# MANAJEMEN KEAMANAN SISTEM INFORMASI

# LAPORAN ANALISIS PADA WEBSITE

# PUSRI.CO.ID DAN PAJAK.GO.ID


**OLEH :**

**Nama : OKTARISIA**

**NIM : 09031281520125**

**Kelas : SI Reguler 6A**

**DosenPembimbing : Deris Stiawan,M.T.,Ph.D.**

**JURUSAN SISTEM INFORMASI**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

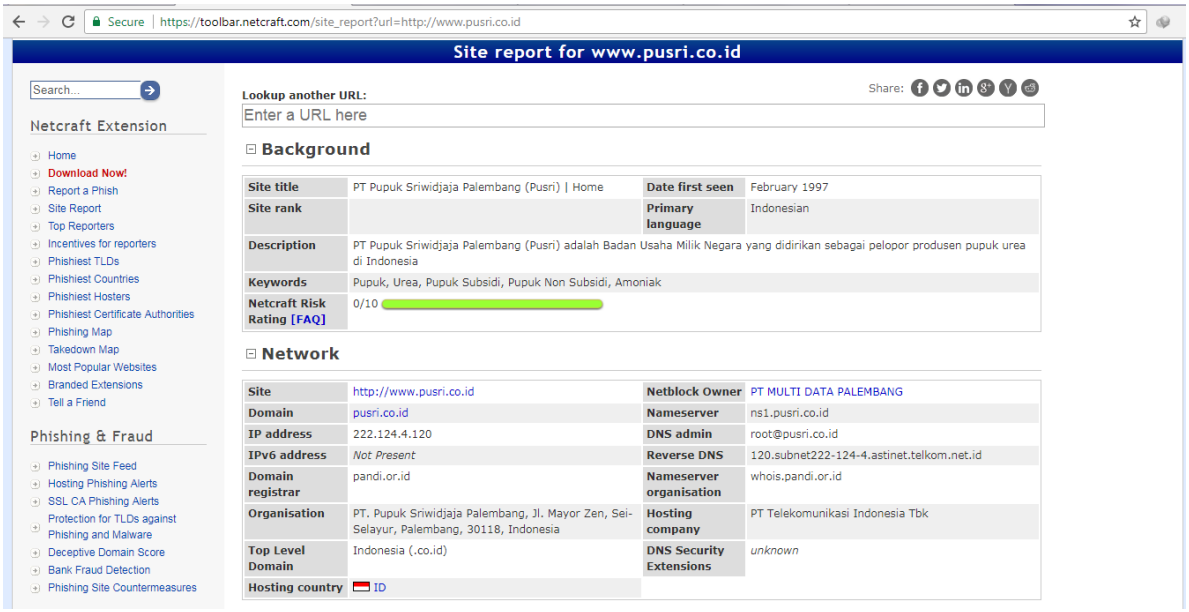
**2018**

- www.pusri.co.id

PT Pupuk Sriwidjaja Palembang (Pusri) adalah perusahaan yang didirikan sebagai pelopor produsen pupuk urea di Indonesia pada tanggal 24 Desember 1959 di Palembang Sumatera Selatan, dengan nama PT Pupuk Sriwidjaja (Persero). PT Pupuk Sriwidjaja menjalankan operasi bisnisnya dengan tujuan untuk melaksanakan dan menunjang kebijaksanaan dan program pemerintah di bidang ekonomi dan pembangunan nasional khususnya di industri pupuk dan kimia lainnya.

