

KEAMANAN JARINGAN KOMPUTER  
“COMMON VULNERABILITIES AND EXPOSURES”

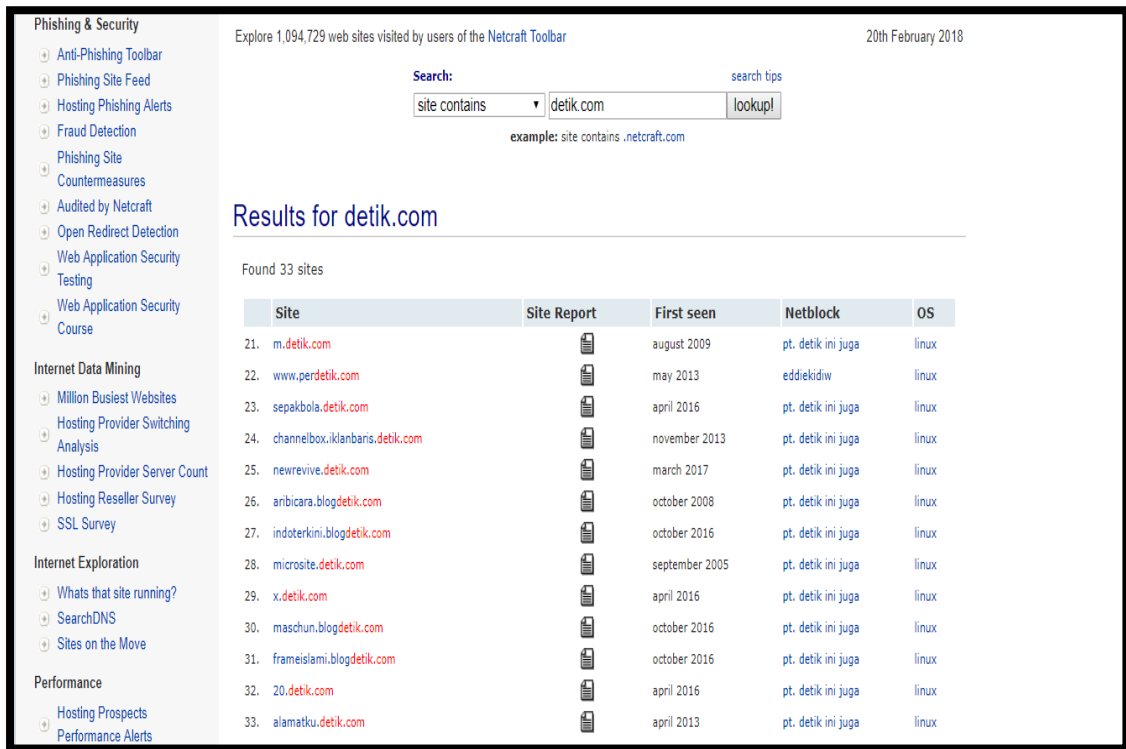


Disusun oleh :

Henny Pratiwi (09011281520129)

SISTEM KOMPUTER  
FASILKOM INDERALAYA  
UNIVERSITAS SRIWIJAYA  
2018

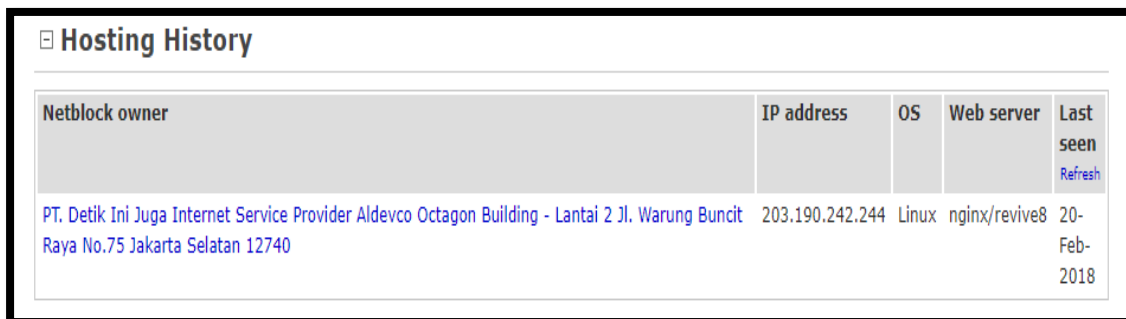
1. Deskripsi hasil pencarian hole pada system DNS ( detik.com )  
Menggunakan netcraft.com



The screenshot shows the Netcraft search interface. The search criteria are 'site contains' and 'detik.com'. The results table lists 33 sites. Item 25 is 'newrevive.detik.com', first seen in March 2017, hosted on pt.detikini.juga on Linux. The left sidebar contains various security and performance tools.

