Andre Savic <andre@rubberducklabs.at>

Meldung kritischer Sicherheitslücke bei klimabonus.gv.at

1 Nachricht

Andre Savic <andre@rubberducklabs.at> 21. August 2024 um 02:44
An: reports@cert.at, servicebuero@bmk.gv.at, Office <office@rubberducklabs.at>

Sehr geehrte Damen und Herren des CERT Austria,
Sehr geehrte Damen und Herren des Bundesministeriums für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK),

ich möchte Sie auf eine Sicherheitslücke auf der Webseite klimabonus.gv.at hinweisen, die mir im Rahmen der Nutzung des Online-Formulars zur Abfrage des Klimabonus aufgefallen ist.

Die Webseite klimabonus.gv.at, betrieben vom Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK), dient dazu, Informationen über den Klimabonus in Österreich bereitzustellen, einschließlich der Höhe des auszuzahlenden Betrags. Zu diesem Zweck bietet die Seite ein Online-Formular an, bei dem Benutzer Ausweisdokumente hochladen oder abfotografieren können, um ihre Berechtigung zu überprüfen.

Zu den wesentlichen Sicherheitslücken, die ich identifiziert habe, gehören:

Unzureichende Überprüfung von Ausweisdokumenten: Die Webseite überprüft nicht ausreichend, ob es sich bei dem hochgeladenen Dokument tatsächlich um einen gültigen Ausweis handelt. In Tests wurden Dokumente akzeptiert, die lediglich grundlegende Kriterien wie Vorname, Nachname und Geburtsdatum erfüllten, ohne dass eine gründliche Validierung erfolgte.

Fehlerhafte Namensüberprüfung: Es ist nicht erforderlich, dass der Vor- und Nachname vollständig auf dem Ausweis enthalten ist. Die Überprüfung scheint primär über das Geburtsdatum zu erfolgen, gefolgt von einem Abgleich mit möglichen Namen in der Datenbank. Dies ermöglicht es, durch systematisches "Herantasten" an die Daten von Personen zu gelangen, was ein erhebliches Sicherheitsrisiko darstellt. Siehe "KarteUnvollstaendig.jpg)

Offenlegung sensibler Informationen: Der zurückgegebene Datensatz enthält hochsensible Informationen, darunter die BIC (Bank Identifier Code), die Rückschlüsse auf die Bankverbindung der betroffenen Person zulässt, sowie die letzten vier Ziffern der IBAN. Diese Informationen sind besonders anfällig für Missbrauch, insbesondere im Zusammenhang mit Betrugsanrufen (Scam Calls) oder gezielten Phishing-Attacken.

Umgehbares Rate Limiting: Das implementierte Rate Limiting kann einfach umgangen werden, indem der .AspNetCore.Session Cookie nicht mitgesendet wird. Dies ermöglicht einem Angreifer, unbegrenzt viele Versuche durchzuführen, ohne dass der Zugriff blockiert wird.

Darüber hinaus erscheint die grundsätzliche Umsetzung der Ausweisprüfung in diesem Kontext fragwürdig. Es erschließt sich nicht, warum für diesen Anwendungsfall eine eigene Lösung implementiert wurde, anstatt eine etablierte und sicherere Alternative wie **ID Austria** zu nutzen, die für solche Identifikationsprozesse deutlich besser geeignet wäre.

Ich möchte betonen, dass es sich bei dieser Entdeckung um einen Zufallsfund handelt. Keine Dateien wurden entwendet, verändert oder missbraucht. Dieser Bericht erhebt auch keinen Anspruch auf Vollständigkeit, sondern soll lediglich auf die dringendsten Probleme hinweisen.

