سامانه جستجوگر آسیب‌پذیری (جویا)

سامانه جستجوگر آسیب‌پذیری چیست؟

۱ یک موتور جستجو آسیب‌پذیری است که این امکان را می‌دهد انواع مختلفی از رایانه های متصل به شبکه (روتر ، سرور، IoT و ...) را با استفاده از انواع فیلترها جستجو کند.

۲ این ابزار می‌تواند اطلاعات مفیدی از جمله در مورد نرم افزار و سیستم عامل سرور، وضعیت پورت‌ها، سرویس‌های فعال، آسیب‌پذیری‌های شناخته شده‌ی هر سرویس و کدهای بهره‌برداری از آن آسیب‌پذیری‌ها را در اختیار بگذارد. همچنین این ابزار می‌تواند کدهای اکسپلویت را نیز اجرا و سعی در اخذ نشست نماید.

۳ اطلاعات سامانه، از ماشین‌های بر بستر اینترنت یا شبکه داخلی بصورت Agent-less بدست می‌آید.

۴ علاوه بر آنکه امکان جستجو از طریق پرس و جو (Query) را فراهم می‌آورد، می‌تواند نتایج حاصله از پویش شبکه را نیز برای درک بیشتر مصورسازی نماید.

اجزای سامانه

موتور جستجوی آسیب‌پذیری از ۵ زیر سامانه اصلی تشکیل شده است:

- زیر سامانه پویش سریع پورت
- زیر سامانه پویش موازی سرویس و سیستم‌عامل
- زیر سامانه پویش تکنولوژی‌های وب
- زیر سامانه جستجو و بهره‌برداری از آسیب‌پذیری
- زیر سامانه ذخیره و مصورسازی

در توسعه سامانه‌های موتور جستجوی آسیب‌پذیری از زبان‌های برنامه‌نویسی C/C++، Lua، Ruby و Python استفاده شده است.

زیرسامانه پویش سریع پورت

زیرسامانه پویش سریع پورت اولین سامانه‌ای است که در موتور جستجوی آسیب‌پذیری مورد استفاده قرار می‌گیرد. این سامانه دارای سه موتور پویش پورت می‌باشد که توانایی انواع پویش پورت‌های باز TCP/UDPرا دارند.

- موتور **Masscan**: این موتور قادر است تا وضعیت بسته یا باز بودن پورت‌های TCP را از طریقSYN Scan و پورت‌هایUDP را از طریق UDP Probeها بررسی نماید. سرعت اسکن این موتور بسته به پهنای باند و رابط شبکه بین ۱۰۰ تا ۱۰ میلیون پکت در هر ثانیه می‌باشد (با حداکثر سرعت خود می‌تواند کل اینترنت را در کمتر از ۵ دقیقه پویش نماید).
- موتور **Zmap**: این موتور نیز همانند موتور Masscan قادر است وضعیت پورت‌ها را بررسی نماید. تفاوت این موتور با Masscan امکان توسعه UDP Probeها می‌باشد. سرعت آن کمتر از Masscan می‌باشد. بهترین عملکرد را در پویش تک پورت دارد.
- موتور **Nmap**: این موتور وضعیت باز یا بسته بودن پورت‌ها را با اطمینان و دقت بیش‌تری بررسی می‌کند. سرعت آن ۱۳۰۰ بار کمتر از Zmap می‌باشد.

زیر سامانه پویش موازی سرویس و سیستم‌عامل

این زیر سامانه که هسته‌ی اصلی موتور جستجوی آسیب‌پذیری را تشکیل می‌دهد، قادر است سیستم‌عامل و انواع سرویس‌های درحال اجرا بر روی پورت‌های بازی را که زیرسامانه پویش سریع پورت بدست آورده است، تشخیص دهد.

از جمله اطلاعاتی که این زیر سامانه از سرویس‌ها جمع‌آوری می‌کند:

- نام سرویس مثلا (SSH)
- نام سیستم‌عامل، نسخه، سازنده، نوع وEoL آن (به عنوان مثال FreeBSD 11.2-RELEASE)
- محصول سرویس (مثلا OpenSSH)
- بنرها شامل بنر سرویس، SSL و هدر HTTP (مثلا SSH-2.0-OpenSSH_7.4)
- نسخه سرویس (مثلا ۷.۴)
- Common Platform Enumeration مثلا (cpe:/a:openbsd:openssh:7.4)
- اطلاعات دیتابیس‌ها و وضعیت احراز هویت آن‌ها
- نوع سیستم‌عامل بر اساس سرویس

زیر سامانه پویش تکنولوژی وب

این زیر سامانه قادر است تا تکنولوژی‌های وب استفاده شده در سرویس Webرا با استفاده از عبارات منظم از پیش تعریف شده، تشخیص دهد.