Site	Site Report	First seen	Netblock	OS
21. m.detik.com		august 2009	pt. detik ini juga	linux
22. www.perdetik.com		may 2013	eddiekidw	linux
23. sepakbola.detik.com		april 2016	pt. detik ini juga	linux
24. channelbox.iklanbis.detik.com		november 2013	pt. detik ini juga	linux
25. newrevive.detik.com		march 2017	pt. detik ini juga	linux
26. arbicara.blogdetik.com		october 2008	pt. detik ini juga	linux
27. indoterkini.blogdetik.com		october 2016	pt. detik ini juga	linux
28. microsite.detik.com		september 2005	pt. detik ini juga	linux
29. x.detik.com		april 2016	pt. detik ini juga	linux
30. maschun.blogdetik.com		october 2016	pt. detik ini juga	linux
31. frameislami.blogdetik.com		october 2016	pt. detik ini juga	linux
32. 20.detik.com		april 2016	pt. detik ini juga	linux
33. alamatku.detik.com		april 2013	pt. detik ini juga	linux

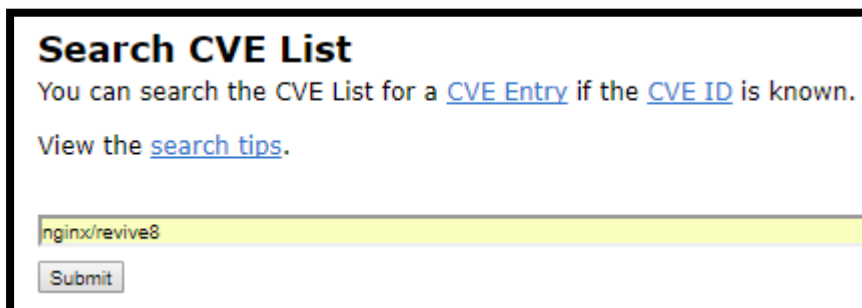
Klik site report pada maret 2017 site number 25 dan lihat hosting historynya lalu akan ada penjelasan pada web servernya "nginx/revive8"



The screenshot shows the 'Hosting History' section for detik.com. It displays a table with columns for Netblock owner, IP address, OS, Web server, and Last seen. The entry for item 25 shows the web server as 'nginx/revive8'.

Netblock owner	IP address	OS	Web server	Last seen
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.244	Linux	nginx/revive8	20-Feb-2018

Lalu buka cve.mitre.org pada bagian search cve list masukan "nginx/revive8"



The screenshot shows the CVE search interface. The search criteria is 'nginx/revive8'. The interface includes a search bar, a submit button, and instructions on how to search for CVE entries.

Maka akan ada tampilan berikut setelah mengklik submit

The screenshot shows the CVE List search results page. At the top, there is a navigation bar with links for CVE List, CNAs, Board, About, and News & Blog. The NVD logo is in the top right corner. Below the navigation bar, there are buttons for Search CVE List, Download CVE, Data Feeds, Request CVE IDs, and Update a CVE Entry. The total number of CVE entries is 96886. The search results section shows 40 entries that match the search. The first entry is CVE-2018-1299, which is highlighted in blue. The description of CVE-2018-1299 is: "In Apache Allura before 1.8.0, unauthenticated attackers may retrieve arbitrary files through the Allura web application. Some web servers used with Allura, such as Nginx, Apache/mod\_wsgi or paster may prevent the attack from succeeding. Others, such as gunicorn do not prevent it and leave Allura vulnerable."

Pada kali ini mendiskripsikan hole mengenai : Di Apache Allura sebelum 1.8.0, penyerang yang tidak diautentikasi dapat mengambil file yang sewenang-wenang melalui aplikasi web Allura. Beberapa webserver yang digunakan dengan Allura, seperti Nginx, Apache / mod\_wsgi atau paster dapat mencegah serangan dengan berhasil. Yang lainnya, seperti gunicorn tidak mencegahnya dan membiarkan Allura rentan.

