



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL

July 7, 2021

TLP:WHITE



AUTO-ISAC ANTITRUST STATEMENT

As Members of the Auto-ISAC, we strictly comply with EU and US antitrust laws. Please do not discuss anything that your company considers commercially sensitive and/or confidential such as pricing or future product plans. A violation of any of the above-mentioned issues will result in us having to quickly terminate the meeting.





Finally, please remember to keep these deliberations confidential. Please do not discuss the substance of these meetings outside of this group.

This meeting is being held at

TLP:WHITE

Disclosure is not limited.

DHS TRAFFIC LIGHT PROTOCOL (TLP) CHART

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

From: <https://www.us-cert.gov/tlp>

AGENDA

Time (ET)	Topic
11:00	Welcome <ul style="list-style-type: none">➤ Why We're Here➤ Expectations for This Community
11:05	Auto-ISAC Update <ul style="list-style-type: none">➤ Auto-ISAC Activities➤ Heard Around the Community➤ What's Trending
11:15	<i>DHS CISA Community Update</i>
11:20	Featured Speaker: <ul style="list-style-type: none">▪ Ben Willis, <i>Principal Security Engineer, HackerOne</i>
11:45	Around the Room <ul style="list-style-type: none">➤ Sharing Around the Virtual Room
11:55	Closing Remarks

WELCOME - AUTO-ISAC COMMUNITY CALL!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

Classification Level: **TLP:GREEN** - May be shared within the Auto-ISAC Community and “off the record”

How to Connect: For further info, questions or to add other POCs to the invite, please contact us!
(sharmilakhadka@automotiveisac.com)



ENGAGING IN THE AUTO-ISAC COMMUNITY

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC membership
- ❖ If you aren't eligible for membership, connect with us as a Partner
- ❖ Get engaged – *“Cybersecurity is everyone's responsibility!”*



❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

22
OEM Members

21
Navigator Partners

❖ Share – *“If you see something, say something!”*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

41 *Supplier & Commercial Vehicle Members*

15
Innovator Partners

*Membership represents **99%** of cars and trucks on the road in North America*

*Coordination with **26** critical infrastructure ISACs through the National Council of ISACs (NCI)*



2021 BOARD OF DIRECTORS

EXECUTIVE COMMITTEE (EXCOM)



Kevin Tierney
*Chair of the
Board of the Directors*
GM



Josh Davis
*Vice Chair of the
Board of the Directors*
Toyota



Jenny Gilger
*Secretary of the
Board of the Directors*
Honda



Tim Geiger
*Treasurer of the
Board of the Directors*
Ford



Todd Lawless
*Chair of the
Advisory Board*
Continental



Todd Lawless
*Chair of the
Advisory Board*
Continental



Michael Feiri
*Vice Chair of the
Advisory Board*
ZF



Chris Lupini
Chair of the SAG
Aptiv



Larry Hilkene
Chair of the CAG
Cummins

2021 ADVISORY BOARD (AB) LEADERSHIP

MEMBER ROSTER

AS OF JULY 1, 2021

62 Members

Aisin	Infineon	Oshkosh Corp
Allison Transmission	Intel	PACCAR
Aptiv	John Deere Electronic	Panasonic
Argo AI, LLC	Kia	Polaris
AT&T	Knorr Bremse	Qualcomm
Blackberry Limited	Lear	Renesas Electronics
BMW Group	LGE	Stellantis
BorgWarner	Luminar	Subaru
Bosch (Escrypt-Affiliate)	Magna	Sumitomo Electric
Continental (Argus-Affiliate)	MARELLI	Tokai Rika
Cummins	Mazda	Toyota
Denso	Mercedes-Benz	TuSimple
Ford	Meritor	Valeo
Garrett	Mitsubishi Motors	Veoneer
General Motors (Cruise-Affiliate)	Mitsubishi Electric	Volkswagen
Geotab	Mobis	Volvo Cars
Google	Motional	Volvo Group
Harman	Navistar	Waymo
Hitachi	Nexteer Automotive Corp	Yamaha Motors
Honda	Nissan	ZF
Hyundai	NXP	

BUSINESS ADMINISTRATION

➤ Members ONLY Activities: TLP:AMBER

➤ **Auto-ISAC Members Teaching Members:** Wednesday, July 21, 2020, 10-11:30 am ET

- Guy Harpak, Head of Product Security, Mercedes-Benz R&D
- **Presentation Topic:** “OEM Perspective on Ongoing Defense for the Fleet: Goals, Motivation, Challenges and Methods for Setting up Fleet Security Operations.”

➤ Community Activities:TLP:WHITE

➤ **Community Call Speaker:** Wednesday, August 4th, 2021, 11-12 pm ET:

- Suzanne Lightman, Sr. Advisor, Information Security, NIST
- Presentation Title: TBA

➤ **Auto-ISAC Mid-year Community Call Survey:** COMPLETE

➤ **Auto-ISAC Annual Cybersecurity Summit:** TLP:WHITE

- Hybrid, October 13-14, 2021, 8:00 am – 5:00 pm
- GM Titanium Sponsor at RenCen, Detroit, MI
- **REGISTER!!! Early Bird Special Ends July 31st !**



AUTO-ISAC INTELLIGENCE

- Know what we track daily by subscribing to the DRIVEN
 - Send feedback, contributions or questions to analyst@automotiveisac.com
- Know our strategic perception of and outlook for the cyber threat environment by reading the 2020 Threat Assessment in the Auto-ISAC 2020 Annual Report. The 2021 Annual Report and Threat Assessment are in production
 - Email us to request the report, provide feedback, or ask questions
- Intelligence Notes
 - Near the start of the US Independence Day holiday weekend, Kaseya urged its customers to immediately shut down on-premises servers running its VSA endpoint management and network monitoring tool due to an active cyberattack reportedly perpetrated by REvil ransomware operators. The ransomware group requested \$50 million for a universal decryptor.

AUTO-ISAC INTELLIGENCE

➤ Intelligence Notes Continued...

- Kaseya reported fewer than 60 of its 36,000 customers were impacted by the ransomware.
- Kaseya estimated fewer than 1,500 businesses downstream from its Managed Service Provider (MSP) customers were impacted by the ransomware.
- The threat actors appear to have leveraged an authentication bypass flaw affecting the VSA web interface to upload a malicious payload and execute arbitrary code on compromised systems.
- Security expert Kevin Beaumont stated the ransomware was pushed via an automated, fake, and malicious software update using Kaseya VSA, also called Kaseya VSA Agent Hot-fix.

Sources: [Securityweek](#), [ZDNet](#)

AUTO-ISAC INTELLIGENCE

➤ Intelligence Notes Continued...