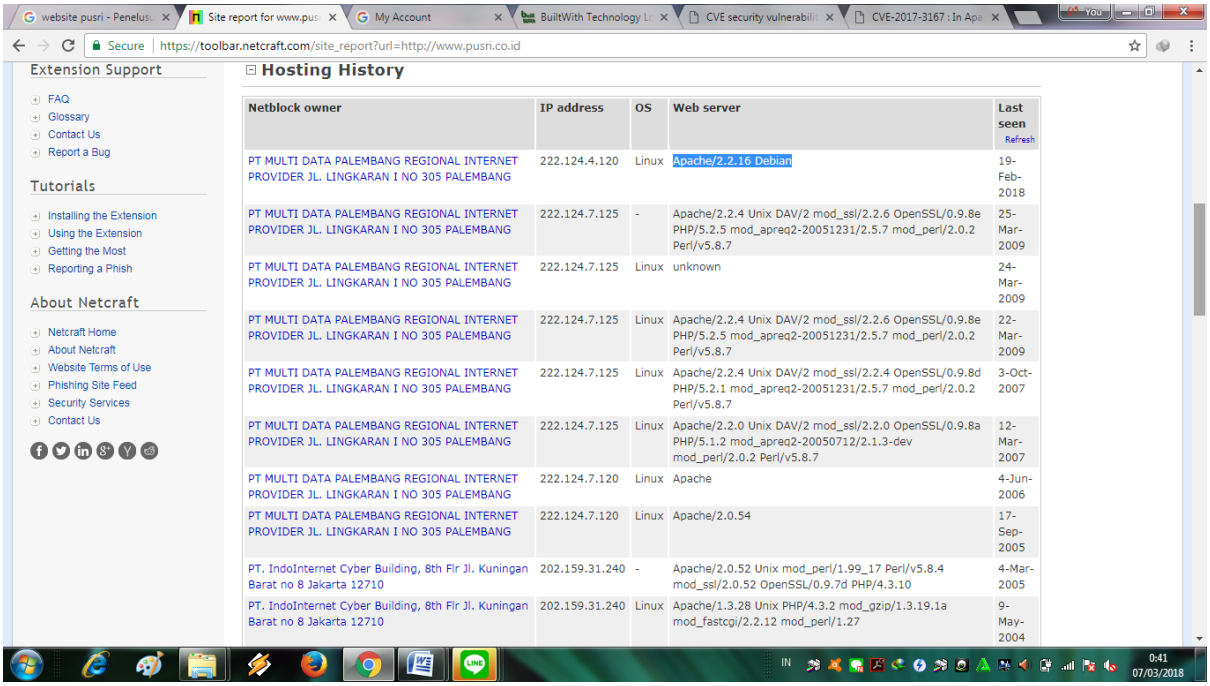
Data yang didapatkan berasal dari website Whois, netcraft, dan aplikasi nmap. Serta untuk mencari vurnerability dicari menggunakan website cvedetails.

Analisis Scanning pada website pusri.co.id dapat dilihat pada tabel dibawah ini :




Data Collection

| | |
|---|---|
| Domain | : pusri.co.id |
| IP Address | : 222.124.4.120 |
| Domain Registrar | : pandi.or.id |
| Top Level Domain | : Indonesia (co.id) |
| Nameserver | : ns1.pusri.co.id |
| DNS Admin | : root@pusri.co.id |
| Reserse DNS | : 120.subnet222-124-4.astinet.telkom.net.id |
| Hosting Company | : PT.Telekomunikasi Indonesia Tbk |



Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Tutorials

- Installing the Extension
- Using the Extension
- Getting the Most
- Reporting a Phish

About Netcraft

- Netcraft Home
- About Netcraft
- Website Terms of Use
- Phishing Site Feed
- Security Services
- Contact Us

