بسمه تعالی

گزارش اولیه کشف آسیب پذیری و تلاش برای نفوذ

Moj.Gov.Jo

شهریور ماه 1403

نسخه 1.0

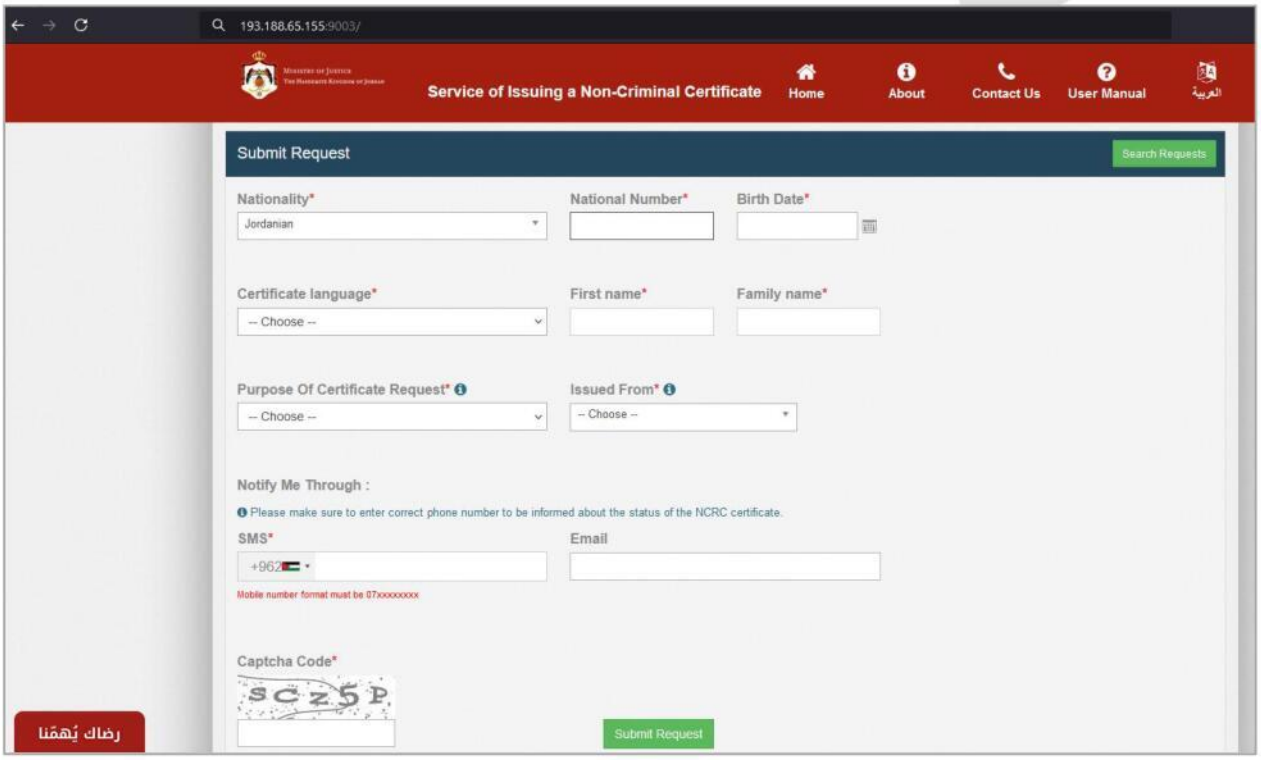
فهرست

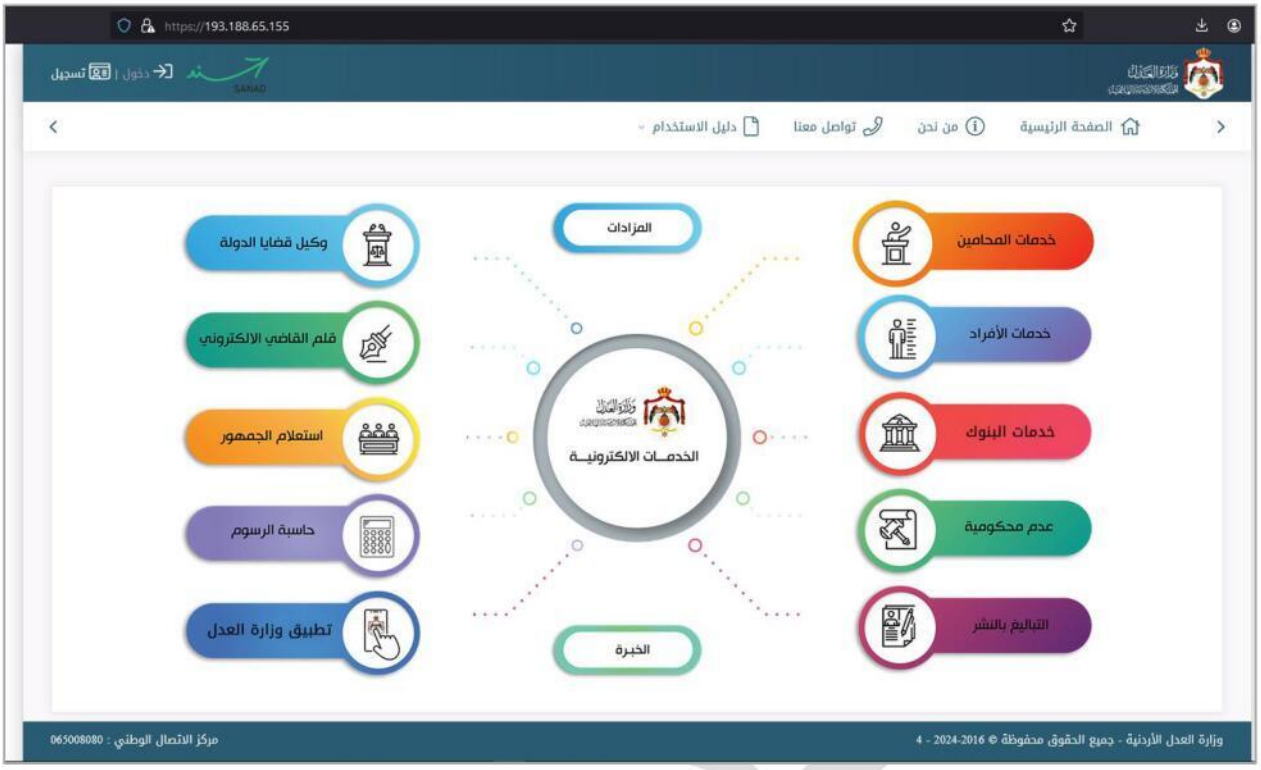
مقدمه

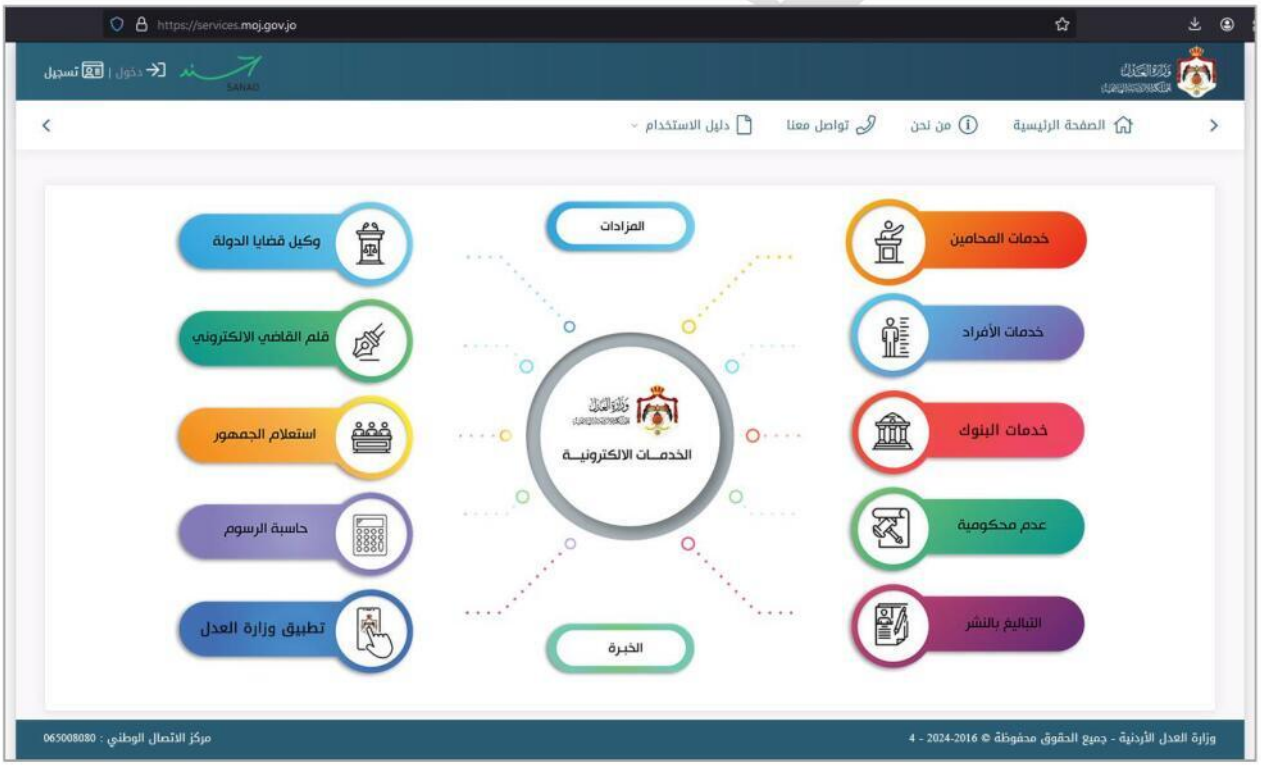
آدرس 193.188.65.155 منتهی به یک وب سایت زیر مجموعه وزارت دادگستری کشور اردن می‌باشد. طی بررسی‌های انجام گرفته تنها دامنه‌ای که مربوط به این آدرس IP می‌شود عبارت است از services.moj.gov.jo که این آدرس در واقع یکی از زیردامنه‌های آدرس moj.gov.jo بوده و محدوده رنج آی پی آن‌ها یکی می‌باشد که در این خصوص در بخش زیرساخت فنی بیشتر توضیح داده شده است. آدرس دامنه مذکور حاوی خدماتی به مردم و وکلا می‌باشد و در این خصوص فایل‌های PDF راهنما برای هر کدام نیز تهیه کرده و در وب سایت قرار داده است که در فایل‌های پیوست قابل مشاهده می‌باشد.

