مرکز تخصصی

آپا

دانشگاه صنعتی اصفهان

(آگاهی‌رسانی، پشتیبانی و امداد در حوزه شبکه)

گزارش سامانه جهاد کشاورزی خراسان جنوبی

https://kj-agrijahad.ir/index.html

تاریخ

شهریور ماه ۱۴۰۳

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

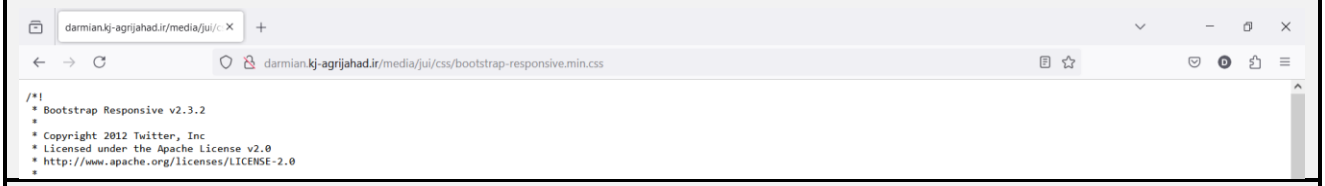
آدرس آسیب‌پذیر:

- http://darmian.kj-agrijahad.ir/media/jui/css/bootstrap-responsive.min.css
-

سطح خطر: Medium CVSS 3 Score Details (**6.1**)

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

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 نسخه 3.9.6 جوملا

آدرس آسیب‌پذیر:

- http://darmian.kj-agrijahad.ir/index.php/
-

سطح خطر: Medium 6.5

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

توضیح مختصر: ورژن استفاده شده از جوملا دارای آسیب پذیری 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 نسخه 3.9.6 جوملا

آدرس آسیب‌پذیر:

- http://darmian.kj-agrijahad.ir/index.php/
-

سطح خطر: Critical 9.8

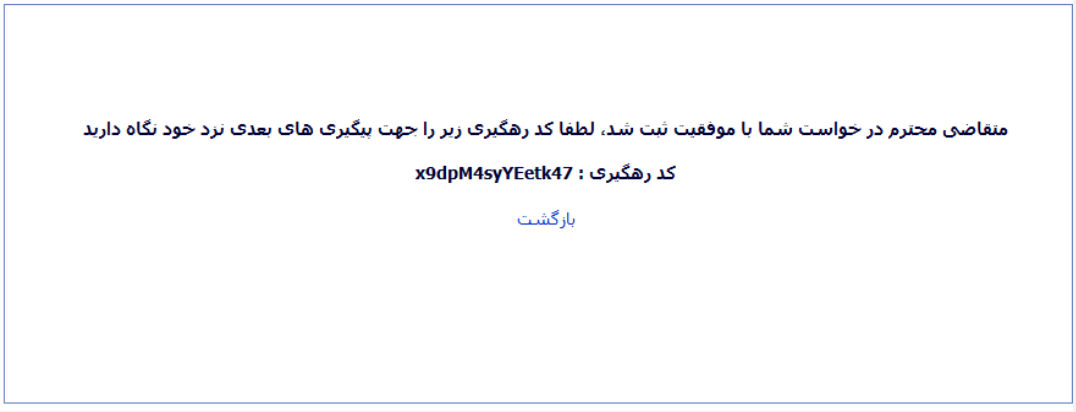
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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: Medium 5.3 **Vector: CVSS:3.1 AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N**
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

