Brew Evaluates Application Defenses with Axiom's Security Assessments

Introduction

Brew is a SaaS platform for CMOs and the extended marketing teams to develop, benchmark, and evaluate the marketing strategy from ideation to execution.

The platform offers a completely automated, real-time view of market dynamics, based on deep integrated and proprietary ML and NLP technology.

The client had reached out to Axiom to get penetration testing done, to determine the security posture of their application.

Customer Requirements

Security Audit and Posture Assessment

The customer needed to audit customer-facing API and application Uniform Resource Locators (URLs) to avoid exploitation of any vulnerabilities if present.

The Solution

Axiom provided penetration testing services to the client. The team also guided the customer to set up security headers in Amazon CloudFront.

OWASP Top 10 checks were performed along with the below vulnerability checks:

- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing

About Brew

Brew is a startup based in Tel Aviv, Israel.

Brew's marketing intelligence platform, with its ML and NLP technology, analyzes companies and activities that influences the audience mindset, across any marketing channel, geography, vertical, audience, and topic - to provide strategic visibility and tactical planning recommendations to its users.

With Brew, teams move much faster, with much more confidence - to drive significant impact on the business growth and results.

Why Axiom?

Axiom, being an AWS Advanced Consulting Partner, has been providing security solutions to startups and SMBs for more than 5 years.
The company has skilled engineers who are adept at performing security assessments and identifying the security posture of an environment.

- Testing for Error Handling
- Testing for Weak Cryptography
- Denial of Service
- Risky Functionality
- Business Logic Testing
- Client-side Testing
- API Testing

The tools used for penetration testing were:

- Burp Suite
- SQLMAP
- WFUZZ
- SSL Labs
- OWASP ZAP
- NMAP

Using automated and manual processes, the engineers ensure that all risks and vulnerabilities are identified, and a roadmap is created for remediation.

> "Working with Axiom is always a delight. The team is highly responsive and caters to all requirements and needs."
>
> - **Gabriel Amram**
> CTO & Co-founder, Brew

The Axiom team has also advised the client to use AWS WAF, a web application firewall that helps protect web applications or APIs against common web exploits and bots.

The Result

With the security assessment performed by the Axiom team, the client is now aware of the security posture of their applications.

The client has since taken the necessary measures to strengthen their posture with recommendations from the Axiom team.

A couple of sanity checks has also been performed by the Axiom team along with a certification provided to the customer validating the checks.

Next Steps

The client will need to perform security assessments every six months, so as to maintain the security posture of their applications and to protect themselves from cyberattacks.

> "Axiom has provided the report with specific remediation recommendations and is open to assist and walk us through, until the problems are solved. I would highly recommend Axiom to any startup, of any size."
>
> -**Gabriel Amram**
> CTO & Co-founder, Brew