از جمله اطلاعاتی که این زیر سامانه از سرویس‌های Web جمع‌آوری می‌کند:

- نام و نسخه وب سرور
- نام و نسخه کتابخانه‌ها و فریمورک‌های JavaScript
- نام و نسخه فریمورک‌های وب
- نام و نسخه Reverse Proxyها
- نام و نسخه فریمورک‌های رابط کاربری
- نام زبان برنامه‌نویسی استفاده شده
- اطلاعات فونت‌ها

زیرسامانه جستجو و بهره‌برداری از آسیب‌پذیری

این زیر سامانه که جنبه‌ی تهاجمی دارد شامل سه عملکرد اصلی می‌شود:

۱. استخراج CVEهای بروز آسیب‌پذیری‌ها مطابق با CPE بدست آمده از زیر سامانه پویش موازی سرویس

۲. گردآوری کدهای بهره‌برداری از آسیب‌پذیری‌ها مطابق با CVE آن‌ها از منابعی همچون Metasploit و ...

۳. بهره‌برداری خودکار از آسیب‌پذیری‌ها با استفاده از کدهای بهره‌برداری گردآوری شده و سعی در دریافت نشست از ماشین هدف

همچنین این قابلیت را دارد تا بتوان کدهای بهره‌برداری شخصی‌سازی شده‌ای را در بستر آن توسعه داد و استفاده نمود.

زیر سامانه ذخیره و مصورسازی

این زیر سامانه از دو بخش اصلی ذخیره سازی و مصورسازی تشکیل شده است.

ذخیره سازی:

در سامانه موتور جستجوی آسیب‌پذیری از ذخیره‌سازی، پشتیبان‌گیری و بازیابی ازطلاعات استفاده شده است. نتایج حاصل از اجرای زیرسامانه پویش سریع پورت در لحظه پشتیبان گیری و ذخیره می‌شوند از این رو در صورت متوقف شدن این زیرسامانه می‌توان در کمترین زمان ممکن آن را بازبابی و از محل توقف اجرا نمود.

همچنین نتایج حاصل از زیر سامانه پویش موازی سرویس و سایر زیر سامانه ها پس از گردآوری، بطور لحظه‌ای در پایگاه داده‌ی Elasticsearch ذخیره می‌شوند. کلیه رکوردهای ذخیره شده نیز برچسب زمانی دریافت می‌کنند تا بتوان تغییرات آن‌ها در مرور زمان ثبت و ضبط کرد.

ذخیره‌سازی اطلاعات بگونه‌ای صورت می‌پذیرد که امکان اجرای انواع پرس‌وجوها (Query) بر روی آن‌ها بطور ساده وجود داشته باشد. برای مثال می‌توان آیپی ماشین‌هایی را که نسخه‌ی مشخصی از سرویس ssh بر روی آن‌ها فعال است را با کوئری زیر بدست آورد:

```
protocols.tcp.ssh.service.version: 7.4
```

زیر سامانه ذخیره و مصورسازی

این زیر سامانه از دو بخش اصلی ذخیره سازی و مصورسازی تشکیل شده است.

مصورسازی:

فرآیند مصورسازی نیز بطور لحظه‌ای براساس نتایج ذخیره‌سازی شده در پایگاه داده Elasticsearch صورت می‌پذیرد. خروجی این فرآیند انواع چارت‌ها و جداولی است که اطلاعات مفیدی از وضعیت کلی یا جزئی هر آیپی در اختیار می‌گذارد.

