Name: Jun Wang 000791814

Lab 8: Attacking the Servers

Web Application Security

Marks: /1

Bonus Marks: -/-

Table of Contents

[Lab Outcome 2](#_Toc25522672)

[Background Reading 2](#_Toc25522673)

[Architecture Diagram 2](#_Toc25522674)

[Required Hardware/Software 2](#_Toc25522675)

[Introduction 3](#_Toc25522676)

[1.0 Buffer Overflows 3](#_Toc25522677)

[2.0 Information Disclosure Exploits 3](#_Toc25522678)

[3.0 Research Attacks and Vulnerabilities of Web Server and Application Architecture 4](#_Toc25522679)

[4.0 Sign-Off – Lab 8: Attacking the Servers 5](#_Toc25522680)

Web Application Security

Lab 8: Attacking the Servers

# Lab Outcome

Exploit natively compiled applications.

Background Reading

Read the textbook sections listed in the Course Schedule.

Architecture Diagram

|  |
| --- |
|  |

Required Hardware/Software

* VM Ubuntu 18.04 – 2 CPU, 4GB Ram, 20 GB hard disk
  + Docker
    - WebGoat v7.1
    - DVWA (Dawn Vulnerable Web App)
* VM Kali
  + Burp or other Web proxy (scanner)

# Introduction

Web applications written in native languages, like C and C++, suffer from vulnerabilities such as buffer overflows and format string errors.

# 1.0 Buffer Overflows

In WebGoat, complete the **Buffer Overflows > Off-by-One Overflows** lesson.

Step1> input random name and room number

Step2> inspect webpage, we can find hidden fields of Name and room number.

Setp3> click on Accept Terms, we can find the POST request in ZAP

Step4> change the room number to a 4097 length random string generated by online tool ( Random String Generator) .

Step5> send the POST request, we can find the other customers information in the hidden fields.

Step6> login as one of the customers, then click on Accept Terms.

|  |
| --- |
| Selection_175 |
| Selection_177 |
| Selection_170 |
| Selection_171 |
| Selection_172 |
| Selection_173 |
| Selection_174 |
| Selection_176 |
| Selection_177 |
| Selection_178 |

# 2.0 Information Disclosure Exploits

From the extracted data on information disclosure exploits and natively compiled applications

D:\> nc www.xyz.com 80

GET / HTTP/1.0

HTTP/1.1 302 Found

Cache-Control: private

Content-Type: text/html; charset=utf-8

Location: /en/us/default.aspx

Server: Microsoft-IIS/7.0

X-AspNet-Version: 4.0.30319

P3P: CP="ALL IND DSP COR ADM CONo CUR CUSo IVAo IVDo PSA PSD TAI TELo OUR SAMo C

NT COM INT NAV ONL PHY PRE PUR UNI"

X-Powered-By: ASP.NET

Date: Sat, 14 Jul 2007 15:22:26 GMT

Connection: keep-alive

Content-Length: 136

|  |  |
| --- | --- |
| Items | Details |
| Exploit Tool | netcat |
| Web Server Type | Microsoft-IIS |
| Web Server Version | 7.0 |
| Web Server App | Asp.Net |
| Web Server App Version | X-AspNet-Version: 4.0.30319 |

# 3.0 Research Attacks and Vulnerabilities of Web Server and Application Architecture

From the information above, research the vulnerability type, CVEID of the web server and the application architecture and describe below:

|  |  |  |  |
| --- | --- | --- | --- |
| Web Server /  Application Type and Version | Vulnerability Type | CVE# | Details |
| Sample – Apache 1.3.34-4 | Sample - Privilege | Sample – [CVE-2006-7098](https://www.cvedetails.com/cve/CVE-2006-7098/" \o "CVE-2006-7098 security vulnerability details) | Sample – does not properly disassociate httpd from a controlling tty when httpd is started interactively, which allows local users to gain privileges to that tty via a CGI program that calls the TIOCSTI ioctl. |
| Microsoft-IIS/7.0 | FTP Command Injection | [CVE-2012-2532](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2532) | Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) processes unspecified commands before TLS is enabled for a session, which allows remote attackers to obtain sensitive information by reading the replies to these commands, aka "FTP Command Injection Vulnerability." |
| Heap-based buffer overflow | [CVE-2010-3972](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3972) | 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. |
| Stack consumption | [CVE-2010-1899](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1899) | 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." |

|  |  |  |  |
| --- | --- | --- | --- |
| Web Server /  Application Type and Version | Vulnerability Type | CVE# | Details |
| ASP.NET  4.0.30319 | Elevation Of Privilege Vulnerability | [CVE-2019-1302](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1302) | An elevation of privilege vulnerability exists when a ASP.NET Core web application, created using vulnerable project templates, fails to properly sanitize web requests, aka 'ASP.NET Core Elevation Of Privilege Vulnerability'. |
| Spoofing vulnerability | [CVE-2019-1075](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1075) | A spoofing vulnerability exists in ASP.NET Core that could lead to an open redirect, aka 'ASP.NET Core Spoofing Vulnerability'. |
| DOS | [CVE-2019-0982](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0982) | A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka 'ASP.NET Core Denial of Service Vulnerability'. |
| .Net Framework Array Offset | [CVE-2011-0664](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0664) | Microsoft .NET Framework 2.0 SP1 and SP2, 3.5 Gold and SP1, 3.5.1, and 4.0, and Silverlight 4 before 4.0.60531.0, does not properly validate arguments to unspecified networking API functions, which allows remote attackers to execute arbitrary code via (1) a crafted XAML browser application (aka XBAP), (2) a crafted ASP.NET application, (3) a crafted .NET Framework application, or (4) a crafted Silverlight application, aka ".NET Framework Array Offset Vulnerability." |
| NET Framework JIT Optimization Vulnerability | [CVE-2011-1271](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1271) | The JIT compiler in Microsoft .NET Framework 3.5 Gold and SP1, 3.5.1, and 4.0, when IsJITOptimizerDisabled is false, does not properly handle expressions related to null strings, which allows context-dependent attackers to bypass intended access restrictions, and consequently execute arbitrary code, in opportunistic circumstances by leveraging a crafted application, as demonstrated by (1) a crafted XAML browser application (aka XBAP), (2) a crafted ASP.NET application, or (3) a crafted .NET Framework application, aka ".NET Framework JIT Optimization Vulnerability." |

# 4.0 Sign-Off – Lab 8: Attacking the Servers

Detach this page and submit it to your instructor to indicate you have completed all sections.

Name:

Student ID:

|  |  |
| --- | --- |
| **Section** | **Instructor Initials** |
| 1.0 Buffer Overflows |  |
| 2.0 Information Disclosure |  |
| 3.0 Attack and Vulnerabilitiies |  |