

**InfoSec Learn Lab - Reconnaissance**

**13.03.2023**

**Grigoraş 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](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

Log In

Register

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

Search

View CVE

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Vulnerability Feeds & Widgets

www.itsecdb.com

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	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 ftptvc.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:

**FERRIS STATE UNIVERSITY**

**Ferris Catalog**

**Information Security Intelligence ISIN**

Degree Type: Bachelor of Science  
College: Business

**Why Choose Information Security Intelligence?**

As the only program of its kind in the country, Ferris' Information Security & Intelligence (ISI) program is at the forefront in its response to the need for skilled workers in Information Security/Data Analysis/Digital Forensics. Developed with input from the U.S. Department of Homeland Security, the Pentagon, and investigative agencies; providing hands-on utilization of state of the art technology; this program, including its emphasis on visual analysis, data mining and geographic information systems, is uniquely positioned to prepare students to address the cyber security issues facing organizations and/or the nation. Exceptionally, and, in some cases, uniquely, qualified faculty bring students the combination of real world experience, academic preparation, specialized training and certifications (e.g., licensed Professional Investigator). In fact, completion of the program satisfies the education credential necessary for our students to be licensed as Professional Investigators in the State of Michigan, while our computer forensics coursework is accepted as meeting the education requirement to sit for computer forensics examinations. The program is also certified by NSA's Information Assurance Courseware Evaluation Program as mapping 100% to the National Security System Standards (CNSS). This is, indeed, a degree that enables its graduates to stand out in the workplace with a set of skills, knowledge and abilities that few others will match.

**Get a Great Job**

The Information Security Intelligence degree prepares you for a variety of career possibilities in fields that allow you to see your contribution in action. Computer Forensics, Fraud Investigation, Information Security, Intelligence, and Terrorism and Crime Analysis are a few of the possibilities. Opportunities exist in the government

**Required Courses**

Required Courses	Credit Hours
<b>MAJOR</b>	
ACCT 201 Principles of Accounting 1	3
HSCJ 202 Intro to Information Security	3
HSCJ 310 Digital Forensics and Analysis	3
HSCJ 317 Fraud Examination	3
ISIN 200 All Things Digital	3
ISIN 300 Link and Visual Analysis	3
ISIN 301 Data-Intelligence Comp Theory	3
ISIN 397 Special Studies in ISIN	3
ISIN 429 Legal-Ethical Issues Infor Sec	3
ISIN 491 ISI Internship	3
ISIN 499 Capstone Experience	3
ISYS 200 Database Design-Implementation	3
MGMT 301 Applied Management	3
MGMT 350 Tools for Decision Making	3
MKTG 321 Principles of Marketing	3
PROJ 320 Proj Management Fundamentals	3
STOM 260 Introduction to Statistics	3

Program home page  
Download PDF  
Locate a Course  
Find a Degree  
Learn about a Program  
Follow a Career Path

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.