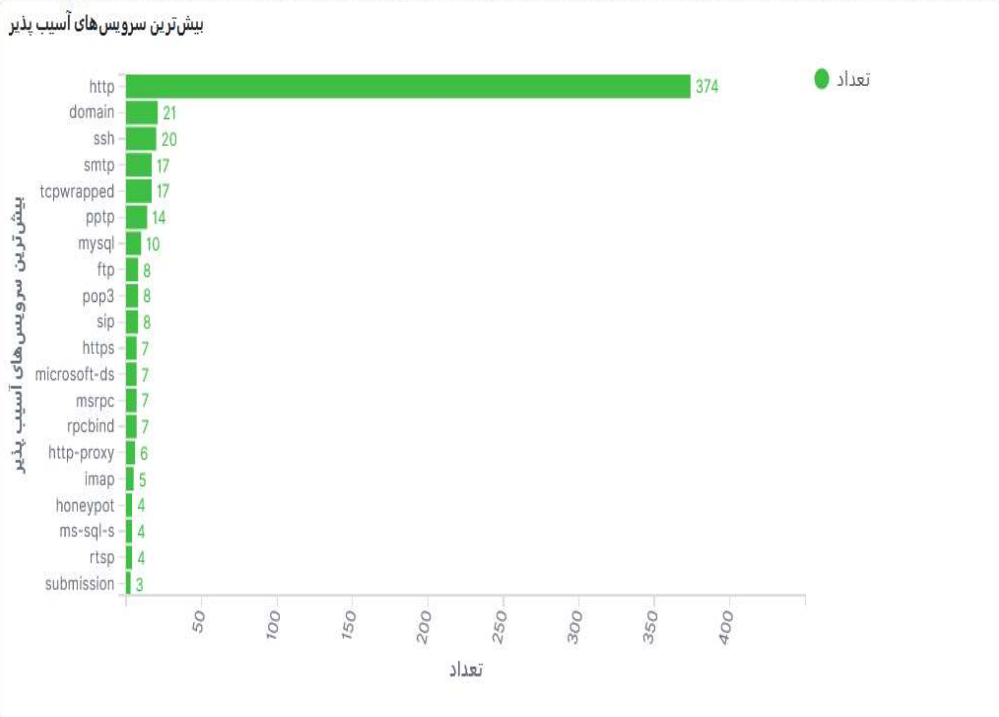
این نتایج در قالب داشبوردهای Elasticsearch ذخیره می‌شوند و امکان خروجی‌های PDF، PNG و ... را دارد.

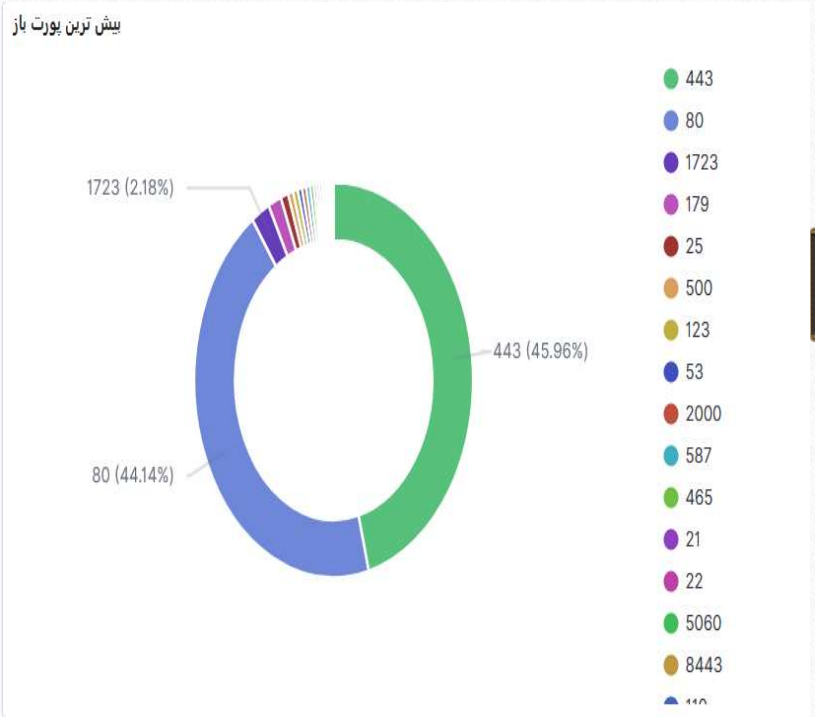
همچنین امکان گرفتن خروجی از اطلاعات ذخیره‌سازی شده در قالب CSV و JSON وجود دارد.

