# *KEAMANAN JARINGAN*
# *ACCESS COTROL*


Disusun oleh:

1. Hoiriyah (14917141)
2. Winda A.W (14917163)
3. Dewi Yunita Sari (14917116)

**MAGISTER TEKNIK INFORMATIKA**
**PASCASARJANA FAKULTAS TEKNOLOGI INDUSTRI**
**UNIVERSITAS ISLAM INDONESIA**
**YOGYAKARTA**
**2015**

**TUGAS**

1. Gunakan salah satu aplikasi untuk pentest vulnerability. Tarik benang merah dari akses kontrol uji coba tools untuk vulnerability test
    - Pilih salah satu tools (open vas, dll)
    - Terapkan pada situs sendiri atau buat sejumlah server pada lingkungan virtual
    - Instal dan terapkan mekanisme vulnerability testing pada situs atau server tersebut
    - Kaitkan temuan dari output dengan issue access control

**JAWABAN**

**1. Eksperimen tahapan *website penetration test*:**

**a. *Identify the target***

- Target *pentest* : www.uii.ac.id
- ping www.uii.ac.id

```
C:\Users\ninkyhade>ping www.uii.ac.id

Pinging uii.ac.id [202.162.37.148] with 32 bytes of data:
Reply from 202.162.37.148: bytes=32 time=780ms TTL=50
Reply from 202.162.37.148: bytes=32 time=288ms TTL=50
Reply from 202.162.37.148: bytes=32 time=288ms TTL=50
Reply from 202.162.37.148: bytes=32 time=300ms TTL=50

Ping statistics for 202.162.37.148:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 288ms, Maximum = 780ms, Average = 414ms

C:\Users\ninkyhade>
```

- ping 202.162.37.148

```
C:\Users\ninkyhade>ping 202.162.37.148

Pinging 202.162.37.148 with 32 bytes of data:
Reply from 202.162.37.148: bytes=32 time=694ms TTL=50
Reply from 202.162.37.148: bytes=32 time=288ms TTL=50
Reply from 202.162.37.148: bytes=32 time=268ms TTL=50
Reply from 202.162.37.148: bytes=32 time=278ms TTL=50

Ping statistics for 202.162.37.148:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 268ms, Maximum = 694ms, Average = 382ms

C:\Users\ninkyhade>
```

- whois 202.162.37.148

```
root@amplopdigital:~# whois 202.162.37.148
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '202.162.32.0 - 202.162.47.255'

inetnum:        202.162.32.0 - 202.162.47.255
netname:        UIINET-ID
descr:          PT Global Prima Utama
descr:          Internet Service Provider
descr:          Jl Cik Di Tiro 1 Yogyakarta
country:        ID
admin-c:        UH11-AP
tech-c:         UH11-AP
mnt-by:         MNT-APJII-ID
mnt-lower:      MAINT-ID-UIINET
changed:        hostmaster@apjii.or.id 20020930
changed:        hostmaster@apjii.or.id 20021231
changed:        hostmaster@apjii.or.id 20031024
status:         ALLOCATED PORTABLE
remarks:        spam and abuse report : abuse@apjii.or.id, abuse@uii.net.id
source:         APNIC

person:         UIInet Hostmaster
address:        Jl Cik Di Tiro 1, UII Building
address:        Yogyakarta Indonesia
country:        ID
phone:          +62-274-555888
fax-no:         +62-274-580821
e-mail:         hostmaster@uii.net.id
nic-hdl:        UH11-AP
mnt-by:         MAINT-ID-UIINET
changed:        hostmaster@uii.net.id 20020208
source:         APNIC

% Information related to '202.162.37.0/24AS17996'

route:          202.162.37.0/24
descr:          PT Global Prima Utama
descr:          Internet Service Provider
descr:          Jl Cik Di Tiro 1 Yogyakarta
country:        ID
origin:         AS17996
mnt-by:         MAINT-ID-UIINET
changed:        hostmaster@apjii.or.id 20030203
source:         APNIC

% This query was served by the APNIC Whois Service version 1.69.1-APNICv1r6-SNAP
SHOT (WHOIS4)
```