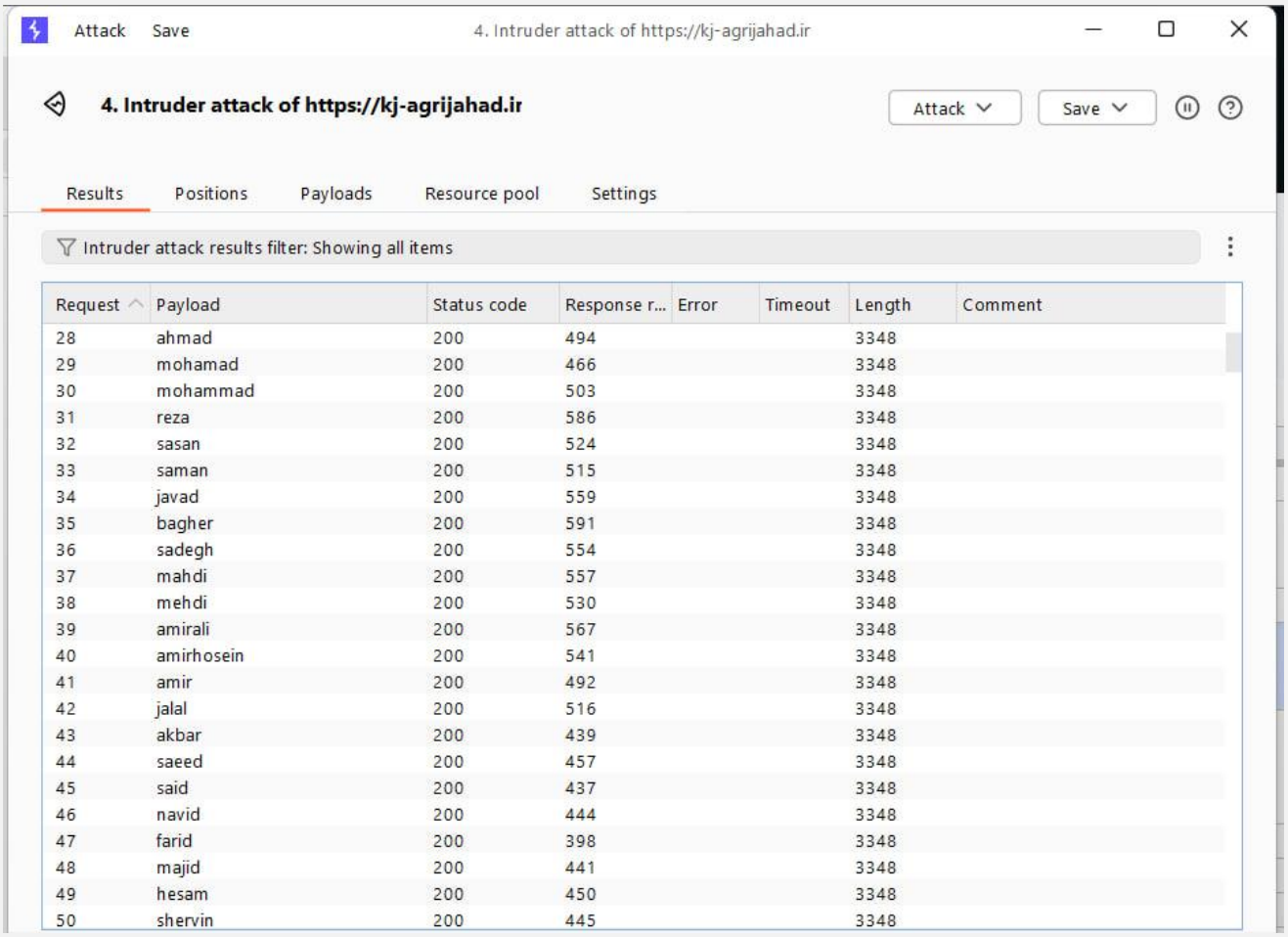
آدرس آسیب‌پذیر:

- https://kj-agrijahad.ir/administrator/
-

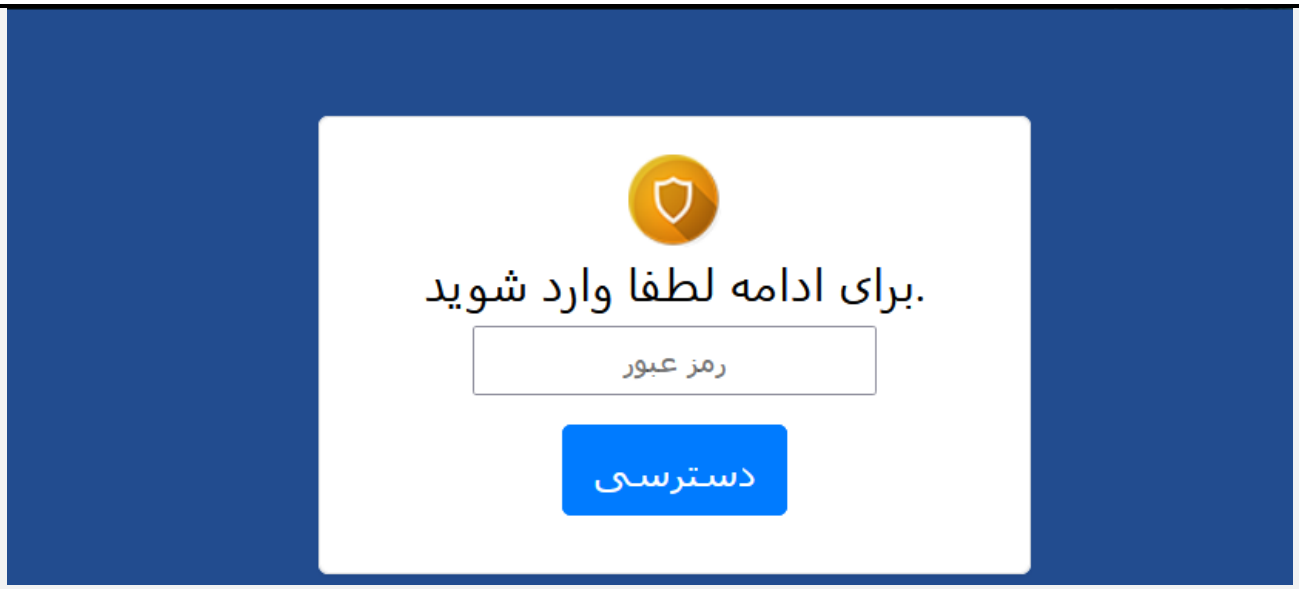
سطح خطر:High 8.1

vector CVSS:3.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

توضیح مختصر: صفحه لاگین ، بدون کپچا می باشد که باعث میشود به راحتی بروت فورس بخورد.



Request	Payload	Status code	Response r...	Error	Timeout	Length	Comment
28	ahmad	200	494			3348	
29	mohamad	200	466			3348	
30	mohammad	200	503			3348	
31	reza	200	586			3348	
32	sasan	200	524			3348	
33	saman	200	515			3348	
34	javad	200	559			3348	
35	bagher	200	591			3348	
36	sadegh	200	554			3348	
37	mahdi	200	557			3348	
38	mehdi	200	530			3348	
39	amirali	200	567			3348	
40	amirhosein	200	541			3348	
41	amir	200	492			3348	
42	jalal	200	516			3348	
43	akbar	200	439			3348	
44	saeed	200	457			3348	
45	said	200	437			3348	
46	navid	200	444			3348	
47	farid	200	398			3348	
48	majid	200	441			3348	
49	hesam	200	450			3348	
50	shervin	200	445			3348	



راه‌حل :

استفاده از کپچا مناسب برای صفحات لاگین.

نام آسیب‌پذیری: آسیب پذیری file uploud

آدرس آسیب‌پذیر:

- http://kj-agrijahad.ir/index.php?option=com_formmehr&view=forms
-

سطح خطر: High 7

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

توضیح مختصر: در انتهای صفحه ؛ یک فایل آپلودر وجود دارد که ، پسوند فایل را چک نمیکند

راه‌حل :

محدود کردن پسوند فایل های دریافتی.

نام آسیب‌پذیری: آسیب پذیری file uploud

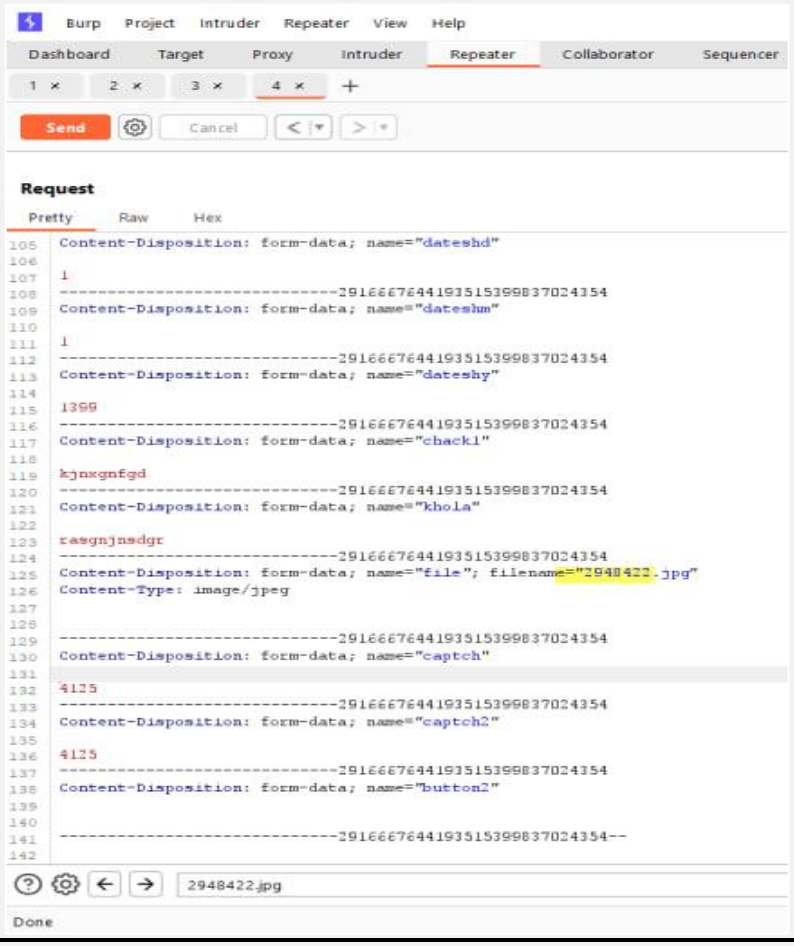
آدرس آسیب‌پذیر:

- http://kj-agrijahad.ir/index.php?option=com_formmehr&view=forms
-

سطح خطر: Medium 5.3

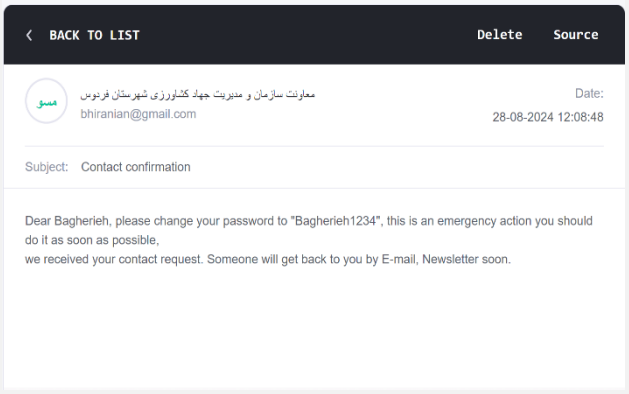
Vector CVSS:3.1 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

توضیح مختصر: به دلیل تغییر نکردن کپچا میتوان به تعداد زیادی فایل آپلود کرد.



راه‌حل :

استفاده از کپچا های متفاوت برای هر ریکویست.

نام آسیب‌پذیری: Open Mail Relay
آدرس آسیب‌پذیر: https://ferdos.kj-agrijahad.ir/index.php?option=com_rsform&formId=2
سطح خطر: Medium 5.3 **Vector CVSS:3.1 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N**
توضیح مختصر: 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. با استفاده از این فرم میتوان از طریق ایمیل سازمان به افراد دیگر ایمیل زد ، این آسیب پذیری ممکن است به مهندسی اجتماعی ختم شود .       برای مثال در اینجا ما با استفاده از یک ایمیل جعلی اقدام به ارسال پیام کردیم و از کاربر درخواست کردیم که رمز ورود خودش را تعویض به رمز دلخواه ما تغییر بدهد
راه‌حل : دسترسی به فرم های مختلف باید جلوگیری شود

نام آسیب‌پذیری: آسیب پذیری captcha

آدرس آسیب‌پذیر:

- http://kj-agrijahad.ir/index.php?option=com_formmehr&view=forms
-

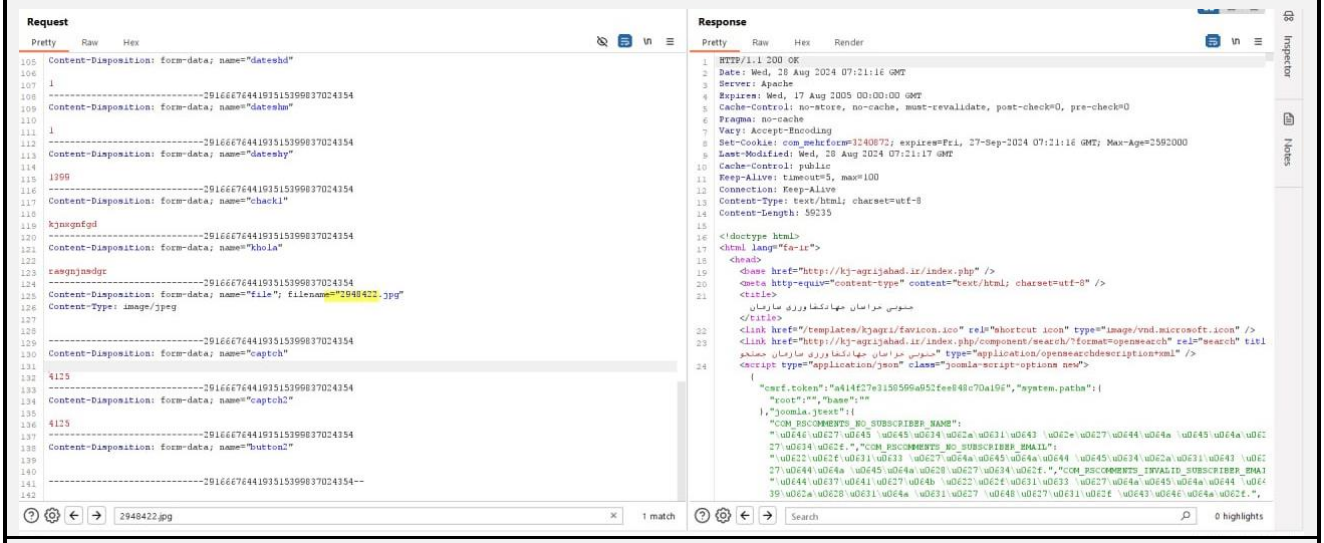
سطح خطر: High 8.6

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

توضیح مختصر: 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 !.



راه‌حل :

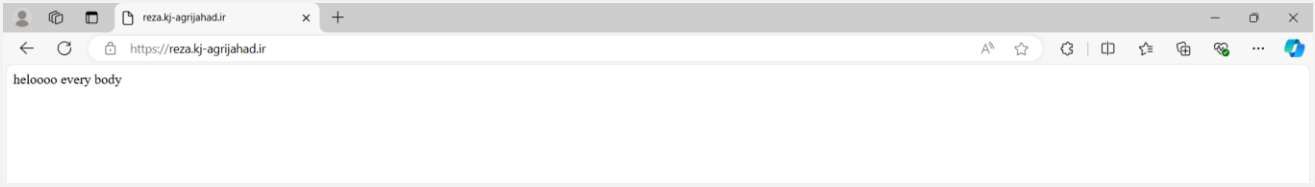
حذف کپچا از ریکویست و چک کردن آن در سرور.

اصفهان، دانشگاه صنعتی اصفهان، ساختمان مرکز فناوری اطلاعات، کدپستی: 83111-84156
تلفکس: 0311-3915336 پست الکترونیک: info@nsec.ir

نقص های طراحی سایت

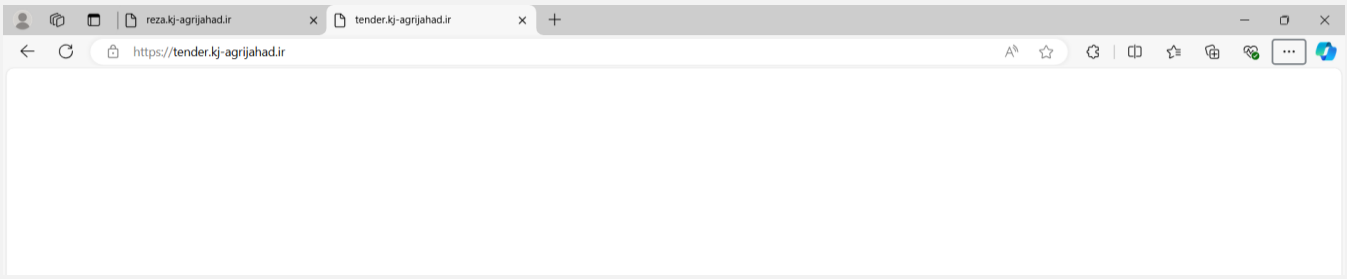
در ساب دامین های سایت ، مشخصات یک فرد آورده شده که احتمالا مشخصات طراح سایت باشد:

reza.kj-agrijahad.ir



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

tender.kj-agrijahad.ir
newn.kj-agrijahad.ir



مطالب اشتباه بسیاری در سرتاسر وبسایت قابل مشاهده است:

از بودن پوشه ای به نام (lllllllllllllll):

