Tugas
Manajemen Keamanan Informasi

Ibnu Anugrah Rahimullah 09031281520101

Jurusan Sitem Informasi
Fakultas Ilmu Komputer
Universitas Sriwijaya
2018

A. Pro Wrestling Tees

1. Data Collection

BIODATA

DATA COLLECTION APP:
1.NETCRAFT.COM
2.ZENMAP
3.BUILTWITH.COM
4.WHOIS.COM

DOMAIN NAME	:	PROWRESTLINGTEES.COM
IP ADDRESS	:	104.25.58.20
CREATION DATE	:	2013-02-13T21:52:32Z
UPDATED DATE	:	2018-02-14T17:19:40Z
EXPIRED DATE	:	2019-02-13T21:52:32Z
REGISTRAR URL	:	HTTP://WWW.GODADDY.COM
WEB SERVER	:	CLOUDFLARE
SERVER OS	:	LINUX 2.6.32-3.10
OPENED PORT	:	53, 80, 443, 8080
JQUERY VER.	:	1.4.2
MAGENTO VER.	:	MAGENTO 2

2. Vulerability Assesment

CVE-2014-6071

- Jquery 1.4.2
- jQuery 1.4.2 allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to use of the text method inside after
- Type : Cross Site Scripting
- CVSS Score : 4.3

CVE-2016-6485

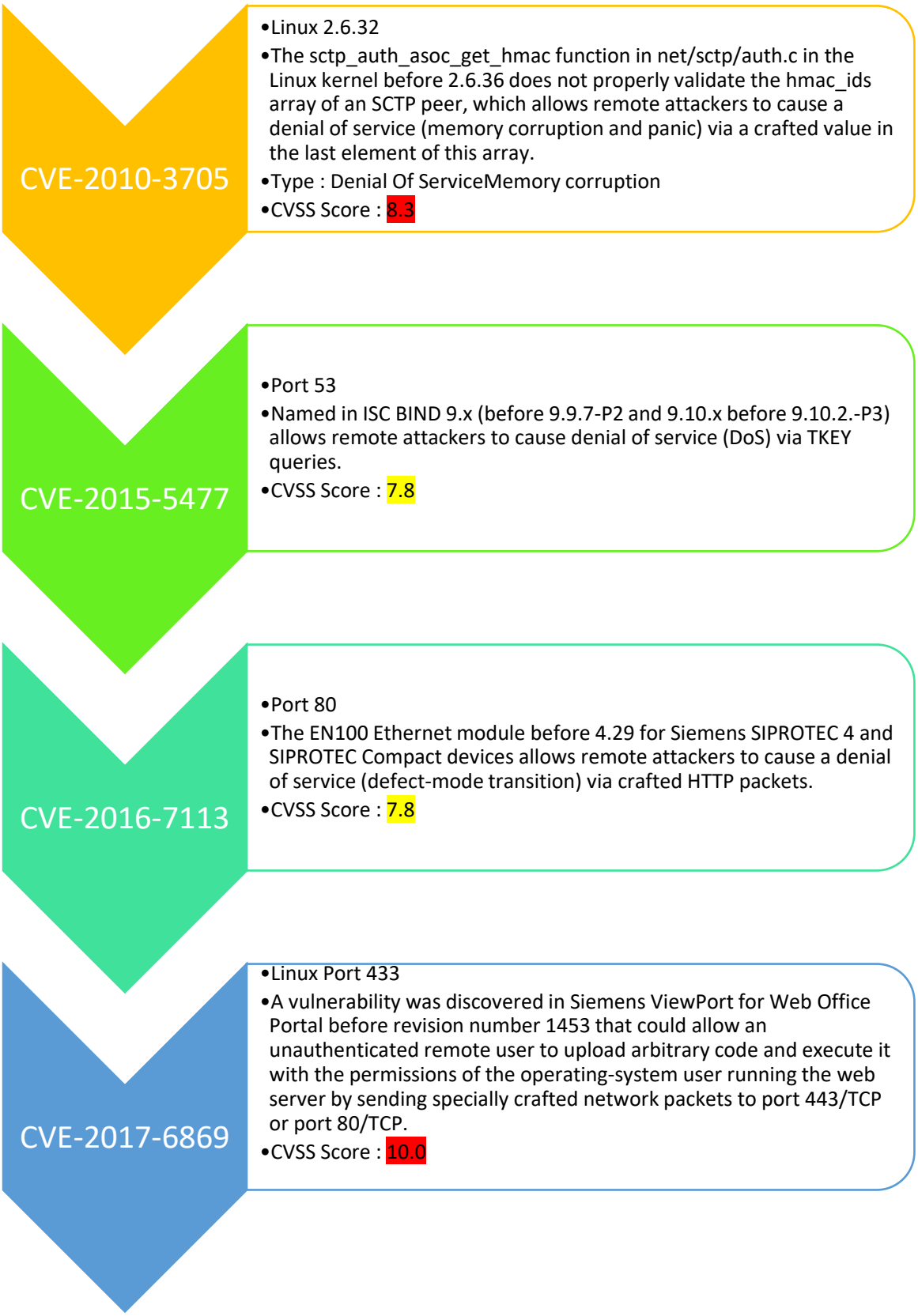
- Magento 2
- The __construct function in Framework/Encryption/Crypt.php in Magento 2 uses the PHP rand function to generate a random number for the initialization vector, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by guessing the value.
- CVSS Score : 5.0