- Automotive companies should seek to maintain visibility of the cybersecurity posture of their suppliers, share information downstream, and assist them with implementing best practices and/or executing incident response, when able
- Kaseya was working on patching vulnerabilities related to the attack after being notified by researchers, but the **threat actors located and exploited the vulnerabilities before it could implement the fixes**
- Automotive companies' cybersecurity teams are aware software often contains unknown vulnerabilities. They should consider what steps they are taking to locate and eliminate significant vulnerabilities before threat actors exploit them to conduct attacks

CISA RESOURCE HIGHLIGHTS



TLP: WHITE – CISA Current Activity (CA) – CISA Begins Cataloging Bad Practices that Increase Cyber Risk

- **Announced by CISA Executive Assistance Director (EAD) Goldstein in his blogpost**
- **Focuses on the importance of organizations to stop bad practices**
- **Will be updated over time based on feedback from risk managers and cybersecurity professionals**
- **See:**
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/06/29/cisa-begins-cataloging-bad-practices-increase-cyber-risk](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/06/29/cisa-begins-cataloging-bad-practices-increase-cyber-risk)
 - [https://www\[.\]cisa\[.\]gov/blog/2021/06/24/bad-practices](https://www[.]cisa[.]gov/blog/2021/06/24/bad-practices)



TLP: WHITE – CISA CA - CISA's Cybersecurity Evaluation Tool (CSET) Tool Sets Sights on Ransomware Threat

- **New CSET Module – Ransomware Readiness Assessment (RRA)**
- **RRA is a self-assessment based on a tiered set of practices to allow organizations to determine how well they are to defend and recover from a ransomware attack**
- **RRA tailored to varying levels of ransomware threat readiness**
- **See:**
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat)
 - [https://github\[.\]com/cisagov/cset/releases/tag/v10.3.0.0](https://github[.]com/cisagov/cset/releases/tag/v10.3.0.0)



TLP: WHITE – CISA CA – PrintNightmare, Critical Windows Print Spooler Vulnerability

- Released on June 30 based on CERT/CC VulNote for a critical remote code execution in the Windows Print Spooler Service; updated on July 1 and July 2 to highlight Microsoft guidance for workarounds and mitigation. Security updates released by Microsoft on July 6.
- CISA encourages administrators to disable the Windows Print spooler service in Domain Controllers and systems that do not print
- Resources:
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability)
 - [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/07/06/microsoft-releases-out-band-security-updates-printnightmare](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/07/06/microsoft-releases-out-band-security-updates-printnightmare)



TLP:WHITE – CISA CA – Kaseya VSA Supply-Chain Ransomware Attack

- **CISA-FBI coordinating efforts to provide guidance for MSPs and their customers affected by the Kaseya VSA supply-chain ransomware attack**
- **Guidance to affected entities includes the download and use of the Kaseya VSA Detection Tool**
- **[https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msp-and-their-customers-affected-kaseya-vsa](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msp-and-their-customers-affected-kaseya-vsa)**
- **[https://Kaseya\[.\]app\[.\]box.com/s/0ysvgss7w48nxh8k1xt7fqhbcjxhas40](https://Kaseya[.]app[.]box.com/s/0ysvgss7w48nxh8k1xt7fqhbcjxhas40)**
- **[https://helpdesk\[.\]Kaseya\[.\]com/hc/en-gb/articles/4403440684689](https://helpdesk[.]Kaseya[.]com/hc/en-gb/articles/4403440684689)**



TLP: WHITE – Additional Resources From CISA

- CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- CISA News Room - [https://www\[.\]cisa\[.\]gov/cisa/newsroom](https://www[.]cisa[.]gov/cisa/newsroom)
- CISA Blog - [https://www\[.\]cisa.gov/blog-list](https://www[.]cisa.gov/blog-list)
- CISA Publications Library - [https://www\[.\]cisa\[.\]gov/publications-library](https://www[.]cisa[.]gov/publications-library)
- CISA Cyber Resource Hub - [https://www\[.\]cisa\[.\]gov/cyber-resource-hub](https://www[.]cisa[.]gov/cyber-resource-hub)
- CISA Vulnerability Management (formerly known as the National Cyber Assessment and Technical Services (NCATS) program) - [https://www\[.\]us-cert\[.\]gov/resources/ncats/](https://www[.]us-cert[.]gov/resources/ncats/)
- CISA Cybersecurity Directives - [https://cyber\[.\]dhs\[.\]gov/directives/](https://cyber[.]dhs[.]gov/directives/)
- CISA COVID-19 Response – [https://www\[.\]cisa\[.\]gov/coronavirus](https://www[.]cisa[.]gov/coronavirus)





For more information:
[cisa.gov](https://www.cisa.gov)

Questions?
CISAServiceDesk@cisa.dhs.gov
1-888-282-0870



AUTO-ISAC COMMUNITY MEETING

Why Do We Feature Speakers?

- ❖ These calls are an opportunity for information exchange & learning
- ❖ Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- ❖ Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- ❖ Goal is to showcase a rich & balanced variety of topics and viewpoints
- ❖ *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

30+
*Featured
Speakers to
date*

How Can I Be Featured?

- ❖ If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

7 *Best
Practice
Guides
available on
website*

2000+
*Community
Participants*





FEATURED SPEAKER

TLP:WHITE



MEET THE SPEAKER- **BEN WILLIS**

PRINCIPAL SECURITY ENGINEER, HACKERONE



Ben Willis is a Principal Software Engineer at HackerOne, the most trusted hacker-powered security platform. He takes leadership positions across engineering in Product, Data, and Security teams to scale processes, execution, and direction.

Prior to HackerOne, he founded three companies and led product and engineering within the e-commerce, telecommunications, and hospitality industries. He studied Computer Engineering Technology and AI with a focus on Computer Vision at Rochester Institute of Technology (RIT).

hackerone

Hacker-Powered Data: The Most Common Security Weaknesses and How to Avoid Them

Ben Willis
Principal Security Engineer

About Me



2 Startups

Head of Engineering

Manilla

Engineering & Security Team

Ben Willis



Rochester Institute of Technology (RIT)

Computer Engineering
Technology & AI Vision

Teldio

Co-Founder &
Head of
Engineering

HackerOne

Principal Security
Engineer, NA

hackerone

About HackerOne

2,000+

Customer Programs



Uber



1M+

Hackers

~250,000

Valid Reports

\$160 Million+

In Bounties Paid

About You

What is your experience working with hackers? In the chat...

- **Enter 1:** I work with hackers through a bug bounty or vulnerability disclosure program
- **Enter 2:** I have had hackers reach out to my company's security@ email, but I don't have a formal process for working with hackers
- **Enter 3:** I sometimes hear from hackers through another channel like Twitter, and I don't have a formal process for working with hackers
- **Enter 4:** I am a hacker
- **Enter 5:** Unknown

Let's define "hacker"

What does the internet think about hackers?



hackers are|



- hackers are **real**
- hackers are **losers**
- hackers are **scum**
- hackers arena
- hackers are
- hackers are **getting smarter**
- hackers are **everywhere**
- hackers are **evil**
- hackers are **us**
- hackers are **here where are you**

Report inappropriate predictions

WHAT IS A HACKER?

Hacker:

NOUN

one who enjoys the intellectual challenge of creatively overcoming limitations.



WHAT IS A HACKER?

- Hackers can now be seen in countries like **Panama, New Zealand, Hungary, Senegal, Cuba, Vietnam, and Venezuela.**
- Hackers across the globe have found nearly **250,000 valid vulnerabilities** in total.
- Nearly 40% of hackers **devote 20 hours or more** per week to their search for vulnerabilities.

