Unlimited trial Burp Professional version via Inconsistent Email Normalization Leading to Authentication Bypass

Observation:

During our assessment, we identified a vulnerability in the trial registration process that allows users to bypass trial restrictions and gain multiple accesses to the premium version of the software. This was achieved by manipulating the email input field using aliasing techniques, such as appending +1 to an already registered email address.

By repeating this process, an attacker can generate an unlimited number of trial accounts, effectively avoiding the need to purchase a valid license. This flaw could be exploited at scale, leading to significant financial and operational consequences for the business.

Impact:

The vulnerability has multiple security and financial implications, including:

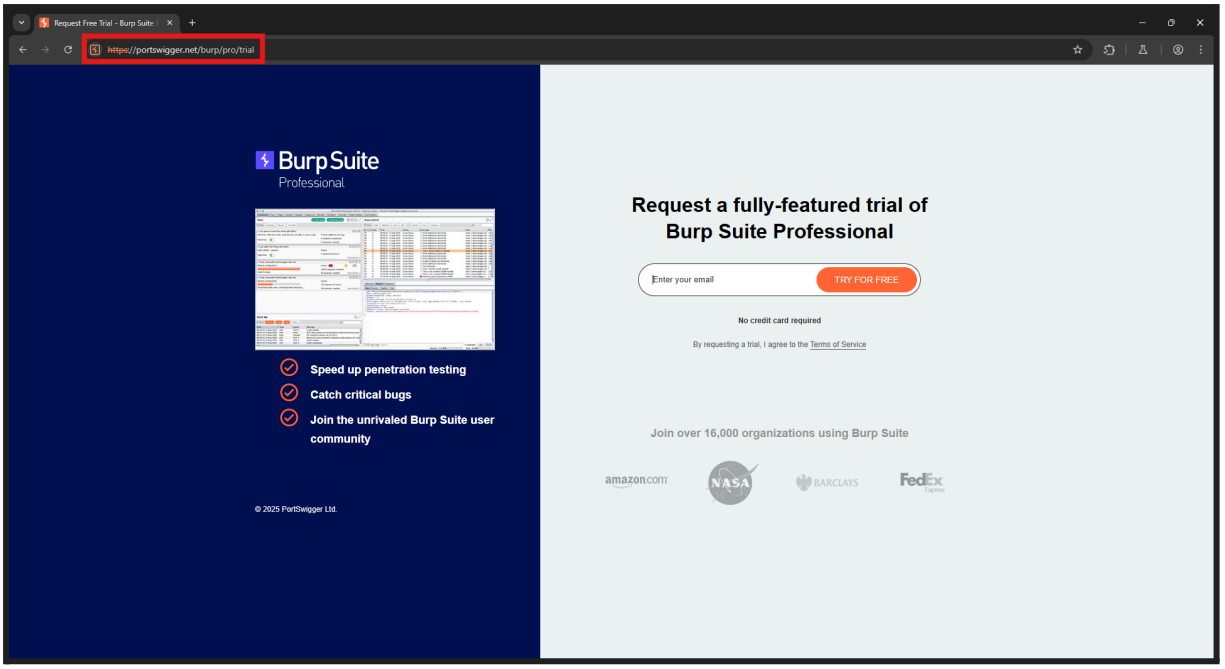
- **Financial Loss**: Attackers can continuously access premium services for free, leading to revenue loss as legitimate customers may opt to abuse the trial instead of purchasing a valid license.
- **Unauthorised Redistribution**: Since the trial keys can be obtained multiple times, an attacker may distribute or resell the keys on third-party platforms, further impacting the organisation's sales.
- **Reputation Damage**: If trial keys are widely shared or sold on the black market, it could undermine the perceived value of the premium offering, eroding customer trust.
- **Increased Operational Costs**: Abuse of the trial system could result in increased server loads and unnecessary customer support inquiries, affecting business operations.