## 2. Analisis Hole

The screenshot shows the CVE-2018-1299 Detail page. The title is "CVE-2018-1299 Detail". The status is "AWAITING ANALYSIS". The description is: "In Apache Allura before 1.8.0, unauthenticated attackers may retrieve arbitrary files through the Allura web application. Some web servers used with Allura, such as Nginx, Apache/mod\_wsgi or paster may prevent the attack from succeeding. Others, such as gunicorn do not prevent it and leave Allura vulnerable." The source is MITRE and the last modified date is 02/06/2018. The quick info section shows: CVE Dictionary Entry: CVE-2018-1299, Original release date: 02/06/2018, Last revised: 02/06/2018, Source: US-CERT/NIST. The references to advisories, solutions, and tools section provides a list of hyperlinks and resource types. The technical details section shows the vulnerability type as "View All".

## NEW FEATURES

Apache Allura 1.8.0 has been released. It contains a Docker setup for production environments, and improved security and auditing around user logins. This release also contains a large number of fixes and smaller improvements. To see all the details, check out the [release changelog](#).

## IMPORTANT SECURITY FIX

CVE-2018-1299 Apache Allura directory traversal vulnerability

### Versions Affected:

Apache Allura 1.7.0 and earlier

### Description:

Unauthenticated attackers may retrieve arbitrary files through the Allura web application. Some web servers used with Allura, such as Nginx, Apache/mod\_wsgi or paster may prevent the attack from succeeding. Others, such as gunicorn do not prevent it and leave Allura vulnerable.

### Mitigation:

Users of vulnerable web servers with Allura should upgrade to Allura 1.8.0 immediately.

### Credit:

This issue was discovered by Everardo Padilla Saca

viewing email #b52069073c13cb0184c9e1e2b34d411nc163a139... (and replies):

[Click to view as flat thread, sort by date](#)

[View Source](#) [Permalink](#) [Reply](#)

**From:** Dave Brondsema <b...@apache.org>  
**To:** de...@allura.apache.org, us...@allura.apache.org, an...@apache.org, os...@lists.openwall.com, se...@apache.org  
**Subject:** [SECURITY] CVE-2018-1299 Apache Allura directory traversal vulnerability  
**Date:** 2018/02/06 17:55:10  
**List:** dev@allura.apache.org

CVE-2018-1299 Apache Allura directory traversal vulnerability

Severity: Important

Vendor: The Apache Software Foundation

Versions Affected: Apache Allura 1.7.0 and earlier

### Description:

Unauthenticated attackers may retrieve arbitrary files through the Allura web application. Some web servers used with Allura, such as Nginx, Apache/mod\_wsgi or paster may prevent the attack from succeeding. Others, such as gunicorn do not prevent it and leave Allura vulnerable.

### Mitigation:

Users of vulnerable web servers with Allura should upgrade to Allura 1.8.0 immediately.

### Credit:

This issue was discovered by Everardo Padilla Saca

Untuk melihat lebih jelas maka bisa kita dilihat pada gambar diatas.

### 3. Cara penyerangan melalui hole yang ada

Dalam dunia hacking (tepatnya cracking ding!?) dikenal beberapa jenis serangan terhadap server. Berikut ini jenis-jenis serangan dasar yang dapat dikelompokkan dalam minimal 6 kelas, yaitu:

### 1. Intrusion

Pada jenis serangan ini seorang cracker (umumnya sudah level hacker) akan dapat menggunakan sistem komputer server. Serangan ini lebih terfokus pada full access granted dan tidak bertujuan merusak. Jenis serangan ini pula yg diterapkan oleh para hacker untuk menguji keamanan sistem jaringan mereka. Dilakukan dalam beberapa tahap dan tidak dalam skema kerja spesifik pada setiap serangannya (dijelaskan pada artikel lain). Hacking is an Art!?! =)

### 2. Denial of Services (DoS)

Penyerangan pada jenis DoS mengakibatkan layanan server mengalami stuck karena banjir request oleh mesin penyerang. Pada contoh kasus Distributed Denial of Services (DDoS) misalnya; dengan menggunakan mesin-mesin zombie, sang penyerang akan melakukan packeting request pada server secara serentak asimetris dan simultan sehingga buffer server akan kelabakan menjawabnya!?! Stuck/hung akan menimpa server. Jadi bukan server lagi namanya!?! (servicenya mati masak dibidang server? hehehe....)