WHY THEY HACK

68%

To be challenged

53%

To earn money

29%

To protect & defend

27%

To do good in the world



Leveraged hackers supplement security teams

hackerone
@nahamsec

HackerOne's extended security team

*Cloud Security
Engineer at
AWS*

*Pentester
Consultant*

*First Year CS
Student*

*Product
Security
Engineer at
Shopify*



Empower the World
to Build a
Safer Internet.





h

Weakness Data



A diversity of information sources is what drives value of our intel sharing and analysis capabilities

Auto-ISAC



OWASP Top 10

- A1** Injection
- A2** Broken authentication
- A3** Sensitive data exposure
- A4** XML External Entities (XXE)
- A5** Broken Access Control
- A6** Security Misconfiguration
- A7** XSS
- A8** Insecure Deserialization
- A9** Using Components with Known Vulnerabilities
- A10** Insufficient Logging & Monitoring



OWASP

Open Web Application
Security Project

OWASP Top 10 Methodology

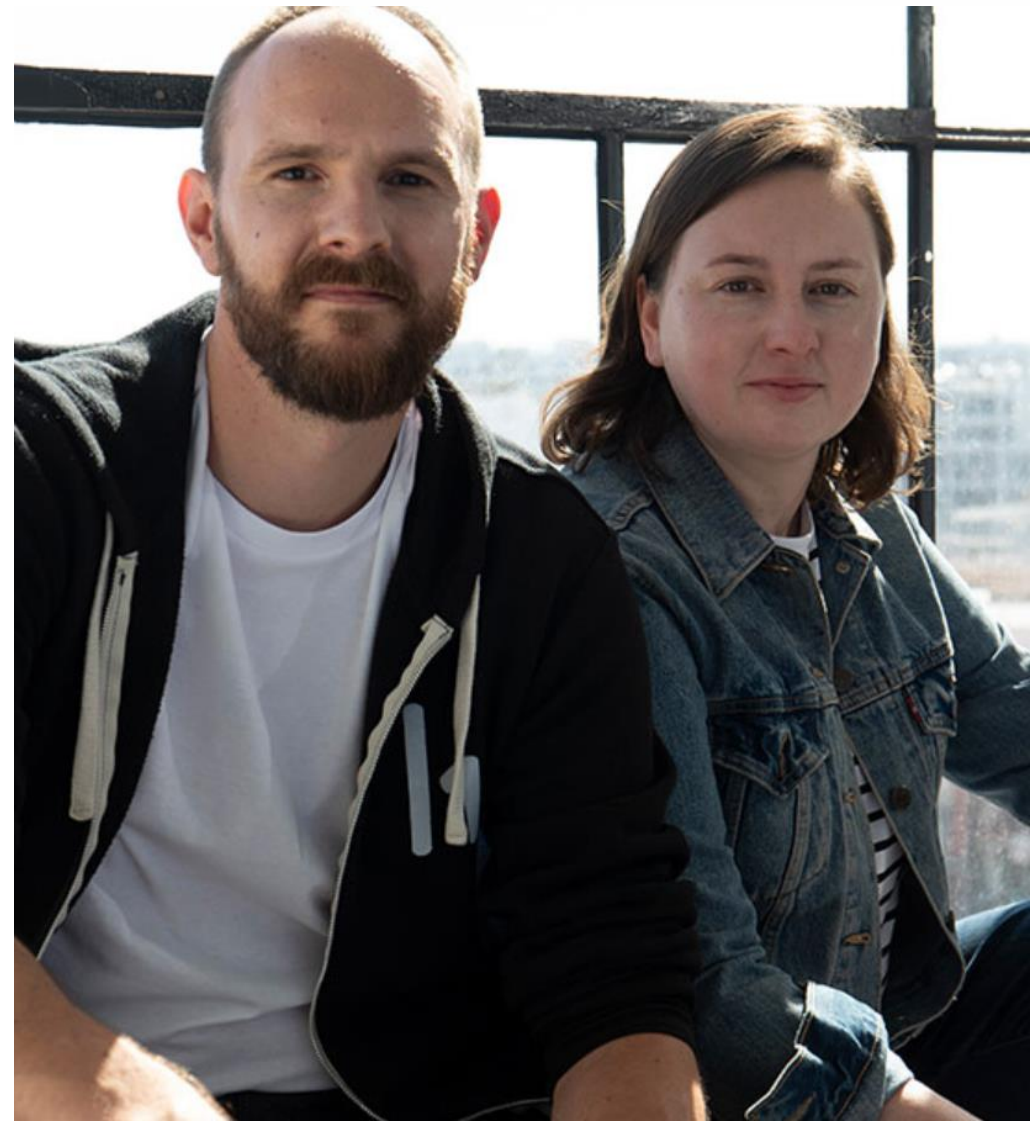
- > Publicly survey data from multiple data sources
- > Yearly performed
- > 2 additional categories are sourced from industry expert

Rank	Survey Vulnerability Categories	Score
1	Exposure of Private Information ('Privacy Violation') [CWE-359]	748
2	Cryptographic Failures [CWE-310/311/312/326/327]	584
3	Deserialization of Untrusted Data [CWE-502]	514
4	Authorization Bypass Through User-Controlled Key (IDOR & Path Traversal) [CWE-639]	493
5	Insufficient Logging and Monitoring [CWE-223 / CWE-778]	440

[HOME](#) > [TOP TEN VULNERABILITIES](#)

THE HACKERONE TOP 10 MOST IMPACTFUL AND REWARDED VULNERABILITY TYPES – 2020 EDITION

As a security leader, you're responsible for a constantly evolving attack surface. The past year has changed the role of the CISO, making it tougher to navigate your operating environment. Distributed decision-making has expanded the volume and variety of risks you must confront, regulators are approaching data privacy with greater scrutiny, and executive teams and boards of directors are starting to think about how information risk impacts strategic planning.