در سناریو حمله که انجام گرفت تمرکز بر روی همین IP، یعنی 193.188.65.155 و پورت 9003 بوده و در بخش پایانی نتیجه این حمله و همچنین کارهای آتی که با توجه به این تارگت می‌توان پیش برد، بیان شده است.

در ادامه تصاویری از این آدرس را در قالب وب مشاهده می‌نمایید.




https://193.188.65.155
تسجيل | دخول
الصفحة الرئيسية
من نحن
تواصل معنا
دليل الاستخدام
خدمات المحامين
خدمات الأفراد
خدمات البنوك
عدم محكومية
التبليغ بالنشر
المزادات
الخبرة
الخدمات الالكترونية
وكيل قضايا الدولة
قلم القاضي الالكتروني
استعلام الجمهور
حاسبة الرسوم
تطبيق وزارة العدل
وزارة العدل الأردنية - جميع الحقوق محفوظة © 2016-2024 - 4
مركز الاتصال الوطني : 065008080


https://services.moj.gov.jo
تسجيل | دخول
الصفحة الرئيسية
من نحن
تواصل معنا
دليل الاستخدام
خدمات المحامين
خدمات الأفراد
خدمات البنوك
عدم محكومية
التبليغ بالنشر
المزادات
الخبرة
الخدمات الالكترونية
وكيل قضايا الدولة
قلم القاضي الالكتروني
استعلام الجمهور
حاسبة الرسوم
تطبيق وزارة العدل
وزارة العدل الأردنية - جميع الحقوق محفوظة © 2016-2024 - 4
مركز الاتصال الوطني : 065008080

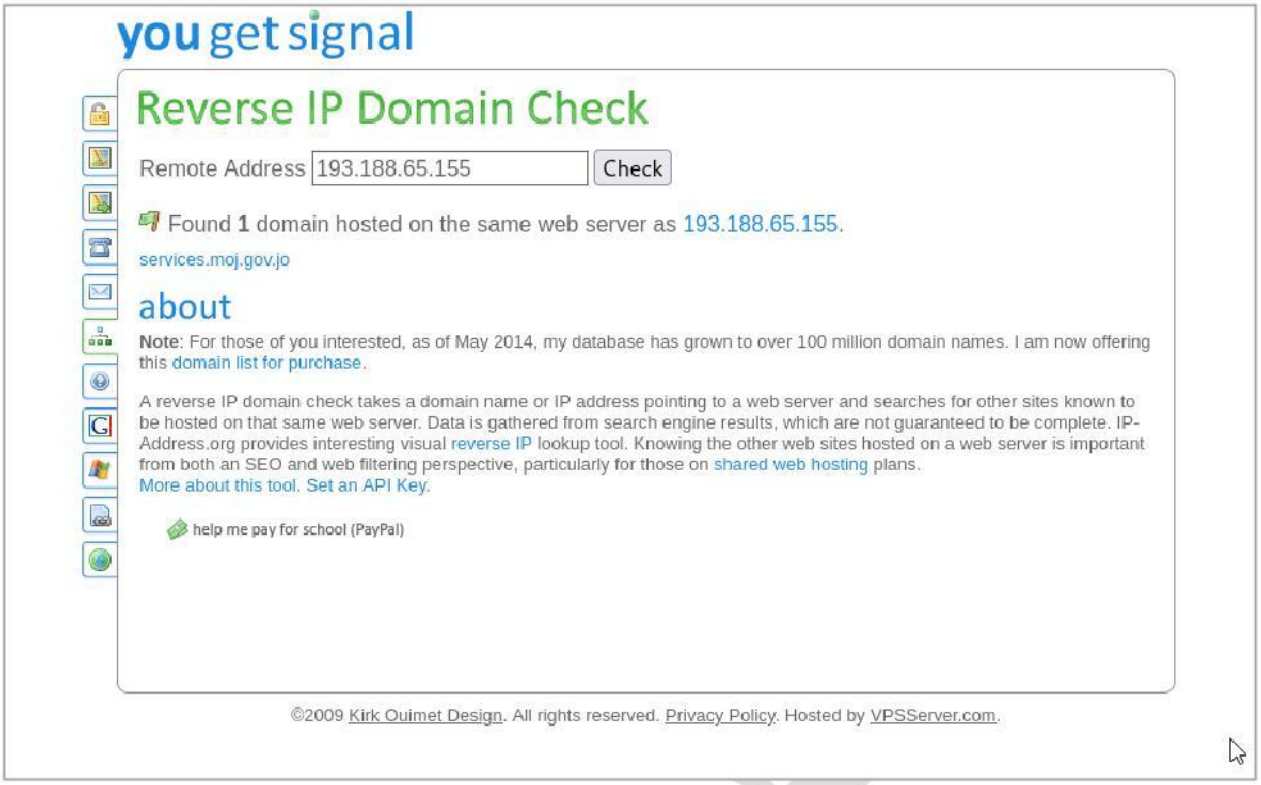
زیرساخت فنی تارگت services.moj.gov.jo

آدرس IP که به تارگت یعنی services.moj.gov.jo مربوط می‌شود عبارت است از 193.188.65.155 که این آدرس IP متعلق به خود کشور اردن بوده و پس از پویش پورت‌های آن نتایج زیر با توجه به ابزار Nmap حاصل شد.

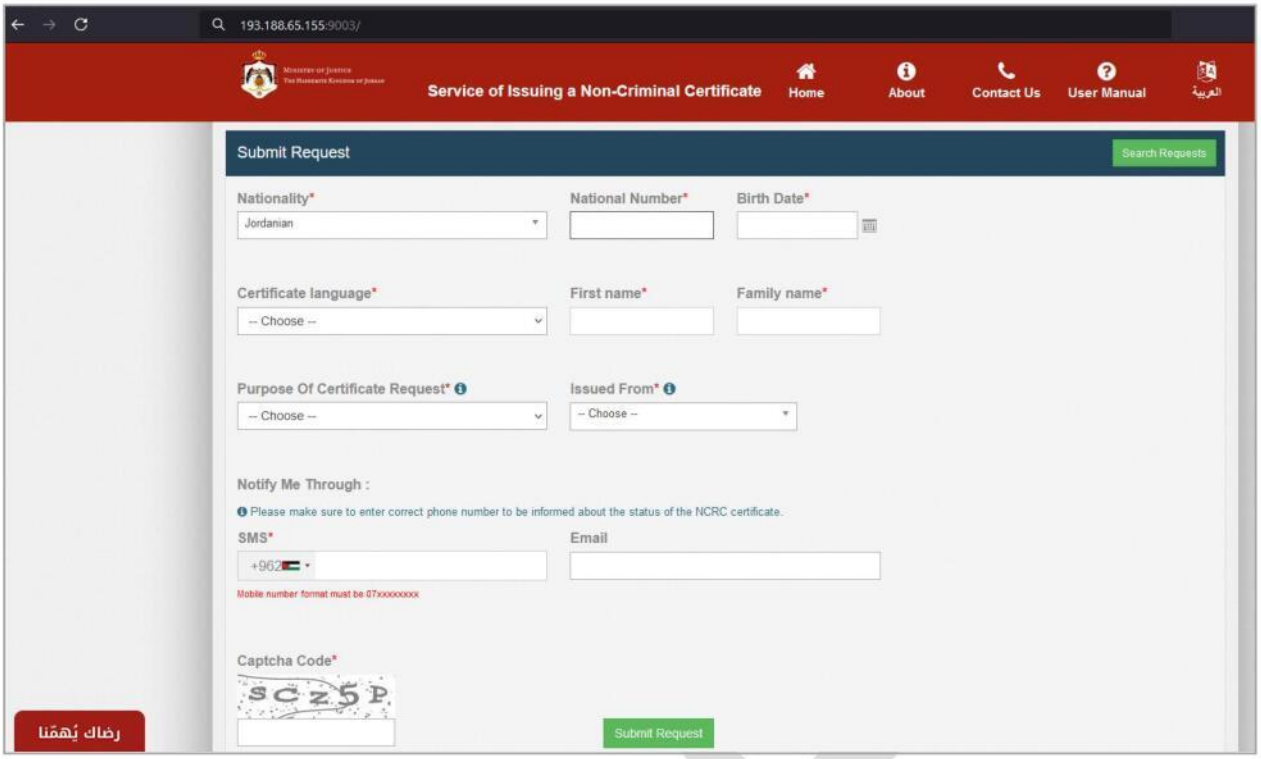
Port	Service	Version
443	https	-
9003	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9005	http	Apache https
9007	http	Microsoft IIS httpd 8.5
9008	ogs-server	-
9009	http	Microsoft IIS httpd 8.5
9010	http	Microsoft IIS httpd 10.0
9011	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9014	http	Microsoft IIS httpd 8.5
9015	http	Microsoft IIS httpd 8.5
9018	http	Microsoft IIS httpd 8.5
9020	http	Microsoft IIS httpd 8.5