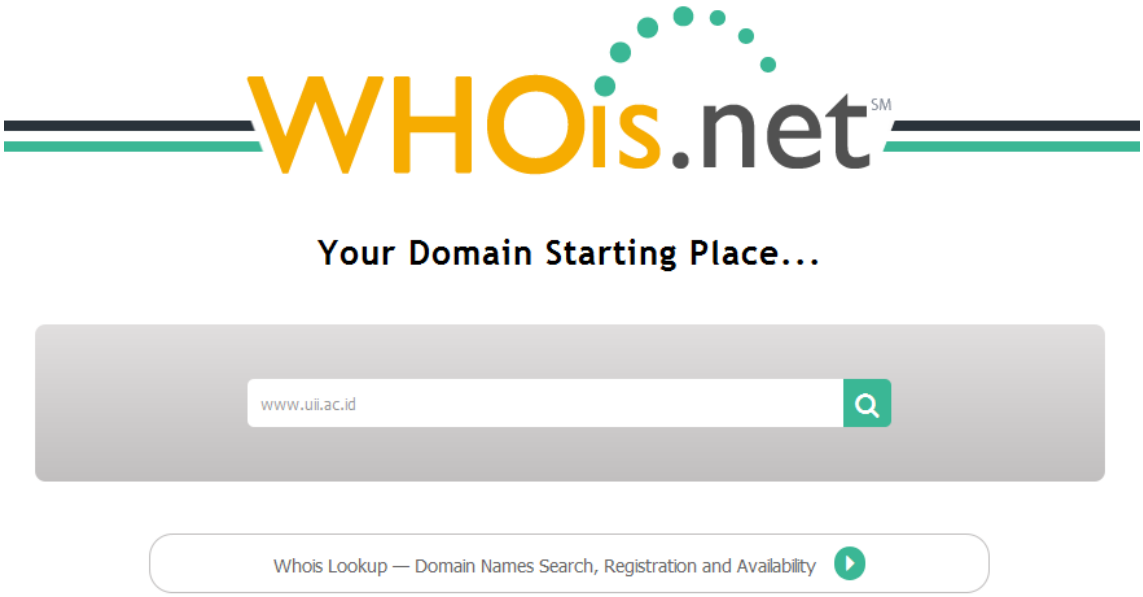
- dnsmap [www.uii.ac.id](http://www.uii.ac.id)

```
root@amplopdigital:~# dnsmap www.uii.ac.id
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for www.uii.ac.id using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests


[+] 0 (sub)domains and 0 IP address(es) found
[+] completion time: 704 second(s)
```

- Melakukan *query* ke whois *database*.



# WHOIS LOOKUP

**uii.ac.id is already registered***

Domain ID:PANDI-DO227785
Domain Name:UII.AC.ID
Created On:18-May-1995 13:32:26 UTC
Last Updated On:16-Sep-2014 08:27:02 UTC
Expiration Date:01-Oct-2016 23:59:59 UTC
Status:clientTransferProhibited
Status:serverTransferProhibited
Registrant ID:01190626g31
Registrant Name:Trisna Samodra
Registrant Organization:personal
Registrant Street1:Gd Prabuningrat UII kampus terpadu
Registrant Street2:Jl Kaliurang Km 14.4
Registrant City:Yogyakarta
Registrant State/Province:DIY
Registrant Postal Code:55584
Registrant Country:ID
Registrant Phone:+62.274898444
Registrant FAX:+62.274898444
Registrant Email:trisna@uii.ac.id
Admin ID:01190626g31
Admin Name:Trisna Samodra
Admin Organization:personal
Admin Street1:Gd Prabuningrat UII kampus terpadu
Admin Street2:Jl Kaliurang Km 14.4
Admin City:Yogyakarta
Admin State/Province:DIY
Admin Postal Code:55584
Admin Country:ID
Admin Phone:+62.274898444
Admin FAX:+62.274898444
Admin Email:trisna@uii.ac.id
Tech ID:01190626g31
Tech Name:Trisna Samodra
Tech Organization:personal
Tech Street1:Gd Prabuningrat UII kampus terpadu
Tech Street2:Jl Kaliurang Km 14.4
Tech City:Yogyakarta
Tech State/Province:DIY
Tech Postal Code:55584
Tech Country:ID
Tech Phone:+62.274898444
Tech FAX:+62.274898444
Tech Email:trisna@uii.ac.id
Billing ID:01190626g31
Billing Name:Trisna Samodra
Billing Organization:personal
Billing Street1:Gd Prabuningrat UII kampus terpadu
Billing Street2:Jl Kaliurang Km 14.4
Billing City:Yogyakarta
Billing State/Province:DIY
Billing Postal Code:55584
Billing Country:ID
Billing Phone:+62.274898444
Billing FAX:+62.274898444
Billing Email:trisna@uii.ac.id
Sponsoring Registrar ID:digitalreg
Sponsoring Registrar Organization:Digital Registra
Sponsoring Registrar Postal Code:55281
Sponsoring Registrar Country:ID
Sponsoring Registrar Phone:0274882257
Name Server:SVR1.UII.AC.ID
Name Server:SVR2.UII.AC.ID
DNSSEC:Unsigned