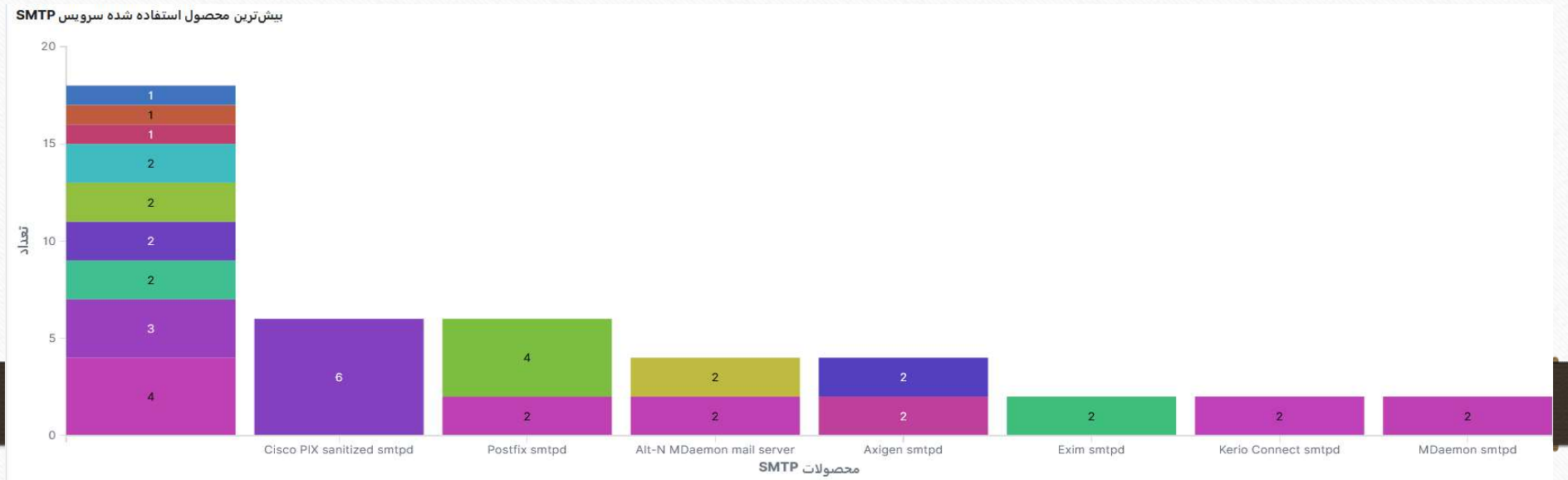
داشبورد

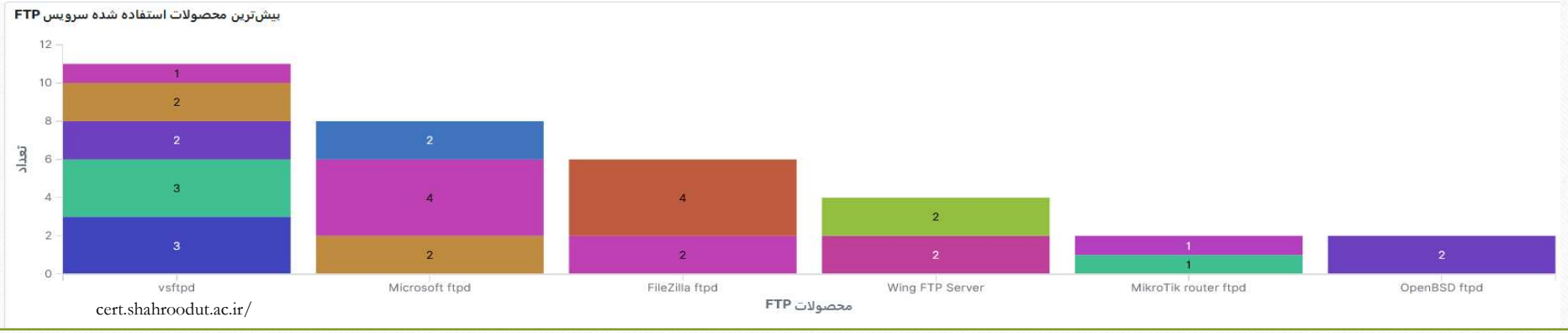

بیش ترین آسیب‌پذیری ها
CVE-2018-1312
CVE-2018-1302
CVE-2018-1301
CVE-2020-1927
CVE-2020-1934
CVE-2000-0115
CVE-1999-0229
CVE-2018-17189
CVE-2009-2299
CVE-2019-0217
CVE-2012-4001
CVE-2007-4723
CVE-2013-0941
CVE-2021-23017
CVE-2013-4365
CVE-2018-17199
CVE-2011-1176
CVE-2013-0942
CVE-2007-0087
CVE-2019-0220
CVE-2013-2765
CVE-2019-20372
CVE-2011-2688
CVE-2009-0796
CVE-2009-1890
CVE-2012-3526
CVE-2012-4360
CVE-2019-10098
CVE-2018-1303
CVE-2019-10092
بیش‌ترین آسیب پذیری - تعداد