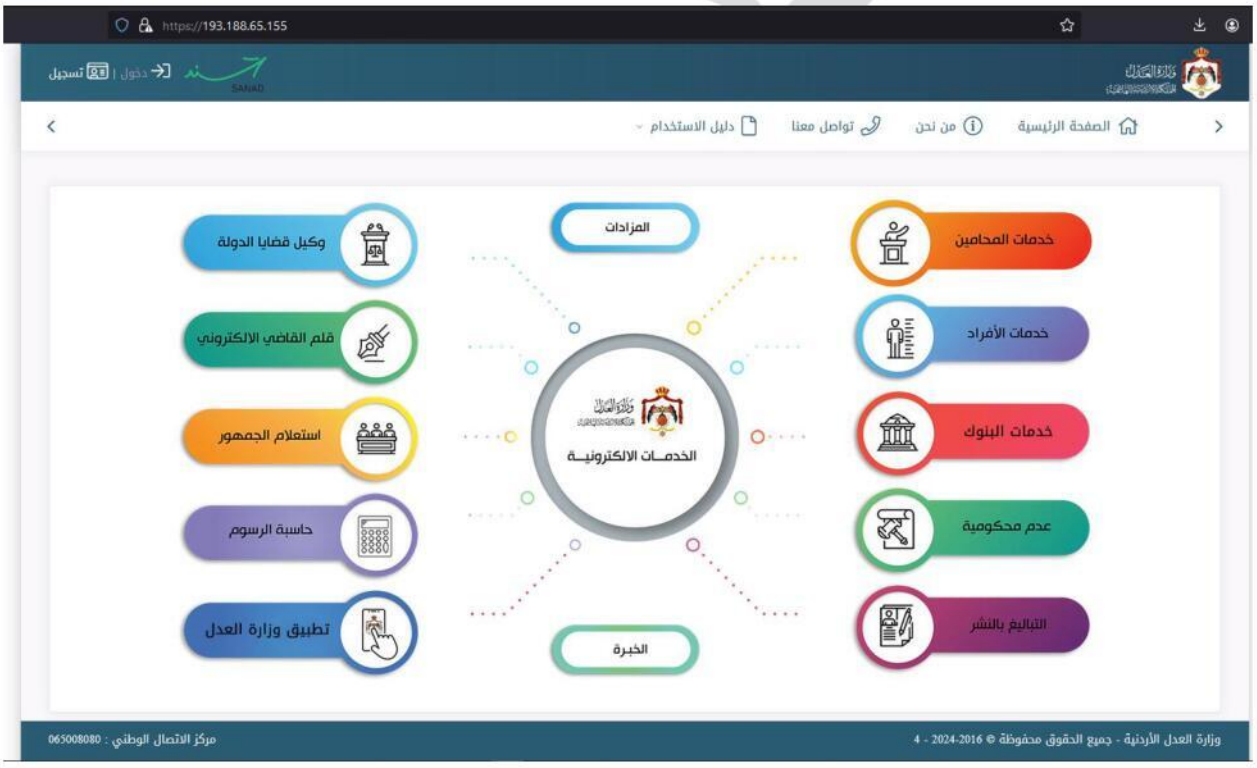
بر روی هر پورت از این سرور که در جدول بالا مشاهده می‌شود، یک سرویس وب و وب سایت راه‌اندازی شده است. لذا اینطور به نظر می‌رسد که بر روی این سرور وب سایت‌ها دیگری غیر از تارگت ما وجود داشته باشد.

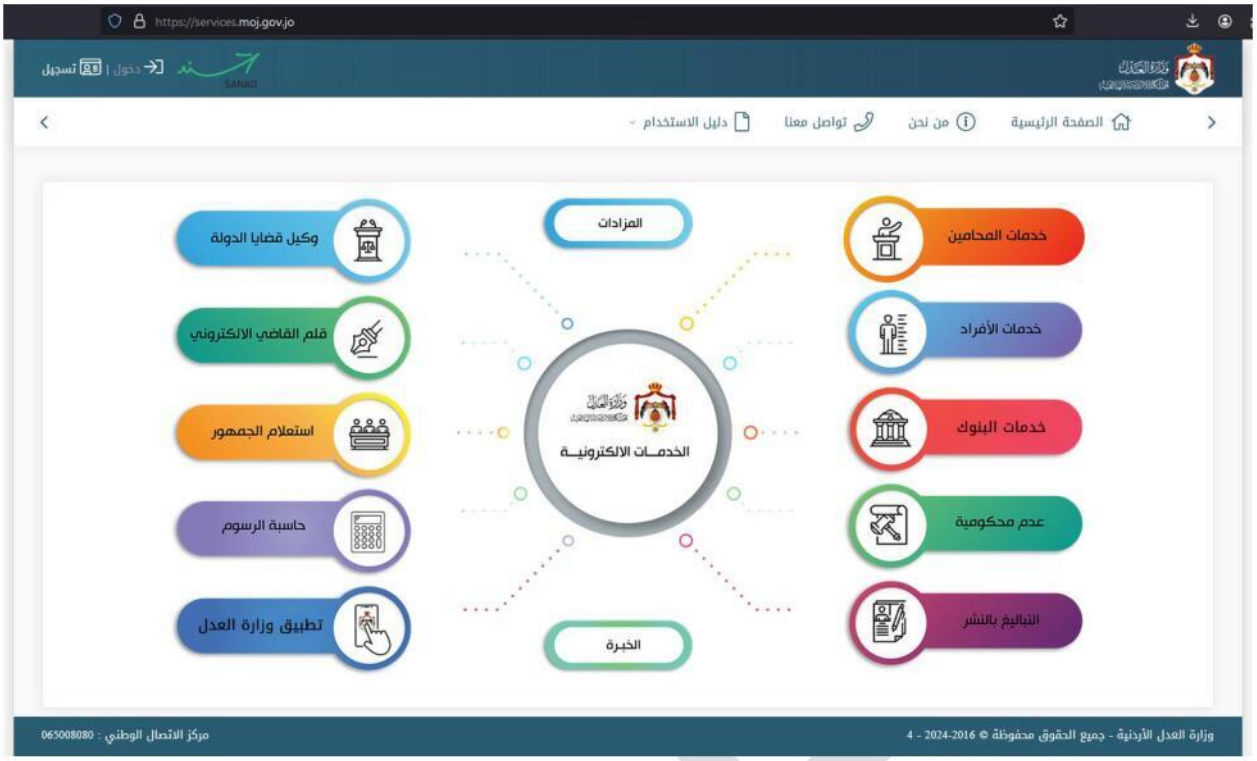
نتایج Reverse IP/Domain در ادامه آورده شده است. طبق این نتایج بر روی این آدرس IP فقط همان دامنه services.moj.gov.jo وجود دارد و رجیستر شده است. در حالی که بر روی پروت‌های مختلف وب سایت‌ها و سرویس‌ها مختلفی مشاهده می‌شود.

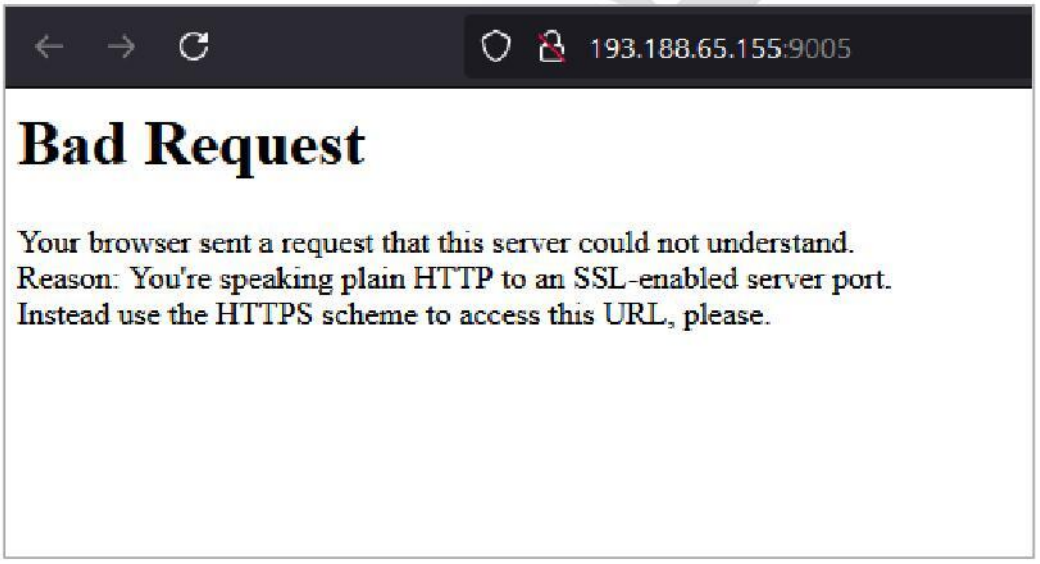


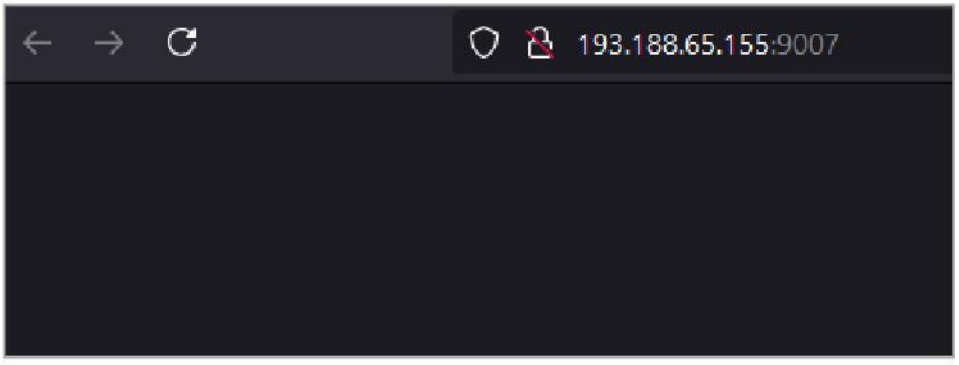
تصاویری از وب‌سایت‌ها و دیگر سرویس‌های موجود بر روی این آدرس IP در ادامه آورده شده است.