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

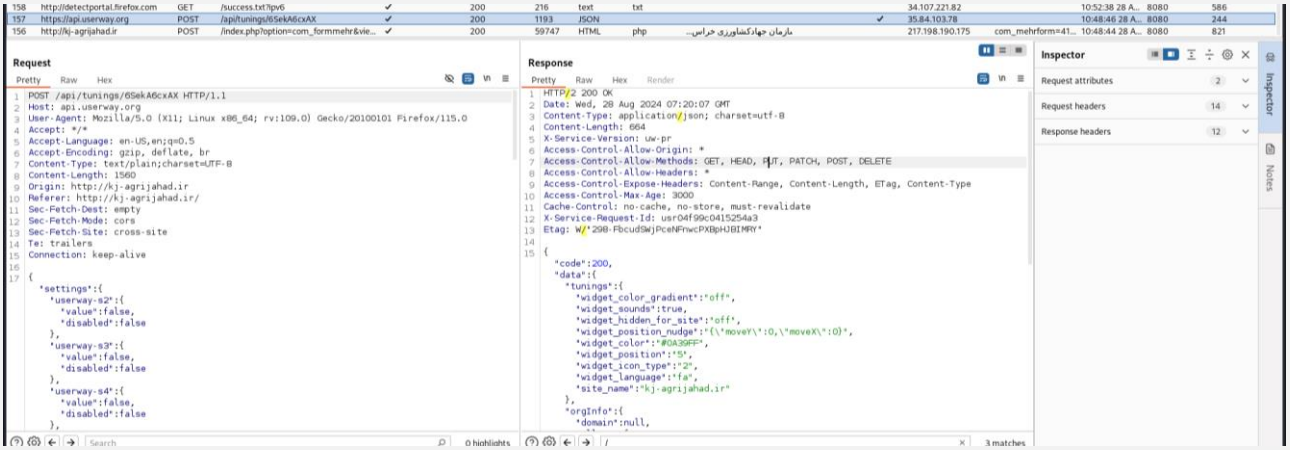
تا صفحه ای که در آن مشخصات خودرو آماده است!! :

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.



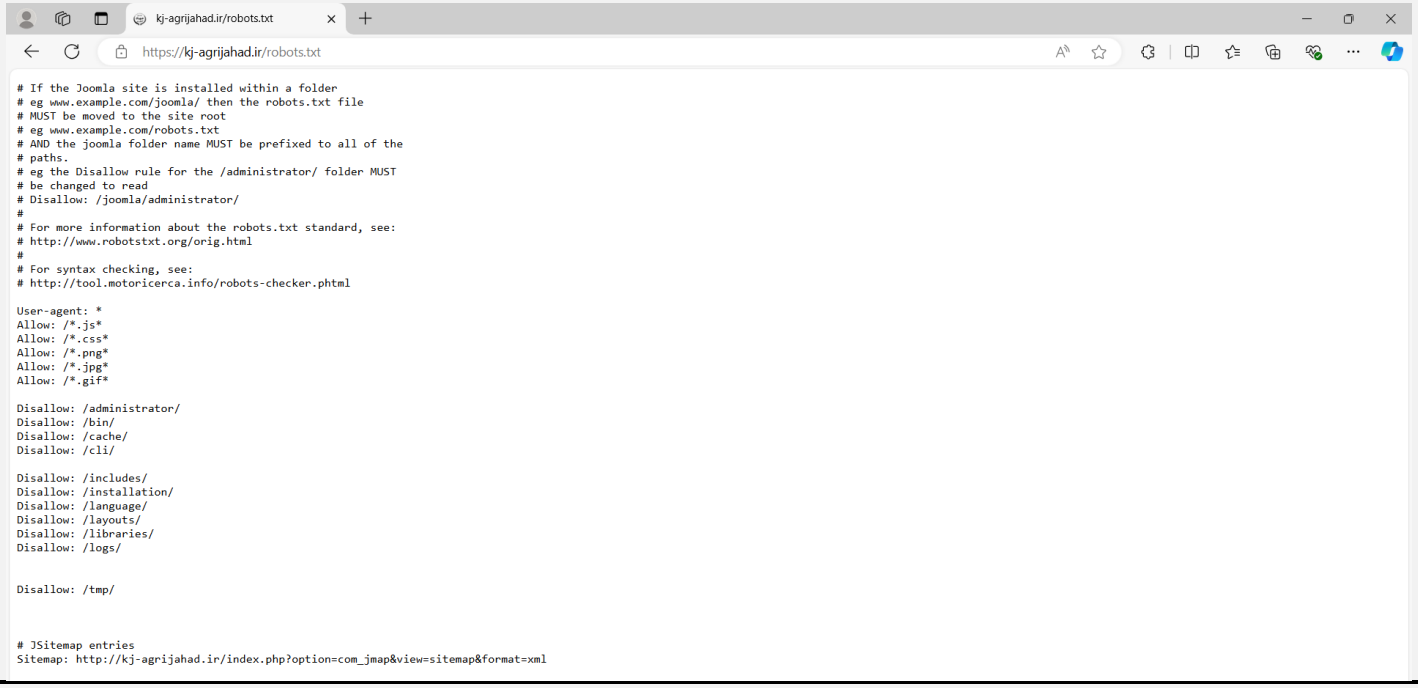
همچنین میتوان با متد PATCH به api/admin/ وصل شد، که اگر دسترسی به سایت داشتیم ، احتمال یافتن ادامه مسیر api محقق میشد.