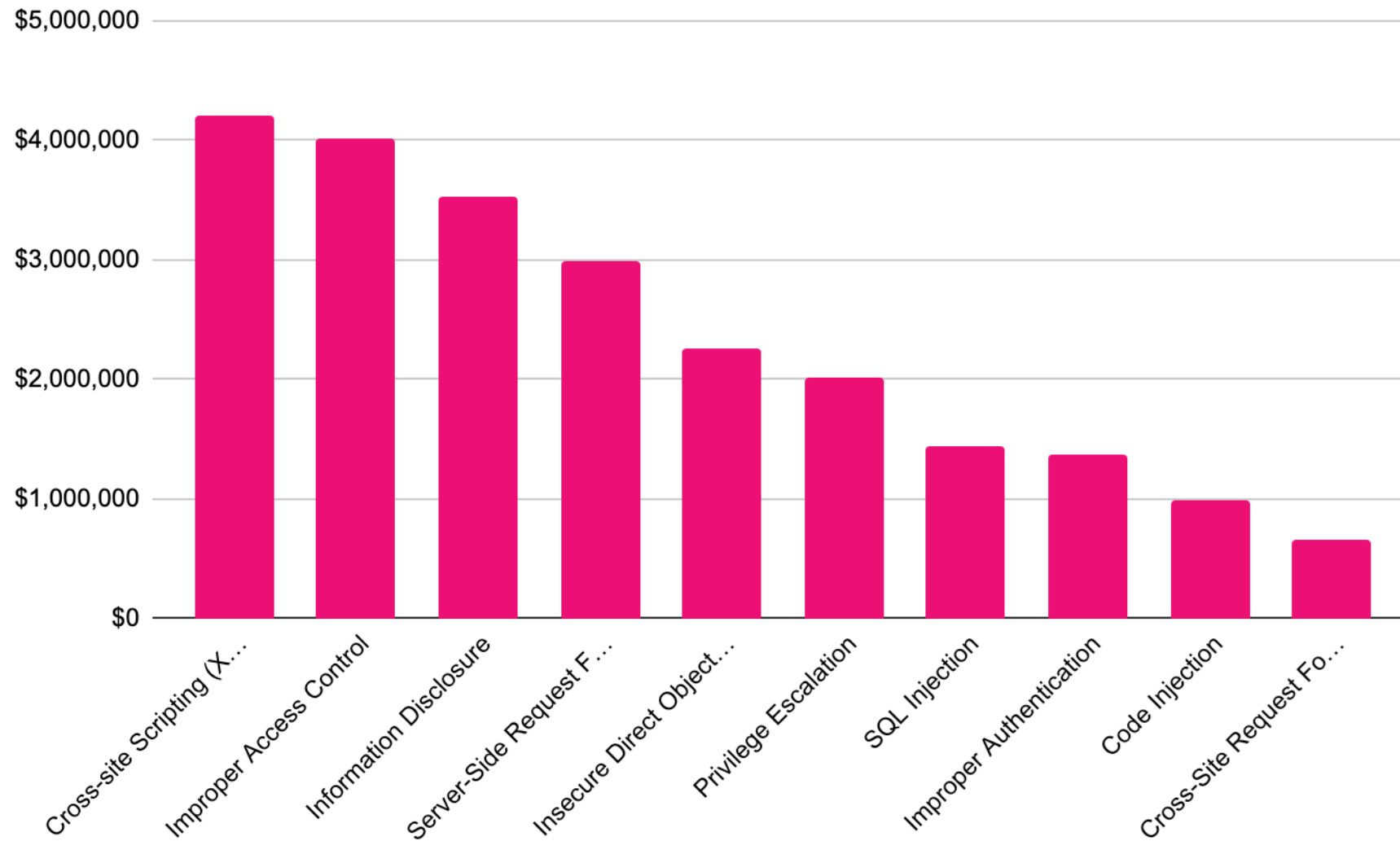
HackerOne Top 10

1. Cross-site Scripting (XSS)
2. Improper Access Control
3. Information Disclosure
4. Server-Side Request Forgery (SSRF)
5. Insecure Direct Object Reference (IDOR)
6. Privilege Escalation
7. SQL Injection
8. Improper Authentication
9. Code Injection
10. Cross-Site Request Forgery (CSRF)





Total Bounties Paid By Weakness Type



Top 10 By Industry

	Automotive & Ground Transportation	Computer Hardware & Peripherals	Travel & Hospitality	Internet & Online Services
Cross-site Scripting (XSS)	12%	12%	34%	16%
Improper Access Control	12%	12%	10%	12%
Information Disclosure	24%	24%	19%	16%
Server-Side Request Forgery (SSRF)	10%	10%	4%	23%
Insecure Direct Object Reference (IDOR)	21%	21%	10%	9%
Privilege Escalation	9%	9%	3%	9%
SQL Injection	2%	2%	3%	5%
Improper Authentication	10%	10%	13%	4%
Code Injection	0%	0%	3%	3%
Cross-Site Request Forgery (CSRF)	1%	1%	2%	3%