193.188.65.155:9003/
Service of Issuing a Non-Criminal Certificate
Home
About
Contact Us
User Manual
العربية
Submit Request
Search Requests
Nationality*
Jordanian
National Number*
Birth Date*
Certificate language*
-- Choose --
First name*
Family name*
Purpose Of Certificate Request*
-- Choose --
Issued From*
-- Choose --
Notify Me Through :
Please make sure to enter correct phone number to be informed about the status of the NCRC certificate.
SMS*
+962
Mobile number format must be 07xxxxxxxx
Email
Captcha Code*
scz5p
Submit Request
رضاك يُهمّنا


https://193.188.65.155
تسجيل
دخول
SANAD
الصفحة الرئيسية
من نحن
تواصل معنا
دليل الاستخدام
المزادات
وكيل قضايا الدولة
قلم القاضي الالكتروني
استعلام الجمهور
حاسبة الرسوم
تطبيق وزارة العدل
الخبرة
الخدمات الالكترونية
خدمات المحامين
خدمات الأفراد
خدمات البنوك
عدم محكومية
التبليغ بالنشر
مركز الاتصال الوطني : 065008080
وزارة العدل الأردنية - جميع الحقوق محفوظة © 2016-2024 - 4


https://services.moj.gov.jo
تسجيل | دخول
الصفحة الرئيسية
من نحن
تواصل معنا
دليل الاستخدام
خدمات المحامين
خدمات الأفراد
خدمات البنوك
عدم محكومية
التبليغ بالنشر
المزادات
الخبرة
وكيل قضايا الدولة
قلم القاضي الالكتروني
استعلام الجمهور
حاسبة الرسوم
تطبيق وزارة العدل
الخدمات الالكترونية
مركز الاتصال الوطني : 065008080
وزارة العدل الأردنية - جميع الحقوق محفوظة © 2016-2024 - 4


193.188.65.155:9005
Bad Request
Your browser sent a request that this server could not understand.
Reason: You're speaking plain HTTP to an SSL-enabled server port.
Instead use the HTTPS scheme to access this URL, please.

