Proto Stream

The Prototyping and Entrepreneurship Platform

Mockup Design

User Dasboard/Profile
Projects
Project Overview/Summary
Activity Timeline
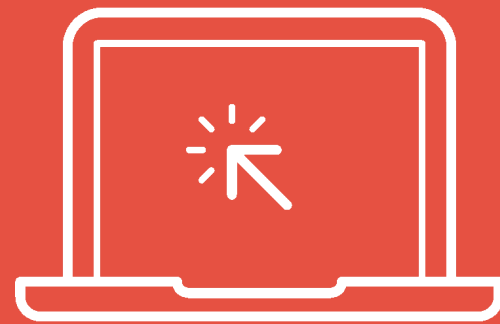Competitions
Internships/Jobs

What?

An E-Portal with CRUD features and Timeline Maintance feature and Prototype Stage and State Monitoring

Hacktivity   Competitions   Inbox   Learner's Dashboard   Job Board   Leaderboards

Profile   Badges

Edit Profile

Steve Wozniak (lucifer_190)

Joined August 2018

Stats   90 Days

–   –
Signal   Percentile

–   –
Impact   Percentile

–   –
Reputation   Rank

Credits

0
Vulnerabilities found

0
Thanks received

Hacktivity ⑦   All ⌄

🐛

No matches found.

Nothing to show yet.

Thanks ⑦
0 thanks received   Reputation   Rank

🐛

No thanks found.

lucifer_190 hasn't received any thanks yet.

Testimonials

No testimonials found.

lucifer_190 hasn't received any testimonials yet.

Hacktivity · Directory · Inbox · Hacker Dashboard · Job Board · Leaderboards

Hacktivity
See the latest Project activities on ProtoStream

Search Hacktivity

Sort
Popular ↓

Type
- ○ All
- ○ Published
- ● Disclosed

Filter
- ☐ Creators I am following

▲ 184 — **New Idea to Purify Sea Water**
By parsiya to | ● Resolved | ▬ Critical | $15,000.00
disclosed 2 days ago

▲ 31 — **A Game Engine**
By tw4v3sx to | ● Resolved | ▬ High | $1,000.00
bounty awarded 10 hrs ago

▲ 13 — **Android App**
By fuomag9 to OPPO | ● Resolved | ▬ High | $600.00
disclosed 8 hrs ago

▲ 17 — **New Cement Mixture that focuses on use of limestone**
By snsn to curl | ● Resolved | ▬ Medium | $700.00
disclosed about 1 day ago

▲ 163 — **Rain Water Harvesting**
By nahamsec to Snapchat | ● Resolved
disclosed 6 days ago

▲ 12 — **Research Paper on Human-AI Singularity**
By ajay_saycure to Automattic | ● Resolved | ▬ High | $200.00
disclosed about 1 day ago

▲ 59 — **Email Verification bypass on signup**
By haqsek2 to Automattic | ● Resolved | ▬ High | $300.00
disclosed 3 days ago

▲ 85 — **Absence of Token expiry leads to Unauthorized login Access**
By yogesh_ojha to Affirm | ● Resolved | ▬ Critical
disclosed 6 days ago

▲ 12 — **An integer overflow found in /lib/urlapi.c**
By 1wc to curl | ● Resolved | ▬ Low | $150.00
disclosed about 1 day ago

▲ 207 — **Remote code execution on Basecamp.com**
By gammarex to Basecamp | ● Resolved | ▬ Critical | $5,000.00
disclosed 10 days ago

▲ 30 — **Bypass of image rewriting / tracking blocker via srcset**
By foobar7 to Basecamp | ● Resolved | ▬ Medium | $1,000.00
disclosed 3 days ago

▲ 7 — **Partial password leak over DNS on HTTP redirect**
By mszpl to curl | ● Resolved | ▬ Medium | $400.00
disclosed about 1 day ago

Parsia (parsiya)

232	-	6.00	91st	30.00	98th
Reputation	Rank	Signal	Percentile	Impact	Percentile

▲
184   #873614   **New Idea to Purify Sea Water**

Share:

State	● Resolved (Closed)		▦ Critical (9.6)
Disclosed	December 4, 2020 11:34pm +0530	Participants	
Project Name	**Poseidon**	Visibility	Disclosed (Limited)
Started On	May 14, 2020 12:14am +0530		
Weakness	Code Injection		
Bounty	$15,000		

Collapse

SUMMARY BY PARSIYA

Summary

The PlayStation Now application version `11.0.2` is vulnerable to remote code execution (RCE). Any website loaded in any browser on the same machine can run arbitrary code on the machine through a vulnerable websocket connection.