**Hosting History**

| Netblock owner | IP address | OS | Web server | Last seen Refresh |
|---|---|---|---|---|
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.4.120 | Linux | Apache/2.2.16 Debian | 19-Feb-2018 |
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.7.125 | - | Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/5.2.5 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7 | 25-Mar-2009 |
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.7.125 | Linux | unknown | 24-Mar-2009 |
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.7.125 | Linux | Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/5.2.5 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7 | 22-Mar-2009 |
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.7.125 | Linux | Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.4 OpenSSL/0.9.8d PHP/5.2.1 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7 | 3-Oct-2007 |
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.7.125 | Linux | Apache/2.2.0 Unix DAV/2 mod_ssl/2.2.0 OpenSSL/0.9.8a PHP/5.1.2 mod_apreq2-20050712/2.1.3-dev mod_perl/2.0.2 Perl/v5.8.7 | 12-Mar-2007 |
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.7.120 | Linux | Apache | 4-Jun-2006 |
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.7.120 | Linux | Apache/2.0.54 | 17-Sep-2005 |
| PT. IndoInternet Cyber Building, 8th Flr Jl. Kuningan Barat no 8 Jakarta 12710 | 202.159.31.240 | - | Apache/2.0.52 Unix mod_perl/1.99_17 Perl/v5.8.4 mod_ssl/2.0.52 OpenSSL/0.9.7d PHP/4.3.10 | 4-Mar-2005 |
| PT. IndoInternet Cyber Building, 8th Flr Jl. Kuningan Barat no 8 Jakarta 12710 | 202.159.31.240 | Linux | Apache/1.3.28 Unix PHP/4.3.2 mod_gzip/1.3.19.1a mod_fastcgi/2.2.12 mod_perl/1.27 | 9-May-2004 |

Web Server : Apache/2.2.16 Debian

| Netblock owner | IP address | OS | Web server | Last seen Refresh |
|---|---|---|---|---|
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.4.120 | Linux | Apache/2.2.16 Debian | 19-Feb-2018 |

Vulnerabillity Details : CVE-2010-0425(1 Metasploit modules), CVSS Score : 10.0

**Vulnerability Details : CVE-2010-0425 (1 Metasploit modules)**

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

Publish Date : 2010-03-05 Last Update Date : 2017-09-18

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | 10.0 |
| Confidentiality Impact | Complete (There is total information disclosure, resulting in all system files being revealed.) |
| Integrity Impact | Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.) |
| Availability Impact | Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Execute Code |
| CWE ID | CWE id is not defined for this vulnerability |

Vulnerabillity Details : CVE-2011-3192(1 Metasploit modules), CVSS Score : 7.8

**Vulnerability Details : CVE-2011-3192 (1 public exploit) (1 Metasploit modules)**

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

Publish Date : 2011-08-29 Last Update Date : 2017-09-18

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | 7.8 |
| Confidentiality Impact | None (There is no impact to the confidentiality of the system.) |
| Integrity Impact | None (There is no impact to the integrity of the system) |
| Availability Impact | Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Denial Of Service |
| CWE ID | 399 |

Vulnerabillity Details : CVE-2007-6423, CVSS Score : 7.8

**Vulnerability Details : CVE-2007-6423**

** DISPUTED ** Unspecified vulnerability in mod_proxy_balancer for Apache HTTP Server 2.2.x before 2.2.7-dev, when running on Windows, allows remote attackers to trigger memory corruption via a long URL. NOTE: the vendor could not reproduce this issue.

Publish Date : 2008-01-11 Last Update Date : 2008-09-05

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | 7.8 |
| Confidentiality Impact | None (There is no impact to the confidentiality of the system.) |
| Integrity Impact | None (There is no impact to the integrity of the system) |
| Availability Impact | Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Memory corruption |
| CWE ID | 399 |

Web Server : Apache

| | | | | |
|---|---|---|---|---|
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.7.120 | Linux | Apache | 4-Jun-2006 |

Vulnerabillity Details : CVE-2017-5638, Score : 10.0

**Vulnerability Details : CVE-2017-5638 (1 Metasploit modules)**

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

Publish Date : 2017-03-10 Last Update Date : 2018-03-03

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | 10.0 |

Vulnerabillity Details : CVE-2016-3082, Score : 10.0

**Vulnerability Details : CVE-2016-3082**

XSLTResult in Apache Struts 2.x before 2.3.20.2, 2.3.24.x before 2.3.24.2, and 2.3.28.x before 2.3.28.1 allows remote attackers to execute arbitrary code via the stylesheet location parameter.

Publish Date : 2016-04-26 Last Update Date : 2016-11-28

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

CVSS Score 10.0

Vulnerabillity Details : CVE-2016-4461, Score : 9.0

**Vulnerability Details : CVE-2016-4461**

Apache Struts 2.x before 2.3.29 allows remote attackers to execute arbitrary code via a "%{}" sequence in a tag attribute, aka forced double OGNL evaluation. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-0785.

