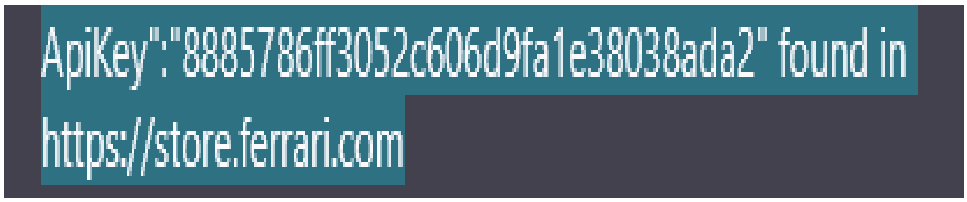
Proof of Concept Report – Exposed API Key

Researcher: Vimalatithyan S.
Target: https://store.ferrari.com

During passive reconnaissance, an API key was discovered exposed within publicly accessible content on Ferrari's e-commerce domain.

Exposed API Key:
8885786ff3052c606d9fa1e38038ada2

Evidence Screenshot:



Safe Proof-of-Concept Testing:

The following safe, read-only curl command was executed:

```
curl -i -L
"https://store.ferrari.com/rest/V1/products?searchCriteria%5BpageSize%5D=1"
\
  -H "Authorization: Bearer 8885786ff3052c606d9fa1e38038ada2" --max-time 15
```

Observation:
The server consistently responded with HTTP 301 redirects followed by HTTP 404 HTML pages. No customer data, product JSON, or order data was returned. This indicates the key is exposed but not actively granting access to protected API endpoints.

Impact Summary:
- Public exposure of an internal API key
- Potential misuse if the key is reused, privileges expanded, or environment changes
- Secrets embedded in client-side code may lead to future security risk

Recommended Remediation:
1. Immediately rotate/invalidate the exposed API key.
2. Remove all secrets from public-facing client-side code.
3. Use secure server-side secret management practices.
4. Apply strict scoping and origin/IP restrictions to API keys.
5. Audit logs for any unauthorized usage of the exposed key.

This testing was performed safely, without attempting to access or modify any user data and fully following responsible disclosure guidelines.