Anatomy of a Vulnerability

*Technical
Exploitability*

Severity

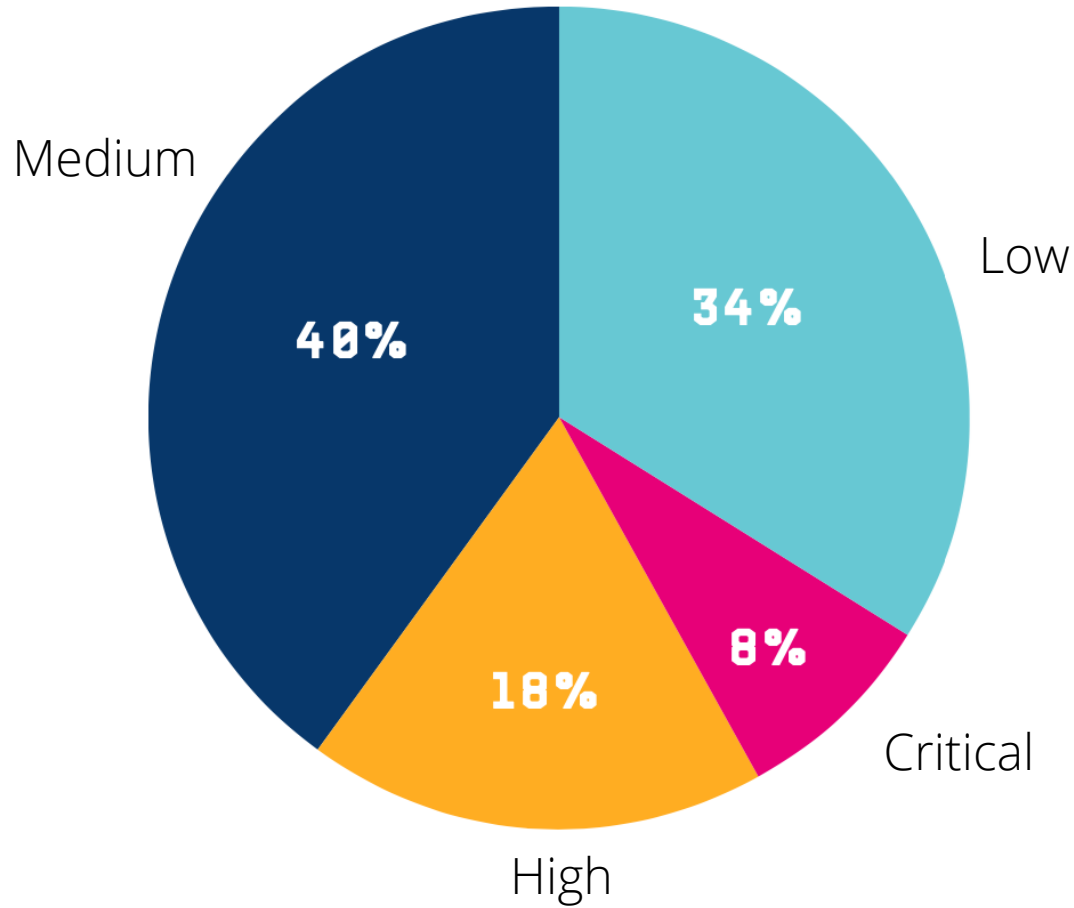
h1

*Hacker
Discoverability*

Impact

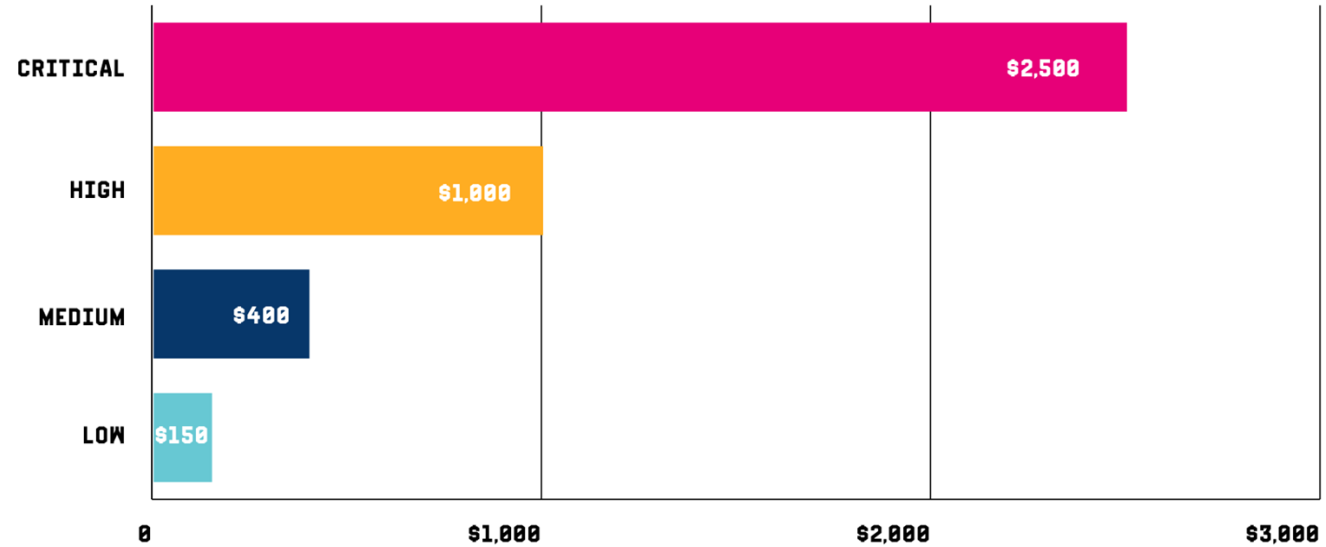
% Found > Discoverability
% Bounties > Impact

% Findings



Discoverability

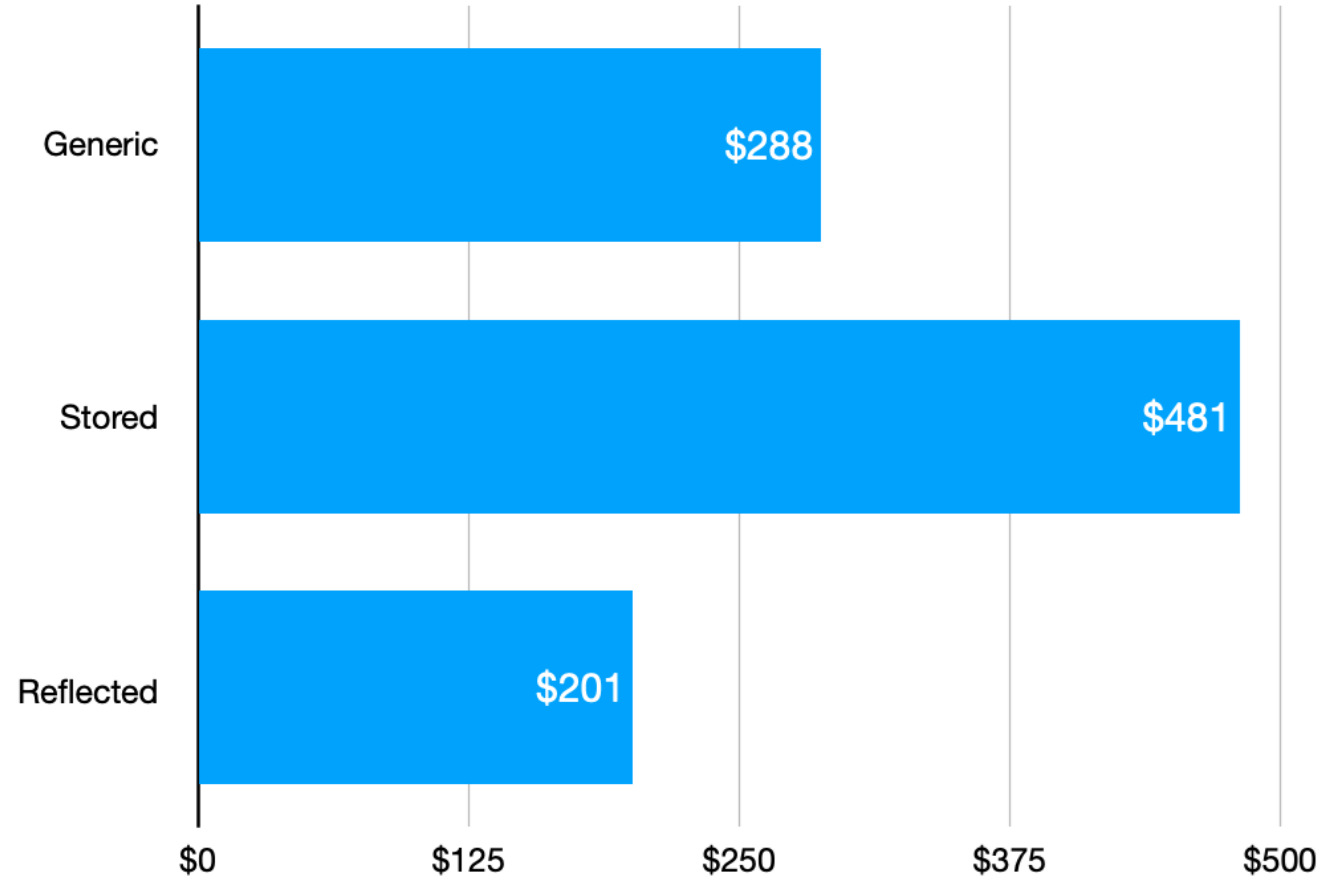
Bounties (\$)



Impact



Average Bounty Per XSS Report





Luke (0x0luke)

233 Reputation - Rank 1.53 Signal 68th Percentile 16.25 Impact 84th Percentile

17

#281283

XSS on partners.uber.com due to no user input sanitisation

Share:

State Resolved (Closed)

Severity Low (0.1 ~ 3.9)

Disclosed **October 4, 2018 2:23pm -0700**

Participants

Reported to [Uber](#)

Visibility Disclosed (Limited)

Reported at **October 20, 2017 3:23pm -0700**

CVE ID

Weakness Cross-site Scripting (XSS) - Generic

Bounty **\$1,000**



Ben Heald (healdb)

1723 Reputation - Rank 5.99 Signal 90th Percentile 19.26 Impact 90th Percentile

364

#340431

Reflected XSS and sensitive data exposure, including payment details, on lioncityrentals.com.sg

Share:

State Resolved (Closed)

Severity High (7 ~ 8.9)

Disclosed **April 30, 2020 2:12pm -0700**

Participants

Reported to [Uber](#)

Visibility Disclosed (Limited)

Reported at **April 19, 2018 4:19am -0700**

CVE ID

Weakness Cleartext Transmission of Sensitive Information

Bounty **\$4,000**

SUMMARY BY UBER



The `/p3/drivers/vehicles/add` endpoint on `partners.uber.com` was vulnerable to cross site scripting, since the endpoint did not validate the data it received, it did not perform encoding on the data to remove or make harmless HTML-sensitive characters such as `<`. The page response was not served with a content-type header. While the content-type header was not set, the `x-content-type-options` header was set to `nosniff`. Additionally, the endpoint was protected against CSRF attacks, making it difficult for an attacker to submit information on behalf of a victim. Without the proper credentials, nothing was returned from the endpoint, mitigating the risk of this issue.

