Top Business Logic reports from HackerOne:

1. Project Template functionality can be used to copy private project data, such as repository, confidential issues, snippets, and merge requests to GitLab - 438 upvotes, $12000
2. Ethereum account balance manipulation to Coinbase - 260 upvotes, $0
3. Account takeover through the combination of cookie manipulation and XSS to Grammarly - 259 upvotes, $0
4. SSRF leaking internal google cloud data through upload function [SSH Keys, etc..] to Vimeo - 250 upvotes, $0
5. Account Takeover via Email ID Change and Forgot Password Functionality to New Relic - 212 upvotes, $2048
6. Blind SQL injection and making any profile comments from any users to disappear using "like" function (2 in 1 issues) to Pornhub - 211 upvotes, $0
7. Abusing "Report as abuse" functionality to delete any user's post. to Vanilla - 159 upvotes, $300
8. OLO Total price manipulation using negative quantities to Upserve - 146 upvotes, $0
9. Unserialize leading to arbitrary PHP function invoke to Rockstar Games - 113 upvotes, $0
10. HTTP Request Smuggling in Transform Rules using hexadecimal escape sequences in the concat() function to Cloudflare Public Bug Bounty - 105 upvotes, $6000
11. Null pointer dereference in SMTP server function smtp_string_parse to Open-Xchange - 105 upvotes, $1500
12. XXE in Site Audit function exposing file and directory contents to Semrush - 101 upvotes, $0
13. Claiming the listing of a non-delivery restaurant through OTP manipulation to Zomato - 87 upvotes, $3250
14. Bypass of biometrics security functionality is possible in Android application (com.shopify.mobile) to Shopify - 74 upvotes, $500
15. Old WebKit HTML agent in Template Preview function has multiple known vulnerabilities leading to RCE to Lob - 68 upvotes, $1500
16. Parameter Manipulation allowed for viewing of other user's teavana.com orders to Starbucks - 66 upvotes, $0
17. Title: Deceptive Manipulation of HTTP to HTTPS with VPN in Burp Suite to PortSwigger Web Security - 66 upvotes, $0
18. Authorization Token on PlayStation Network Leaks via postMessage function to PlayStation - 65 upvotes, $1000
19. Manipulating response leads to free access to Streamlabs Prime to Logitech - 62 upvotes, $0

20. [api.tumblr.com] Denial of Service by cookies manipulation to Automattic - 51 upvotes, $0
21. Captcha bypass for the most important function - At en.instagram-brand.com to Automattic - 50 upvotes, $0
22. SSRF in VCARD photo upload functionality to Open-Xchange - 49 upvotes, $850
23. Stored XSS in photo comment functionality to Pornhub - 44 upvotes, $0
24. [intensedebate.com] No Rate Limit On The report Functionality Lead To Delete Any Comment When it is enabled to Automattic - 43 upvotes, $0
25. SSRF in the application's image export functionality to Visma Public - 42 upvotes, $250
26. Able to steal private files by manipulating response using Compose Email function of Lark to Lark Technologies - 42 upvotes, $0
27. Unrestricted access to quiesce functionality in dss.api.playstation.com REST API leads to unavailability of application to PlayStation - 40 upvotes, $1000
28. [stored xss, pornhub.com] stream post function to Pornhub - 35 upvotes, $1500
29. SSRF in Functional Administrative Support Tool pdf generator ([redacted]) [HtUS] to U.S. Dept Of Defense - 34 upvotes, $4000
30. Parameter Manipulation allowed for editing the shipping address for other user's teavana.com subscriptions. to Starbucks - 33 upvotes, $0
31. Logic flaw in the Post creation process allows creating posts with arbitrary types without needing the corresponding nonce to WordPress - 33 upvotes, $0
32. Price manipulation via fraction values (Parameter Tampering) to Shipt - 32 upvotes, $100
33. Able to steal private files by manipulating response using Auto Reply function of Lark to Lark Technologies - 32 upvotes, $0
34. Business Logic Flaw in the subscription of the app to Kraden - 31 upvotes, $250
35. Privilege escalation allows to use iframe functionality w/o upgrade to Infogram - 31 upvotes, $0
36. Week Passwords generated by password reset function to MTN Group - 30 upvotes, $0
37. Self-XSS in password reset functionality to Shopify - 29 upvotes, $500
38. Parameter tampering can result in product price manipulation to Adobe - 28 upvotes, $0
39. Manipulation of exam results at Semrush.Academy to Semrush - 27 upvotes, $0
40. RCE via Print function [Simplenote 1.1.3 - Desktop app] to Automattic - 26 upvotes, $0
41. GoldSrc: Buffer Overflow in DELTA_ParseDelta function leads to RCE to Valve - 25 upvotes, $3000
42. Argument/Code Injection via ActiveStorage's image transformation functionality to Ruby on Rails - 25 upvotes, $0
43. Add more seats by paying less via PUT /v2/seats request manipulation to Krisp - 24