Publish Date : 2017-10-16 Last Update Date : 2017-11-07

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

CVSS Score 9.0

Web Server : Apache/2.0.54

| | | | | |
|---|---|---|---|---|
| PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG | 222.124.7.120 | Linux | Apache/2.0.54 | 17-Sep-2005 |

Vulnerabillity Details : CVE-2005-2700, Score : 10.0

**Vulnerability Details : CVE-2005-2700**

ssl_engine_kernel.c in mod_ssl before 2.8.24, when using "SSLVerifyClient optional" in the global virtual host configuration, does not properly enforce "SSLVerifyClient require" in a per-location context, which allows remote attackers to bypass intended access restrictions.

Publish Date : 2005-09-06 Last Update Date : 2017-10-10

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

CVSS Score 10.0

Vulnerabillity Details : CVE-2003-0016 Score : 7.5

**Vulnerability Details : CVE-2003-0016**

Apache before 2.0.44, when running on unpatched Windows 9x and Me operating systems, allows remote attackers to cause a denial of service or execute arbitrary code via an HTTP request containing MS-DOS device names.

Publish Date : 2003-02-07 Last Update Date : 2017-10-09

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

CVSS Score 7.5

Vulnerabillity Details : CVE-2004-0488, Score : 7.5

**Vulnerability Details : CVE-2004-0488**

Stack-based buffer overflow in the ssl_util_uuencode_binary function in ssl_util.c for Apache mod_ssl, when mod_ssl is configured to trust the issuing CA, may allow remote attackers to execute arbitrary code via a client certificate with a long subject DN.

