Bugcrowd public reports

Bug

1. XSS reflected https://www.indeed.com/hire/employer-confirmation
2. prototype pollution in tesla
3. Reflected XSS via HTML Injection
4. You link way porn
5. OAuth misconfiguration found on https://wemedia.opera.com
6. business logic flaw
7. Subdomain Takeover for rtncf-rci.ral.r4.fws.gov
8. Stored Xss on Portfolio
9. Reflected cross site scripting in login page
10. sensitive Data Exposure (User Personal Details)
11. 2FA Secret is not rotated
12. Vulnerable to Log4j
13. Panel access at https://news-push-88.op-mobile.opera.com
14. Password change does not invalidate API keys
15. Email HTML Injection at https://baito.indeed.com
16. Secret Board Name Exposure
17. XSS
18. Failed to validate Session after Password Change
19. IDOR_4 [on Add] services into victims account
20. Unrestricted file upload {Stored Xss for Token hijacking}
21. Able to change other publishers' payment details
22. CSRF- On Adding Bank Account
23. Open Redirect Via Chrome Extension
24. Authorized drivers can disable remote monitoring
25. HTTP Desync Attack (Request Smuggling)Mass Session Hijacking
26. 1.7M Password hashes, No Auth Required Access Tokens
27. User Role has Access to too much Information via Changelog
28. Link hijacking leads to open redirection on accounts.yoyogames.com
29. Pre-Auth Denial of Service in Crowd
30. Improper Authorization Second (Additional) Driver can list "add-driver" invitation links
31. XXE via JUnit Preview in Confluence Cloud
32. Stored-xss is working
33. Local file read (CVE2020-3452 in CISCO ASA)
34. ExpressVPN Router] Integer Buffer Overflow: Server Info Disclosure When Router's Nginx Server used as Reverse Proxy Server
35. Broken Twitter Handle Link
36. privilege escalation allow the admin to takeover the org by invite the user as owner
37. CSRF Bypass/plugins/servlet/oauth/consumer-info/XXX in Confluence Server
38. XSS on Yoyogames Search
39. Impersonation via Broken Link Hijacking on https://sv.hellosign.com

40. Auth.Tesla.com Account Takeover of Internal Tesla Accounts
41. Authentication Bypass through HTTP Request Smuggling on https://apm.ap.tesla.services
42. Self XSS on my.indeed.com affecting multiple input fields
43. Reflected Cross Site Scripting while connection with Slack integration in Jira Server
44. Several internal applications have open CORS, allowing external folks to access the content
45. Android app allows authentication with new fingerprints
46. exploitable weaknesses in functionality
47. SpaceX debug page accessible when using Starlink
48. Exif Data not Removed after uploading image to Indox
49. Session fixation
50. Host `docker` binary overwrite from Kata VM
51. Stored XSS [doi.gov/iacb/indian-arts-and-crafts-board-potential-violation-report
52. CSRF leads to name change
53. No DMARC Record Found
54. Xss Vulnerability of upload svg files in a collection section that triggers xss
55. Leaking issue details in linked Jira/plugins/servlet/jira-chart-proxy
56. Source code leakage due to exposed sourcemap
57. Backend Stock access which can be accessed to the admin
58. information Disclosure via url tampering
59. Linksys RE6500 UNAUTHENTICATED RCE working across multiple FW versions
60. Discord Link expiredPossible vanity address could be used to link a malicious Discord server
61. testdrive form user data info leak via [3rdparty] exploit
62. Linux clientLack of certificate validation leading to RCE
63. Linux clientcommand injectionlocal privilege escalation
64. html injection in [https://edoiu.doi.gov/login/signup.php]
65. Clickjacking
66. Pre-auth Dos in Jira Server
67. config files with vpn pre-shared-key and other credentials in them
68. Information Disclosure of sensitive data CVE-2017-5487
69. Lack of Security Headers
70. Xss in resume
71. Xss onemployers.indeed.com
72. Price Manipulation
73. Bypass URL and IP Address Restrictions on analytics.starlink.com
74. XSS in image with user-controlled src
75. Reflected XSS via HTML Injection2
76. postMessage XSS in Tesla Payment page
77. Open Redirect On login Page
78. HTML Injection &gt; licensing.fcc.gov
79. Public access to bill
80. text injection
81. Sensitive Log Files exposed to Public through Directory listing
82. Grafana admin login via default credentials

82. Bypassing security controls for authorisation bypass on identity.yoyogames.com
83. Asana Desktop Application Includes Personal Access Token
84. Blind stored XSS in indeed
85. Reflected Cross Site Scripting (XSS) on https://gamemaker.io
86. CSRF Leads to Logout any Loggedin user from their session
87. No Rate Limiting on resend email option when signing up for an account
88. REFLECTED XSS
89. RCE in Bitbucket DataCenter via HazelCastPort
90. Critical Local File Read in Electron Desktop App
91. Log4Shell (CVE-2021-44228)
92. Multiple privilege escalations using a low privileged user
93. Bypass Sanitizetion for Stored XSS + Blind SSRF External + Open Redirect on publisher description
94. RCE on https://beta-partners.tesla.com due to CVE-2020-0618
95. Reflected XSS
96. Privilege Escalation of Publisher Account due to IDOR
97. Slack is able to connect any user to a confluence page without even prompting anything
98. RCE on https://beta-partners.tesla.com due to CVE-2020-0618
99. Reflected XSS
100. Pinterest Lite can be opened via LauncherActivity to load arbitrary urls and execute javascript in a webview