1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **chivpn.transunion.com**. The analysis commenced on **April 11th** at **01:00** and concluded in **00h:11m:59s**. The assessment was categorized as a **Basic** type scan. The methodology employed adheres to OWASP and OSCP standards, focusing on identifying critical vulnerabilities within web applications and infrastructure.

1.2 Short Summary of Main Issues

The security assessment identified **1 high-risk**, **3 medium-risk**, **2 low-risk**, and **13 informational issues**. The most critical finding is a Denial of Service (DoS) vulnerability with a **97.04% timeout rate** on port 80, posing a significant threat to service availability and requiring immediate mitigation. Medium-risk issues include the absence of Web Application Firewall (WAF) protection, exposing the system to injection attacks, and insecure open ports detected via Nmap, which could lead to unauthorized access. Additionally, sensitive subdomains were identified, potentially exposing critical systems. Immediate actions include implementing DoS protection, enhancing WAF coverage, and securing exposed ports to mitigate these vulnerabilities.

1.3 Key Security Issues

Title	Risk
Denial of Service (DoS) Assessment	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
Shared Hosting Environment Analysis	Low
SSL/TLS Protocols Security Assessment	Low

1.3.1 Denial of Service (DoS) Assessment

Description:
A high-severity DoS vulnerability was identified on port 80 (HTTP) with a **97.04% timeout rate** out of **169 total responses**, indicating a severe risk to service availability.

Affected Assets:
- **chivpn.transunion.com:80**

Recommendations:
Immediate implementation of DoS protection mechanisms is recommended. This includes configuring rate limiting, deploying network-level protections such as intrusion prevention systems (IPS), and considering the use of content delivery networks (CDNs) to absorb traffic spikes.

1.3.2 Absence of WAF

Description:
The absence of a Web Application Firewall (WAF) was detected, resulting in a **100% vulnerability rate** across the analyzed host. This significantly increases the risk of successful cyber-attacks, particularly injection-based attacks.

Affected Assets:
- **chivpn.transunion.com**

Recommendations:
Deploy a robust WAF solution to filter and monitor HTTP requests between the web application and the internet. This will help protect against common web exploits that could compromise application security.

1.3.3 Nmap Port Scan Results Analysis

Description:
The scan revealed **2 open ports**, including port 10000 associated with a potentially insecure service, specifically the Webmin interface exposure.

Affected Assets:
- IP Address: **66.175.247.22**

Recommendations:
Close unnecessary ports and restrict access to essential services only. Implement firewall rules to limit access to trusted IP addresses and consider using VPNs for secure remote access.

1.3.4 Subdomain Naming Security Assessment

Description:
A sensitive subdomain, **chivpn.transunion.com**, was identified, categorized under "Sensitive Services" with a high-risk level due to potential exposure of critical systems and sensitive data.

Affected Assets:
- Subdomain: **chivpn.transunion.com**

Recommendations:
Review and secure sensitive subdomains by implementing strict access controls and monitoring for unauthorized access attempts. Regularly audit subdomain configurations to ensure they do not expose critical infrastructure.

1.4 General Recommendations

To enhance overall security posture, it is recommended to implement comprehensive monitoring solutions to detect and respond to threats in real-time. Regular security audits and penetration testing should be conducted to identify new vulnerabilities promptly. Additionally, employee training on cybersecurity best practices can help mitigate risks associated with human error.