We enjoyed working with [@0x0luke](#) on this report and look forward to their future submissions to Uber's program.

\$1,000

<https://hackerone.com/reports/281283>

hackerone

SUMMARY BY UBER



lioncityrentals.com.sg employed a Wordpress installation that possessed a vulnerable plugin, Formidable Forms, which was vulnerable to reflected XSS, and exposed sensitive form data.

Thanks again for the report, [@healdb](#)!

SUMMARY BY HEALDB



This was the first bug I ever found that exposed a large amount of PII, thanks for disclosing [@uber](#)!

This bug reinforces to me that hackers should always examine microsites as well as core domains, sometimes bugs on microsites can lead to significant data exposure. In this case, lioncityrentals.com.sg was collecting data on thousands of Uber Singapore users, which was then exposed by the outdated Wordpress plugin.

You can read more about the formidable forms vulnerability here - <https://klikki.fi/adv/formidable.html>

And be sure to check out my blog <https://healdb.tech/blog/> or my twitter https://twitter.com/heald_ben for Bug Bounty tips and guides!

\$1,000

<https://hackerone.com/reports/340431>

hackerone



Total Bounty Amount by

	Weakness Type	Bounties Total Financial Rewards Amount	YOY % Chage
1	XSS	\$4,211,006	26%
2	Improper Access Control - Generic	\$4,013,316	134%
3	Information Disclosure	\$3,520,801	63%
4	Server-Side Request Forgery (SSRF)	\$2,995,755	103%
5	Insecure Direct Object Reference (IDOR)	\$2,264,833	70%
6	Privilege Escalation	\$2,017,592	48%
7	SQL Injection	\$1,437,341	40%
8	Improper Authentication - Generic	\$1,371,863	36%
9	Code Injection	\$982,247	-7%
10	Cross-Site Request Forgery (CSRF)	\$662,751	-34%

HackerOne Top 10

1. Cross-site Scripting (XSS)
2. Improper Access Control
3. Information Disclosure
4. Server-Side Request Forgery (SSRF)
5. Insecure Direct Object Reference (IDOR)
6. Privilege Escalation
7. SQL Injection
8. Improper Authentication
9. Code Injection
10. Cross-Site Request Forgery (CSRF)

OWASP Top 10

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring



HackerOne Auto & Ground Top 10

1. Information Disclosure
2. Insecure Direct Object Reference (IDOR)
3. Cross-site Scripting (XSS)
4. Improper Access Control
5. Server-Side Request Forgery (SSRF)
6. Improper Authentication
7. Privilege Escalation
8. SQL Injection
9. Cross-Site Request Forgery (CSRF)
10. Code Injection



Get a bug if you find a bug.

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway. There's a catch, though. Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy. Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing. And since it's delivered in 4K bytes of ROM, VRTX will perform for you the way it's performing in hundreds of real-time applications from avionics to video games. Bug free. So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306. Describe your application and the microprocessors you're using—Z8000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.* But don't feel bad if in a year from now there isn't a bug in your driveway. There isn't one in your operating system either.

HUNTER & READY
VRTX
Operating Systems in Silicon.

*Call or write for details. But, considering our taste in cars, you might want to accept our offer of \$1,000 cash instead. © 1983 Hunter & Ready, Inc.



h

Weakness Analysis & Comparison

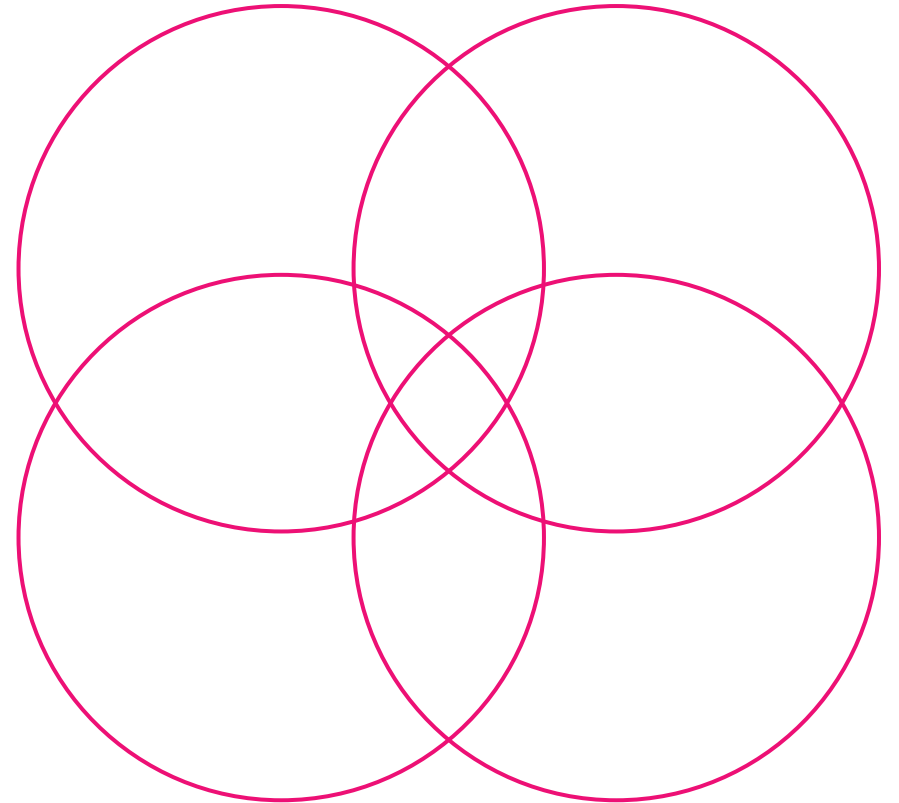
Looking at OWASP Top 10, HackerOne Top 10 or others

HackerOne's Top 10

	COMPUTER SOFTWARE	HACKERONE
Cross-site Scripting (XSS)	13%	5%
Improper Access Control	36%	4%
Information Disclosure	11%	24%
Server-Side Request Forgery (SSRF)	4%	1.3%
Insecure Direct Object Reference (IDOR)	7%	3%
Privilege Escalation	12%	3%
SQL Injection	2%	0%
Improper Authentication	6%	10%
Code Injection	7%	0%
Cross-Site Request Forgery (CSRF)	3%	3%