**b. *Fingerprint website***

- Menggunakan *tool* Netcraft untuk mengetahui detail informasi dari [www.uii.ac.id](http://www.uii.ac.id)

## Site report for www.uii.ac.id

Share:

**Lookup another URL:**

Enter a URL here

### Background

| | | | |
|---|---|---|---|
| **Site title** | 503 Service Unavailable | **Date first seen** | February 1999 |
| **Site rank** | 727428 | **Primary language** | English |
| **Description** | *Not Present* | | |
| **Keywords** | *Not Present* | | |

### Network

| | | | |
|---|---|---|---|
| **Site** | http://www.uii.ac.id | **Netblock Owner** | PT Global Prima Utama |
| **Domain** | uii.ac.id | **Nameserver** | svr1.uii.ac.id |
| **IP address** | 202.162.37.148 | **DNS admin** | prayitna@yahoo.com |
| **IPv6 address** | *Not Present* | **Reverse DNS** | 202.162.37.148-static.reverse.uii.net.id |
| **Domain registrar** | pandi.or.id | **Nameserver organisation** | whois.pandi.or.id |
| **Organisation** | personal, Gd Prabuningrat UII kampus terpadu, Jl Kaliurang Km 14.4, Yogyakarta, 55584, Indonesia | **Hosting company** | uii.net.id |
| **Top Level Domain** | Indonesia (.ac.id) | **DNS Security Extensions** | *unknown* |
| **Hosting country** | ID | | |

## Hosting History

| Netblock owner | IP address | OS | Web server | Last seen Refresh |
|---|---|---|---|---|
| PT Global Prima Utama Internet Service Provider Jl Cik Di Tiro 1 Yogyakarta | 202.162.37.148 | Linux | Apache/2.2.15 CentOS | 4-Oct-2015 |
| PT Global Prima Utama Internet Service Provider Jl Cik Di Tiro 1 Yogyakarta | 202.162.37.148 | Linux | unknown | 30-Sep-2015 |
| PT Global Prima Utama Internet Service Provider Jl Cik Di Tiro 1 Yogyakarta | 202.162.37.148 | Linux | Apache/2.2.15 CentOS | 9-Jun-2015 |
| PT Global Prima Utama Internet Service Provider Jl Cik Di Tiro 1 Yogyakarta | 202.162.37.148 | Linux | unknown | 31-Mar-2015 |
| PT Global Prima Utama Internet Service Provider Jl Cik Di Tiro 1 Yogyakarta | 202.162.37.148 | Linux | Apache/2.2.15 CentOS | 30-Mar-2015 |
| PT Global Prima Utama Internet Service Provider Jl Cik Di Tiro 1 Yogyakarta | 202.162.37.148 | Linux | Apache/2.2.3 CentOS | 19-Jul-2014 |
| PT Global Prima Utama Internet Service Provider Jl Cik Di Tiro 1 Yogyakarta | 202.162.37.148 | unknown | Apache/2.2.3 CentOS | 22-Sep-2013 |
| PT Global Prima Utama Internet Service Provider Jl Cik Di Tiro 1 Yogyakarta | 202.162.37.164 | Linux | Apache/2.2.11 Unix mod_ssl/2.2.11 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.5 | 1-Mar-2012 |
| PT Global Prima Utama Internet Service Provider Jl Cik Di Tiro 1 Yogyakarta | 202.162.37.164 | unknown | Apache/2.2.10 Unix mod_ssl/2.2.10 OpenSSL/0.9.8b mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.5 | 27-Nov-2008 |
| PT Global Prima Utama Internet Service Provider Jl Cik Di Tiro 1 Yogyakarta | 202.162.37.164 | Linux | Apache/2.0.63 Unix mod_ssl/2.0.63 OpenSSL/0.9.8b mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.5 | 1-Jul-2008 |

## Security

| | | | |
|---|---|---|---|
| **Netcraft Risk Rating [FAQ]** | 0/10  | | |
| **On Spamhaus Block List** | No | **On Exploits Block List** | No |
| **On Policy Block List** | No | **On Domain Block List** | No |

- Analisis file robots.txt untuk mengetahui direktori yang diperbolehkan untuk diakses dan yang tidak diperbolehkan.


```
User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /components/
Disallow: /editor/
Disallow: /help/
Disallow: /includes/
Disallow: /language/
Disallow: /mambots/
Disallow: /media/
Disallow: /modules/
Disallow: /templates/
Disallow: /installation/
Allow: /images
Allow: /images/stories/pengumuman
Allow: /images/stories/agenda
Allow: /images/stories/scholarship
Allow: /dmdocuments
```

