Hacktivity

See the latest hacker activity on HackerOne

Search Hacktivity

Sort

Popular

Type

○ All

○ Bug Bounty

○ Published

● Disclosed

Filter

□ Hackers I am following

□ Collaborations

77

RCE of Burp Scanner / Crawler via Clickjacking

By **mattaustin** to **PortSwigger Web Security** | ● Resolved | High | **$3,000.00** | disclosed 6 days ago

A vulnerability was discovered in Burp Suite, a web application security testing tool. The vulnerability allowed an attacker to exploit a known XSS vulnerability in the embedded Chrome browser used by Burp Suite. By leveraging this vulnerability, an attacker could execute arbitrary commands on the victim's computer with the same permissions as the user running the scanner. This summary was automatically generated.

22

Potential Spoofing Risk through Firefox Private Relay Service

By **nicholas_cw** to **Mozilla Core Services** | ● Resolved | Medium | **$1,000.00** | disclosed 3 days ago

A potential spoofing risk was identified in the Firefox Private Relay service. Adversaries were able to send spoofing emails to users by leveraging the service. The design of the service allowed these spoofing emails to bypass security measures and reach the target inbox. This was due to the re-composition of the email and modification of the "From" header, which invalidated DKIM and ARC headers. Recommendations were made to address this vulnerability, including authentication checks, ARC validation, and avoiding modification of the original email. This summary was automatically generated.

343

Reset password link sent over unsecured http protocol

By **uchihaluckycs** to **Mattermost** | ● Resolved | High | **$750.00** | swag awarded 17 days ago

A vulnerability was found where the reset password link sent over email after creating a workspace was unsecured http protocol, allowing anyone from intermediate computers through network or sniffer to reset the password if the victim opens the link and forgets to update the password. The vulnerability could have been mitigated by generating the reset password link with secured https protocol. This summary was automatically generated.

10

Client Side string length check

By **tomh** to **Khan Academy** | ● Resolved | Medium | disclosed 2 days ago

A client-side string length check vulnerability allowed an attacker to bypass the expected character limit for renaming a class on Khan Academy's "Class Settings" page. This could lead to various issues such as saving excessive content, breaking page templates, crashing the page for low-memory visitors, and causing unexpected behavior. This summary was automatically generated.

39

CVE-2023-38545: socks5 heap buffer overflow

By **raysatiro** to **curl** | ● Resolved | High | disclosed 5 days ago

18

UAF on JSEthereumProvider

By **nick0ve** to **Brave Software** | ● Resolved | Critical | **$3,000.00** | disclosed 4 days ago

A UAF (Use After Free) vulnerability was discovered in the renderer implementation of the Ethereum wallet. This vulnerability allowed an attacker to trigger a crash in the renderer process and potentially execute arbitrary code. This summary was automatically generated.

7

CSRF to XSS in /htdocs/modules/system/admin.php

By **d3addog** to **ImpressCMS** | ● Resolved | Medium | disclosed about 1 day ago

The "admin.php" file in the "system" module of ImpressCMS version 1.4.2 was vulnerable to a Cross-Site Scripting (XSS) attack. This vulnerability allowed an attacker to execute malicious scripts in the context of an authorized user by exploiting a lack of input sanitization. The vulnerability was triggered by sending a crafted request to the application, which could be done through a Cross-Site Request Forgery (CSRF) attack. This summary was automatically generated.

30

XSS from Mastodon embeds

By **lotsofloops** to **IRCCloud** | ● Resolved | High | disclosed 7 days ago

An XSS vulnerability was discovered in the IRCCloud web client that allowed an attacker to execute arbitrary JavaScript in the context of the web client. This was possible due to the default embedding of Mastodon toots, which could be manipulated to include a malicious `javascript:` URL. By tricking a user into viewing the embedded content, an attacker could obtain the user's session token and potentially compromise their account. This summary was automatically generated.

55

Draft report exposure via slack alerting system for programs

By **imranhudaa** to **HackerOne** | ● Resolved | Medium | **$2,500.00** | disclosed 10 days ago

181

AWS keys and user cookie leakage via uninitialized memory leak in outdated librsvg version in Basecamp

By **neex** to **Basecamp** | ● Resolved | High | **$8,868.00** | disclosed 25 days ago

Sensitive data, including AWS keys and user cookies, could be leaked due to an uninitialized memory leak in an outdated version of librsvg used by Basecamp. This vulnerability allowed an attacker to upload a specially crafted SVG image as an avatar, triggering the memory leak. By extracting fragments of memory from the image conversion process, the attacker could access sensitive information from the Basecamp servers. The vulnerability has been mitigated by updating librsvg and implementing isolation measures for image preview generation. This summary was automatically generated.

