RTA Integrated RPA

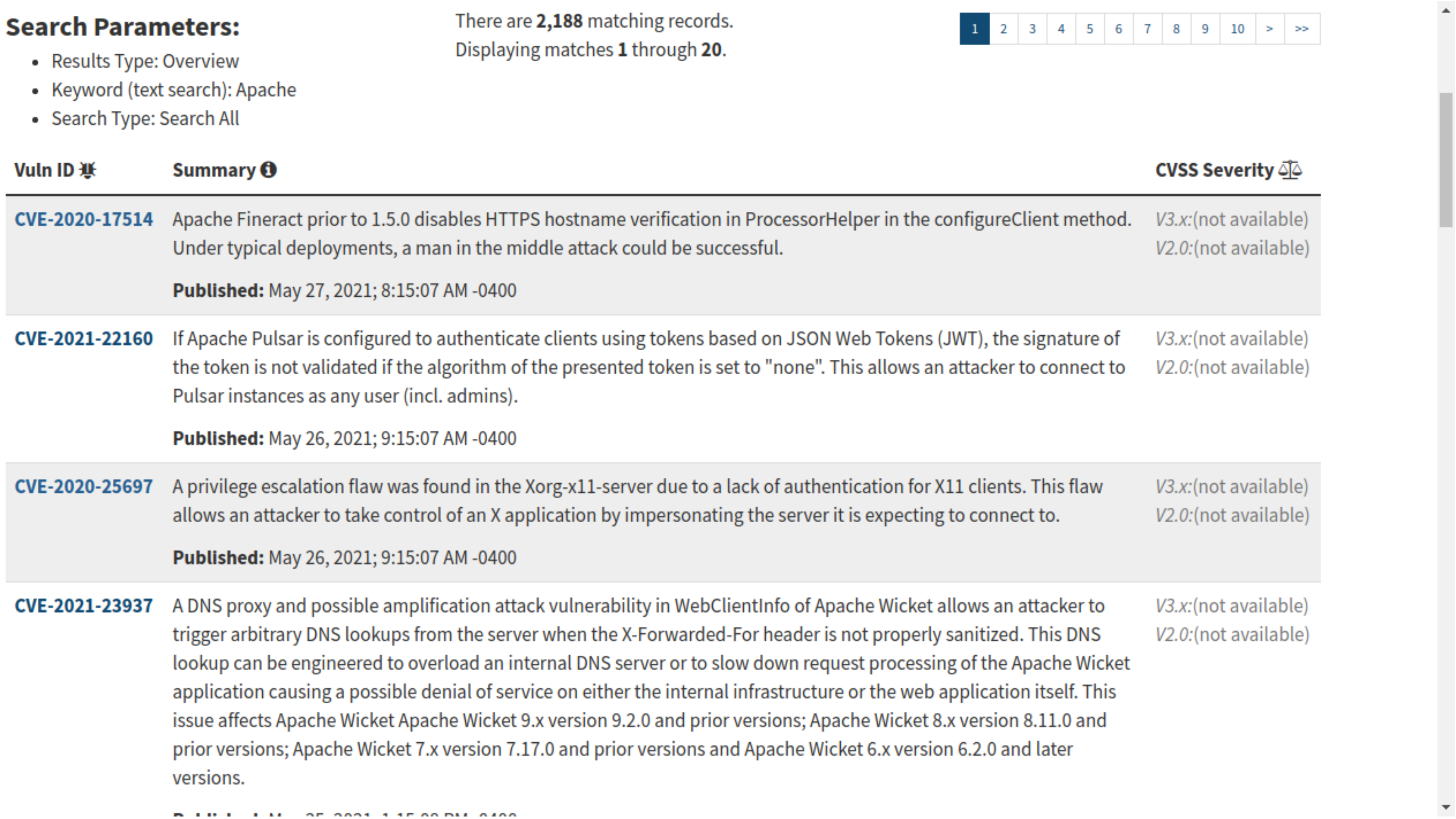
Scanner: Using Components with Known Vulnerabilities