Publish Date : 2004-07-07 Last Update Date : 2017-10-10

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

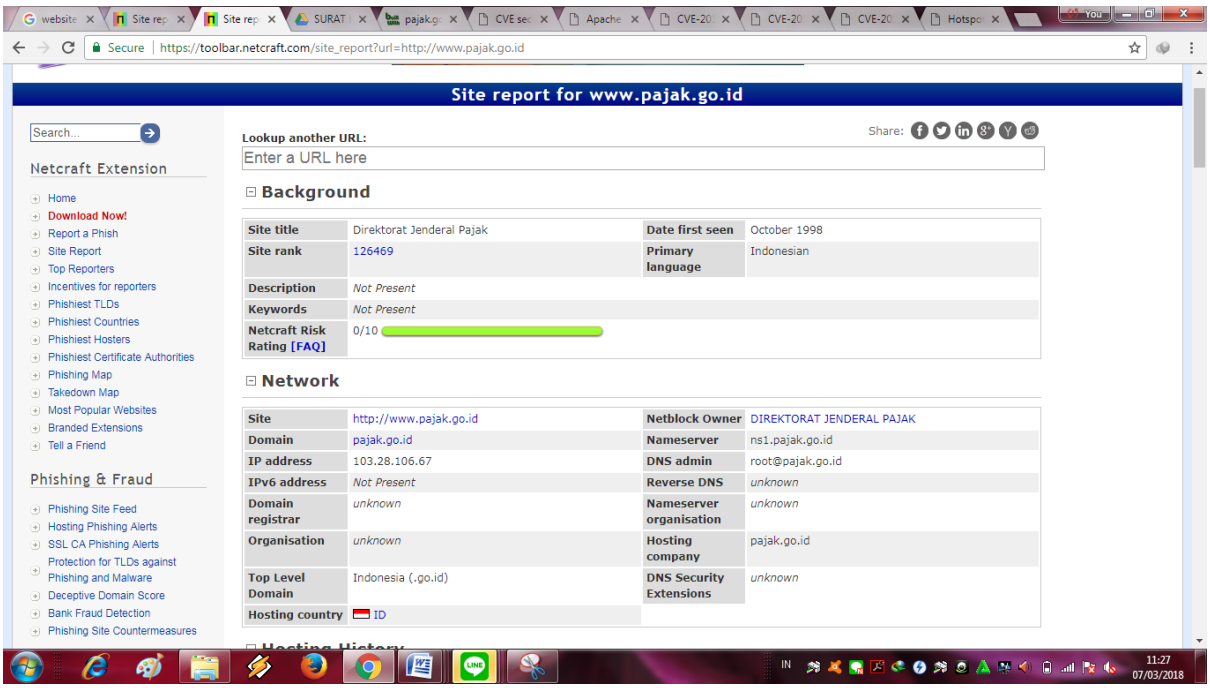
CVSS Score 7.5

- www.pajak.go.id

Pajak merupakan kata yang sangat familiar dimasyarakat kita, apalagi akhir-akhir ini lagi boomingnya pemberitaan negatif yang tentunya mendiskreditkan institusi kita, menggeneralisasikan semua insan pajak dikarenakan ulah oleh segelintir oknum di tubuh Direktorat Jenderal Pajak (DJP). Itulah salah satu cobaan institusi kita, hal tersebut merupakan badai kecil kawan, kenapa kita goyah? Itulah kerikil yang harus kita lewati/bersihkan dalam proses perjalanan reformasi di tubuh Direktorat Jenderal Pajak ini, kita harus bangga bahwa kementerian keuangan merupakan pelopor/pilot project dari reformasi birokrasi di republik ini, kementerian keuangan menjadi contoh dari kementerian/lembaga lain. Gaung nilai-nilai Kementerian Keuangan begitu menggema diseantero negeri dan menjadi pedoman perilaku, berfikir, serta bertindak seluruh insan Direktorat Jenderal Pajak dalam menjalankan tugas sehari-hari termasuk memberikan edukasi perpajakan kepada masyarakat. Oleh karena itu, memasyarakatkan pajak merupakan kewajiban kita bersama.

Data yang didapatkan berasal dari website Whois, netcraft, dan aplikasi nmap. Serta untuk mencari vurnerability dicari menggunakan website cvedetails.

Analisis Scanning pada website pajak.go.id dapat dilihat pada tabel dibawah ini :