1. The local websocket server at `localhost:1235` does not check the origin of incoming requests.
    1. This allows websites loaded in browsers on the same machine to send requests to the websocket server.
    2. Websockets are not bound by the Same-Origin Policy so the websocket server has to do this manually.

2. psnow launches an Electron application named `AGL`.
    1. It's possible to tell AGL to load a specific website with a command sent to the websocket server.
    2. As a result, the websites above can tell AGL to load any remote URL.
    3. It's also possible to tell `AGL` to run any local application via the `setUrlDefaultBrowser` command.

3. The AGL Electron application has `nodeIntegration: true` so JavaScript running in any loaded URL can spawn new processes.
    1. So any URL loaded in the AGL application can run code on the target machine.

Chaining these three issues gives us RCE.

Description

The PlayStation Now application (`psnow` moving forward) is an online streaming application for playing PlayStation games. Version `11.0.2` is the current version at the time of writing. The latest version can be downloaded from https://download-psnow.playstation.com/downloads/psnow/pc/latest ↗.

It has two major components: `QAS` and `AGL`.

QAS

Hacktivity   Directory   Inbox   Hacker Dashboard   Job Board   Leaderboards

Attackers can run code on users' machines. They can get to the other side of the airtight hatchway.

TIMELINE · EXPORT

parsiya submitted a report to **PlayStation**.   May 14th (7 months ago)

parsiya updated the severity to Critical (9.6).   May 14th (7 months ago)

parsiya closed the report and changed the status to ● **Not Applicable**.   May 14th (7 months ago)

hacker-01 PlayStation staff **reopened** this report.   May 14th (7 months ago)

hacker-01 PlayStation staff changed the status to ● **Triaged**.   May 14th (7 months ago)

hacker-01 PlayStation staff posted a comment.   May 19th (7 months ago)

parsiya posted a comment.   May 19th (7 months ago)

parsiya posted a comment.   May 20th (7 months ago)

PlayStation rewarded **parsiya** with a **$15,000** bounty.   May 22nd (7 months ago)

parsiya posted a comment.   May 22nd (7 months ago)

parsiya posted a comment.   Jun 8th (6 months ago)

serv HackerOne staff closed the report and changed the status to ● **Resolved**. Jun 25th (5 months ago)

parsiya posted a comment.   Jun 28th (5 months ago)

parsiya requested to disclose this report.   Jun 28th (5 months ago)

serv HackerOne staff posted a comment.   Aug 19th (4 months ago)

parsiya posted a comment.   Aug 20th (4 months ago)

parsiya posted a comment.   Aug 20th (4 months ago)

hacker-01 PlayStation staff posted a comment.   Sep 9th (3 months ago)

Hacktivity Projects Inbox Hacker Dashboard Job Board Leaderboards

Programs

Directory
List of Currently Active and Upcoming Competitions to Participate into

Search Projects

Program features

- ☐ IBB ⍰
- ☐ Offers bounties ⍰
- ☐ High response efficiency ⍰
- ☐ Managed by HackerOne ⍰
- ☐ Offers retesting ⍰
- ☑ Active program ⍰

Asset type
- ⦿ Any
- ○ CIDR
- ○ Domain
- ○ iOS: App Store
- ○ iOS: Testflight
- ○ iOS: .ipa
- ○ Android: Play Store
- ○ Android: .apk
- ○ Windows: Microsoft Store
- ○ Source code
- ○ Executable
- ○ Hardware/IoT
- ○ Other

Program	Launch date ↓	Participations resolved ↓	Prize minimum ↓	Prize average ↓	
Sixt GmbH & Co. Autovermietung KG BBP `Managed`	12 / 2020	14	$50	$50-$100	☆
Lark Technologies `Managed`	12 / 2020	191	$100	$500	☆
Xilinx BBP `Managed`	11 / 2020	2	$50	$2k	☆
RMS `Managed`	11 / 2020	13	-	-	☆
Jimdo GmbH `Managed`	11 / 2020	4	-	-	☆
ImpressCMS	11 / 2020	4	-	-	☆
Navient Solutions LLC `Managed`	11 / 2020	4	-	-	☆
Mendix `Managed`	11 / 2020	28	-	-	☆
Exodus `Managed`	11 / 2020	22	$100	$500	☆
Yoti	11 / 2020	44	$100	$350-$500	☆

Add this program to your bookmarks

Job Board

Find Internships and Jobs or Roles in your favourite Startups and Companies based on your skills

Search jobs

Location

Enter location

☐ Full-time

☐ Contract

☐ Remote-friendly

Android Developer

Poseidon /

HackerOne is looking for security-minded, customer-service oriented individuals to join the team responsible for HackerOne's Fully Managed service offering. You will be responsible for vetting security vulnerability reports from some of the world's best hackers being submitted to Fortune 500 and other companies as part of their bug bounty programs. You will have the opportunity to work with some of the best hackers in the world and the security teams behind some of the most competitive...