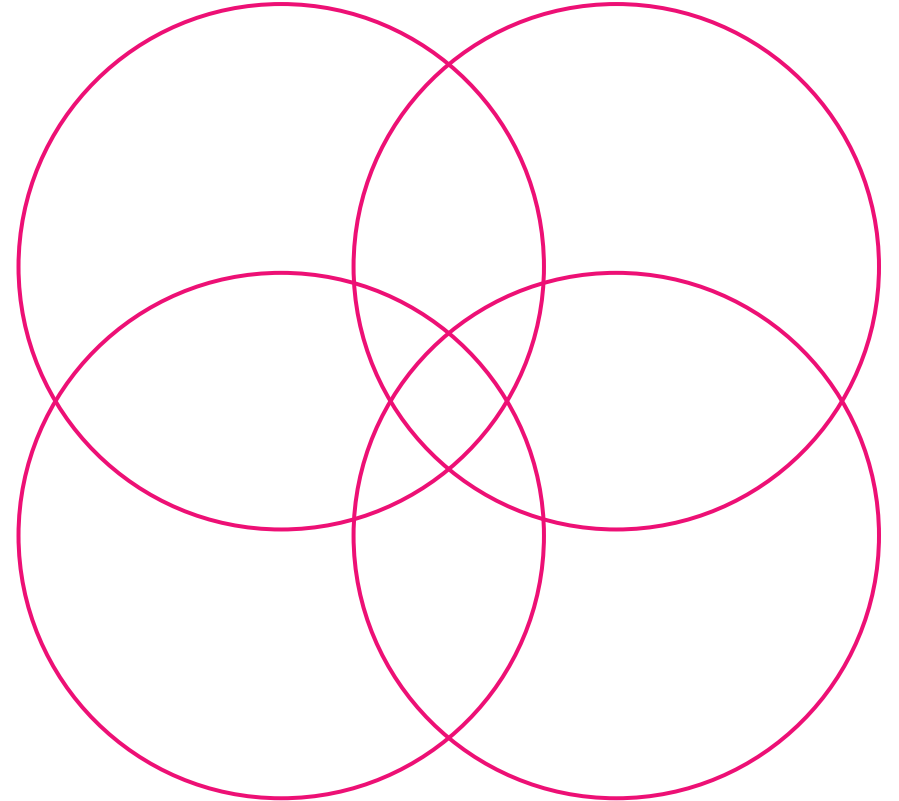
Opportunities to learn

- > Overlaps in data sets within *OWASP Top 10* can show you broad industry and **potential threats to your environment**
- > Overlaps in data sets within *HackerOne Top 10* can show you more **discoverable and impactful vulnerabilities**
- > Overlaps in data sets within *Industry* can **show technology challenges within weakness types**

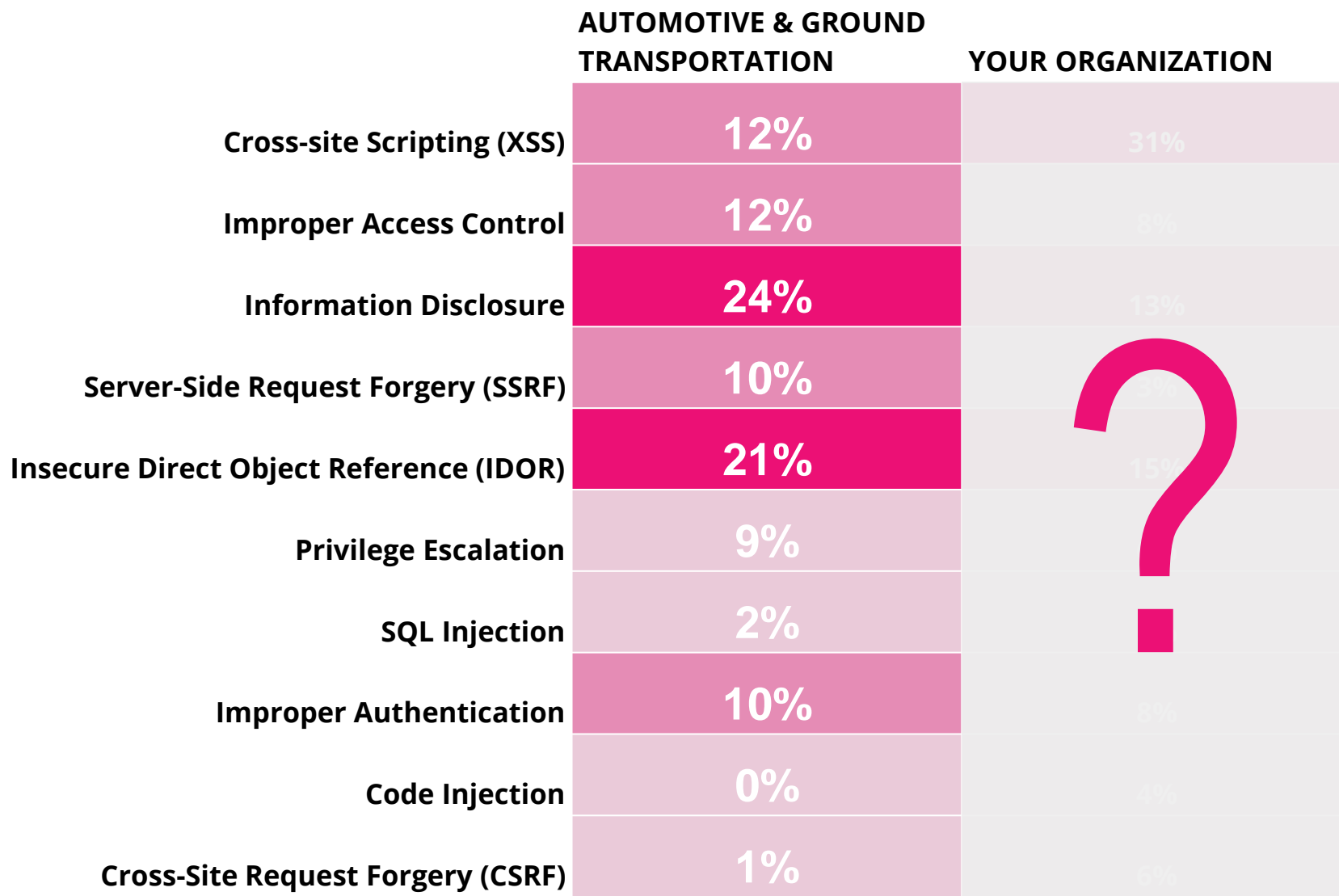


Opportunities to share

- > Weaknesses missing from data sets within *OWASP Top 10* can show you not applicable or **strengths in your security posture**
- > Weaknesses missing from data sets within *HackerOne Top 10* can show you not applicable or **areas of hardened attack surface**
- > Weaknesses missing from data sets within *Industry* can show you opportunities to **share your strategies** with your extended security team



Your Top 10





h1

Key Takeaways

Data, analysis and sharing



Hackers are an extension to your security team to share data with.



