medium-risk issues promptly, you can significantly reduce the likelihood of successful cyber-attacks and protect sensitive data from potential breaches.