### 3. Joyrider

Nah, ini namanya serangan iseng!?! Karena kebanyakan baca novel-novel hacking dan gak bisa belajar benar, isenglah jadinya nyoba-nyoba nyerang pake ilmu-ilmu instan super cepat (istilahnya 'onani' dimesin orang). Atau dengan alasan pengen tau isinya mesin orang!?! =). Yang jelas serangan jenis ini rata-rata karena rasa ingin tau, tapi ada juga yang sampe menyebabkan kerusakan atau kehilangan data.

### 4. Vandal

Jenis serangan spesialis pengrusak!?! nothing else to explain mbah!?! =)

### 5. Scorekeeper

Serangan yang bertujuan mencapai reputasi hasil cracking terbanyak. Biasanya hanya berbentuk deface halaman web (index/nambah halaman) dengan memampangkan NickName dan kelompok tertentu. Sebagian besar masih tidak peduli dengan isi mesin sasarannya =). Saat ini jenis penyerang ini lebih dikenal dengan sebutan WannaBe/Script kiddies.

### 6. Spy

Tiga hurup saja. Jenis serangan untuk memperoleh data atau informasi rahasia dari mesin target. Biasanya menyerang pada mesin-mesin dengan aplikasi database didalamnya. Kadang kala suatu perusahaan menyewa 'mata-mata' untuk mencuri data perusahaan rivalnya

Attach signature (signatures can be changed in profile) close

### 1. IP Spoofing

IP Spoofing juga dikenal sebagai Source Address Spoofing, yaitu pemalsuan alamat IP attacker sehingga sasaran menganggap alamat IP attacker adalah alamat IP dari host di dalam network bukan dari luar network. Misalkan attacker mempunyai IP address type A 66.25.xx.xx ketika attacker melakukan serangan jenis ini maka Network yang diserang akan menganggap IP attacker adalah bagian dari Networknya misal 192.xx.xx.xx yaitu IP type C. IP Spoofing terjadi ketika seorang attacker 'mengakali' packet routing untuk mengubah arah dari data atau transmisi ke tujuan yang berbeda. Packet untuk routing biasanya di transmisikan secara transparan dan jelas sehingga membuat attacker dengan mudah untuk memodifikasi asal data ataupun tujuan dari data. Teknik ini bukan hanya dipakai oleh attacker tetapi juga dipakai oleh para security profesional untuk men tracing identitas dari para attacker.

### 2. FTP Attack

Salah satu serangan yang dilakukan terhadap File Transfer Protocol adalah serangan buffer overflow yang diakibatkan oleh malformed command. tujuan menyerang FTP server ini rata-rata adalah untuk mendapatkan command shell ataupun untuk melakukan Denial Of Service. Serangan Denial Of Service akhirnya dapat menyebabkan seorang user atau attacker untuk mengambil resource didalam network tanpa adanya otorisasi, sedangkan command shell dapat membuat seorang attacker mendapatkan akses ke sistem server dan file-file data yang akhirnya seorang attacker bisa membuat anonymous root-acces yang mempunyai hak penuh terhadap system bahkan network yang diserang. Tidak pernah atau jarang mengupdate versi server dan mempatchnya adalah kesalahan yang sering dilakukan oleh seorang admin dan inilah yang membuat server FTP menjadi rawan untuk dimasuki. Sebagai contoh adalah FTP server yang populer di keluarga UNIX yaitu WU-FTPD yang selalu diupgrade dua kali dalam sehari untuk memperbaiki kondisi yang mengizinkan terjadinya bufferoverflow. Mengexploitasi FTP juga berguna untuk mengetahui password yang terdapat dalam sistem, FTP Bounce attack (menggunakan server ftp orang lain untuk melakukan serangan), dan mengetahui atau mensniff informasi yang berada dalam sistem

