InfoSec Learn Lab - Reconnaissance

13.03.2023

Grigoraș Ana-Maria

Application Security and Pentesting ILV mcr22

Dr. Gerald Emerick

Task 2:

Google advanced commands:

1. site:cfrcalatori.ro intitle:login - https://www.cfrcalatori.ro/cum-cumpar-online/capture-login/
2. site:ratbv.ro inurl:16-dus.html - https://www.ratbv.ro/afisaje/16-dus.html
3. filetype:pdf intitle:train - https://www.oebb.at/static/tarife/en/guide_for_travelling_with_the_oebb_night_train_in_germany/Resources/pdf/1834078859__en.pdf
4. filetype:ppt intext:mama - https://t1.daumcdn.net/cfile/tistory/153A5B4450179A6028?download

Task 3:

3.1:

3.1. a:

312Ville 192.168.1.10/isihack/

Web server type: Microsoft-IIS/7.5

Web server version: 7.5

3.1. b:

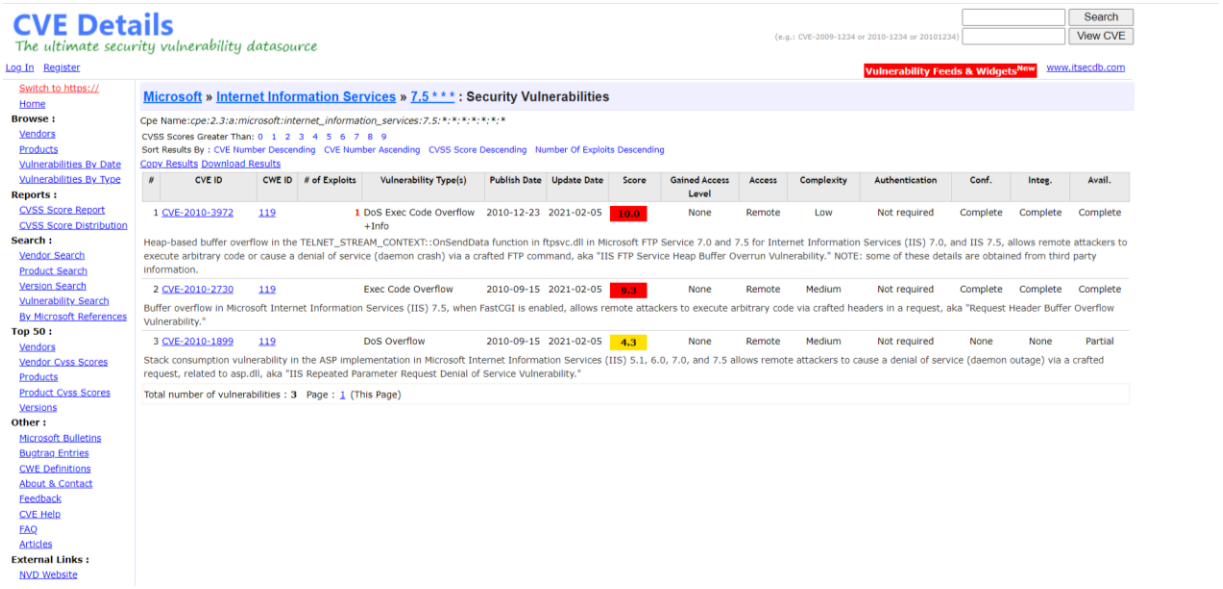
MSP2 192.168.1.40/dvwa

Web server type: Apache/2.2.8 (Ubuntu) DAV/2

Web server version: 2.2.8

3.2:

By using the website provided, I have discovered a vulnerability that involves denial of service, code overflow, and unauthorized information access. Specifically, there is a heap-based buffer overflow in Microsoft-IIS/7.5 that allows hackers to execute malicious and oppressive code or cause a server disruption. This vulnerability is identified by the Common Weakness Enumeration (CWE) ID, 119, which relates to the operations performed on memory buffers and the lack of certainty in validating each location.



