**Week -11**

**Ethical Hacking & Security Testing Report**

1. **Security Audit: Basic Security Assessment of Duolingo**

Duolingo operates an extensive cloud-based infrastructure integrated with web and mobile applications. A basic security audit was conducted to assess the current state of security for its production environment and AI modules.

**Audit Scope:**

* Web application endpoints (login, course content, and AI chatbots)
* Mobile application APIs
* Cloud-hosted backend (user data, AI models, ML pipelines)
* IAM (Identity and Access Management) configurations
* Data storage and transmission encryption protocols

**Key Findings:**

During the audit, several misconfigurations and vulnerabilities were identified that could impact Duolingo's confidentiality, integrity, and availability. The most significant findings are outlined below:

**1. Website Security**

We discovered that some essential security headers and misconfigurations

* **Secure Cookies *Not Used***: The application did not consistently set the ‘Secure’ flag on cookies. This could allow cookies to be transmitted over non-encrypted (HTTP) connections, increasing the risk of session hijacking.
* **Content Security Policy (CSP) *Not Implemented***: The absence of a CSP header means that the website is more vulnerable to cross-site scripting (XSS) attacks. A well-defined Content Security Policy (CSP) would restrict where scripts, images, and other resources can be loaded from, thereby reducing exposure to malicious content.
* **HTTP Strict Transport Security (HSTS) *Not Enforced***: Without HSTS, browsers may connect to the website over an insecure HTTP connection, especially on initial visits. This increases the risk of man-in-the-middle (MITM) attacks.
* **NGINX Web Server *Outdated***: The web server was found to be running an end-of-life version of NGINX. Using outdated software that is no longer supported means missing out on critical security patches, leaving the system open to exploitation through known vulnerabilities.

**2. DNS Configuration**

A review of Duolingo’s public DNS records revealed the following gaps:

* **DNSSEC Not Enabled**: DNSSEC (Domain Name System Security Extensions) was not configured. Without it, DNS responses can be spoofed, potentially redirecting users to malicious websites.
* **CAA Record Not Set**: Certificate Authority Authorization (CAA) records were not found in the DNS zone. CAA helps restrict which certificate authorities (CAs) are allowed to issue SSL/TLS certificates for the domain, which helps prevent unauthorized or fraudulent certificate issuance.

**3. AI Model Endpoint**

The AI-powered chatbot functionality on Duolingo was found to expose REST APIs without adequate **rate-limiting or access control mechanisms**. This could allow attackers to:

* Send a high number of queries to the model in a short period (leading to denial of service).
* Attempt **model extraction attacks**, where the attacker tries to learn the underlying AI model’s logic or training data through repeated querying.

**4. Identity and Access Management (IAM)**

In the cloud environment, several IAM roles granted **excessive permissions** beyond what was necessary for users to perform their tasks. This violates the **principle of least privilege**, increasing the risk of misuse or exploitation if an account is compromised.

**5. Encryption Protocols**

Although data-at-rest encryption using **AES-256** was correctly implemented, we identified that some legacy endpoints still support **TLS 1.0**, which is outdated and no longer considered secure. This leaves those connections susceptible to downgrade attacks or known vulnerabilities in older TLS versions.

**6. Insufficient Logging and Monitoring Configuration**

Duolingo has integrated **Prisma Cloud** for security monitoring, making a strong attempt towards cloud-native security. However, from our observation, we found:

* **Leniently, alert thresholds**: causing some unusual or potentially malicious activities to go undetected.
* **Real-time alerts were not consistently triggered**, which can delay incident detection and response efforts.

**2. System Vulnerabilities in Duolingo's IT Infrastructure**

The audit findings were further classified to better understand the scope of risk:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Vulnerability** | **Risk Level** | **Impact** |
| Authentication | Weak password policy, missing MFA on admin accounts | High | Unauthorized access to critical systems |
| AI Systems | Lack of protection from model extraction attacks | High | Exposure of proprietary AI training data |
| Cloud Infrastructure | Excessive privileges in IAM roles | Medium | Lateral movement within cloud services |
| Network Security | Use of deprecated TLS 1.0 on some endpoints | Medium | Vulnerability to MITM and downgrade attacks |
| Monitoring & Response | Poorly tuned alerting thresholds in Prisma Cloud | Medium | Delayed detection and response to security incidents |

**3. Cybersecurity Recommendations**

To improve the overall security posture of Duolingo’s AI-driven platform, the following strategies are recommended:

**a. Penetration Testing**

* Perform quarterly **black-box and white-box tests** for both web and mobile apps.
* Conduct **adversarial AI testing** such as prompt injection or model evasion on the chatbot.
* Organize **red-team exercises** to simulate real-world cyberattack scenarios and assess internal resilience.

**b. Multi-Factor Authentication (MFA)**

* Enforce MFA across all employee accounts, especially for administrative and privileged roles.
* Use identity providers like **Okta** or **Azure AD** to centralize and secure identity management.

**c. AI-Specific Security Controls**

* Introduce **rate-limiting and CAPTCHA** mechanisms on AI endpoints.
* Implement **differential privacy** techniques to protect training data from inference attacks.
* Regularly **audit third-party datasets** to prevent model poisoning or data leakage.

**d. IAM Hardening**

* Apply **Role-Based Access Control (RBAC)** and restrict permissions to the minimum necessary.
* Conduct **regular access reviews** to eliminate stale or unnecessary privileges.
* Use **automated access revocation** tools for inactive users or completed projects.

**e. Encryption Enhancements**

* Enforce **TLS 1.2 or higher** across all communication channels.
* Audit SSL/TLS configurations using tools like **SSL Labs** or **testssl.sh** to identify weak cipher suites and deprecated protocols.

**f. Security Monitoring & Automation**

* Fine-tune **Prisma Cloud alerts** to detect unusual behavior with greater accuracy.
* Integrate advanced SIEM tools such as **Splunk** or **Azure Sentinel** for better visibility and threat detection.
* Incorporate **automated patch management** in CI/CD pipelines using tools like **Jenkins** to ensure timely updates of legacy systems.

**Reference:**

<https://www.upguard.com/security-report/duolingo>

<https://investors.duolingo.com/static-files/105c67d0-980a-4c74-86c0-d922ad285c6b>

<https://www.cequence.ai/blog/api-security/api-breach-duolingo/>