View more & apply

Full-time   Remote   2 months ago

Software Engineer - Full Stack

HackTheBox /

Are you convinced that data is only as useful as the product built to access and interpret it? Are you inspired by user feedback to constantly elevate not just the product experience but also the engineering experience? Are you energized by innovating new products, finding ones that stick in the market and ones that don't? Most importantly, do you just want to get stuff done?

At HackerOne, we're on a mission to empower the world to build a safer internet. We're a strong engineering...

View more & apply

Full-time   Remote   2 months ago

Graphic Designer

Drat /

Are you convinced that data is only as useful as the product built to access and interpret it? Are you inspired by user feedback to constantly elevate not just the product experience but also the engineering experience? Are you energized by innovating new products, finding ones that stick in the market and ones that don't? Most importantly, do you just want to get stuff done?

At HackerOne, we're on a mission to empower the world to build a safer internet. We're a strong engineering...

View more & apply

Full-time   Remote   2 months ago

h1 | Hacktivity | Directory | Inbox | Hacker Dashboard | Job Board | Leaderboards

♛ ProtoStream Leaderboards

Jan-Mar 2020 | Apr-Jun 2020 | Jul-Sep 2020 | **Oct-Dec 2020** | 2020

All leaderboards are based on the selected time period.

Highest Reputation
Ranking is calculated based on reputation earned.

		Reputation	Signal	Impact
— 1.	todayisnew	9764	6.35	21.42
▲ 2.	jayesh25	3435	6.92	18.09
▲ 3.	emperor	3261	6.97	20.24
▲ 4.	d0xing	3224	7.00	24.30
▲ 5.	ahmd_halabi	2844	6.85	15.63
-	lucifer_190	-	-	-

View all rankings →

Highest Critical Reputation
Based on reputation gain for high and critical submissions that are triaged or resolved.

		Reputation	Signal	Impact
— 1.	todayisnew	877	6.14	24.25
▲ 2.	d0xing	629	7.00	29.80
▲ 3.	m0chan	557	6.85	26.50

Up and Comers
Based on reputation gain from hackers that submitted their first valid report within the last 90 days.

		Reputation
▲ 1.	kirkx	860
▲ 2.	i_hack_every one	443
▲ 3.	namle	321
▲ 4.	ltidi	310
▲ 5.	twelvesix	255
-	lucifer_190	-

View all rankings →

Most Upvoted
Hackers with the highest number of report upvotes on Hacktivity.

		Votes
▲ 1.	mygf	785
▲ 2.	bugra	513

11

Hacktivity Directory Inbox Learner's Dashboard Job Board Leaderboards

Overview My Programs Followed Creators Pending Invitations

Steve Wozniak (lucifer_190)

Resolved reports **0%** ⊙

Low	Medium	High	Critical
0	0	0	0

My stats 90 Days ⌄

- -
Signal Percentile

- -
Impact Percentile

- -
Reputation Rank

Getting started
Complete these items to get started on ProtoStream

☑ Bookmark 5 programs on the Directory.

Overview

About ProtoStream
Learn about how ProtoStream works.

Learn About Entrepreneurship
Learn more about Products and Business

Explore programs
Find programs you're interested to participate in.

Resources
Get and Learn yourself from this list of Resources

Experience by vulnerability type 153 vulnerability types	Submissions Count	Bounties Total	Criticals Submitted	Reputation Change
HTTP Response Splitting CWE-113	0	-	0	-
Memory Corruption - Generic CWE-119	0	-	0	-
Classic Buffer Overflow CWE-120	0	-	0	-
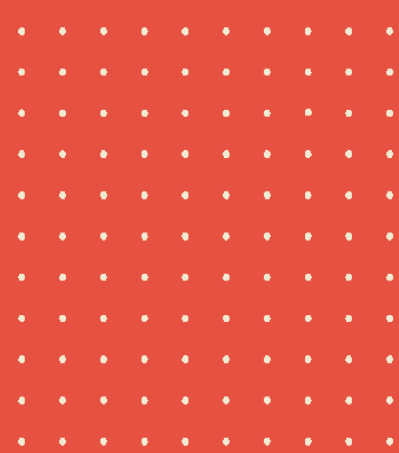
Thankyou

But Here's a Demand

13

Contact

Meerut

www.tomriddle.in

siddhant.1721cs1132@kiet.edu