upvotes, $0

44. Notifications sent due to "Transfer report" functionality may be sent to users who are no longer authorized to see the report to HackerOne - 19 upvotes, $500
45. Business Logic Flaw - A non premium user can change/update retailers to get cashback on all the retailers associated with Curve to Curve - 19 upvotes, $0
46. IDOR in report download functionality on ads.tiktok.com to TikTok - 16 upvotes, $500
47. Response Manipulation leads to Admin Panel Login Bypass at https://[redacted]/ to Sony - 16 upvotes, $0
48. Multiple File Manipulation bugs in WP Super Cache to Automattic - 15 upvotes, $0
49. response manipulation leads to bypass in register at employee website than 0 click account takeover to IBM - 15 upvotes, $0
50. Spoof Email with Hyperlink Injection via Invites functionality to Pushwoosh - 14 upvotes, $0
51. XSS in main search, use class tag to imitate Reverb.com core functionality, create false login window to Reverb.com - 14 upvotes, $0
52. Remote Code Execution through Extension Bypass on Log Functionality to Concrete CMS - 14 upvotes, $0
53. Incorrect handling of certain characters passed to the redirection functionality in Rails can lead to a single-click XSS vulnerability. to Ruby on Rails - 14 upvotes, $0
54. Privilege escalation in the client impersonation functionality to Ubiquiti Inc. - 12 upvotes, $0
55. CSV-injection in export functionality to Passit - 12 upvotes, $0
56. Unauthenticated reflected XSS in preview_as_user function to Concrete CMS - 12 upvotes, $0
57. DoS in bigdecimal's sqrt function due to miscalculation of loop iterations to Ruby - 12 upvotes, $0
58. Stored self XSS at auto.mail.ru using add_review functionality to Mail.ru - 11 upvotes, $0
59. [CVE-2020-27194] Linux kernel: eBPF verifier bug in `or` binary operation tracking function leads to LPE to Internet Bug Bounty - 10 upvotes, $750
60. [kb.informatica.com] DOM based XSS in the bindBreadCrumb function to Informatica - 10 upvotes, $0
61. Logic issue in email change process to Legal Robot - 10 upvotes, $0
62. No Rate limit on Password Reset Function to Infogram - 10 upvotes, $0
63. Impact of Using the PHP Function "phpinfo()" on System Security - PHP info page disclosure to U.S. Department of State - 10 upvotes, $0
64. Time-of-check to time-of-use vulnerability in the std::fs::remove_dir_all() function of the Rust standard library to Internet Bug Bounty - 9 upvotes, $4000
65. Improperly implemented password recovery link functionality to Phabricator - 9 upvotes,

$300

66. Missing rate limiting on password reset functionality allows to send lot of emails to Nextcloud - 9 upvotes, $100
67. Reflected XSS by way of jQuery function to Pornhub - 9 upvotes, $50
68. Business Logic, currency arbitrage - Possibility to pay less than the price in USD to PortSwigger Web Security - 9 upvotes, $0
69. CSRF in the "Add restaurant picture" function to Zomato - 8 upvotes, $50
70. Server Side Request Forgery In Video to GIF Functionality to Imgur - 8 upvotes, $0
71. Reputation Manipulation (Theoretical) to HackerOne - 8 upvotes, $0
72. Impersonation of Wakatime user using Invitation functionality. to WakaTime - 8 upvotes, $0
73. Change password logic inversion to Legal Robot - 8 upvotes, $0
74. Logic issue in email change process to Legal Robot - 8 upvotes, $0
75. Missing Password Confirmation at a Critical Function (Payout Method) to HackerOne - 8 upvotes, $0
76. Allow authenticated users can edit, trash,and add new in BuddyPress Emails function to WordPress - 8 upvotes, $0
77. memory corruption in wordwrap function to Internet Bug Bounty - 7 upvotes, $500
78. Logic flaw enables restricted account to access account license key to New Relic - 7 upvotes, $500
79. Logic Issue with Reputation: Boost Reputation Points to HackerOne - 7 upvotes, $0
80. Business logic Failure - Browser cache management and logout vulnerability in Certly to Certly - 7 upvotes, $0
81. unchecked unserialize usage in WordPress-Functionality-Plugin-Skeleton/functionality-plugin-skeleton.php to Ian Dunn - 7 upvotes, $0
82. Application XSS filter function Bypass may allow Multiple stored XSS to Vimeo - 7 upvotes, $0
83. Firefly's verify_access_token() function does a byte-by-byte comparison of HMAC values. to Yelp - 7 upvotes, $0
84. Remote Code Execution in the Import Channel function to ExpressionEngine - 7 upvotes, $0
85. Parameter tampering : Price Manipulation of Products to WordPress - 7 upvotes, $0
86. Rate limit function bypass can leads to occur huge critical problem into website. to Courier - 7 upvotes, $0
87. CSV export/import functionality allows administrators to modify member and message content of a workspace to Slack - 6 upvotes, $250
88. Deleted name still present via mouseover functionality for user accounts to HackerOne - 6