داشبورد

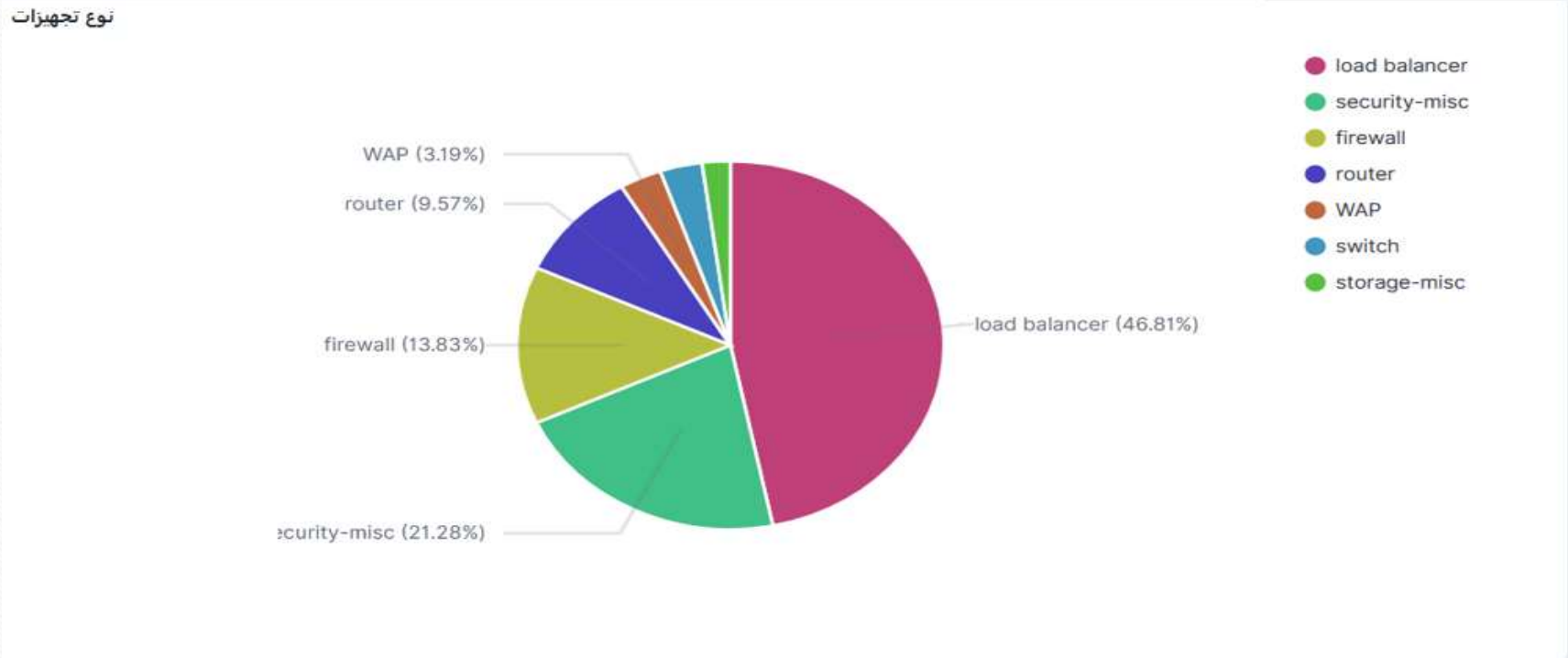

بیش‌ترین سرویس‌های آسیب پذیر
تعداد
http 374
domain 21
ssh 20
smtp 17
tcpwrapped 17
pptp 14
mysql 10
ftp 8
pop3 8
sip 8
https 7
microsoft-ds 7
msrpc 7
rpcbind 7
http-proxy 6
imap 5
honeypot 4
ms-sql-s 4
rtsp 4
submission 3
50
100
150
200
250
300
350
400
تعداد


بیش ترین پورت باز
1723 (2.18%)
443 (45.96%)
80 (44.14%)
443
80
1723
179
25
500
123
53
2000
587
465
21
22
5060
8443