Affected function:

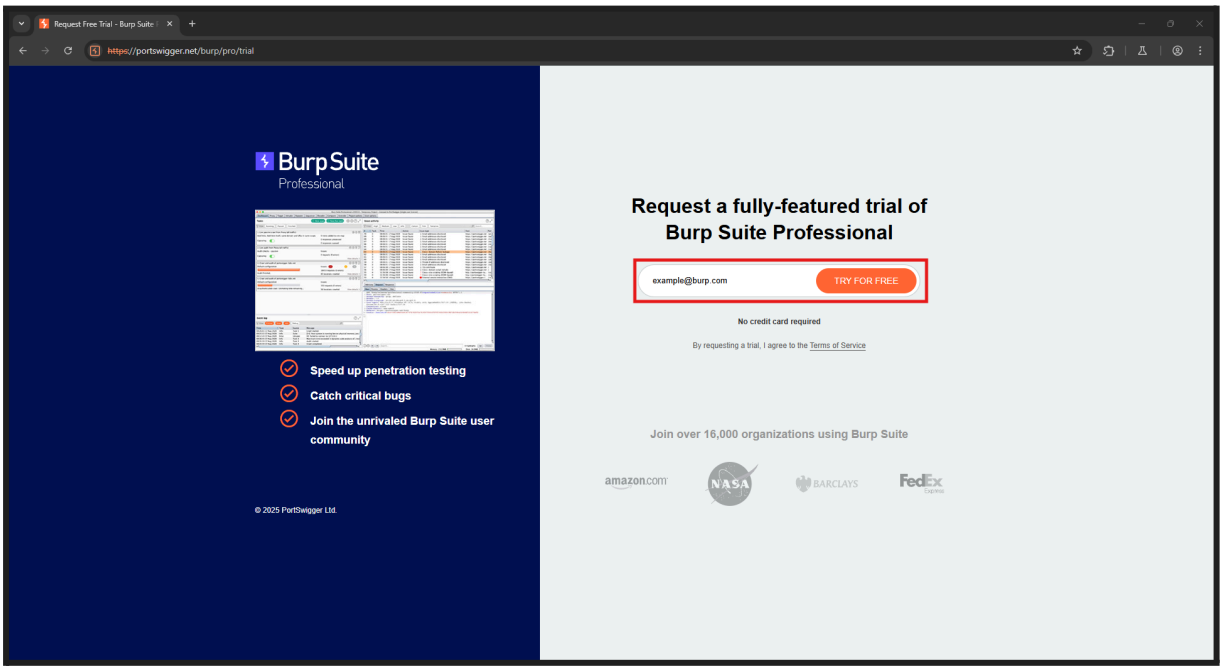
Request a fully-featured trial of Burp Suite Professional > Try for free