Diverse data helps you see opportunities to learn or share.



Data analysis can lead to better
priority decisions with development
teams.

If you want to learn more...



ben@hackerone.com



22 4th St, 5th Fl
San Francisco, CA 94103



hackerone.com



[@Hacker0x01](https://twitter.com/Hacker0x01)



[HackerOne](https://www.linkedin.com/company/hackerone)

- > [The 2021 Hacker Report](#)
- > [The Top 10 Vulnerabilities Report](#)
- > [5 Ways CISOs Derive Value From Hacker-Powered Security](#)
- > [Security Leaders Handbook](#)



h

Questions?

Ben Willis

ben@hackerone.com

@benjaminjwillis

OPEN DISCUSSION

*ANY QUESTIONS ABOUT THE AUTO-ISAC OR FUTURE
TOPICS FOR DISCUSSION?*

HOW TO GET INVOLVED: MEMBERSHIP

IF YOU ARE AN OEM, SUPPLIER OR COMMERCIAL VEHICLE, CARRIER OR FLEET, PLEASE JOIN THE AUTO-ISAC!

- *REAL-TIME INTELLIGENCE SHARING*
- *INTELLIGENCE SUMMARIES*
- *REGULAR INTELLIGENCE MEETINGS*
- *CRISIS NOTIFICATIONS*
- *MEMBER CONTACT DIRECTORY*
- *DEVELOPMENT OF BEST PRACTICE GUIDES*
- *EXCHANGES AND WORKSHOPS*
- *TABLETOP EXERCISES*
- *WEBINARS AND PRESENTATIONS*
- *ANNUAL AUTO-ISAC SUMMIT EVENT*

To learn more about Auto-ISAC Membership or Partnership, please contact Auto-ISAC! fayefrancy@automotiveisac.com

AUTO-ISAC PARTNERSHIP PROGRAMS

Strategic Partner

Solutions Providers

For-profit companies that sell connected vehicle cybersecurity products & services.

Examples: Hacker ONE, IOActive, Karamba, Grimm

INNOVATOR
Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed
- Must be educational provide awareness

Community Partners

Associations

Industry associations and others who want to support and invest in the Auto-ISAC activities.

Examples: Auto Alliance, ATA, ACEA, JAMA

NAVIGATOR
Support Partnership

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities
- Supports Auto-ISAC

Affiliations

Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.

Examples: NCI, DHS, NHTSA, Colorado State

COLLABORATOR
Coordination Partnership

- "See something, say something"
- May not require a formal agreement
- Information exchanges-coordination activities
- Information Sharing / research & development

Community

Companies interested in engaging the automotive ecosystem and supporting & educating the community.

Examples: Sponsors for key events, technical experts, etc.

BENEFACTOR
Sponsorship Partnership

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

CURRENT PARTNERSHIPS

MANY ORGANIZATIONS ENGAGING

INNOVATOR

**Strategic Partnership
(15)**

ArmorText
Celerium
Cybellum
Ernst and Young
FEV
GRIMM
HackerOne
Karamba Security
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Trillium Secure
Upstream

NAVIGATOR

Support Partnership

AAA
ACEA
ACM
American Trucking
Associations (ATA)
ASC
ATIS
Auto Alliance
EMA
Global Automakers
IARA
IIC
JAMA
MEMA
NADA
NAFA
NMFTA
RVIA
SAE
TIA
Transport Canada

COLLABORATOR

**Coordination
Partnership**

AUTOSAR
Billington Cybersecurity
Cal-CSIC
Computest
Cyber Truck Challenge
DHS CSVI
DHS HQ
DOT-PIF
FASTR
FBI
GAO
ISAO
Macomb Business/MADCAT
Merit (training, np)
MITRE
National White Collar Crime Center
NCFTA
NDIA
NHTSA
NIST
Northern California Regional Intelligence
Center (NCRIC)
NTIA - DoCommerce
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsch College

BENEFACTOR

**Sponsorship
Partnership**

2020 Summit Sponsors-

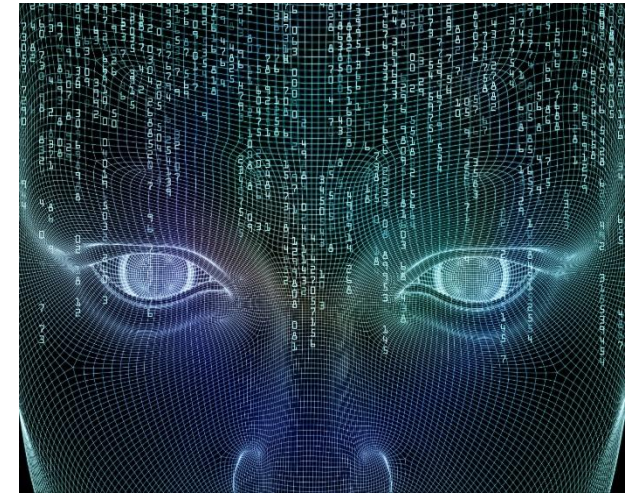
Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsignts
ValiMail

2019 Summit Sponsors-

Argus
Arxan
Blackberry
Booz Allen Hamilton
Bugcrowd
Celerium
Cyber Future Foundation
Deloitte
GM
HackerOne
Harman
IOActive
Karamba Security
Keysight
Micron
NXP
PACCAR
Recorded Future
Red Balloon Security
Saferide
Symantec
Toyota
Transmit Security
Upstream
Valimail

AUTO-ISAC BENEFITS

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency



Building Resiliency Across the Auto Industry

MAAKE
 TERMA KASIH RAIBH MAITH AGAT
 JUSPAXAR
 OBRIGADO
 MATONDO
 SALAMAT
 KIITOS
 MOCHCHAKKERAM
 MULTUMESC
 CHOKRANE
 KIA ORA
 SALAMAT
 CAM ON BAN
 GRAZIE
 MULTUMESC
 MERCI
 RAIBH MAITH AGAT
 OBRIGADO
 MOCHCHAKKERAM
 MERCI
 MOCHCHAKKERAM
THANK
 CHOKRANE
 MATUR NUWUN
ASANTE
 UA TSAUG RAU KOJ
 MOCHCHAKKERAM
 MATONDO
 CHOKRANE
 UA TSAUG RAU KOJ
YOU
 DANK JE
 RAIBH MAITH AGAT
 SPASIBO
 MAAKE
 OBRIGADO
WELALIN
 SPASIBO
 ARIGATO
 MOCHCHAKKERAM
 OBRIGADO
 KIITOS
 DANKON
 NIRRINGRAZZJAK
 MOCHCHAKKERAM
 MULTUMESC
VINAKA
 NIRRINGRAZZJAK
 MAMANA
 OBRIGADO
 DANK JE
 KIITOS

OUR CONTACT INFO

Faye Francy
Executive Director



20 F Street NW, Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

Sharmila Khadka
Information Technology & Executive
Coordinator



20 F Street NW, Suite 700
Washington, DC 20001
443-962-5663
sharmilakhadka@automotiveisac.com



www.automotiveisac.com
[@auto-ISAC](https://twitter.com/auto-ISAC)