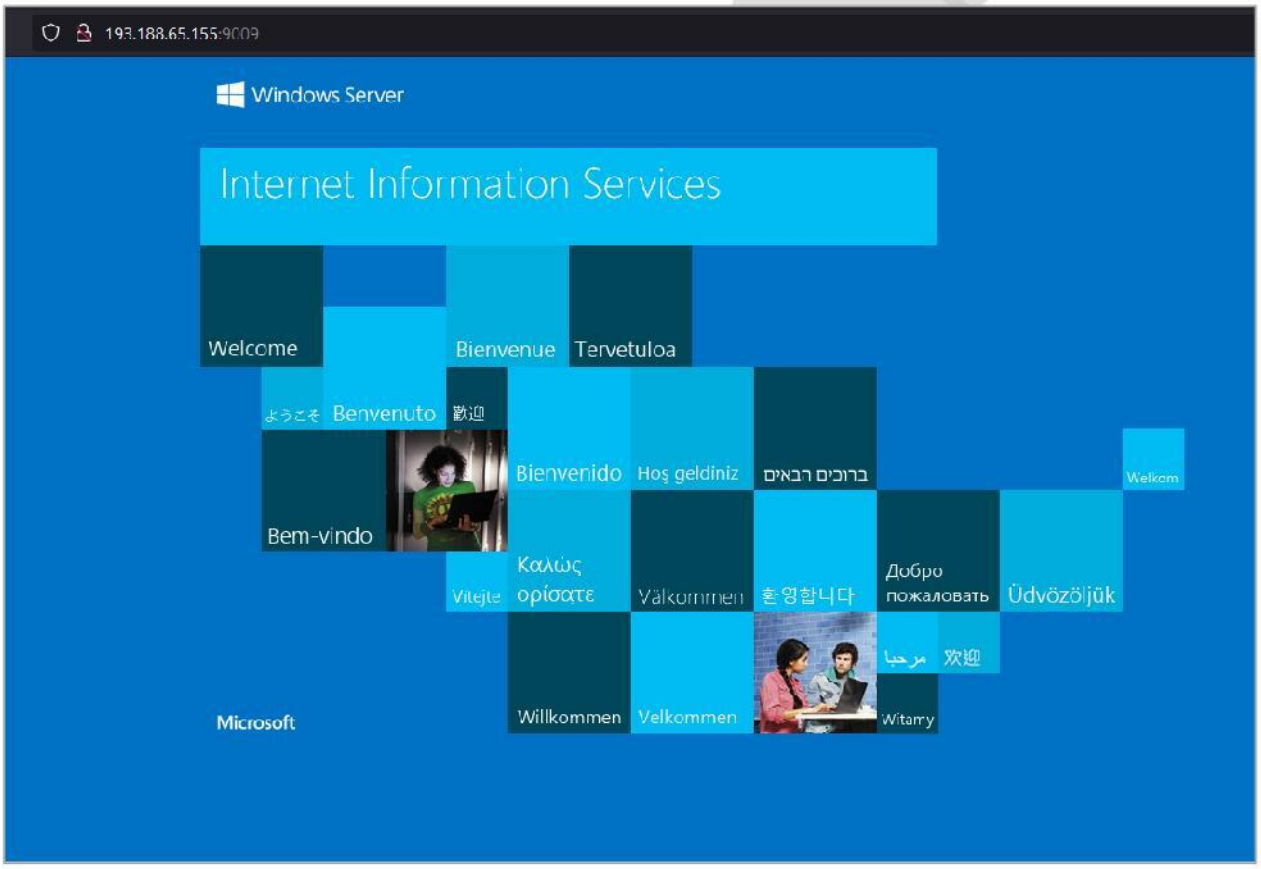

193.188.65.155:9007

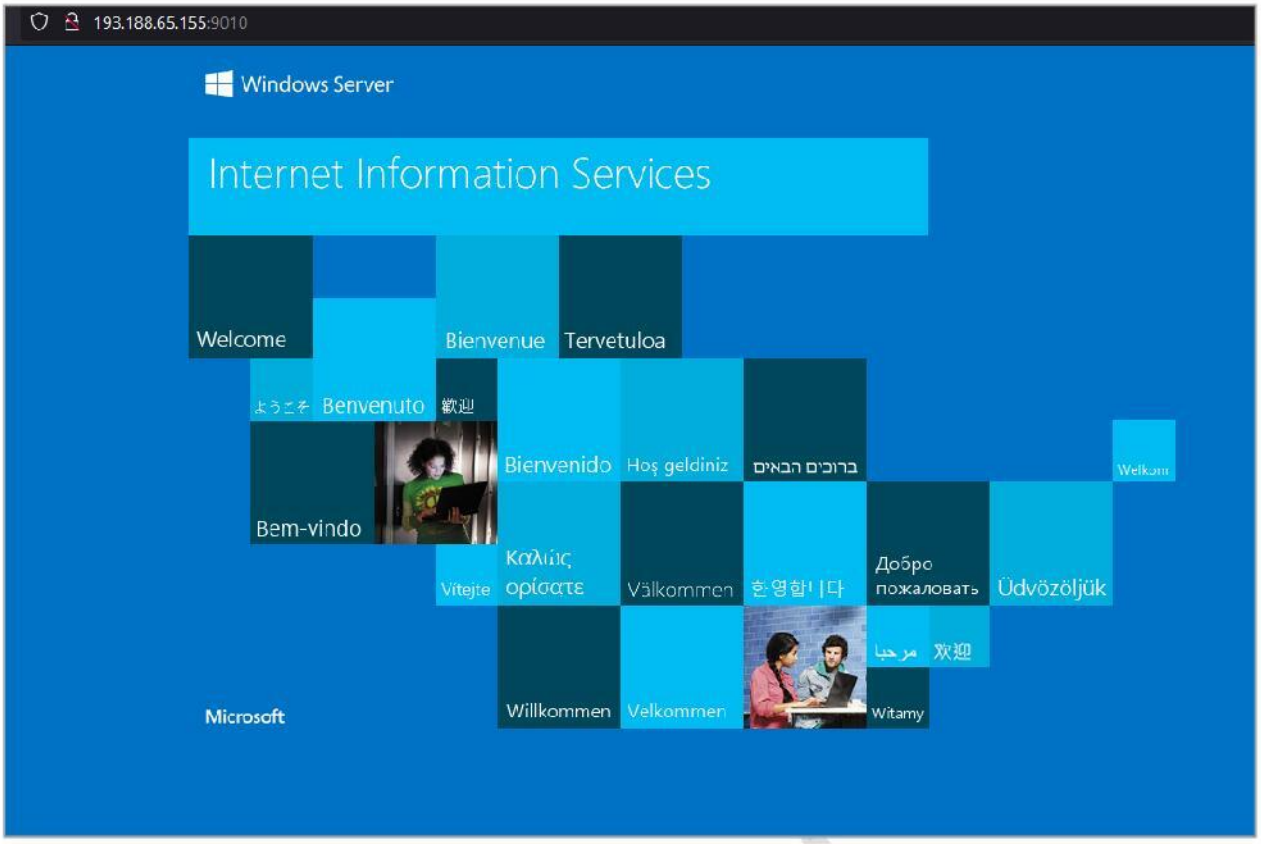
193.188.65.155:9008

Whitelabel Error Page

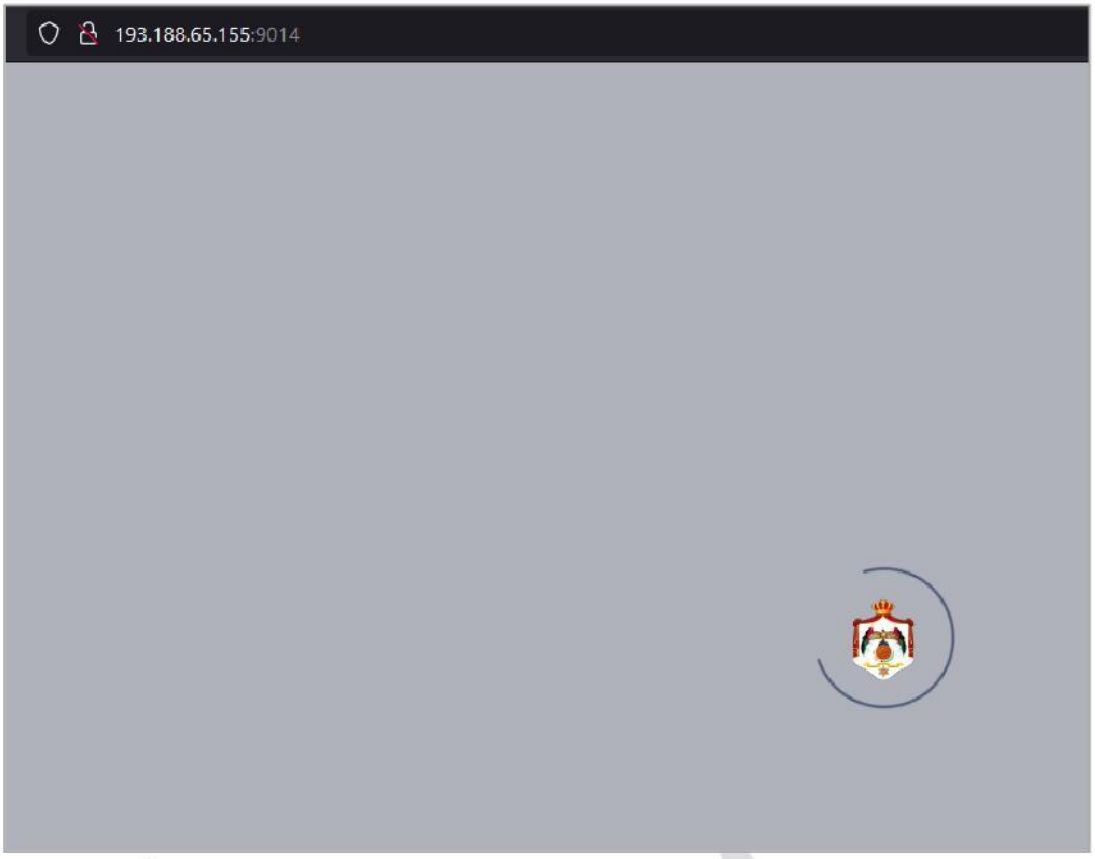
This application has no explicit mapping for /error, so you are seeing this as a fallback.

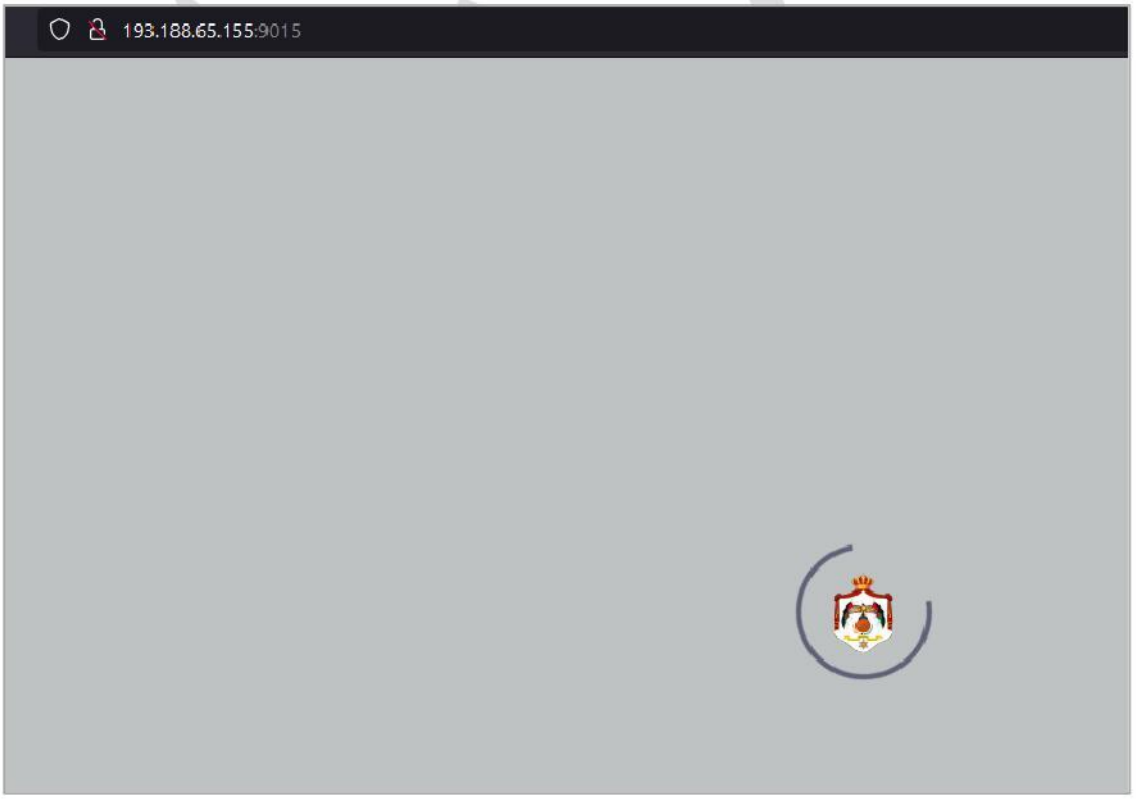
Sat Sep 14 11:12:09 AST 2024
There was an unexpected error (type=Not Found, status=404).
Not Found