- https://portswigger.net/burp/pro/trial
    - *Parameter: Email*

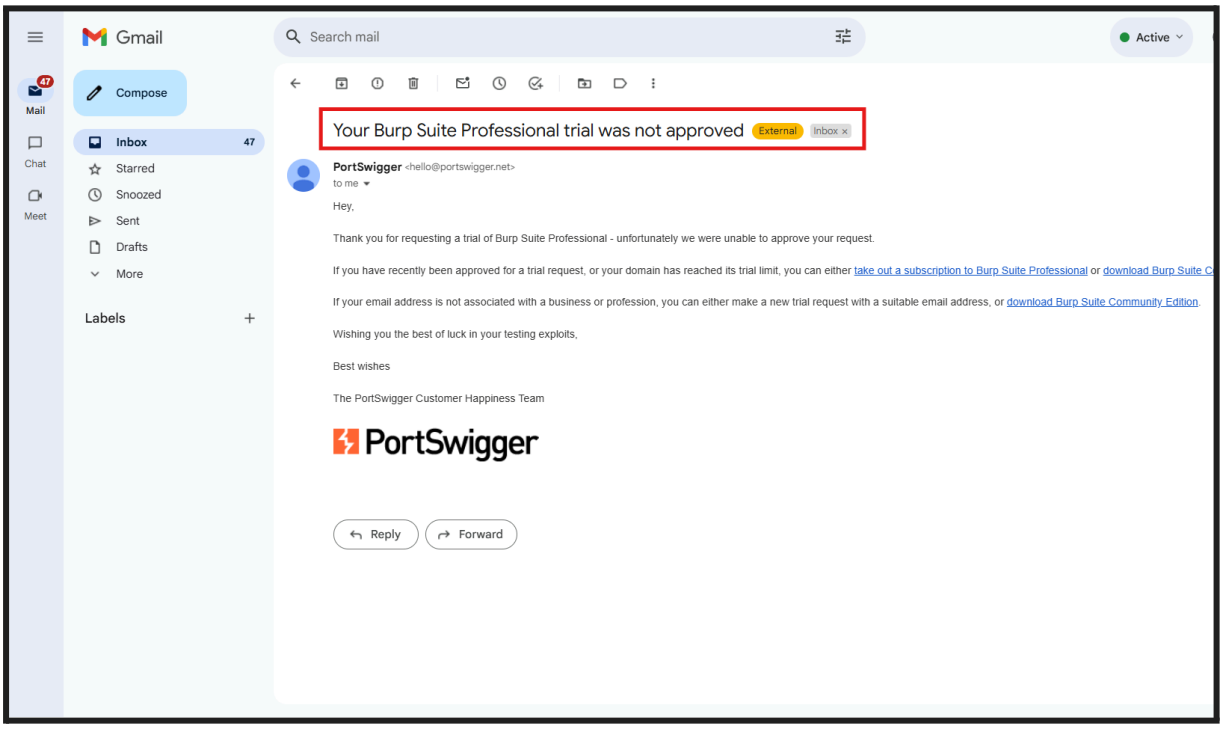
We identified a vulnerability in the trial registration process by submitting a web request that allowed the use of business or student email addresses.



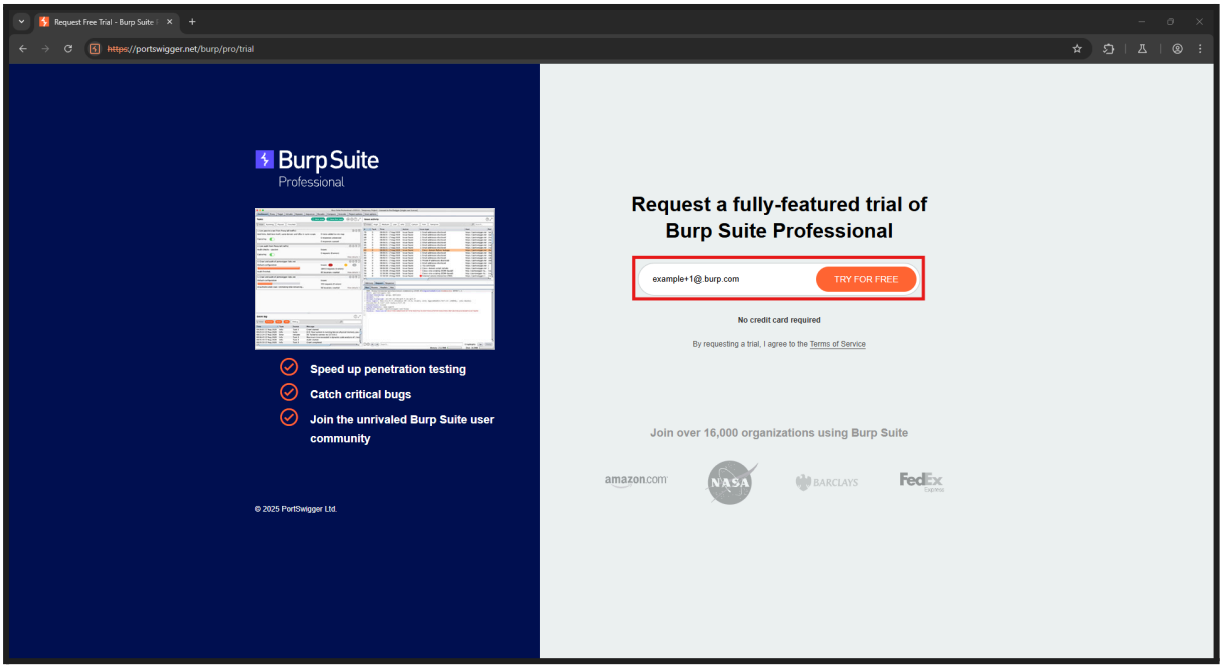
We initially registered with used email, previously used email address and completed all required steps.