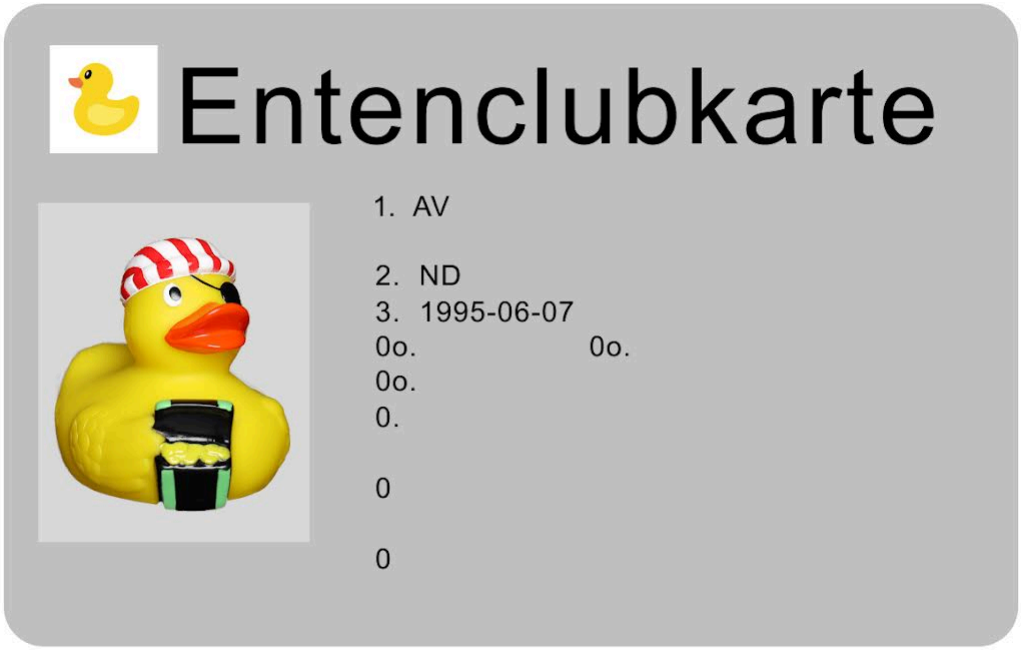
Zur Verdeutlichung des gesamten Ablaufs habe ich einige Dateien beigefügt:

Auf den Screenshots "Beispiel_1_Upload.png" und "Beispiel_2_Done.png" lässt sich der Prozess direkt auf der Webseite nachvollziehen. In den Entwicklertools des Browsers kann auch die gesamte Antwort als JSON eingesehen werden.
Das JSON "serverresposne.json" meines persönlichen Datensatzes zeigt auf, welche sensiblen Informationen offengelegt werden.

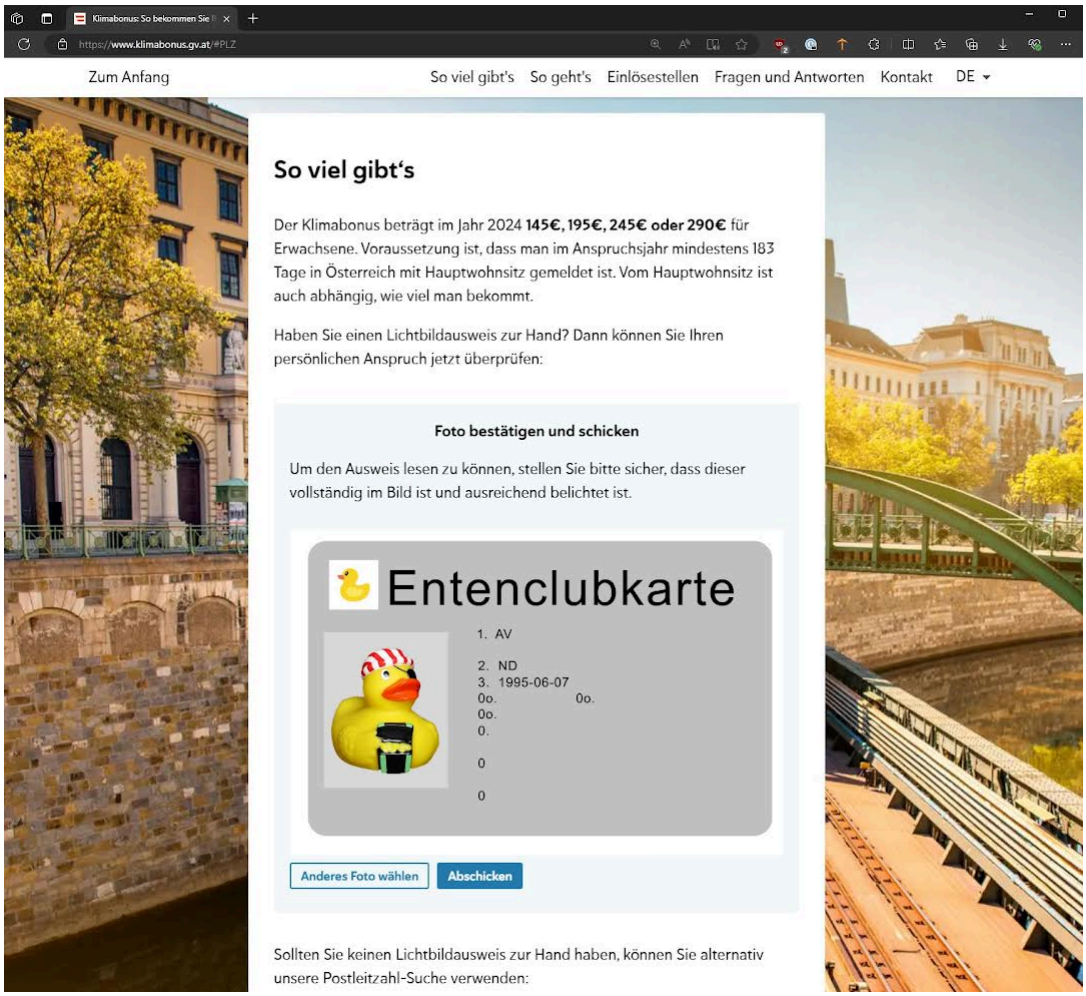
Angesichts der Sensibilität der verarbeiteten Daten und der breiten Bevölkerungsgruppe, die durch den Klimabonus abgedeckt wird, stellen diese Schwachstellen ein erhebliches Risiko für die Privatsphäre und Sicherheit der betroffenen Personen dar. Es ist daher von größter Bedeutung, dass diese Sicherheitslücken zeitnah behoben werden.

