مرکز تخصصی
آپا
دانشگاه صنعتی اصفهان
(آگاهی‌رسانی، پشتیبانی و امداد در حوزه شبکه)

گزارش سامانه جهاد خراسان جنوبی

تاریخ
شهریور ماه ۱۴۰۳

www.nsec.ir

1-1 مقدمه

این ارزیابی با شرایط ذیل انجام شده است:

نسخه مورد بررسی	
وب سرویس مورد استفاده	
نوع ارزیابی	

1-2 ارزیابی سرویس

طبق ارزیابی های انجام شده، موارد زیر در این سامانه مشاهده شد.

نام آسیب‌پذیری: آسیب پذیری bootstrap
آدرس آسیب‌پذیر: • http://darmian.kj-agrijahad.ir/media/jui/css/bootstrap-responsive.min.css •
سطح خطر: Medium CVSS 3 Score Details (**6.1**)
توضیح مختصر: برای این نسخه استفاده شده، آسیب پذیری وجود دارد
راه‌حل : برای اطلاعات بیشتر در مورد نحوه اکسپلویت و برطرف کردن آن به لینک زیر مراجعه کنید. https://nvd.nist.gov/vuln/detail/cve-2018-14041 https://github.com/prateek-77/RANGO/issues/2

نام آسیب‌پذیری: آسیب پذیری joomla
آدرس آسیب‌پذیر: • http://darmian.kj-agrijahad.ir/index.php/ •  kj-agrijahad.ir_repo rt_2024-8-28_at_12.4 •
سطح خطر: Medium 6.5
توضیح مختصر: ورژن استفاده شده از جوملا دارای آسیب پذیر Security Bypass میباشد.
راه‌حل : https://nvd.nist.gov/vuln/detail/CVE-2019-12764 استفاده از نسخه های بروز تر و بالاتر.

نام آسیب‌پذیری: آسیب پذیری joomla
آدرس آسیب‌پذیر: • http://darmian.kj-agrijahad.ir/index.php/ •  kj-agrijahad.ir_repo rt_2024-8-28_at_12.4 •
سطح خطر: Critical 9.8
توضیح مختصر: ورژن استفاده شده از جوملا دارای آسیب پذیری CSV Injection میباشد.
راه‌حل : https://nvd.nist.gov/vuln/detail/CVE-2019-12765 استفاده از نسخه های بروز تر و بالاتر.

نام آسیب‌پذیری: آسیب پذیری idor
آدرس آسیب‌پذیر: • https://www.kj-agrijahad.ir/form/proposal/form/answer.php • https://www.kj-agrijahad.ir/form/proposal/form/index2.php?id=1 •
سطح خطر: High 7.5
توضـــیح مختصـــر: به کمک لینک دوم که idor میخورد، میتوانیم مقدار پارامتر id را تغییر بدهیم(برای مثال 157) و کد رهگیری دیگران را برداریم. حال به کمک لینک اول ، کد رهگیری را وارد میکنیم و اطلاعات شخ صی رو مشاهده میکنیم. لازم به ذکر است که الان لینک اول از دسترس خارج شده است!
راه‌حل : استفاده از شناسه‌های غیرقابل حدس : از شناسه‌های غیرقابل حدس مانند UUID یا GUID به جای اعداد ترتیبی استفاده کنید. این شناسه‌ها به راحتی توسط کاربران قابل تغییر و حدس نیستند، که از دستکاری و دسترسی غیرمجاز جلوگیری می‌کند.

نام آسیب‌پذیری: آسیب پذیری login
آدرس آسیب‌پذیر: • https://kj-agrijahad.ir/administrator/ •
سطح خطر: Medium 5.3
توضیح مختصر: صفحه لاگین ، بدون کپچا می باشد که باعث میشود به راحتی بروت فورس بخورد.
راه‌حل : استفاده از کپچا برای صفحات لاگین

نام آسیب‌پذیری: آسیب پذیری file uploud
آدرس آسیب‌پذیر: • http://kj-agrijahad.ir/index.php?option=com_formmehr&view=forms •
سطح خطر: Medium 6.5
توضیح مختصر: در انتهای صفحه ؛ یک فایل آپلودر وجود دارد که ، پسوند فایل را چک نمیکند و به دلیل تغییر نکردن کپچا میتوان به تعداد زیادی فایل آپلود کرد.
راه‌حل : استفاده از کپچا های متفاوت برای هر ریکویست و محدود کردن پسوند فایل های دریافتی.

نقص های طراحی سایت:

در ساب دامین های سایت ، مشخصات یک فرد آورده شده که احتمالا مشخصات طراح سایت باشد:
https://reza.kj-agrijahad.ir

صفحات و ساب دامین های خالی بسیاری وجود دارد. برای مثال:

https://tender.kj-agrijahad.ir
/https://newn.kj-agrijahad.ir

مطالب اشتباه بسیاری در سرتاسر وبسایت قابل مشاهده است:

از بودن پوشه ای به نام (لللللللللللللل):

https://ferdos.kj-agrijahad.ir/index.php/2019-06-27-10-46-08

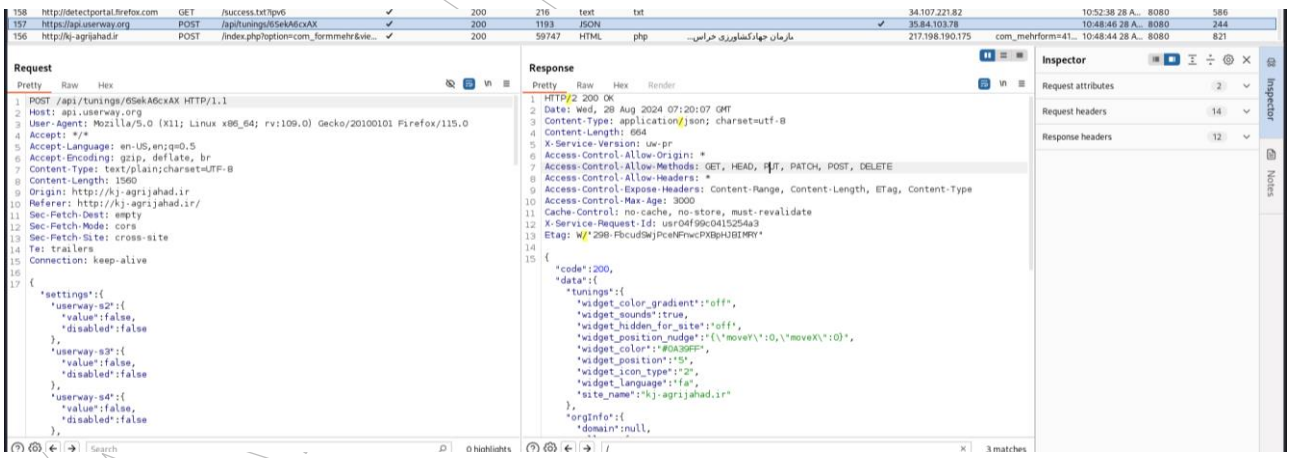
تا صفحه ای که در آن مشخصات خودرو آماده است!! :

http://darmian.kj-agrijahad.ir/index.php?option=com_rsform&formId=4

در بخش ارتباط با رییس :

/https://kj-agrijahad.ir/index.php/manager

از api استفاده میشود که تمامی هدر ها و متد ها برای یوزر باز است و می تواند از هدر ها و متد های مختلفی استفاده کند.



همچنین میتوان با متد PATCH به api/admin/ وصل شد، که اگر دسترسی به سایت داشتیم ، احتمال یافتن ادامه مسیر api محقق میشد.

ارسال ایمیل از طرف سایت:

به کمک idor میتوان مسیر هایی از وبسایت را یافت که از طریق پنل وبسایت دسترسی به آنها ناممکن است.

به کمک لینک زیر:

https://ferdos.kj-agrijahad.ir/index.php?option=com_rsform&formId=2

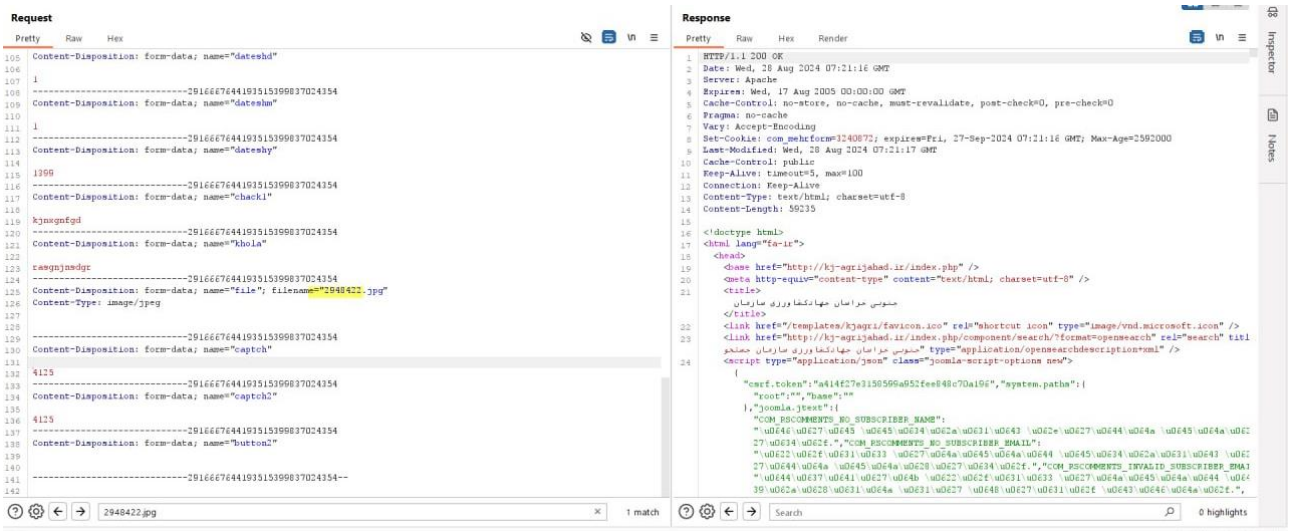
میتوان از طرف سایت ایمیل زد.

کد کپچا:

در سایت ، فرم های مختلفی برای وارد کردن اطلاعات، نظرها و ... وجود دارد.

در اکثر این بخش ها کد کپچایی وجود دارد که به راحتی میتوان بای پس کرد.

همانطور که در تصویر زیر مشخص است ، کد کپچا در ریکوست اماده است که به راحتی می توان آنرا برداشت و در قسمت پایینی نوشت !.



Robots.txt:

در تمامی ساب دامین ها و دامین اصلی سایت ، یوزر به این فایل دسترسی دارد و میتواند به بعضی از اطلاعات به راحتی دست پیدا کند.

بهتر است که دسترسی این فایل محدود شود.

https://kj-agrijahad.ir/robots.txt

صفحه forum :

http://forum.kj-agrijahad.ir/

در صفحه forum ارور هایی از سمت سرور قابل مشاهده است که در حالت عادی به کاربر نباید نشان داده شود.