Data Collection

Domain : pajak.co.id

IP Address : 103.28.106.67

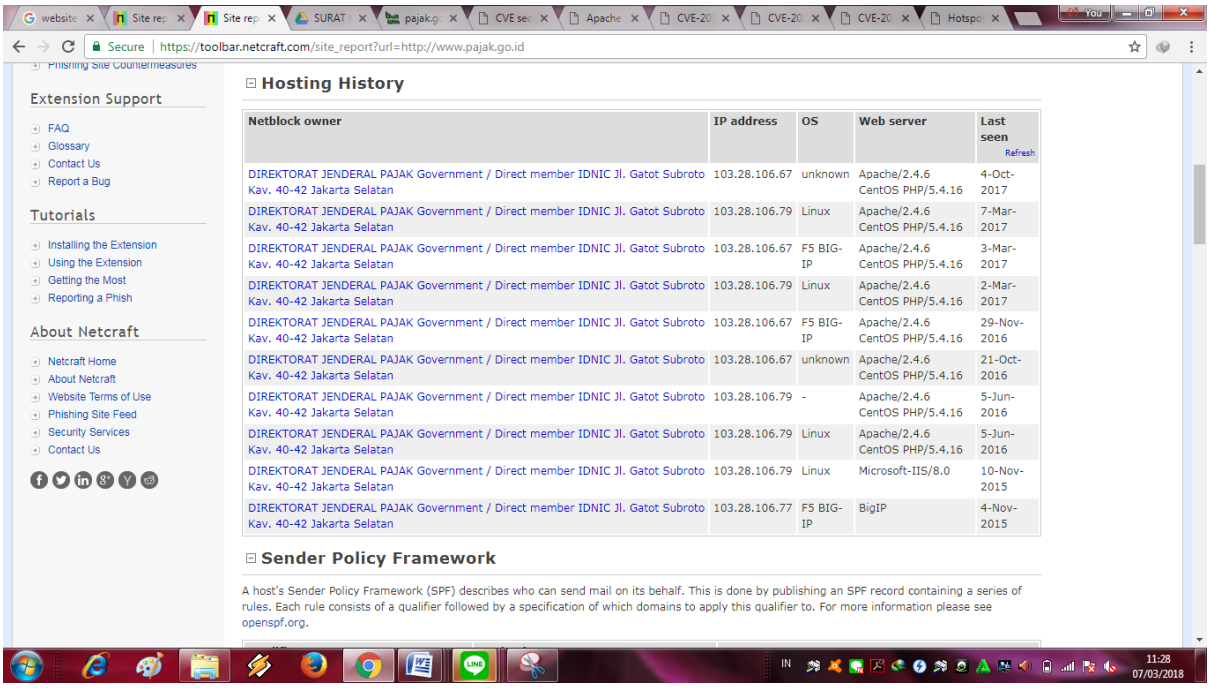
Domain Registrar : unknown

Top Level Domain : Indonesia (.go.id)

Nameserver : ns1.pajak.go.id

DNS Admin : root@pajak.go.id

Hosting Company : pajak.go.id




Web Server : Apache/2.4.6 CentOS PHP/5.4.16

| Netblock owner | IP address | OS | Web server | Last seen Refresh |
|---|---|---|---|---|
| DIREKTORAT JENDERAL PAJAK Government / Direct member IDNIC Jl. Gatot Subroto Kav. 40-42 Jakarta Selatan | 103.28.106.67 | unknown | Apache/2.4.6 CentOS PHP/5.4.16 | 4-Oct-2017 |

Vulnerability Details : CVE-2012-2379, Score : 10.0

Vulnerability Details : CVE-2017-9788, Score : 6.4

**Vulnerability Details : CVE-2017-9788**

In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

Publish Date : 2017-07-13 Last Update Date : 2018-01-04

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

CVSS Score 6.4

Vulnerability Details : CVE-2014-0226, Score : 6.8

**Vulnerability Details : CVE-2014-0226 (1 public exploit)**

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

Publish Date : 2014-07-20 Last Update Date : 2017-12-08

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

CVSS Score 6.8

Web Server : BigIP

| | | | | |
|---|---|---|---|---|
| DIREKTORAT JENDERAL PAJAK Government / Direct member IDNIC Jl. Gatot Subroto Kav. 40-42 Jakarta Selatan | 103.28.106.77 | F5 BIG-IP | BigIP | 4-Nov-2015 |

Vulnerability Details : CVE-2014-2927, Score : 9.3

**Vulnerability Details : CVE-2014-2927 (1 public exploit)**

The rsync daemon in F5 BIG-IP 11.6 before 11.6.0, 11.5.1 before HF3, 11.5.0 before HF4, 11.4.1 before HF4, 11.4.0 before HF7, 11.3.0 before HF9, and 11.2.1 before HF11 and Enterprise Manager 3.x before 3.1.1 HF2, when configured in failover mode, does not require authentication, which allows remote attackers to read or write to arbitrary files via a cmi request to the ConfigSync IP address.

Publish Date : 2014-10-15 Last Update Date : 2015-01-26

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

CVSS Score 9.3

Vulnerability Details : CVE-2016-5700, Score : 9.3

**Vulnerability Details : CVE-2016-5700**

Virtual servers in F5 BIG-IP systems 11.5.0, 11.5.1 before HF11, 11.5.2, 11.5.3, 11.5.4 before HF2, 11.6.0 before HF8, 11.6.1 before HF1, 12.0.0 before HF4, and 12.1.0 before HF2, when configured with the HTTP Explicit Proxy functionality or SOCKS profile, allow remote attackers to modify the system configuration, read system files, and possibly execute arbitrary code via unspecified vectors.

Publish Date : 2016-10-03 Last Update Date : 2016-11-28

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

CVSS Score 9.3

Vulnerability Details : CVE-2016-5020, Score : 9.0

**Vulnerability Details : CVE-2016-5020**

F5 BIG-IP before 12.0.0 HF3 allows remote authenticated users to modify the account configuration of users with the Resource Administration role and gain privilege via a crafted external Extended Application Verification (EAV) monitor script.

Publish Date : 2016-06-30 Last Update Date : 2016-12-06

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

CVSS Score 9.0