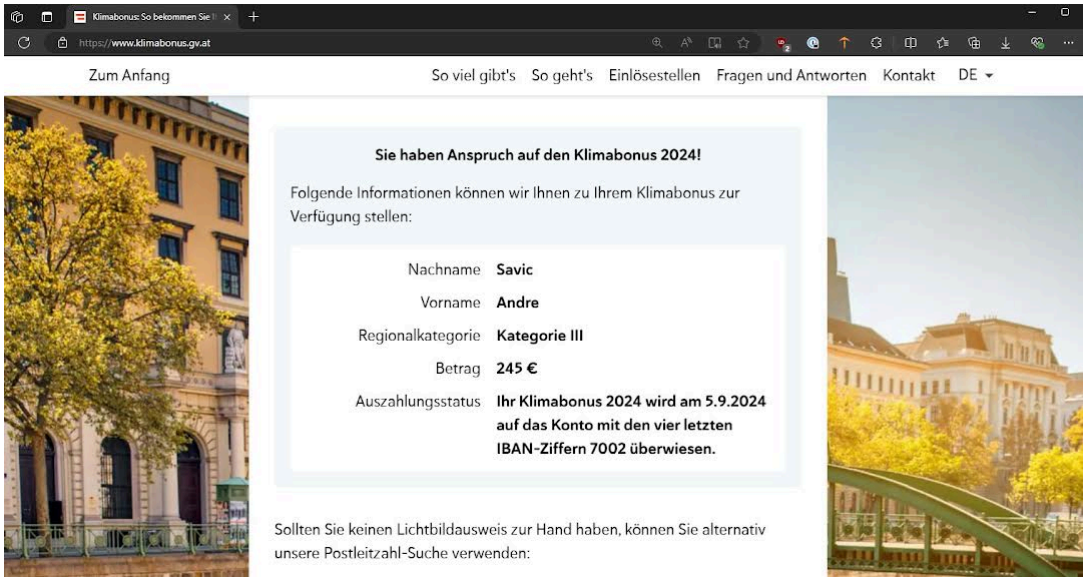
Weitere technische Details und ein Proof of Concept als Python Script stelle ich gerne bei persönlicher Kontaktaufnahme zur Verfügung!

Ich würde mich sehr über eine Rückmeldung freuen und stehe Ihnen für Rückfragen jederzeit zur Verfügung. Gerne unterstützen wir Sie auch als Dienstleister bei der Verbesserung Ihres Services, zum Beispiel durch Penetrationstes



ts.





Mit freundlichen Grüßen,
Andre Savic
+436641947241

--

Andre Savic
Geschäftsführung Rubberduck Labs OG
Schlachtbrücke 5, 7061 Trausdorf an der Wulka

Mobile: +43 6641947241
Email: andre@rubberducklabs.at
Web: www.rubberducklabs.at

serverresposne.json
2K