CVE Details

The ultimate security vulnerability datasource

Search | View CVE

Log In | Register

Vulnerability Feeds & Widgets New | www.itsecdb.com

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website

Microsoft » Internet Information Services » 7.5 * * : Security Vulnerabilities

Cpe Name:cpe:2.3:a:microsoft:internet_information_services:7.5:*:*:*:*:*:*:*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

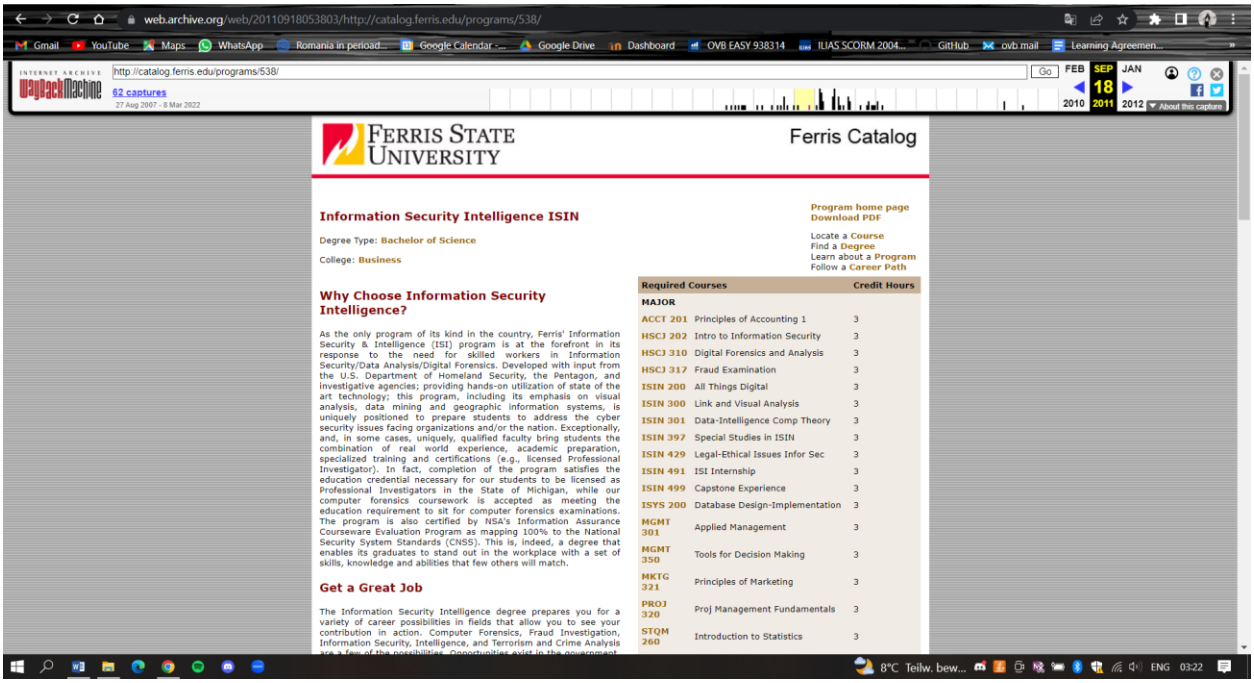
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2010-3972	119	1	DoS Exec Code Overflow +Info	2010-12-23	2021-02-05	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
	Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information.													
2	CVE-2010-2730	119		Exec Code Overflow	2010-09-15	2021-02-05	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
	Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability."													
3	CVE-2010-1899	119		DoS Overflow	2010-09-15	2021-02-05	4.3	None	Remote	Medium	Not required	None	None	Partial
	Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability."													

Total number of vulnerabilities : 3 Page : 1 (This Page)

Task 4:



PREL 240 -> it appears until 25 Feb 2011. Since 18 Sept 2011, it does not appear anymore because it is not required anymore.

The GISC ones are the same, all present at 25 Feb 2011 and 18 Sept 2011. They appear in 2012 too.