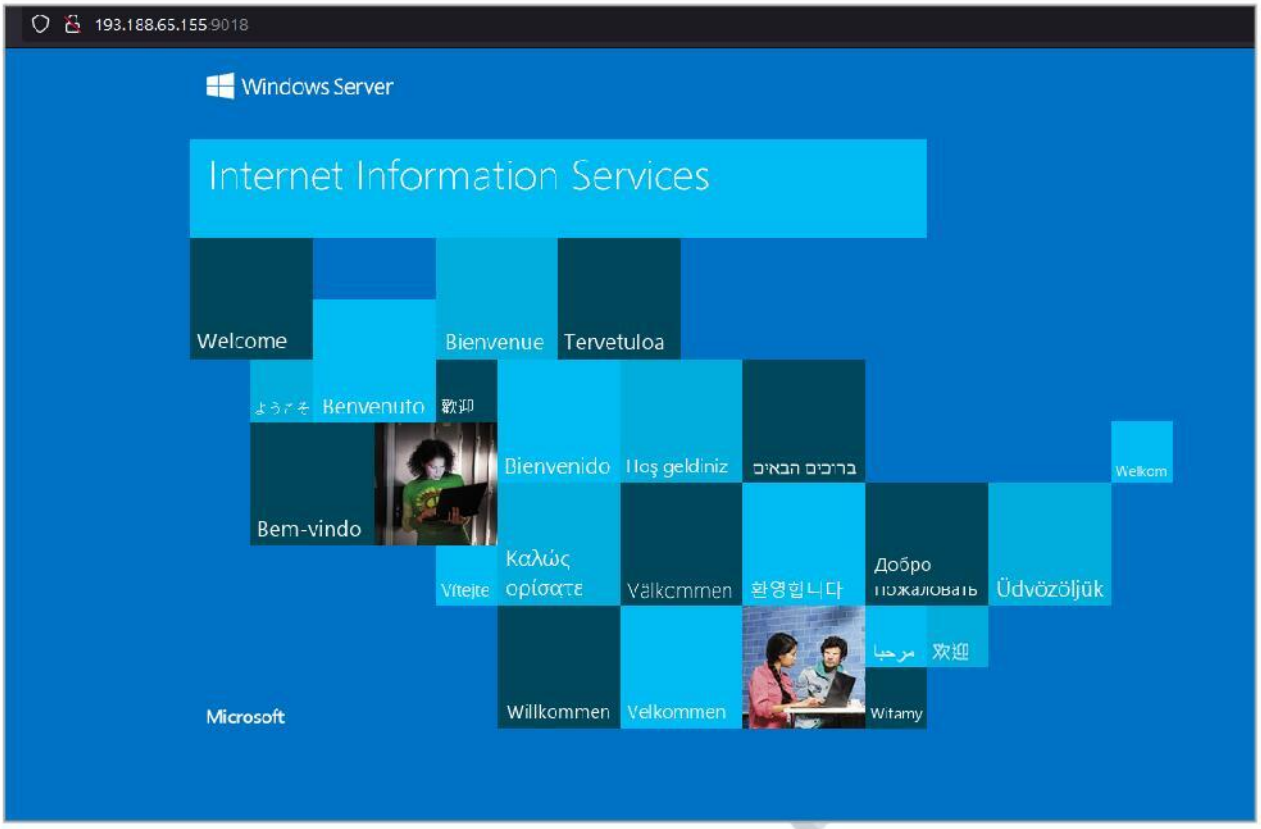


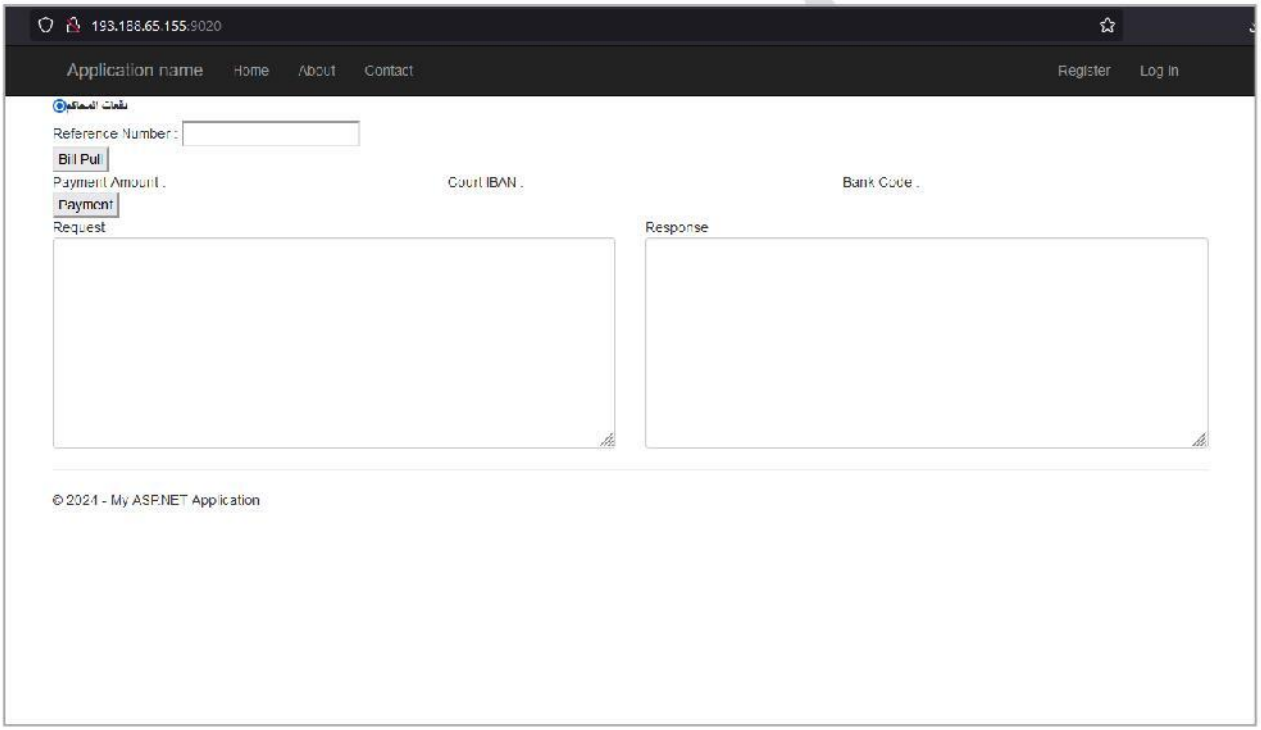

193.188.65.155:9010
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bienvenido
Hoş geldiniz
ברוכים הבאים
Bem-vindo
Vítejte
Καλώς ορίσατε
Välkommen
환영합니다
Добро пожаловать
Üdvözöljük
مرحبا
欢迎
Willkommen
Velkommen
Witamy
Microsoft


193.188.65.155:9011
وزارة العدل
الصفحة الرئيسية
بحث
من نحن
تواصل معنا
دليل المستخدم
تعليمات المزاد الإلكتروني
الشروط والأحكام
تسجيل الدخول
عرض الفيديو التوضيحي
المزادات الإلكترونية
مركبة (18)
أخرى (2)
شقة/ مكتب (5)
أرض/ مجمع (7)
شركة / علامة تجارية (2)
eauctions@moj.gov.jo
2019 2018 ©
الإصدارة الثامنة