### 3. Unix Finger Exploits

Pada masa awal internet, Unix OS finger utility digunakan secara efficient untuk men sharing informasi diantara pengguna. Karena permintaan informasi terhadap informasi finger ini tidak menyalahkan peraturan, kebanyakan system Administrator meninggalkan utility ini (finger) dengan keamanan yang sangat minim, bahkan tanpa kemanan sama sekali. Bagi seorang attacker utility ini sangat berharga untuk melakukan informasi tentang footprinting, termasuk nama login dan informasi contact. Utility ini juga menyediakan keterangan yang sangat baik tentang aktivitas user didalam sistem, berapa lama user berada dalam sistem dan seberapa jauh user merawat sistem. Informasi yang dihasilkan dari finger ini dapat meminimalisasi usaha cracker dalam menembus sebuah sistem. Keterangan pribadi tentang user yang dimunculkan oleh finger daemon ini sudah cukup bagi seorang atacker untuk melakukan social

engineering dengan menggunakan social skillnya untuk memanfaatkan user agar 'memberitahu' password dan kode akses terhadap system.

#### 4. Flooding & Broadcasting

Seorang attacker bisa menguarangi kecepatan network dan host-host yang berada di dalamnya secara significant dengan cara terus melakukan request/permintaan terhadap suatu informasi dari sever yang bisa menangani serangan classic Denial Of Service (Dos), mengirim request ke satu port secara berlebihan dinamakan flooding, kadang hal ini juga disebut spraying. Ketika permintaan flood ini dikirim ke semua station yang berada dalam network serangan ini dinamakan broadcasting. Tujuan dari kedua serangan ini adalah sama yaitu membuat network resource yang menyediakan informasi menjadi lemah dan akhirnya menyerah. Serangan dengan cara Flooding bergantung kepada dua faktor yaitu: ukuran dan/atau volume (size and/or volume). Seorang attacker dapat menyebabkan Denial Of Service dengan cara melempar file berkapasitas besar atau volume yang besar dari paket yang kecil kepada sebuah system. Dalam keadaan seperti itu network server akan menghadapi kemacetan: terlalu banyak informasi yang diminta dan tidak cukup power untuk mendorong data agar berjalan. Pada dasarnya paket yang besar membutuhkan kapasitas proses yang besar pula, tetapi secara tidak normal paket yang kecil dan sama dalam volume yang besar akan menghabiskan resource secara percuma, dan mengakibatkan kemacetan.

#### 5. Fragmented Packet Attacks

Data-data internet yang di transmisikan melalui TCP/IP bisa dibagi lagi ke dalam paket-paket yang hanya mengandung paket pertama yang isinya berupa informasi bagian utama( kepala) dari TCP. Beberapa firewall akan mengizinkan untuk memroses bagian dari paket-paket yang tidak mengandung informasi alamat asal pada paket pertamanya, hal ini akan mengakibatkan beberapa type system menjadi crash. Contohnya, server NT akan menjadi crash jika paket-paket yang dipecah(fragmented packet) cukup untuk menulis ulang informasi paket pertama dari suatu protokol.

#### 6. E-mail Exploits

Peng-exploitasian e-mail terjadi dalam lima bentuk yaitu: mail floods, manipulasi perintah (command manipulation), serangan tingkat transportasi(transport level attack), memasukkan berbagai macam kode (malicious code inserting) dan social engineering(memanfaatkan sosialisasi secara fisik). Penyerangan email bisa membuat system menjadi crash, membuka dan menulis ulang bahkan mengeksekusi file-file aplikasi atau juga membuat akses ke fungsi fungsi perintah (command function).

#### 7. DNS and BIND Vulnerabilities

Berita baru-baru ini tentang kerawanan (vulnerabilities) tentang aplikasi Berkeley Internet Name Domain (BIND) dalam berbagai versi mengilustrasikan kerapuhan dari Domain Name System (DNS), yaitu krisis yang diarahkan pada operasi dasar dari Internet (basic internet operation).