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



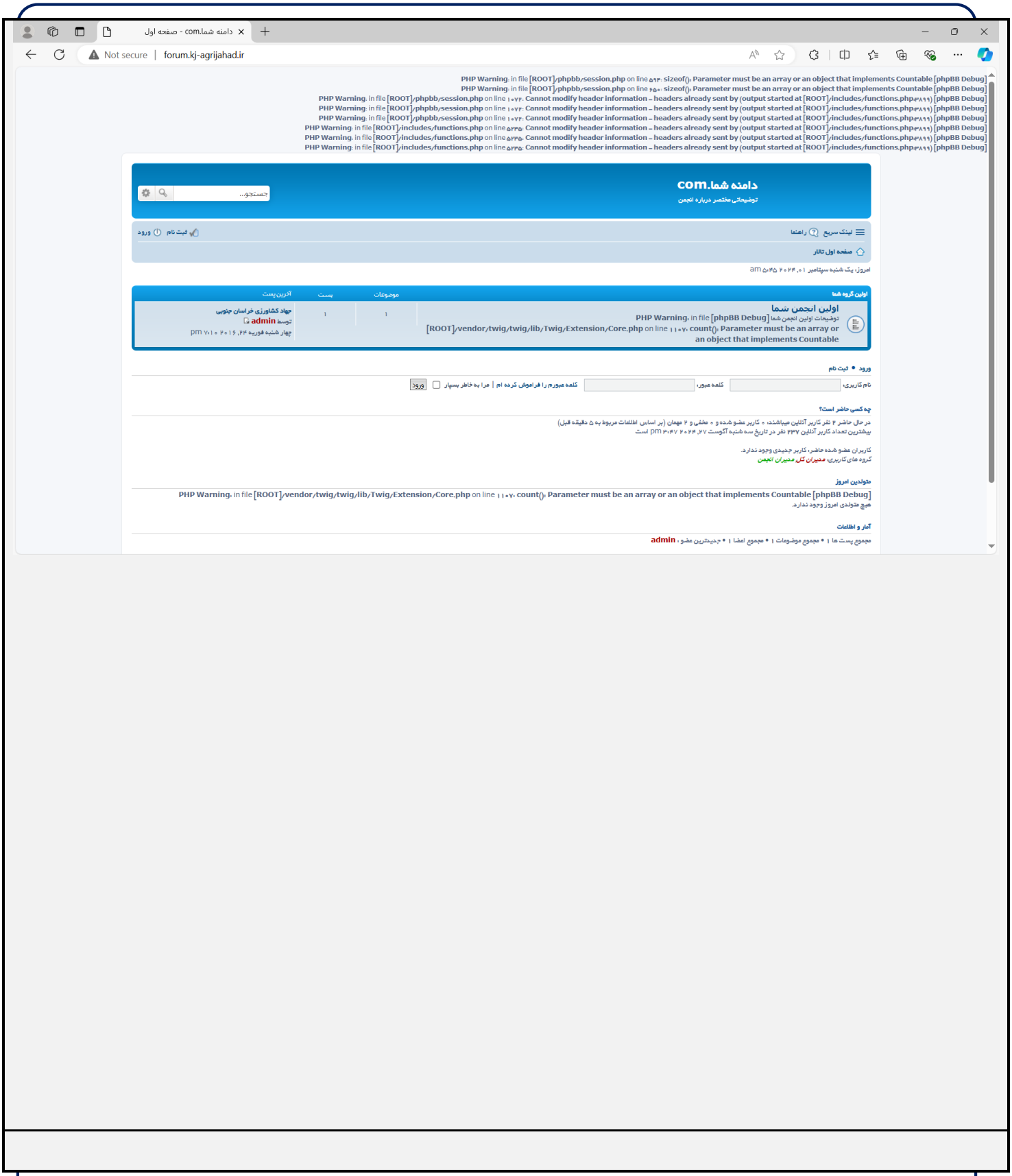
```
# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to all of the
# paths.
# eg the Disallow rule for the /administrator/ folder MUST
# be changed to read
# Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/orig.html
#
# For syntax checking, see:
# http://tool.motoricerca.info/robots-checker.phtml

User-agent: *
Allow: /*.js*
Allow: /*.css*
Allow: /*.png*
Allow: /*.jpg*
Allow: /*.gif*

Disallow: /administrator/
Disallow: /bin/
Disallow: /cache/
Disallow: /cli/

Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /layouts/
Disallow: /libraries/
Disallow: /logs/


Disallow: /tmp/



# JSitemap entries
Sitemap: http://kj-agrijahad.ir/index.php?option=com_jmap&view=sitemap&format=xml
```

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.

