Soroush Dalili (@irsdl) Blog

A web application security ninja 🧣 , a semicolon enthusiast!

HOME

ADVISORIES

PRIVACY POLICY

BUG BOUNTY INVITES!

WORK

A Dotty Salty Directory: A Secret Place in NTFS for Secret Files!

I was playing with "::\$Index_allocation" and ":\$I30:\$Index_Allocation" in an NTFS partition to make a directory which ends with some dot characters (".") or just includes some dots!

The result was a bit interesting data can be hidden in as well malware writers might already feature!

In order to create a dotty direc

- 1- Open the Windows Commar
- 2- Go to a test directory.
- 3.0- Now, insert the following c

md ..::\$index allocation

md ...::\$index_allocation

md ...::\$index_allocatio

md irsdl

md irsdl.::\$index_allocat

md irsdl..::\$index alloca

- 3.1- You can use "echo test >
- 4- Now get a directory list from
- 5- In order to open each of the

cd ...::\$index allocation 6- You can create some files in



Soroush Dalili's blog asks for your consent to use your personal data to:



Personalised advertising and content, advertising and content measurement, audience research and services development



Store and/or access information on a device



Learn more

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with 134 TCF vendor(s) and 63 ad partner(s), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.

Do not consent

Consent

Manage options



The result in **Windows XP**:

The double dot ("..") directory is hidden and you cannot see it.

7- Now use Windows Explorer to see these directories.

- In windows explorer, directories with a single dot at the end show the files which are inside a directory with same name but without any dot. For example: "irsdl." shows content of "irsdl". Directories with a double dot at the end show the files which are inside a directory with the same name but with a single dot. For example: "irsdl.." shows content of "irsdl.". And so on.
- In Windows Explorer, if you modify a directory with some dots at the end, the modification will be applied on a directory with a dot lesser than the modified directory. Therefore, if you delete "irsdl.", "irsdl" folder will be deleted instead!
- It is not possible to delete these directories by Windows Explorer. (use "del DirName::\$Index_Allocation*.* & RD DirName::\$Index_Allocation" instead)









Search

oDB NoSQL Injection with

23. 2024

ieless DuoDrop: IIS Auth Bypass &

Pool Privesc in ASP.NET Framework

-2023-36899 & CVE-2023-36560)

st 8, 2023

or Tag XSS Exploitation in Firefox with

et=" blank"

st 1, 2023

en Years On: Advancing the

rstanding of IIS Short File Name

MDSec Blog Posts so far in 2020/2021!

er 31, 2020

Upload Attack using XAMLX Files

mber 21, 2019

<u>Uploading web.config for Fun and Profit 2</u>

August 15, 2019

Blackbox Testing

July 9, 2019

<u>Danger of Stealing Auto Generated .NET</u>

Machine Keys

May 10, 2019

x-up-devcap-post-charset Header in

ASP.NET to Bypass WAFs Again!

May 4, 2019

Exploiting Deserialisation in ASP.NET via

<u>ViewState</u>

April 23, 2019

Yet Other Examples of Abusing CSRF in

April 23, 2019

How to win BIG and even more!

April 17, 2019

In Windows 7:

- It is very similar to Windows XP. However, if you click on the directories by Windows Explorer, it may show you the content of a specific directory for all the Dotty ones.
- It is not also possible to create a folder with only double dots "..".

The directories which only contain several dots such as "...", show the content of their root directory although it is not so real!

Result:

Dotty directories are very good places to hide some files and data! It is not easy to be detected and it is not easy to be deleted! As malwares can use the same technique to hide themselves inside an NTFS partition, we should be very careful about it.

Notes:

Note 0: I might miss some other interesting points. Please let me know when you find one.

Note 1: some of these directori

Note 2: I experienced a crash directories.

Note 3: Norton Internet Securit inside these folders. It's not tes Note 4: Windows XP did check

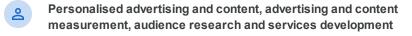
Note 5: You can do the same it by "del *.*".