CVE-2009-4538

- Linux 2.6.32
- drivers/net/e1000e/netdev.c in the e1000e driver in the Linux kernel 2.6.32.3 and earlier does not properly check the size of an Ethernet frame that exceeds the MTU, which allows remote attackers to have an unspecified impact via crafted packets, a related issue to CVE-2009-4537.
- CVSS Score : 10.0

CVE-2010-2495

- Linux 2.6.32
- The pppol2tp_xmit function in drivers/net/pppol2tp.c in the L2TP implementation in the Linux kernel before 2.6.34 does not properly validate certain values associated with an interface, which allows attackers to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via vectors related to a routing change.
- Type : Denial Of Service
- CVSS Score : 10.0


CVE-2010-3705
•Linux 2.6.32
•The sctp_auth_asoc_get_hmac function in net/sctp/auth.c in the Linux kernel before 2.6.36 does not properly validate the hmac_ids array of an SCTP peer, which allows remote attackers to cause a denial of service (memory corruption and panic) via a crafted value in the last element of this array.
•Type : Denial Of ServiceMemory corruption
•CVSS Score : 8.3
CVE-2015-5477
•Port 53
•Named in ISC BIND 9.x (before 9.9.7-P2 and 9.10.x before 9.10.2.-P3) allows remote attackers to cause denial of service (DoS) via TKEY queries.
•CVSS Score : 7.8
CVE-2016-7113
•Port 80
•The EN100 Ethernet module before 4.29 for Siemens SIPROTEC 4 and SIPROTEC Compact devices allows remote attackers to cause a denial of service (defect-mode transition) via crafted HTTP packets.
•CVSS Score : 7.8
CVE-2017-6869
•Linux Port 433
•A vulnerability was discovered in Siemens ViewPort for Web Office Portal before revision number 1453 that could allow an unauthenticated remote user to upload arbitrary code and execute it with the permissions of the operating-system user running the web server by sending specially crafted network packets to port 443/TCP or port 80/TCP.
•CVSS Score : 10.0

CVE-2017-2682

- Port 8080
- The Siemens web application RUGGEDCOM NMS < V1.2 on port 8080/TCP and 8081/TCP could allow a remote attacker to perform a Cross-Site Request Forgery (CSRF) attack, potentially allowing an attacker to execute administrative operations, provided the targeted user has an active session and is induced to trigger a malicious request.
- CVSS Score : 6.8

