IOTHREAT

Security Review: hooli.xyz

Objective

Conduct an external security review and provide a detailed report listing all the findings, including mitigation recommendations to improve the security and reputation of your website.

Website

https://hooli.xyz

Findings and Recommendations

1. Malware Infections

1.1. Website

Your website is clean from malware infections - well done!

1.2. Hosting Server

Your hosting server is clean from malware infections - well done!

2. Subdomains

3 subdomains were detected on your domain.

This is the list of the discovered subdomains:

1. dc-2726e4eb.hooli.xyz
2. stg.hooli.xyz
3. www.hooli.xyz

Each subdomain increases the attack surface of your business.
Carefully review each subdomain and consider removing the ones you do not need anymore.

Make sure to scan all of your subdomains for malware infections, SSL issues, open ports, and vulnerabilities.

3. Exposed Credentials

0 leaked passwords were detected for your domain.

4. Email Security

4.1. MX

Your domain is not configured to receive email messages as it is missing MX records.

In case you do not need to receive email messages using this domain, then you may disregard this finding.

How to set up MX records for Google Workspace email?
https://support.google.com/a/answer/140034?hl=en

A mail exchanger record (MX record) specifies the mail servers responsible for accepting email messages on behalf of a domain name.

4.2. SPF

No issues - well done!

Sender Policy Framework (SPF) lets the domain owner authorize IP addresses that are allowed to send email for the domain. Receiving servers can verify that messages appearing to come from a specific domain are sent from servers allowed by the domain owner.

4.3. DMARC

No issues - well done!

Domain-based Message Authentication, Reporting, and Conformance (DMARC) tells receiving mail servers what to do when they get a message that appears to be from your organization, but does not pass authentication checks, or does not meet the authentication requirements in your DMARC policy record. Messages that are not authenticated might be impersonating your organization, or might be sent from unauthorized servers.

5. SSL Certificates

Your SSL Certificate is graded NA.
This server's certificate is not trusted.

6. Open Ports

2 open ports were detected on your server.

This is the list of the discovered open ports and services:

1. 80 / HTTP
2. 443 / SSL

Each open port increases the attack surface of your business.
Typically, a public web server should have only two public open ports (80 for HTTP, and 443 for SSL).

Carefully review your list of open ports and consider closing the ones you do not need anymore.
Protect your web server with a Firewall to filter any incoming connection requests to unauthorized ports.

7. Vulnerabilities

9 web application vulnerabilities were detected on your website.

IOTHREAT

This is the list of the discovered web application vulnerabilities, sorted by their severity level:

1. [MEDIUM]: X-Frame-Options Header Not Set
2. [MEDIUM]: Vulnerable JS Library
3. [MEDIUM]: Content Security Policy (CSP) Header Not Set
4. [MEDIUM]: Reverse Tabnabbing
5. [LOW]: X-Content-Type-Options Header Missing
6. [LOW]: Strict-Transport-Security Header Not Set
7. [LOW]: Server Leaks Version Information via "Server" HTTP Response Header Field
8. [LOW]: Incomplete or No Cache-control and Pragma HTTP Header Set
9. [LOW]: Cross-Domain JavaScript Source File Inclusion

Download and review the Excel file with the full technical details of the discovered vulnerabilities and remediation recommendations (check the "Vulnerabilities" tab in the Excel file), as we could not fit all the data in this PDF report due to format and space issues.

Cybercriminals often exploit software vulnerabilities to steal sensitive data and infect website visitors with malware. Carefully review the list of discovered vulnerabilities and apply the suggested mitigation recommendations ASAP.

For a quick fix of the discovered web application vulnerabilities, you should consider subscribing to a cloud-based WAF (Web Application Firewall). This will remediate most of your security issues.

Methodology

The DAST methodology was used to test your website. Dynamic Application Security Testing (DAST) is a black-box security testing methodology in which an application is tested from the outside. A tester using DAST examines an application when it is running and tries to hack it just like an attacker would.

Contact Email

security@iothreat.com