193.188.65.155:9014

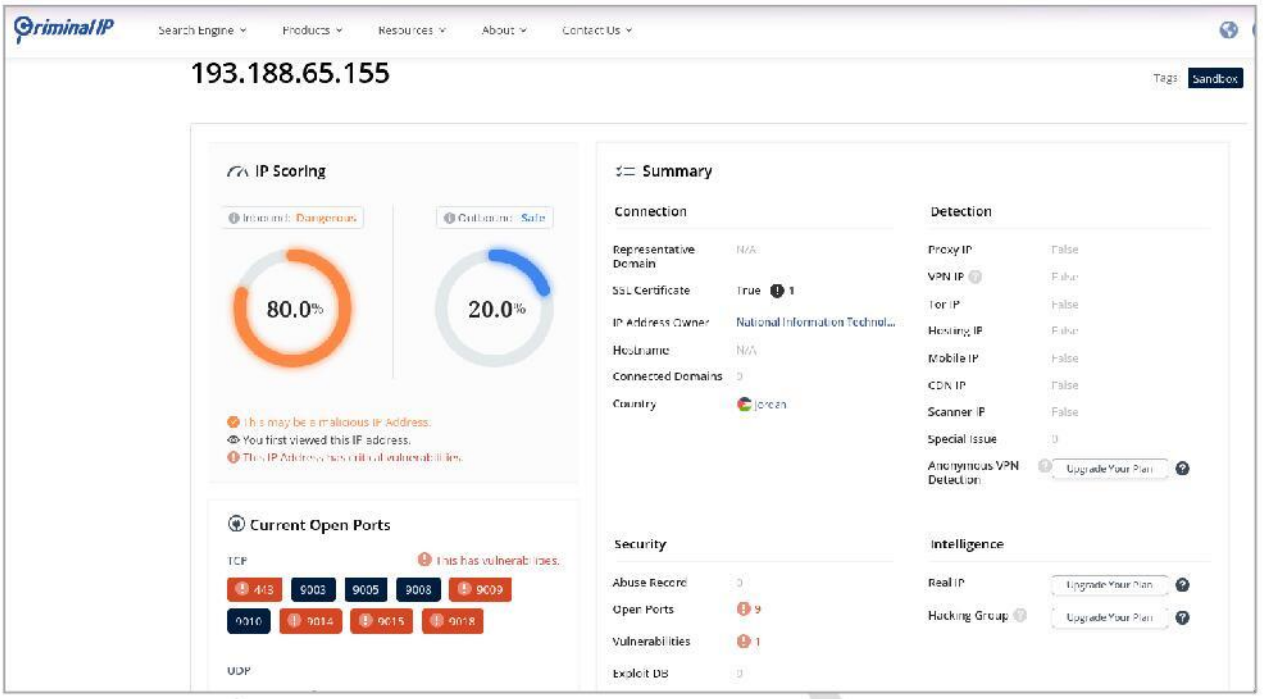

193.188.65.155:9015

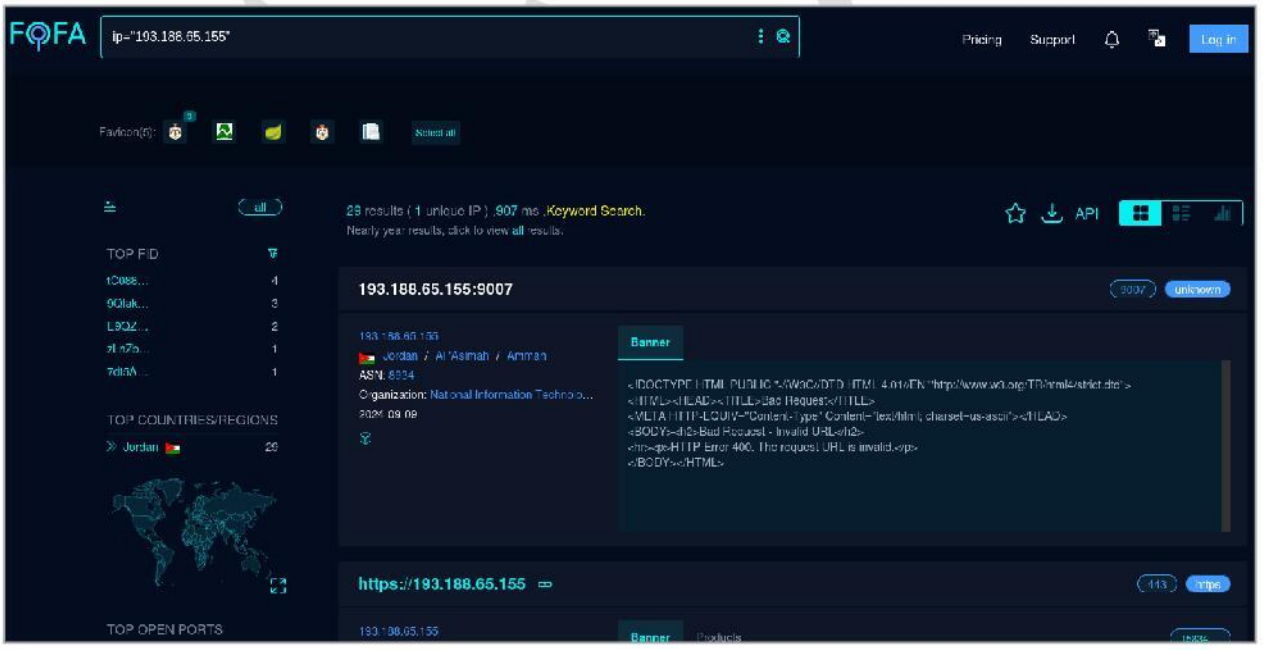


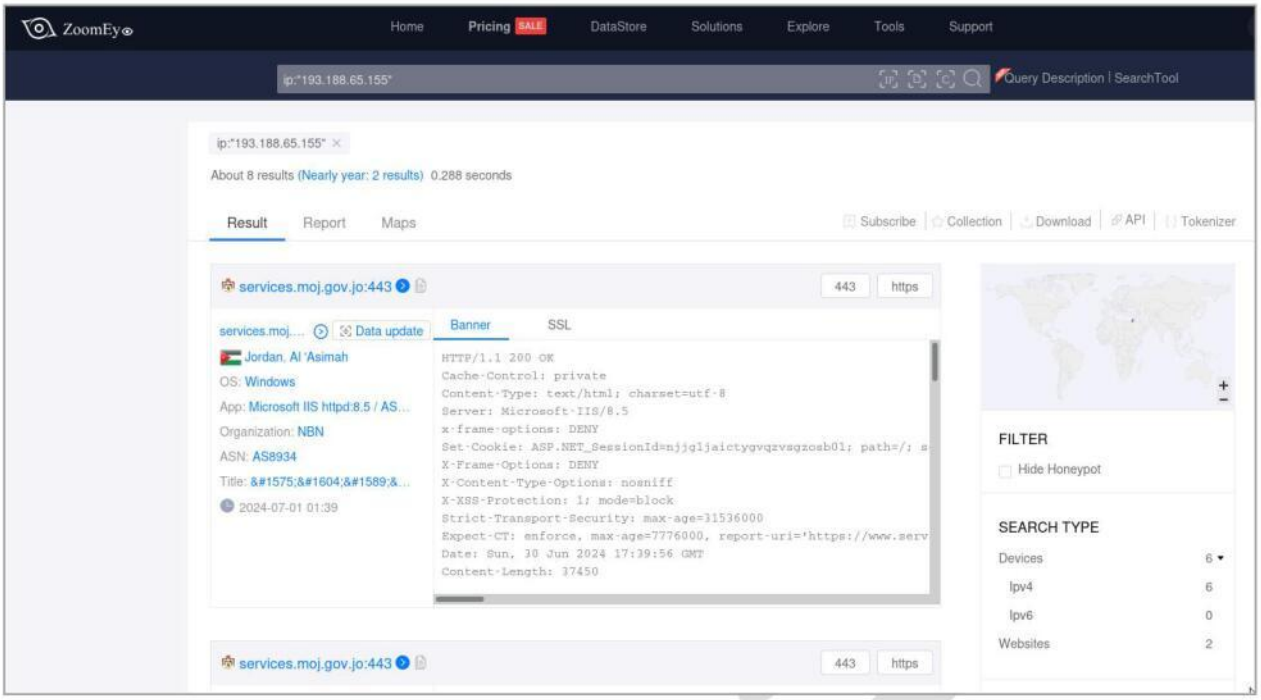


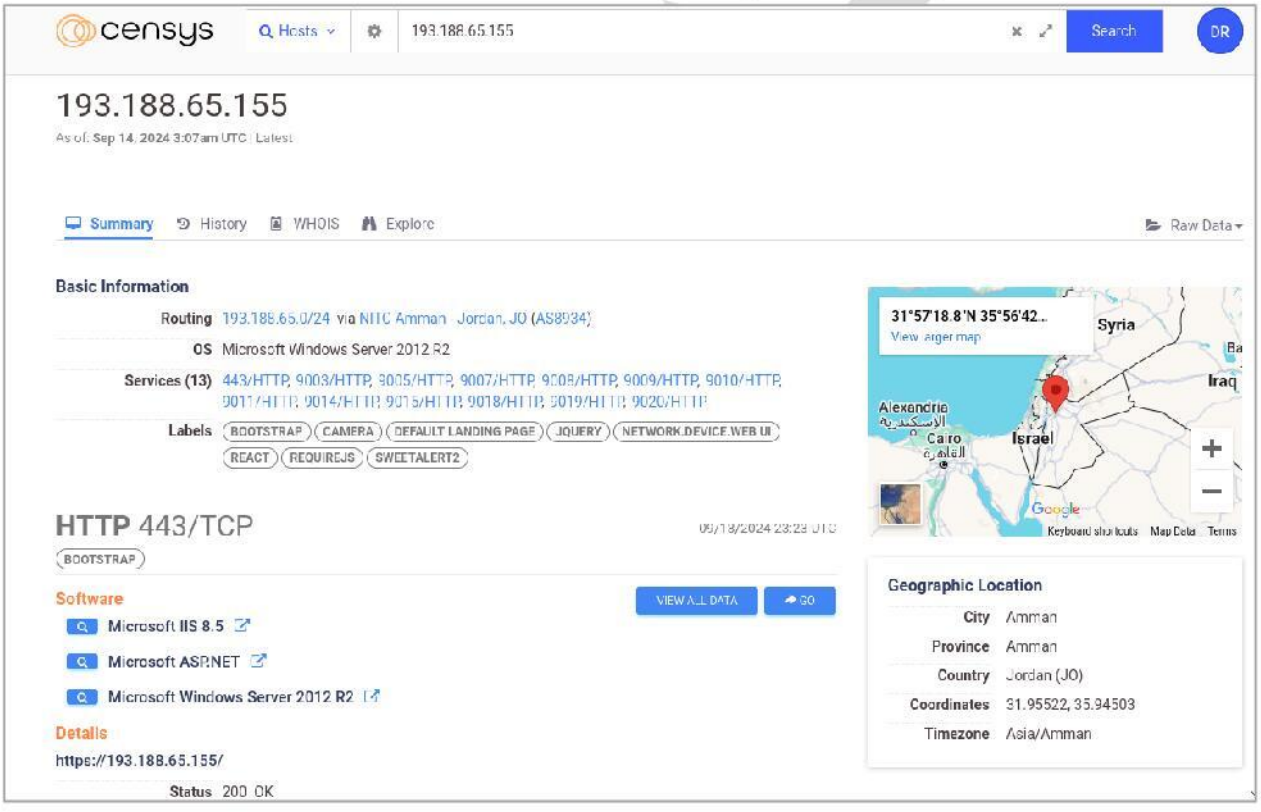
در این گزارش حمله به آدرس http://193.188.65.155:9003 مورد بررسی قرار گرفته است.

آدرس IP مذکور یعنی 193.188.65.155 با استفاده از موتورهای جستجو زیر مورد بررسی قرار گرفت که در ادامه تصاویری از نتایج آن‌ها ارائه می‌شود. خروجی این ابزارها در قالب فایل html. در فایل‌های پیوست قرار داده شده است.









در بررسی‌های انجام شده برای کشف دامنه‌های هم IP با آدرس 193.188.65.155 با استفاده از روش Reverse IP/Domain نیز اقدام شد و تنها موردی که ثبت شده بود آدرس دامنه services.moj.gov.jo بود. مقادیر Name Server و MX Record های زیر برای آدرس تارگت جستجو شد اما نتیجه مستقیم

برای آن یافت نشد. لذا برای کسب اطلاعات بیشتر به سراغ دامنه یک Level بالاتر یعنی moj.gov.jo رفتیم.