## 8. Password Attacks

Password merupakan sesuatu yang umum jika kita bicara tentang keamanan. Kadang seorang user tidak peduli dengan nomor pin yang mereka miliki, seperti bertransaksi online di warnet, bahkan bertransaksi online dirumah pun sangat berbahaya jika tidak dilengkapi dengan software security seperti SSL dan PGP. Password adalah salah satu prosedur keamanan yang sangat sulit untuk diserang, seorang attacker mungkin saja mempunyai banyak tools (secara teknik maupun dalam kehidupan sosial) hanya untuk membuka sesuatu yang dilindungi oleh password. Ketika seorang attacker berhasil mendapatkan password yang dimiliki oleh seorang user, maka ia akan mempunyai kekuasaan yang sama dengan user tersebut. Melatih karyawan/user agar tetap waspada dalam menjaga passwordnya dari social engineering setidaknya dapat meminimalisir risiko, selain berjaga-jaga dari praktek social engineering organisasi pun harus mewaspadai hal ini dengan cara teknikal. Kebanyakan serangan yang dilakukan terhadap password adalah menebak (guessing), brute force, cracking dan sniffing.

## 9. Proxy Server Attacks

Salah satu fungsi Proxy server adalah untuk mempercepat waktu response dengan cara menyatukan proses dari beberapa host dalam suatu trusted network. Dalam kebanyakan kasus, tiap host mempunyai kekuasaan untuk membaca dan menulis (read/write) yang berarti apa yang bisa saya lakukan dalam system saya akan bisa juga saya lakukan dalam system anda dan sebaliknya.

## 10. Remote Command Processing Attacks

Trusted Relationship antara dua atau lebih host menyediakan fasilitas pertukaran informasi dan resource sharing. Sama halnya dengan proxy server, trusted relationship memberikan kepada semua anggota network kekuasaan akses yang sama di satu dan lain system (dalam network). Attacker akan menyerang server yang merupakan anggota dari trusted system. Sama seperti kerawanan pada proxy server, ketika akses diterima, seorang attacker akan mempunyai kemampuan mengeksekusi perintah dan mengakses data yang tersedia bagi user lainnya.

## 11. Remote File System Attack

Protocol-protokol untuk transportasi data –tulang punggung dari internet— adalah tingkat TCP (TCPLevel) yang mempunyai kemampuan dengan mekanisme untuk baca/tulis (read/write) Antara network dan host. Attacker bisa dengan mudah mendapatkan jejak informasi dari mekanisme ini untuk mendapatkan akses ke direktori file.

## 12. Selective Program Insertions

Selective Program Insertions adalah serangan yang dilakukan ketika attacker menaruh program-program penghancur, seperti virus, worm dan trojan (mungkin istilah ini sudah anda kenal dengan baik ?) pada system sasaran. Program-program penghancur ini sering juga disebut malware. Program-program ini mempunyai kemampuan untuk merusak system, pemusnahan file, pencurian password sampai dengan membuka backdoor.



### 13. Port Scanning

Melalui port scanning seorang attacker bisa melihat fungsi dan cara bertahan sebuah system dari berbagai macam port. Seorang atacker bisa mendapatkan akses kedalam sistem melalui port yang tidak dilindungi. Sebaia contoh, scanning bisa digunakan untuk menentukan dimana default SNMP string di buka untuk publik, yang artinya informasi bisa di extract untuk digunakan dalam remote command attack.

### 14. TCP/IP Sequence Stealing

Passive Port Listening and Packet Interception TCP/IP Sequence Stealing, Passive Port Listening dan Packet Interception berjalan untuk mengumpulkan informasi yang sensitif untuk mengkases network. Tidak seperti serangan aktif maupun brute-force, serangan yang menggunakan metoda ini mempunyai lebih banyak kualitas stealth-like.

### 15. HTTPD Attacks

Kerawanan yang terdapat dalam HTTPD ataupun webservice ada lima macam: buffer overflows, httpd bypasses, cross scripting, web code vulnerabilities, dan URL floods. HTTPD Buffer Overflow bisa terjadi karena attacker menambahkan errors pada port yang digunakan untuk web traffic dengan cara memasukan banyak carackter dan string untuk menemukan tempat overflow yang sesuai. Ketika tempat untuk overflow ditemukan, seorang attacker akan memasukkan string yang akan menjadi perintah yang dapat dieksekusi. Bufer-overflow dapat memberikan attacker akses ke command prompt. Smile Beer

Daftar pustaka :

<https://www.netcraft.com/>

[http://cve.mitre.org/cve/search\\_cve\\_list.html](http://cve.mitre.org/cve/search_cve_list.html)

<https://jombreng.wordpress.com/cara-dan-jenis-hacker-menyerang-situs/>