6

Exposing Django Debug Panel and Sensitive Infrastructure Information at https://dev.fxprivaterelay.nonprod.cloudops.mozgcp.net

By **aliend89** to **Mozilla Core Services** | ● Resolved | Low | disclosed 3 days ago

The Django Debug Panel was exposed in a development environment, allowing sensitive infrastructure information to be accessed. This included details about the locations of databases, user information, and internal IP addresses. The exposure of this information posed significant security risks and potential vulnerabilities. This summary was automatically generated.

16

RCE and DoS in Cosmovisor

By **strikeout** to **Cosmos** | ● Resolved | Medium | **$1,250.00** | disclosed 6 days ago

4

Admin.MyTVA.com Customer lookup and internal notes bypass

By **itssixtynein** to **Tennessee Valley Authority** | ● Resolved | Medium | disclosed 3 days ago

The admin.mytva.com site had a vulnerability that allowed an attacker to bypass the login and access admin-only endpoints. This could lead to unauthorized access to customer information and the ability to add internal notes. This summary was automatically generated.

3

Subdomain takeover on one of the subdomain under mozaws.net

By **holybugx** to **Mozilla Core Services** | ● Resolved | Medium | disclosed 3 days ago

6

Stored XSS at nordvpn.com

By **tvmbug** to **Nord Security** | ● Resolved | Medium | disclosed 4 days ago

18

No Rate Limit in Login Page

By **mr_sparrow** to **On** | ● Resolved | Low | disclosed 7 days ago

The login page of the website did not have a rate limit implemented, allowing an attacker to perform brute force attacks by trying multiple login attempts without being restricted. This summary was automatically generated.

9

CVE-2023-38546: cookie injection with none file

By **w0x42** to **curl** | ● Resolved | Low | disclosed 5 days ago

3

xss reflected - pqm.tva.com

By **tvmbug** to **Tennessee Valley Authority** | ● Resolved | Medium | disclosed 3 days ago

An XSS vulnerability was discovered on pqm.tva.com. This vulnerability allowed an attacker to inject malicious code into the website, potentially leading to various attacks such as stealing user information or redirecting users to malicious websites. This summary was automatically generated.

9

Stored XSS in plan name field (Acronis Cyber Protect)

By **und3sc0n0c1d0** to **Acronis** | ● Resolved | Medium | **$500.00** | disclosed 7 days ago

A stored XSS vulnerability was identified in the plan name field of Acronis Cyber Protect. This vulnerability allowed an attacker to execute arbitrary JavaScript code in the context of the affected user, potentially leading to unauthorized access or phishing attacks. This summary was automatically generated.

9

Limited path traversal in Node.js SDK leads to PII disclosure

By **zerodivisi0n** to **Stripe** | ● Resolved | Medium | **$1,000.00** | disclosed 6 days ago

A limited path traversal vulnerability in the Node.js SDK allowed an attacker to retrieve personally identifiable information (PII) of users. By using . and .. as identifiers in API methods, the attacker could call parent API methods and access sensitive data such as email addresses, names, and addresses. This summary was automatically generated.

61

LinkedIn users primary email + full name visibilty

By **headhunter** to **LinkedIn** | ● Resolved | High | disclosed 20 days ago

206

IDOR - Delete all Licenses and certifications from users account using CreateOrUpdateHackerCertification GraphQL query

By **callmed0_4** to **HackerOne** | ● Resolved | High | bounty awarded about 1 month ago

All licenses and certifications in HackerOne could be deleted by changing the ID number in the CreateOrUpdateHackerCertification GraphQL query. This summary was automatically generated.

2

Path traversal through path stored in Uint8Array

By **tniessen** to **Node.js** | ● Resolved | High | disclosed 2 days ago

A vulnerability was discovered in Node.js that allowed path traversal through Uint8Array objects. This vulnerability affected users using the experimental permission model in Node.js 20. This summary was automatically generated.