upvotes, $0

89. Deleted Post and Administrative Function Access in eCommerce Forum to Shopify - 6 upvotes, $0
90. Non-functional 2FA recovery codes to Legal Robot - 6 upvotes, $0
91. Incorrect Functionality of Password reset links to Infogram - 6 upvotes, $0
92. Business Logic Flaw allowing Privilege Escalation to Inflection - 6 upvotes, $0
93. Lodash "difference" (possibly others) Function Denial of Service Through Unvalidated Input to Node.js third-party modules - 6 upvotes, $0
94. Owner can change themself for another Role Mode but application doesnot have this function. to Doppler - 6 upvotes, $0
95. ihsinme: CPP Add query for CWE-783 Operator Precedence Logic Error When Use Bool Type to GitHub Security Lab - 5 upvotes, $1800
96. Business logic Failure - Browser cache management and logout vulnerability. to Localize - 5 upvotes, $0
97. Issue with password reset functionality [Minor] to Paragon Initiative Enterprises - 5 upvotes, $0
98. The PdfServlet-functionality used by the "Tee vakuutustodistus" allows injection of custom PDF-content via CSRF-attack to LocalTapiola - 5 upvotes, $0
99. Weak e-mail change functionality could lead to account takeover to Weblate - 5 upvotes, $0
00. Amount Manipulation Buy Unlimited Credits in just $1.00 to Inflection - 5 upvotes, $0
01. Locked_Transfer functional burning to Monero - 5 upvotes, $0
02. HTTP Host injection in redirect_to function to Ruby on Rails - 5 upvotes, $0
03. 2 Cache Poisoning Attack Methods Affect Core Functionality www.exodus.com to Exodus - 5 upvotes, $0
04. Manipulation of submit payment request allows me to obtain Infrastructure Pro/Other Services for free or at greatly reduced price to New Relic - 4 upvotes, $600
05. Invalid parameter in memcpy function trough openssl_pbkdf2 to Internet Bug Bounty - 4 upvotes, $500
06. Logic error with notifications: user that has left team continues to receive notifications and can not 'clean' this area on account to HackerOne - 4 upvotes, $0
07. Spamming any user from Reset Password Function to HackerOne - 4 upvotes, $0
08. Spamming any user from Reset Password Function to Weblate - 4 upvotes, $0
09. New team invitation functionality allows extend team without upgrade to Infogram - 4 upvotes, $0
10. Command Injection due to lack of sanitisation of tar.gz filename passed as an argument to pm2.install() function to Node.js third-party modules - 4 upvotes, $0