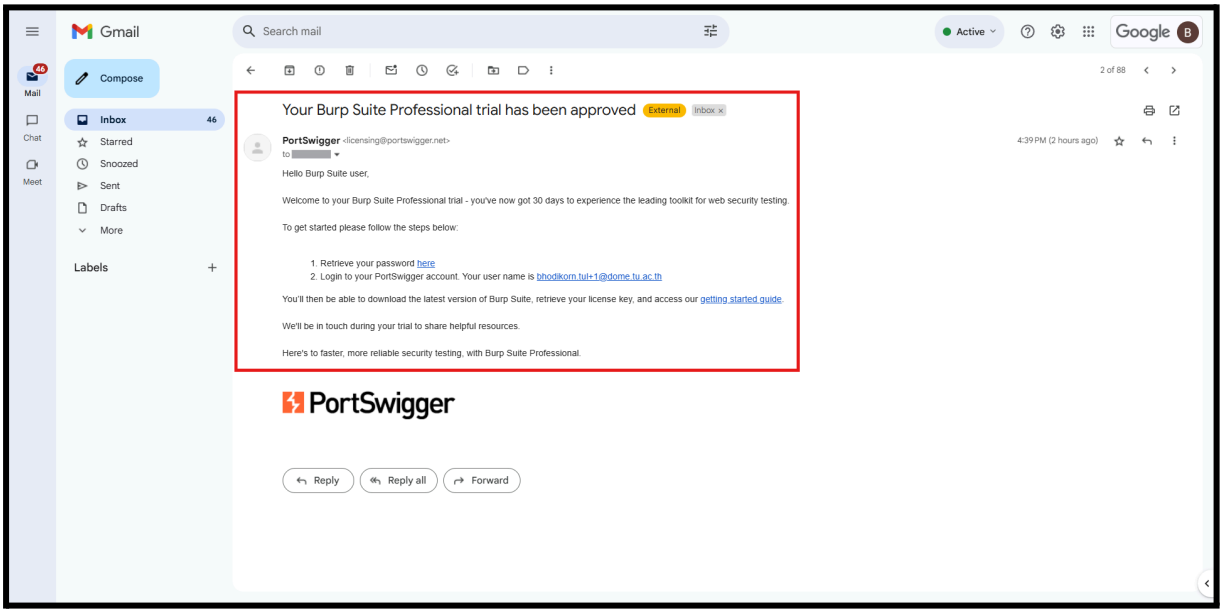
The system responded with an email stating that the trial request was not approved.