Scan Time: 27/05/2021 10:33:09

Results:

```
[!] Scanned file: https://www.etsy.com/paula/v3/polyfill.min.js?etsy-v=v2&flags=gated&ua-hash=e5d34a2af

[-] No vulnerabiities found

[!] Scanned file: https://www.etsy.com/ac/primary/js/en-US/corelibs-with-preact.e3458f772b35f14d3a1a.js

[     {          "version": "2.2.4",          "component": "jquery",          "detection": "filecontent",          "vulnerabilities

[!] Scanned file: https://www.etsy.com/ac/primary/js/en-US/base.c0871bfde6281b5bc4c8.js

[-] No vulnerabiities found

[!] Scanned file: https://www.etsy.com/ac/primary/js/en-US/bootstrap/category-nav/v2/nav.94b1ba9671d7d

[-] No vulnerabiities found

[!] Scanned file: https://www.etsy.com/ac/primary/js/en-US/vesta_homepage/bootstrap.e0071d437c58aa2

[-] No vulnerabiities found

[!] Scanned file: https://www.etsy.com/ac/primary/js/en-US/neu-views/common/listing-card.c263c3837f7e1

[-] No vulnerabiities found

[!] Server Version: Apache
```

National Vulnerability Database query result for [Apache]



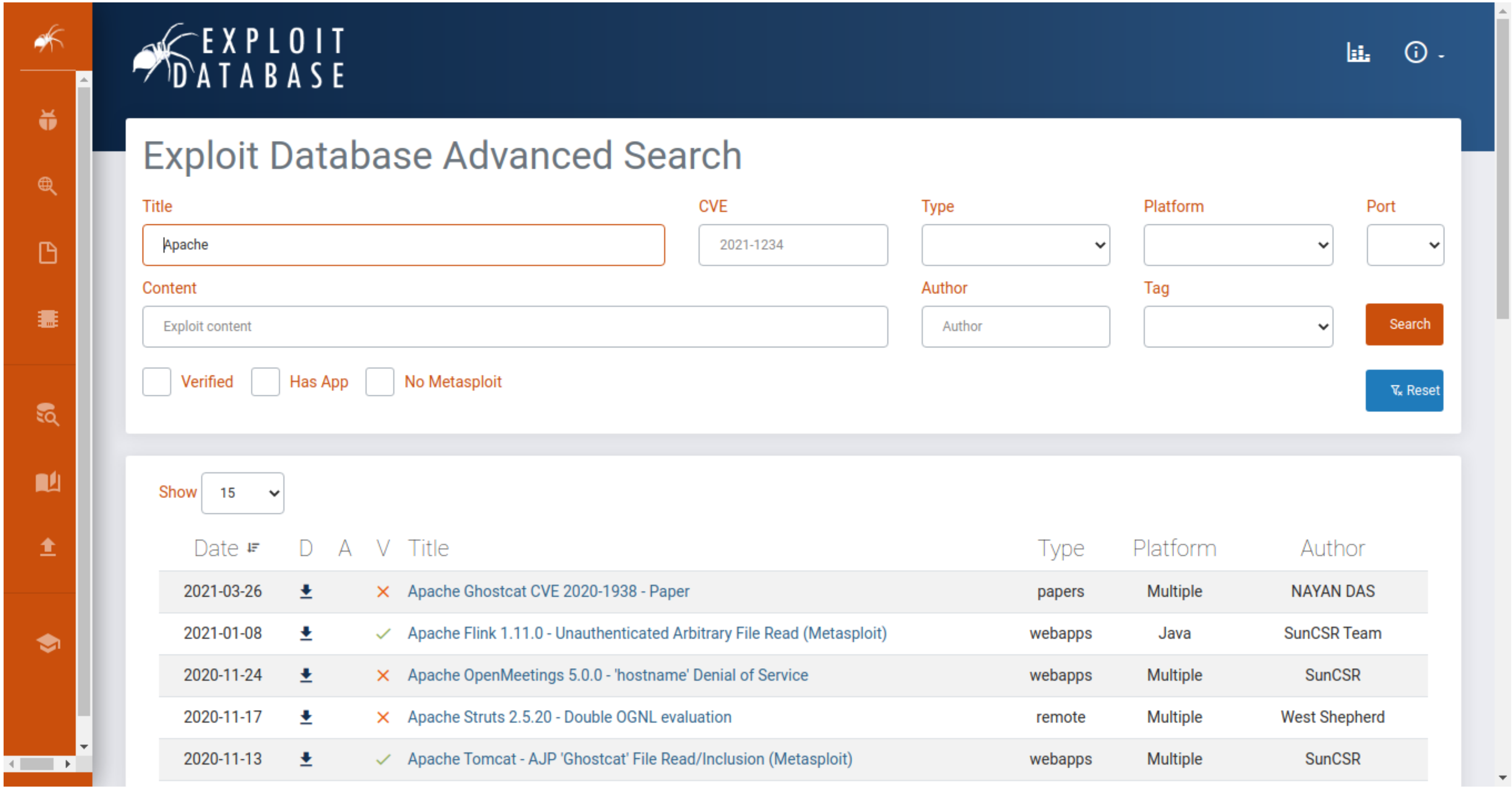
Search Parameters:

- Results Type: Overview
- Keyword (text search): Apache
- Search Type: Search All

There are **2,188** matching records.
Displaying matches **1** through **20**.

Vuln ID	Summary	CVSS Severity
CVE-2020-17514	Apache Fineract prior to 1.5.0 disables HTTPS hostname verification in ProcessorHelper in the configureClient method. Under typical deployments, a man in the middle attack could be successful. **Published:** May 27, 2021; 8:15:07 AM -0400	*V3.x:*(not available) *V2.0:*(not available)
CVE-2021-22160	If Apache Pulsar is configured to authenticate clients using tokens based on JSON Web Tokens (JWT), the signature of the token is not validated if the algorithm of the presented token is set to "none". This allows an attacker to connect to Pulsar instances as any user (incl. admins). **Published:** May 26, 2021; 9:15:07 AM -0400	*V3.x:*(not available) *V2.0:*(not available)
CVE-2020-25697	A privilege escalation flaw was found in the Xorg-x11-server due to a lack of authentication for X11 clients. This flaw allows an attacker to take control of an X application by impersonating the server it is expecting to connect to. **Published:** May 26, 2021; 9:15:07 AM -0400	*V3.x:*(not available) *V2.0:*(not available)
CVE-2021-23937	A DNS proxy and possible amplification attack vulnerability in WebClientInfo of Apache Wicket allows an attacker to trigger arbitrary DNS lookups from the server when the X-Forwarded-For header is not properly sanitized. This DNS lookup can be engineered to overload an internal DNS server or to slow down request processing of the Apache Wicket application causing a possible denial of service on either the internal infrastructure or the web application itself. This issue affects Apache Wicket Apache Wicket 9.x version 9.2.0 and prior versions; Apache Wicket 8.x version 8.11.0 and prior versions; Apache Wicket 7.x version 7.17.0 and prior versions and Apache Wicket 6.x version 6.2.0 and later versions. **Published:** May 25, 2021; 1:15:08 PM -0400	*V3.x:*(not available) *V2.0:*(not available)

Exploit-DB query result for [Apache]



Exploit Database Advanced Search

Title: Apache

CVE: 2021-1234

Type:

Platform:

Port:

Content: Exploit content

Author: Author

Tag:

Search

Reset

□ Verified □ Has App □ No Metasploit

Show 15

Date	D	A	V	Title	Type	Platform	Author
2021-03-26	⬇		✗	Apache Ghostcat CVE 2020-1938 - Paper	papers	Multiple	NAYAN DAS
2021-01-08	⬇		✓	Apache Flink 1.11.0 - Unauthenticated Arbitrary File Read (Metasploit)	webapps	Java	SunCSR Team
2020-11-24	⬇		✗	Apache OpenMeetings 5.0.0 - 'hostname' Denial of Service	webapps	Multiple	SunCSR
2020-11-17	⬇		✗	Apache Struts 2.5.20 - Double OGNL evaluation	remote	Multiple	West Shepherd
2020-11-13	⬇		✓	Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit)	webapps	Multiple	SunCSR