11. idor on upload profile functionality to U.S. Dept Of Defense - 4 upvotes, $0
12. crash in locale_compose() function to Internet Bug Bounty - 3 upvotes, $500
13. Issue with Password reset functionality to Uber - 3 upvotes, $100
14. Null pointer dereference in SMTP server function smtp_command_parse_data_with_size to Open-Xchange - 3 upvotes, $50
15. SSRF (Portscan) via Register Function (Custom Server) to RelateIQ - 3 upvotes, $0
16. Redirect URL in /intent/ functionality is not properly escaped to X (Formerly Twitter) - 3 upvotes, $0
17. Missing Function Level Access Control in /cindex.php/widget/customize/ to Bookfresh - 3 upvotes, $0
18. Business/Functional logic bypass: Remove admins from admin group. to Nextcloud - 3 upvotes, $0
19. Enumeration in unsubscribe -function of /omatalousuk (viestinta.lahitapiola.fi) to LocalTapiola - 3 upvotes, $0
20. CSRF token manipulation in every possible form submits. NO server side Validation to Liberapay - 3 upvotes, $0
21. Open redirect in switch account functionality to Revive Adserver - 3 upvotes, $0
22. Command Injection in npm module name passed as an argument to pm2.install() function to Node.js third-party modules - 3 upvotes, $0
23. Incorrect logic in MySQL & MariaDB protocol leads to remote SSRF/Remote file read to Internet Bug Bounty - 3 upvotes, $0
24. [yarn] yarn.lock integrity & hash check logic is broken to Node.js third-party modules - 3 upvotes, $0
25. Java : Add a query to detect Spring View Manipulation Vulnerability to GitHub Security Lab - 3 upvotes, $0
26. ihsinme: CPP Add query for CWE-401 memory leak on unsuccessful call to realloc function to GitHub Security Lab - 2 upvotes, $1800
27. Price Manipulation to Uzbey - 2 upvotes, $0
28. csrf on password change functionality to Cloudflare Vulnerability Disclosure - 2 upvotes, $0
29. Abuse of "Remember Me" functionality. to X (Formerly Twitter) - 2 upvotes, $0
30. Balance Manipulation - BUG to Coinbase - 2 upvotes, $0
31. Missing function level access controls allowing attacker to abuse file access controls. Multiple vulnerabilities to Zendesk - 2 upvotes, $0
32. Text manipulation in https://checkout.rbk.money to RBKmoney - 2 upvotes, $0
33. SQL injection (stacked queries) in the export to Excel functionality on Vidyo Server to 8x8 -

2 upvotes, $0

34. Secure credentials values disclosure to regular users due to access control issue in monitor creating function to New Relic - 2 upvotes, $0
35. Integer overlow in "header_append" function to curl - 2 upvotes, $0
36. crash in openssl_random_pseudo_bytes function to Internet Bug Bounty - 1 upvotes, $500
37. heap overflow in php_ereg_replace function to Internet Bug Bounty - 1 upvotes, $500
38. crash in implode() function to Internet Bug Bounty - 1 upvotes, $500
39. iconv() function missing string length check to Internet Bug Bounty - 1 upvotes, $500
40. crash in bzcompress function to Internet Bug Bounty - 1 upvotes, $500
41. crash in get_icu_value_internal function to Internet Bug Bounty - 1 upvotes, $500
42. another crash in locale_get_keywords function to Internet Bug Bounty - 1 upvotes, $500
43. Invalid memory access in zend_strtod() function to Internet Bug Bounty - 1 upvotes, $500
44. crash in simplestring_addn function to Internet Bug Bounty - 1 upvotes, $500
45. Invalid memory access in spl_filesystem_dir_open function to Internet Bug Bounty - 1 upvotes, $500
46. Invalid memory access in php_basename function to Internet Bug Bounty - 1 upvotes, $500
47. Invalid memory access in spl_filesystem_info_set_filename function to Internet Bug Bounty - 1 upvotes, $500
48. CSRF in function "Set as primary" on accounts page to Coinbase - 1 upvotes, $0
49. Rank Creation function not validating user inputs. to WordPoints - 1 upvotes, $0
50. XSS in Search Communities Function to Informatica - 1 upvotes, $0
51. XSS In /zuora/ functionality to Zendesk - 1 upvotes, $0
52. Runtime manipulation iOS app breaking the PIN to Coinbase - 1 upvotes, $0
53. DOM based XSS in search functionality to SecNews - 1 upvotes, $0
54. Password Functionality not working correctly to Khan Academy - 1 upvotes, $0
55. User provided values passed to PHP unset() function to Coinbase - 1 upvotes, $0
56. Heap overflow due to integer overflow in bzdecompress() function to Internet Bug Bounty - 1 upvotes, $0
57. Heap overflow due to integer overflow in pg_escape_string() function to Internet Bug Bounty - 1 upvotes, $0
58. Heap overflow due to integer overflow in php_escape_html_entities_ex() function to Internet Bug Bounty - 1 upvotes, $0
59. Use of Unsafe function || Strcpy to curl - 1 upvotes, $0
60. AddressSanitizer reports a global buffer overflow in mkgmtime() function to Internet Bug Bounty - 0 upvotes, $500

61. Arbitrary code execution in str_ireplace function to Internet Bug Bounty - 0 upvotes, $0
62. DOS in browser using window.print() function to Brave Software - 0 upvotes, $0
63. Not using Binary::safe* functions for substr/strlen function to Paragon Initiative Enterprises - 0 upvotes, $0
64. integer overflow in the _csv module's join_append_data function to Internet Bug Bounty - 0 upvotes, $0
65. Business logic error to UPchieve - 0 upvotes, $0