B. Pemkot Bukittinggi

1. Data Collection

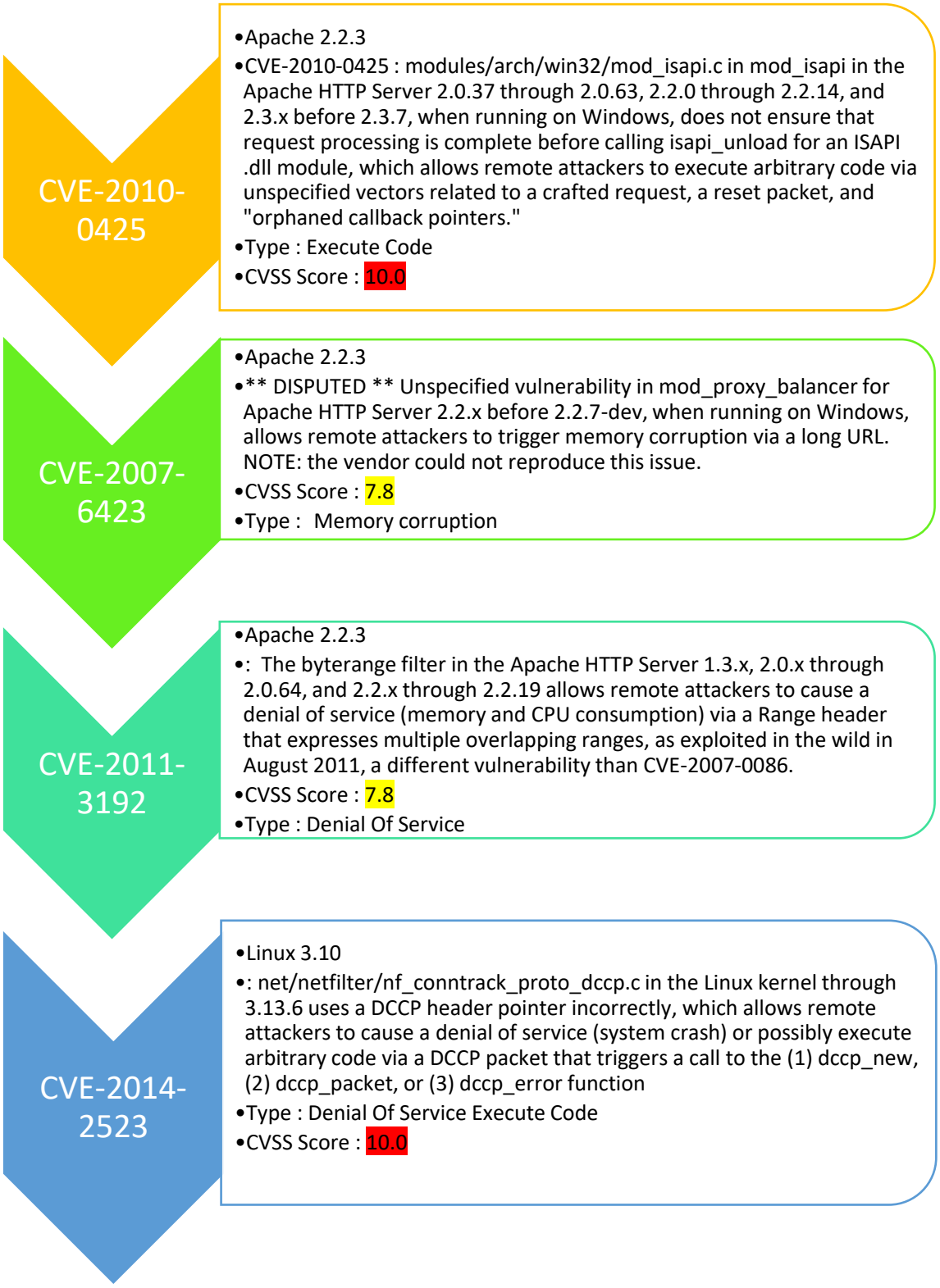
BIODATA

DATA COLLECTION APP:
1.NETCRAFT.COM
2.ZENMAP
3.BUILTWITH.COM
4.WHOIS.COM

DOMAIN NAME : bukittinggikota.go.id
IP ADDRESS : 180.250.46.109
CREATION DATE : 04-Jan-2007 13:29:28 UTC
UPDATED DATE : 19-Mar-2017 00:10:04 UTC
EXPIRED DATE : 01-Feb-2019 23:59:59 UTC

WEB SERVER : Apache/2.2.3 ClearOS
SERVER OS : linux 3.10
OPENED PORT : 25. 53. 80. 110

2. Vulnerability Assesment



CVE-2015-0573

a.: drivers/media/platform/msm/broadcast/tsc.c in the TSC driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (invalid pointer dereference) or possibly have unspecified other impact via a crafted application that makes a TSC_GET_CARD_STATUS ioctl call.

- Type : Denial Of Service
- CVSS Score : 10.0