Analyzing Cryptographic Vulnerabilities on HackerOne

Atefeh Fakhari
Seminar Software Composition, MCS 2020
Supervisor: Mohammadreza Hazhirpasand
Objective

We are interested in looking for what types of cryptographic vulnerability exist on HackerOne.
What is HackerOne?

Hacker finds a vulnerability

Hacker submits it to the company via their Security page

Company rewards the hacker
HackerOne

Hacketivity

See the latest hacker activity on HackerOne

Sort
- New

Type
- All
- Bug Bounty
- Published
- Disclosed

1. IDOR Vulnerability in Job Preferences
   - By root_geek to Glassdoor
   - Resolved
   - Low
   - Disclosed about 1 hr ago

2. SQL Injection intensedebate.com
   - By k3y-13 to Automattic
   - Resolved
   - Medium
   - $350.00
   - Disclosed 3 hrs ago

3. No rate limit in email subscription
   - By splint3tic to Zengo Inc
   - Resolved
   - Medium
   - Disclosed 8 hrs ago

4. GraphQL introspection query works through unauthenticated WebSocket
   - By zeroadvision to Bitwala
   - Resolved
   - Medium
   - Disclosed 2 days ago

5. Login page vulnerable to brute force attacks via rate limiting bypass
   - By sh00ck to Khan Academy
   - Resolved
   - Low
   - Disclosed 2 days ago

6. Owner can change themself for another Role Mode but application does not have this function.
   - By bugera to Doppler
   - Resolved
   - Low
   - Disclosed 2 days ago

7. Stored XSS in [https://dashboard.doppler.com/workplace/*/logs] pages
   - Disclosed 3 days ago
Data extraction with python
Dataset

- 9311 Hacktivity
- 3160 Hackers
- 315 Companies
- 5,342,500
Top 20 hackers

Top hackers based on the total money earned

- Series 1
- Series 2

Reward earned vs. Number of bug reports

Top hacker based on the total bug report

Reward earned vs. Number of bug reports
Top 20 companies

Mail.ru 684
HackerOne 433
U.S. Dept Of Defense 352
Shopify 335
Node.js third-party modules 291
Nextcloud 290
PHP (IBB) 251
Twitter 221
New Relic 195
Uber 187
Shopify-scripts 161
Legal Robot 154
GitLab 148
Weblate 139
Gratipay 136
VK.com 126
Starbucks 125
Zomato 114
Slack 110
LocalTapiola 105

Number of Bug
Analyzing cryptographic vulnerability
Weaknesses

There are 121 unique weaknesses
## Weaknesses

<table>
<thead>
<tr>
<th>Criteria</th>
<th>On HackerOne</th>
<th>Manual analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weakness like ‘%crypto%’</td>
<td>180</td>
<td>115</td>
</tr>
<tr>
<td>Weakness like ‘%encrypt%’ or ‘%auth%’ or ‘%pass%’ or ‘%private%’ or ‘%ssl%’</td>
<td>670</td>
<td>167</td>
</tr>
<tr>
<td>Summary like ‘%crypto%’ or ‘%encrypt%’ or ‘%auth%’ or ‘%pass%’ or ‘%private%’ or ‘%ssl%’</td>
<td>55</td>
<td>33</td>
</tr>
</tbody>
</table>
Crypto bug types

- Clear text transfer / Mix content https-http: 25 bugs
- Certificates related problems (validation, CAA ..): 21 bugs
- Weak crypto defaults / Default encryption password and salt: 18 bugs
- The POODLE attack: 13 bugs
- The side channel attacks / The timing attacks: 11 bugs
- Secret key / Key disclosure / Hard-coded password / Session cookie disclosure: 11 bugs
- OpenSSL bugs: 9 bugs
- Cookie ssl flag / HTTP Strict Transport Security: 9 bugs
- Weak Pseudo-Random Number Generator: 8 bugs
- The sweet32 attack: 7 bugs
- Key forgery / Signing issues / Signature verification: 6 bugs
- The Breach attack: 4 bugs
- The Drown attack: 4 bugs
- The padding oracle attack: 4 bugs
- Cross-site request forgery: 3 bugs
- SSL pinning: 3 bugs
- The Beast attack: 3 bugs
- Reduced key size / premutation / key id collision: 3 bugs
- Encryption without authentication: 2 bugs
- Insecure data storage: 2 bugs
- The freak attack: 1 bug
- The ssl stripping attack: 1 bug
- Divide-and-conquer session key recovery: 1 bug
- The CBC cut and paste attack: 1 bug
- The hash length extension attack: 1 bug
- The chosen-cipher text attack: 1 bug
- The Invalid Curve attack: 1 bug
- Heartbleed: 1 bug
- Key poisoning: 1 bug
- Dragonfly handshake of WPA3: 1 bug
- The KRACK attack: 1 bug
Companies’ crypto bugs

<table>
<thead>
<tr>
<th>Company</th>
<th>Number of bug</th>
<th>Paid reward</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenSSL (IIB)</td>
<td></td>
<td>37,250</td>
</tr>
<tr>
<td>Twitter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Internet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.S. Dept Of Defense</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grapixpy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HackerOne</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LocalTaylola</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nextcloud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uber</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ownCloud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MariaDB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ReleaseQ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shopify</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weblate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coinbase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LocalIre</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number of bug vs. Paid reward for various companies.
Authentication bugs types
Authentication bug types

- Bypassing authentication / Weak authorization: 91
- Weak password reset workflow: 30
- OAuth: 29
- Bypass Two Factor Authentication / Multi-Factor Authentication: 20
- Password policy mistakes: 11
- One-time password: 8
- JSON Web Token: 3
- Replay protection: 3
- Biometric: 1

(Number of Bug)
Companies’ authentication bugs

[Graph showing the number of bugs and paid rewards for different companies.]

- NextCloud: 9 bugs, $55,600 reward
- Twitter: 5 bugs, $0 reward
- Uber: 8 bugs, $0 reward
- HackerOne: 7 bugs, $0 reward
- Shopify: 6 bugs, $0 reward
- Weblate: 5 bugs, $0 reward
- Wakatime: 4 bugs, $0 reward
- Automatic: 3 bugs, $0 reward
- Coinbase: 2 bugs, $0 reward
- New Relic: 1 bug, $0 reward
- Slack: 1 bug, $0 reward
- GitLab: 1 bug, $0 reward
- Legal Robot: 1 bug, $0 reward
- Phlacticator: 1 bug, $0 reward
- Zomato: 1 bug, $0 reward
- Algolia: 1 bug, $0 reward
- Badoo: 1 bug, $0 reward
- Boots Fashion: 1 bug, $0 reward
- Dropbox: 1 bug, $0 reward
- Grab: 1 bug, $0 reward