در خصوص دامنه moj.gov.jo اطلاعات زیادی وجود دارد. این دامنه در واقع آدرس اصلی وزارت دادگستری در کشور اردن می‌باشد که آدرس IP آن عبارت است از 193.188.66.205 که در واقع در رنج آدرس IP تارگت مد نظر در این گزارش نیز می‌باشد. پس از تحقیقات بیشتر متوجه شدیم که زیردامنه‌هایی که در جستجو و Recon اولیه از دامنه moj.gov.jo بدست آمده است برابر با لیست زیر، همگی ذیل یک رنج IP بر روی اینترنت قرار گرفته‌اند. در ادامه علاوه بر زیردامنه‌های آدرس moj.gov.jo ، اطلاعات زیرساخت شبکه و MX Record ها نیز ارائه شده است.

ncrc.moj.gov.jo	193.188.65.152
apprep.moj.gov.jo	193.188.65.153
services.moj.gov.jo	193.188.65.155
waj.moj.gov.jo	193.188.65.155
semsmob.moj.gov.jo	193.188.71.112
auctions.moj.gov.jo	193.188.71.119
ftp.moj.gov.jo	193.188.66.196
www.moj.gov.jo	193.188.66.205
appointmentpoj.moj.gov.jo	193.188.65.53
join.moj.gov.jo	193.188.71.52
mob.moj.gov.jo	193.188.65.58
eservices.moj.gov.jo	193.188.71.71
dm.moj.gov.jo	193.188.74.82
dms.moj.gov.jo	193.188.71.94
eng.moj.gov.jo	212.118.0.133
hrights.moj.gov.jo	69.46.25.141
links.moj.gov.jo	69.46.25.141
www1.moj.gov.jo	212.118.24.169

NS	ns1.nitc.gov.jo
	ns2.nitc.gov.jo
	ns3.nitc.gov.jo

rname	dns.nitc.gov.jo
mname	ns1.nitc.gov.jo
Mail Exchanger	mx01.govmail.gov.jo
	mx02.govmail.gov.jo
A Records	193.188.66.205
ASN	AS8934

تست نفوذ دامنه 193.188.65.155

برای حمله به سرور http://193.188.65.155 ، تمرکز بررسی خود را بر روی پورت 9003 قرار دادیم. چراکه با بررسی‌های انجام شده، وب سایت ارائه شده بر روی این پورت دارای آسیب‌پذیری‌های مهمی می‌باشد که در ادامه به آن اشاره خواهد شد.

در این مرحله با استفاده از پویش‌های انجام شده سعی شد تا آسیب‌پذیری‌های حیاتی آدرس 193.188.65.155 کشف شود. برای این کار ابتدا وب سایت مد نظر از نظر تکنولوژی‌های مورد استفاده برای طراحی و پیاده‌سازی مورد بررسی قرار گرفت. این این بررسی‌ها مشخص شد که این وب سایت از زبان برنامه نویسی ASP.NET و چارچوب .NET Framework. و وب سرور Microsoft IIS 8.5 استفاده می‌کند.

علاوه‌بر اینکه نسخه وب سرور مورد استفاده از نسخه‌های قدیمی و بوده دارای آسیب‌پذیری‌های از پیش ثبت شده است، به سراغ معروف‌ترین و البته آسیب‌پذیرترین Component که در وب سایت‌های ASP مورد استفاده قرار می‌گیرد رفتیم.

در این بررسی‌ها مشخص شد که آدرس /Telerik/Web/UI/WebResource.axd?type=rau که مربوط به یک Handler برای بارگذاری فایل می‌باشد باز بوده و قابل استفاده می‌باشد و مکانیزم‌های امنیتی بر روی آن وجود ندارد. در قدم بعدی با استفاده از بررسی نسخه مورد استفاده، متوجه شدیم که این وب سایت از نسخه Telerik Web UI 2017.1.118 استفاده می‌کند. برای این نسخه آسیب‌پذیری‌های RCE به واسطه نقص در عملیات Deserialization و همچنین آسیب‌پذیری File Upload به دلیل نقص در مکانیزم‌های کنترلی بارگذاری فایل، ثبت شده است.

لذا ابتدا سعی شد با استفاده از CVE-2019-18935 دسترسی RCE بر روی این تارگت گرفته شود. در تست‌های انجام شده مشخص شد که نقص Deserialization وجود دارد، اما دائماً دچار خطاهای شبکه‌ای و ارتباطی شده و فرآیند گرفتن دسترسی دچار اختلال می‌شود. مسائل بسیاری مورد بررسی قرار گرفت، از آدرس IP مبدأ که احتمال می‌رفت مشکل از آن باشد تا وضعیت شبکه.

با توجه به وضعیت موجود تصمیم گرفته شد تا مسیر دیگری برای نفوذ به تارگت طی شود. برای این کار ابتدا سامانه مورد بررسی امنیتی و تست نفوذ سطحی قرار گرفت. مشخص شد که شرایط Debug در سامانه فعال بوده و به دلیل نقص در بحث مدیریت خطا در سمت سرور، امکان برگردانی اطلاعات خطا

اعم از Stack Trace و اطلاعات فایل به خطا خورده از سمت سرور به سمت کاربر وجود دارد. لذا سعی شد تا با ایجاد خطا در فایل‌های اجرایی سمت سرور، به اطلاعات Absolute Path که در واقع همان آدرس از درایو C:\ می‌باشد دست پیدا کنیم. چراکه همانطور که گفته شد این نسخه از Telerik دارای آسیب‌پذیری File Upload می‌باشد و برای این کار با استفاده از CVE-2019-18935 نیازمند Absolute Path برای قرار دادن فایلی مانند یک Web Shell در محل دقیق ذیل پروژه وب، برای دسترسی از طریق وب، می‌باشد. در این خصوص تست‌های مکرر انجام گرفت اما تا الان مسیری پیدا نشد. امکان بارگذاری فایل در مسیر دلخواه وجود دارد اما باید مسیر دلخواه حتما وجود داشته باشد. برای این کار مسیر C:\Windows\ و C:\Windows\Temp را با استفاده از اکسپلویت CVE-2019-18935 برای بارگذاری فایل دلخواه مورد بررسی و تست قرار دادیم. که همانطور که پیش‌تر گفته شد فرآیند دائماً با خطا برخورد می‌شد. لذا برای ادامه مسیر و نفوذ به تارگت، سناریو دیگری پیش گرفته شد.

در سناریو بعدی با استفاده از یک کد اکسپلویت دیگر بر مبنای آسیب‌پذیری CVE-2017-11317 تلاش شد تا فایل مد نظر در مسیرهای مذکور در سناریوی قبلی بارگذاری شود. در ابتدا فایل‌های dll ساده که صرفاً باعث ایجاد یک Delay به اندازه چند ثانیه می‌شد، مورد استفاده قرار گرفتند تا امکان بارگذاری فایل و استفاده از این آسیب‌پذیری مورد بررسی قرار گیرد. چراکه در سناریوهای قبلی نیز فرآیند بارگذاری فایل ناتمام باقی مانده و هنوز به پاسخ قطعی رسیده نشده بود. در این مرحله باز هم نتایج منفی بود. اما این بار موضوع خطاهای شبکه‌ای یا تکمیل نشدن فرآیند نبود، بلکه خطاها از نوع اجرایی و ASP بود.

در این مرحله گمان برده شد که به احتمال زیاد یک AV و یا Windows Defender فایل بارگذاری شده توسط کد اکسپلویت ما را به محض قرار گرفتن بر روی سرور قرنطینه و حذف می‌کند. پس در این شرایط به کلی فایل را تغییر داده و از یک فایل Text ساده استفاده کردیم. نتیجه همانطور که حدس زده می‌شد مثبت بود و فایل Text مد نظر ما بر روی سرور و در مسیر C:\Windows\Temp قرار گرفت! این موضوع با توجه به پاسخ اکسپلویت Verify شد.

وضعیت فعلی و کارهای آتی

وضعیت فعلی اینگونه است که مطمئن هستیم که دامنه مسیر http://193.188.65.155:9003 به واسطه آسیب‌پذیری در کامپوننت Telerik مورد استفاده، قابل نفوذ می‌باشد. اما به دلیل حضور AV یا Defender هشیار بر روی سیستم عامل، باید از سناریوهای پیچیده‌تر برای نفوذ به سامانه استفاده شد. در حال حاضر امکان بارگذاری فایل بر روی سرور سامانه وجود دارد.

برای ادامه کار سناریوهای مختلف زیر مد نظر می‌باشد :

الف) سناریو دو مرحله‌ای به کمک File Upload :

- در مرحله اول : بارگذاری یک فایل DLL یا Malware یا RAT به نحوی که Obfuscate شده باشد و توسط مکانیزم‌های امنیتی نظیر AV یا Defender قابل شناسایی نباشد.

- در مرحله دوم : استفاده از روشی برای Triger کردن آن فایل DLL برای ایجاد RCE یا اموری دیگر بر روی سرور تارگت. روش‌های مانند DLL Hijacking که در فاز Triger کردن صرفاً کافیست کاری کنیم تا ادمین سامانه مجبور به Restart کردن سرور شود.

ب) حمله و نفوذ و به دیگر پورت‌های باز آدرس IP تارگت که در حال سرویس‌دهی در وب می‌باشند.

پ) همچنین این سناریو که با استفاده از CVE-2019-18935 بتوان خطاها را مرتفع کرده و در همان یک بار حمله کردن، فایل DLL را بارگذاری و به واسطه Deserialization آن را اجرا کرده و دسترسی RCE اخذ شود. این سناریو مقداری نیازمند تحقیق و بررسی است. چراکه در تلاش‌های انجام شده تا الان این امکان وجود نداشته و مکانیزم‌های امنیتی این فرآیند را مختلف می‌کنند.

نتیجه گیری

در این گزارش مراحل بررسی تارگت services.moj.gov.jo از فاز شناخت تا بارگذاری فایل و اقدامات انجام شده در خصوص انجام آن‌ها به تفصیل ارائه شد. همچنین در انتها وضعیت فعلی و کارهای آتی که انجام خواهد گرفت نیز مشخص و معرفی شدند. با توجه به زیردامنه‌های کشف شده از دامنه اصلی وزارت دادگستری کشور اردن یعنی moj.gov.jo ، این احتمال داده می‌شود که با نفوذ به سرور services.moj.gov.jo بتوانیم به دیگر سامانه‌هایی که در رنج IP همین تارگت هستند نیز نفوذ پیدا کنیم.