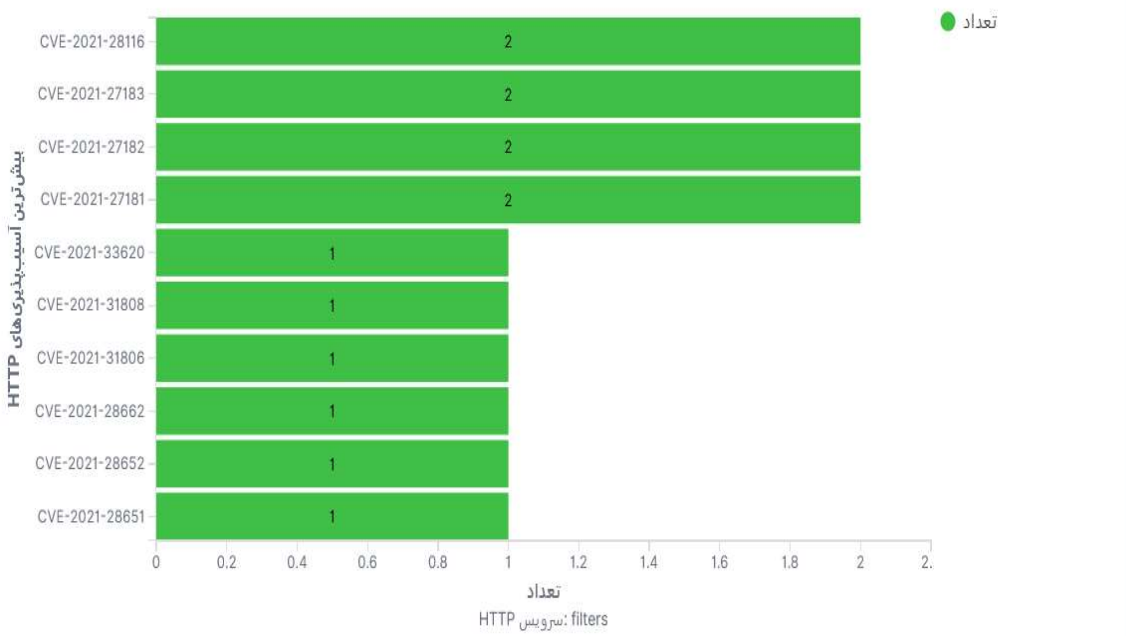


داشبورد


نوع تجهیزات
load balancer
security-misc
firewall
router
WAP
switch
storage-misc
WAP (3.19%)
router (9.57%)
firewall (13.83%)
ecurity-misc (21.28%)
load balancer (46.81%)

داشبورد

بیش‌ترین آسیب‌پذیری‌های HTTP



گواهی‌های منقضی شده سرویس https

بانک	آیپی	پورت	تاریخ انقضا	تعداد
پرداخت الکترونیک سامان کیش	91.24	443	Jul 9, 2022 @ 11:17:44.000	2
ملت	46.34	443	Apr 21, 2022 @ 04:29:59.000	2
پست بانک	217.2	443	Mar 16, 2018 @ 18:31:43.000	2
سپه	94.18	443	Jun 24, 2021 @ 04:51:24.000	2
سپه	94.18	443	Jun 24, 2021 @ 04:51:24.000	2
شهر	45.91	443	Mar 2, 2022 @ 10:43:52.000	2
شهر	45.91	443	Mar 2, 2022 @ 10:43:52.000	2
شاپرک	185.1	443	Apr 27, 2022 @ 15:07:29.000	2
شاپرک	185.1	443	Jun 16, 2022 @ 14:31:03.000	2
شاپرک	185.1	443	Apr 27, 2022 @ 15:07:29.000	2

180

Export: Raw Formatted

ویژگی‌های متمایز سامانه جویا

از جمله ویژگی‌هایی که این سامانه را از سایر سامانه‌های مشابه خارجی همچون Shodan متمایز می‌کند:

۱. قابلیت اسکن شبکه‌های داخلی و قابل دسترس از ایران (Iran Access)

۲. قابلیت بروزرسانی، پیکربندی و افزودن انواع پویشگرها و کدهای بهره‌برداری خاص منظوره

۳. قابلیت تولید انواع خروجی

۴. گردآوری کدهای بهره‌برداری آسیب‌پذیری

۵. زیرسامانه جستجو و بهره‌برداری خودکار آسیب‌پذیری که خود یک ویژگی متمایز نسبت به سایر موتورهای جستجوی آسیب‌پذیری می‌باشد که فاقد آن هستند.

۶. تشخیص Honeypotهای بد پیکربندی شده

با تشکر از توجه شما

آدرس ایمیل: cert@shahroodut.ac.ir

آدرس وبسایت: cert.shahroodut.ac.ir