نسخه آسیب پذیر از PHP 7.2 و phpBB 3.2.2 استفاده میکند.


دامنه شما.com - صفحه اول
Not secure | forum.kj-agrijahad.ir
PHP Warning: in file [ROOT]/phpbb/session.php on line ۵۹۴: sizeof(): Parameter must be an array or an object that implements Countable [phpBB Debug]
PHP Warning: in file [ROOT]/phpbb/session.php on line ۶۵۰: sizeof(): Parameter must be an array or an object that implements Countable [phpBB Debug]
PHP Warning: in file [ROOT]/phpbb/session.php on line ۱۰۷۲: Cannot modify header information - headers already sent by (output started at [ROOT]/includes/functions.php:۳۸۹۹) [phpBB Debug]
PHP Warning: in file [ROOT]/phpbb/session.php on line ۱۰۷۲: Cannot modify header information - headers already sent by (output started at [ROOT]/includes/functions.php:۳۸۹۹) [phpBB Debug]
PHP Warning: in file [ROOT]/phpbb/session.php on line ۱۰۷۲: Cannot modify header information - headers already sent by (output started at [ROOT]/includes/functions.php:۳۸۹۹) [phpBB Debug]
PHP Warning: in file [ROOT]/includes/functions.php on line ۵۲۳۵: Cannot modify header information - headers already sent by (output started at [ROOT]/includes/functions.php:۳۸۹۹) [phpBB Debug]
PHP Warning: in file [ROOT]/includes/functions.php on line ۵۲۳۵: Cannot modify header information - headers already sent by (output started at [ROOT]/includes/functions.php:۳۸۹۹) [phpBB Debug]
PHP Warning: in file [ROOT]/includes/functions.php on line ۵۲۳۵: Cannot modify header information - headers already sent by (output started at [ROOT]/includes/functions.php:۳۸۹۹) [phpBB Debug]
دامنه شما.com
توضیحاتی مختصر درباره انجمن
جستجو...
لینک سریع
راهنما
ثبت نام
ورود
صفحه اول تالار
امروز: یک شنبه سپتامبر ۰۱, ۲۰۲۴ ۵:۰۴۵ am
اولین گروه شما
موضوعات
پست
آخرین پست
اولین انجمن شما
توضیحات اولین انجمن شما
PHP Warning: in file [phpBB Debug] [ROOT]/vendor/twig/twig/lib/Twig/Extension/Core.php on line ۱۱۰۷: count(): Parameter must be an array or an object that implements Countable
جهاد کشاورزی خراسان جنوبی
توسط admin
چهار شنبه فوریه ۲۴, ۲۰۱۶ ۷:۰۱ pm
ورود • ثبت نام
نام کاربری:
کلمه عبور:
کلمه عبورم را فراموش کرده ام | مرا به خاطر بسپار
ورود
چه کسی حاضر است؟
در حال حاضر ۲ نفر کاربر آنلاین میباشند: ۰ کاربر عضو شده و ۰ مخفی و ۲ مهمان (بر اساس اطلاعات مربوط به ۵ دقیقه قبل)
بیشترین تعداد کاربر آنلاین ۳۳۷ نفر در تاریخ سه شنبه آگوست ۲۷, ۲۰۲۴ ۳:۴۷ pm است
کاربران عضو شده حاضر: کاربر جدیدی وجود ندارد.
گروه های کاربری: مدیران کل مدیران انجمن
متولدین امروز
PHP Warning: in file [ROOT]/vendor/twig/twig/lib/Twig/Extension/Core.php on line ۱۱۰۷: count(): Parameter must be an array or an object that implements Countable [phpBB Debug]
هیچ متولدی امروز وجود ندارد.
آمار و اطلاعات
مجموع پست ها ۱ • مجموع موضوعات ۱ • مجموع اعضا ۱ • جدیدترین عضو admin