29

[mysupport.informatica.com] - reflected XSS

By **mtk0308** to **Informatica** | ● Resolved | High | disclosed 11 days ago

12

Context isolation bypass via nested unserializable return value

By **marshallofsound** to **Internet Bug Bounty** | ● Resolved | Medium | **$2,550.00** | disclosed 8 days ago

A vulnerability was discovered in Electron that allowed for a bypass of context isolation. This meant that code running in the main world context in the renderer could access the isolated Electron context and perform privileged actions. The vulnerability was fixed in versions 25.0.0-alpha.2, 24.0.1, 23.2.3, and 22.3.6. This summary was automatically generated.

60

Access to resumes applied through LinkedIn Jobs

By **headhunter** to **LinkedIn** | ● Resolved | Critical | disclosed 23 days ago

27

Subdomain takeover on one of the subdomain under mozilla.org

By **d0xing** to **Mozilla Core Services** | ● Resolved | Medium | disclosed 11 days ago

4

Test 4 [redacted]

By **ideborah** to **Mars** | ● Resolved | Medium | disclosed 4 days ago

23

LY

Reflected XSS in OAUTH2 login flow (https://access.line.me)

By **tosun** to **LY Corporation** | ● Resolved | Medium | disclosed 12 days ago

36

HTTP Request Smuggling (CL.0) leads to mass redirect users to attacker server without user interaction

By **vampirex** to **LinkedIn** | ● Resolved | High | disclosed 20 days ago

21

Bypassing Garbage Collection with Uppercase Endpoint

By **h1xploit** to **inDrive** ● Resolved disclosed 12 days ago

A vulnerability was discovered in the garbage collection process, allowing the bypass of the "/metrics" endpoint by using uppercase letters. This could potentially lead to unauthorized access to sensitive information or resources and possible data manipulation. Other endpoints with similar patterns may also be vulnerable to this bypass method. This summary was automatically generated.

1

Integrity checks according to policies can be circumvented

By **tniessen** to **Node.js** ● Resolved Medium disclosed 2 days ago

The Node.js policy feature, which checks the integrity of a resource against a trusted manifest, could be circumvented by intercepting the operation and returning a forged checksum, effectively disabling the integrity check. This vulnerability affected all users using the experimental policy mechanism in all active release lines: 18.x and 20.x. This summary was automatically generated.

1

Permission model improperly protects against path traversal

By **tniessen** to **Node.js** | ● Resolved | High | disclosed 2 days ago

268

yelp.com XSS ATO (via login keylogger, link Google account)

By **lil_endian** to **Yelp** | ● Resolved | High | **$6,000.00** | disclosed 2 months ago

6

IBB

(CVE-2023-32006) Permissions policies can impersonate other modules in using module.constructor.createRequire()

By **haxatron1** to **Internet Bug Bounty** | ● Resolved | Medium | disclosed 7 days ago

A vulnerability was discovered in Node.js that allowed permissions policies to impersonate other modules using the module.constructor.createRequire() function. This could bypass the policy mechanism and enable the loading of modules outside of the defined policy. The vulnerability affected all users using the experimental policy mechanism in Node.js versions 16.x, 18.x, and 20.x. The issue has been fixed in the latest security releases. This summary was automatically generated.

89

Able to see Bonus amount given to a report even if the bounty and Bonus is not visible to public or mentioned in {Report-Id}.json

By **callmed0_4** to **HackerOne** | ● Resolved | Medium | disclosed about 1 month ago

A vulnerability allowed users to see the bonus amount given to a report, even if the bounty and bonus were not visible to the public or mentioned in the report's JSON file. This resulted in the exposure of confidential information. This summary was automatically generated.

21

CVE-2023-30587 Process-based permissions can be bypassed with the "inspector" module.

By **mattaustin** to **Internet Bug Bounty** | ● Resolved | High | **$3,495.00** | disclosed 15 days ago

A vulnerability in Node.js version 20 allowed for the bypassing of restrictions set by the --experimental-permission flag using the built-in inspector module. This vulnerability affected Node.js users who were using the permission model mechanism in Node.js 20. This summary was automatically generated.

67

2FA BYPASS

By **imtheking** to **Cloudflare Public Bug Bounty** | ● Resolved | High | disclosed 28 days ago

A vulnerability in Cloudflare's Dashboard allowed for the retrieval of recovery codes without completing the authentication process. The issue was resolved by disallowing requests to the vulnerable API endpoint until users were fully authenticated. This summary was automatically generated.

39

Hashed data exposure via WebSockets to Workspace Members

By **d3f4u17** to **Slack** | ● Resolved | Critical | disclosed 24 days ago

A vulnerability in Slack's system allowed for the exposure of members' email addresses and sensitive data through WebSockets. This occurred when users created or revoked a Shared Invite Link for their workspace, resulting in the transmission of hashed passwords to other workspace members. The issue was promptly addressed, with affected users' passwords reset and notifications sent to customers. This summary was automatically generated.

