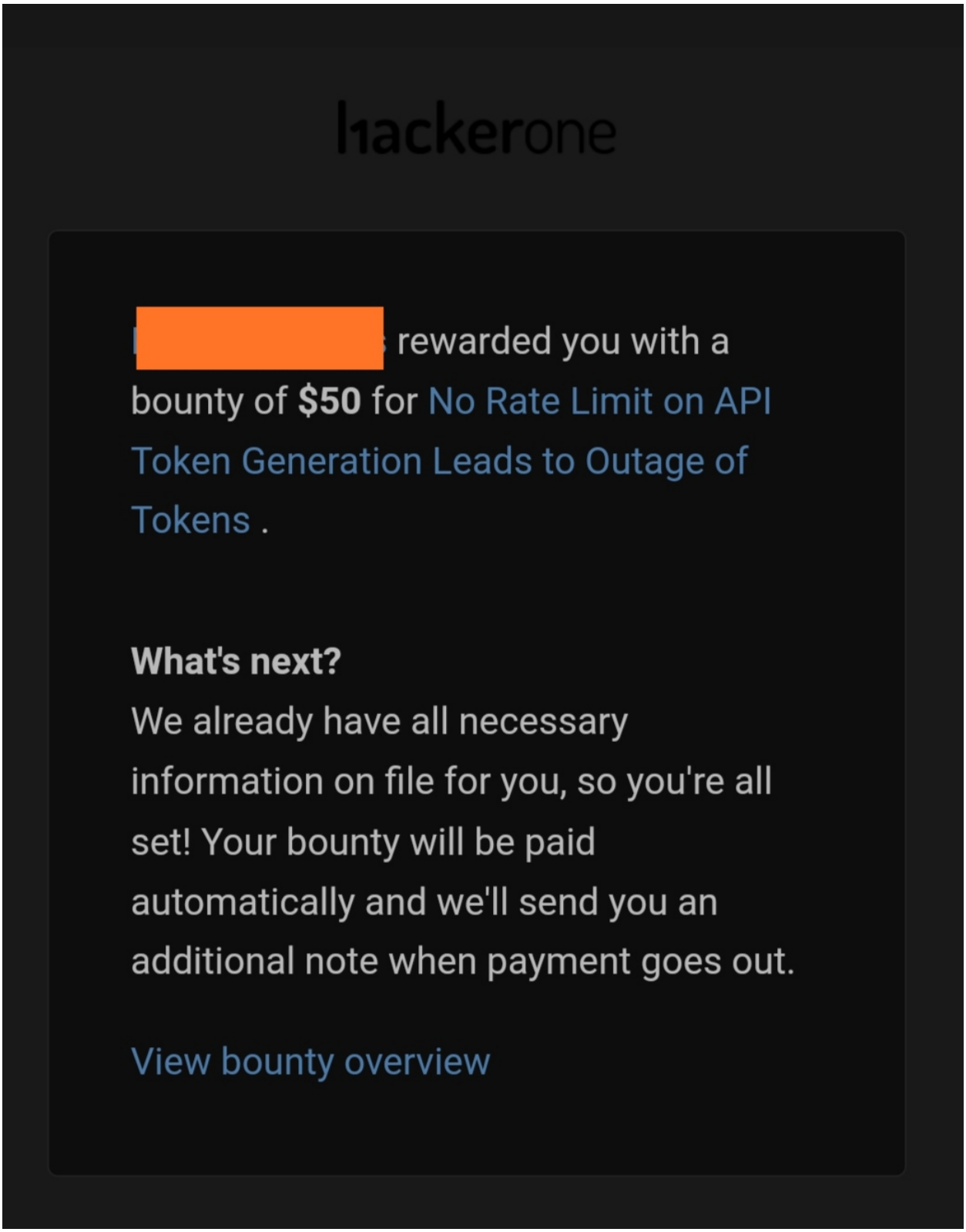
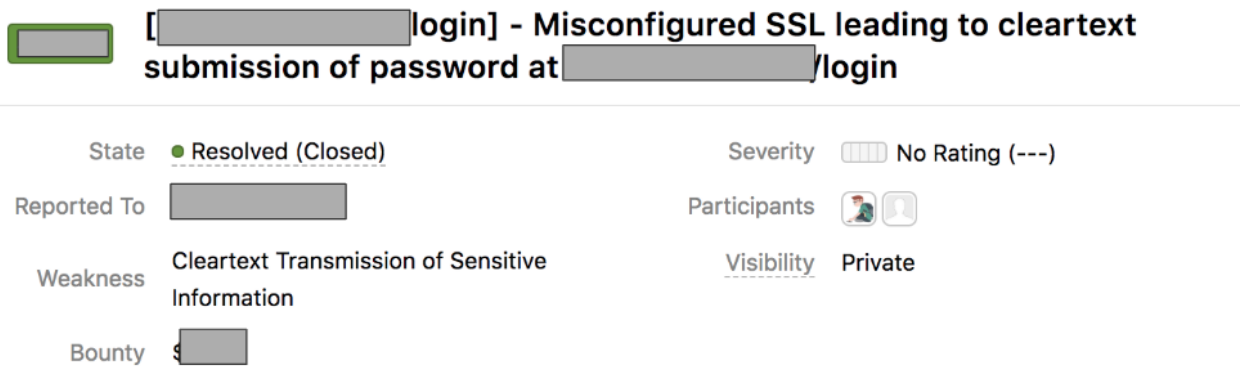
Easily Win


hackerone
[redacted] rewarded you with a bounty of $50 for No Rate Limit on API Token Generation Leads to Outage of Tokens .
What's next?
We already have all necessary information on file for you, so you're all set! Your bounty will be paid automatically and we'll send you an additional note when payment goes out.
View bounty overview

- [ ] Always check if Strict transport security is enforced? Many a times, hxxp://redacted.com is not redirected to https, many companies are interested to hear about “Weak Login function over HTTP”.



- [ ] Check for cache purge https://medium.com/@priyanshbansal25/unauthenticated-cache-purge-c56fac8569e8 https://hackerone.com/reports/154278
- [ ] `P4` Check for rate limiting

```
1. No Rate Limiting on Form Registration
2. No Rate Limiting on Form Login
3. No Rate Limiting on Form Email-Triggering
4. No Rate Limiting on Form SMS-Triggering
5. Current password to delete account https://hackerone.com/reports/1392287
```

- [ ] `P4` Failure to Invalidate Session

```
1. On Logout (Client and Server-Side)
2. On Password Reset and/or Change
```

- [ ] `P4` Content Spoofing

```
1. Email HTML Injection
2. Broken Link Hijacking
```

- [ ] Missing Secure or `HTTPOnly` Cookie Flag
- [ ] Lack of Password Confirmation Delete Account

- [ ] Token Leakage via `Referer` 3rd Party **|** Over HTTP
- [ ] Via `localStorage` / `sessionStorag` Sensitive Token

```
one more tip from https://hackerone.com/reports/8846
1. Login to your account & now logged out
2. Go to localStorage and check for information like email or token
```

- [ ] Reset token lean to 3rd party

```
1. Open your reset link
2. Don't enter new password, click on images. Open all images and social link.
3. Check referer for leaks
```