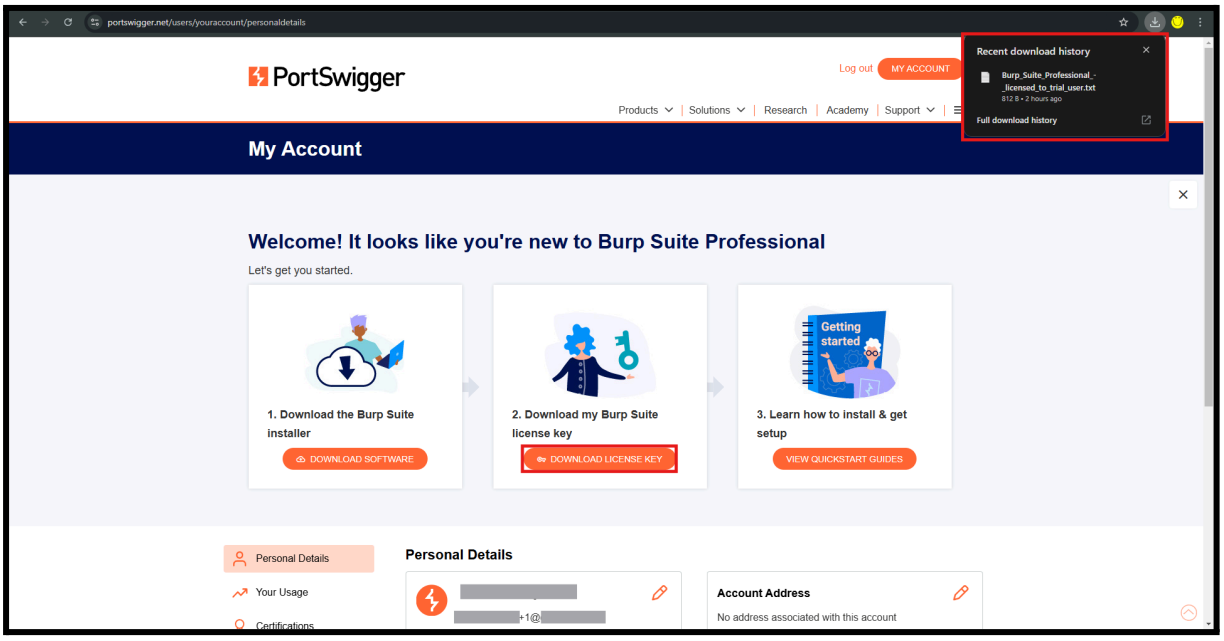
We then modified the email address by appending **+1** to the local part (e.g., **`user@example.com`** → **`user+1@example.com`**) and repeated the registration process.



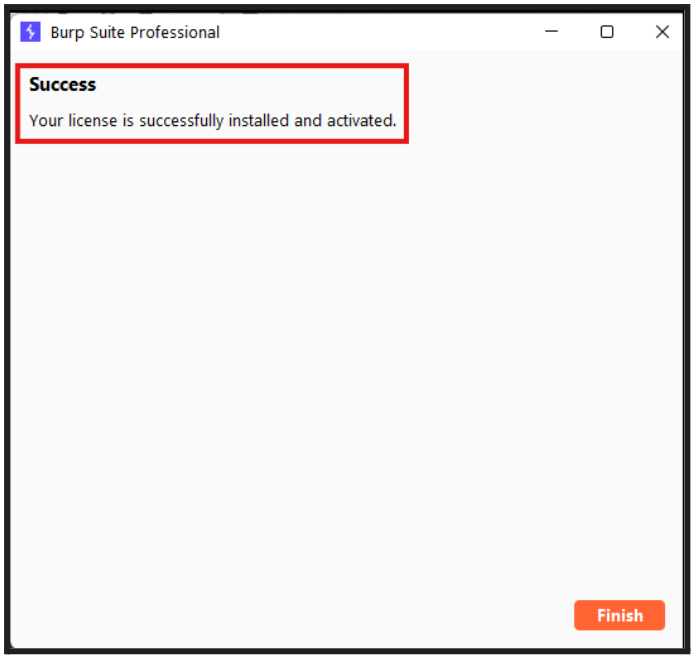
This time, we successfully received a confirmation email approving the trial request.



Next, using the provided credentials, we accessed the web application and downloaded the trial license key.



To verify the impact, we used the downloaded key to activate the **Pro Version**, confirming that the email bypass was successful.



Recommendation:

To mitigate this issue, we strongly recommend implementing strict email validation to prevent aliasing techniques such as adding +1 to existing emails. Normalising email inputs before processing registrations can effectively block this method of abuse.

Furthermore, monitoring and blocking suspicious trial registration patterns can help identify and prevent abuse in real time. The organisation should also update its Terms of Service to explicitly prohibit trial abuse and unauthorised redistribution, while implementing measures to track and disable fraudulently obtained licenses. By adopting these measures, the organisation can protect its revenue, maintain the integrity of its premium services, and prevent reputational damage caused by unauthorised access and key reselling.