85

IDOR: Authorization Bypass in LockReport Mutation for public reports

By **0verw4tch** to **HackerOne** | ● Resolved | Medium | disclosed about 1 month ago

An authorization bypass vulnerability allowed an attacker to lock any public report, potentially disrupting the reporting process. This summary was automatically generated.

86

yelp.com and biz.yelp.com ATO via XSS + Cookie Bridge

By **lil_endian** to **Yelp** | ● Resolved | Medium | **$3,000.00** | disclosed about 1 month ago

An XSS vulnerability was discovered on Yelp.com and biz.yelp.com, allowing an attacker to execute arbitrary JavaScript code. This vulnerability could be combined with the cookie bridge functionality to target other users and potentially perform account takeovers. This summary was automatically generated.

38

Reflected XSS in OAuth complete endpoints

By **zerodivisi0n** to **Mattermost** | ● Resolved | Low | **$150.00** | disclosed 18 days ago

Reflected XSS vulnerabilities were discovered in several OAuth complete endpoints in Mattermost. These endpoints failed to sanitize the "redirect_to" field in the "state" query parameter, allowing an attacker to execute malicious JavaScript code in the context of the user's browser. This could lead to unauthorized actions being performed on behalf of the user. This summary was automatically generated.

13

Linked in

[ADMIN FEATURE ACCESS] Knowing The Competitors analytics of any company

By **mainteemoforfun** to **LinkedIn** | ● Resolved | Medium | disclosed 10 days ago

Subdomain takeover on one of the subdomain under mozaws.net

By **d0xing** to **Mozilla Core Services** | ● Resolved | Medium | disclosed 11 days ago

173

Cache Poisoning allows redirection on JS files

By **youstin** to **Glassdoor** | ● Resolved | High | **$1,000.00** | disclosed 2 months ago

A cache poisoning vulnerability was discovered in Glassdoor's design website. By sending a specific request, an attacker could redirect the /test.js file to a malicious website. This could potentially lead to a stored cross-site scripting (XSS) attack if other Glassdoor websites import javascript files from the affected domain. This summary was automatically generated.

58

Admin account/panel takeOver and Doing actions in admin panel via DOM-based XSS

By **mouhannadlrx** to **Radancy** | ● Resolved | Medium | **$160.00** | disclosed about 1 month ago

A DOM-based XSS vulnerability was discovered in the webmail admin panel. This vulnerability allowed an attacker to execute malicious code in the admin panel, potentially leading to the theft of sensitive information and unauthorized actions within the panel. The vulnerability was caused by a lack of sanitization and validation of user-controlled data, which was then used in a document.write function without proper filtration. This summary was automatically generated.

18

[curl] CVE-2023-38039: HTTP header allocation DOS

By **selmelc** to **Internet Bug Bounty** | ● Resolved | Medium | **$2,540.00** | disclosed 18 days ago

CVE-2023-38039 is a security vulnerability in the curl library that allowed a malicious server to send an unlimited number of headers in an HTTP response, causing curl to exhaust heap memory and potentially leading to a denial-of-service condition. This summary was automatically generated.

6

IBB

OpenSSL engines can be used to bypass and/or disable the Node.js permission model

By **tniessen** to **Internet Bug Bounty** | ● Resolved | Medium | **$2,540.00** | disclosed 8 days ago

Arbitrary OpenSSL engines could be loaded in Node.js 20, bypassing and disabling the permission model. This allowed for the execution of arbitrary code, unaffected by the permission model. This summary was automatically generated.

47

IDOR - send a message on behalf of other user

By **lamscun** to **Mozilla Core Services** | ● Resolved | Medium | disclosed 26 days ago

An insecure direct object reference (IDOR) vulnerability was discovered in the messaging feature of the website. This vulnerability allowed an attacker to send messages on behalf of other users by manipulating the session ID parameter in the request. This summary was automatically generated.

337

An attacker can can view any hacker email via /SaveCollaboratorsMutation operation name

By **0xrayan1996** to **HackerOne** | ● Resolved | High | **$7,500.00** | disclosed 3 months ago

An attacker could view any hacker or normal user's email on HackerOne by sending an invitation via a dummy report, thereby disclosing their private email. This summary was automatically generated.