This entry was posted in **Security Pos**

← Skype Privacy Concern: It send: <u>numbers + URLs to its server!</u>



Soroush Dalili's blog asks for your consent to use your personal data to:





Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with 134 TCF vendor(s) and 63 ad partner(s), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.









(SS bypass ASP.NI <u>bounty</u> bugbounty bypass _{lenge} deserialisation serialization ecommerce allnterface ExternalInterface.call upload file upload bypass ploader security bypass financial ile Extension Security Bypass rt file name IIS Tilde bug IIS tilde feature nekey penetration testing RCE uest encoding sharepoint

amew ork Anti-XSS bypass

Finding and Exploiting .NET Remoting over

More research on .NET deserialization

Feel honoured to be there again after 8

years: Top 10 Web Hacking Techniques of

Story of my two (but actually three) RCEs

ASP.NET resource files (.RESX) and

MS 2018 Q4 - Top 5 Bounty Hunter for 2

WAF Bypass Techniques – Using HTTP Standard and Web Servers' Behaviour

HTTP using Deserialisation

March 26, 2019

2017

December 19, 2018

December 19, 2018

August 12, 2018

August 12, 2018

st 12. 2018

ives ect Year

in SharePoint in 2018 December 19, 2018

RCEs in SharePoint Online

restricted File Upload view state w af WAF bypass web.config XSS vulnerability

t name scanner SQL Injection

NEDDIT WEB SECURITY

RESEARCH

How to turn a file write vulnerability in a Node.js application into RCE – even though the target's file system is read-only

October 10, 2024 /u/albinowax

Class Pollution in Ruby: A Deep Dive into **Exploiting Recursive Merges** October 3,

2024 /u/albinowax

Exploiting trust: Weaponizing permissive

CORS configurations October 1, 2024

/u/t0xodile

<u>lconv, set the charset to RCE (part 3):</u>

Blind file read to RCE in PHP September

30, 2024 /u/cfambionics

DNS poisoning in 30M domains caused by

the Great Firewall September 27, 2024

/u/albinowax

Splitting the email atom: exploiting parsers

to bypass access controls August 23, 2024

/u/garethheyes

Gotta cache 'em all: bending the rules of

web cache exploitation August 22, 2024

/u/albinowax

<u>Listen to the whispers: web timing attacks</u>

hat actually work August 8, 2024

binowax

to create a Burp Suite Extension from

ATCH (Python) July 23, 2024

ectronic_Village_8

mmonly overlooked xss vector July

024 /u/Puzzleheaded-Put-693

use your personal data to:

Soroush Dalili's blog asks for your consent to



Personalised advertising and content, advertising and content measurement, audience research and services development



Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with 134 TCF vendor(s) and 63 ad partner(s), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.

REDDIT NETSEC

ANNEL FEED

cking APIs using JSON Injection

tober 21, 2024

ck Exploit in South Korea's biggest

ile chat app October 20, 2024

ng Vulnerability Variants at Scale

ober 17, 2024

stack spoofing explained using APT41

<u>vare</u> October 17, 2024

CVE-2024-45844: Privilege escalation in F5

BIG-IP October 17, 2024

■ EXPLOIT-DB FEED

[webapps] dizqueTV 1.5.3 - Remote Code Execution (RCE)

[webapps] openSIS 9.1 - SQLi

(Authenticated)

[webapps] reNgine 2.2.0 - Command

<u>Injection (Authenticated)</u>

[dos] Windows TCP/IP - RCE Checker and

Denial of Service

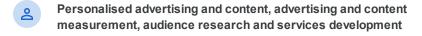
[webapps] Invesalius3 - Remote Code

Execution

<u>Privacy Policy</u> / <u>Proudly powered by WordPress</u>



Soroush Dalili's blog asks for your consent to use your personal data to:



Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with 134 TCF vendor(s) and 63 ad partner(s), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.