- nmap 202.162.37.148

nmap 202.162.37.148.txt

**c.** ***Perform vulnerability assessment***

- nikto -h 202.162.37.148

nikto -h 202.162.37.148.txt

- nikto -h www.uii.ac.id

```
root@amplopdigital:~# nikto -h www.uii.ac.id
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          202.162.37.148
+ Target Hostname:    www.uii.ac.id
+ Target Port:        80
+ Start Time:         2015-11-30 18:48:05 (GMT7)
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (CentOS)
+ Cookie e27f0eaed25ee8ebbb575d5abc084539 created without the httponly flag
+ Cookie lang created without the httponly flag
+ Cookie mbfcookie created without the httponly flag
+ Cookie mbfcookie[lang] created without the httponly flag
+ Cookie mosvisitor created without the httponly flag
+ Cookie JATheme created without the httponly flag
+ Cookie ColorCSS created without the httponly flag
+ Cookie ScreenType created without the httponly flag
+ Cookie FontSize created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.3
+ The anti-clickjacking X-Frame-Options header is not present.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  10 error(s) and 11 item(s) reported on remote host
+ End Time:           2015-11-30 18:54:09 (GMT7) (364 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- Cek *vulnerability* hasil nikto. *Vulnerability* yang ditemukan menggunakan nikto, didasarkan pada kode dari OSVDB (*Open Sourced Vulnerability Database*). Kode tersebut dapat di-*crosscheck* menggunakan web www.osvdb.org.

hasil vulnerability assessment.txt

**d. Kesimpulan**

- Target adalah www.uii.ac.id yang memiliki IP *address* publik 202.162.37.148.
- IP 202.162.37.148 tersebut berada pada *range* IP *address* 202.162.32.0 - 202.162.48.255 yang dimiliki oleh UIINET-ID (PT. Global Prima Utama). *Range* IP *address* tersebut berada di bawah APNIC.
- Penanggung jawab nama domain uii.ac.id adalah Trisna Samodra dengan email trisna@uii.ac.id.
- www.uii.ac.id di-*hosting* di perusahaan *hosting* uii.net.id (PT. Global Prima Utama), dengan *nameserver*-nya adalah svr1.uii.ac.id dan *nameserver admin*-nya memiliki alamat email kusprayitna@yahoo.com.
- Dari sejarah *hosting* diketahui bahwa www.uii.ac.id selalu di-*hosting* di PT. Global Prima Utama. Sejak 22 September 2013 berubah IP *address* publiknya dari 202.162.37.164 ke 202.162.37.148. Pada 4 Oktober 2015 tercatat bahwa www.uii.ac.id menggunakan sistem operasi Linux CentOS dengan web server Apache 2.2.15.

- Berdasarkan hasil *scan* port menggunakan IP *address* web server, ditemukan banyak sekali port yang terbuka. Hal ini dapat membahayakan karena penyerang dapat memanfaatkan port-port tersebut untuk mendapatkan akses ke server secara ilegal.
- Setelah dilakukan *vulnerability assessment*, ditemukan bahwa banyak sekali celah keamanan yang perlu diperbaiki.

**2. Saran/*counter-measures* untuk perbaikan *website*:**

**a. Saran untuk perbaikan web server**

- Cek hasil *vulnerability assessment* menggunakan web www.osvdb.org. Oleh karena banyaknya *vulnerability* yang ditemukan, maka penulis hanya mengambil beberapa saja dan dibagi menjadi 3 kategori, yaitu:
  - ❖ ***High*** → sangat mendesak

| ***Buffer Overflow*** | |
|---|---|
| OSVDB-2017 | ***Problem:*** Buffer overflow in index.cgi administration interface for Boozt! Standard 0.9.8 allows local users to execute arbitrary code via a long name field when creating a new banner. ***Solution:*** Upgrade to version 0.9.9alpha or higher, as it has been reported to fix this vulnerability. |
| OSVDB-2735 | ***Problem:*** Buffer overflow in Musicqueue 1.2.0 allows local users to execute arbitrary code via a long language variable in the configuration file. ***Solution:*** Incomplete. |
| OSVDB-3384 | ***Problem:*** Microsoft Personal Web Servers contain a flaw that allows a remote attacker to execute arbitrary code on a vulnerable server. The issue is due to a buffer overflow in htimage.exe. If the mapname portion of the request exceeds 741 characters, the web server will crash and allow the code to be executed. ***Solution:*** Remove the htimage.exe and imagemap.exe files from the web server. |
| OSVDB-4192 | ***Problem:*** Buffer overflow in Sun AnswerBook2 1.4 through 1.4.3 allows remote attackers to execute arbitrary code via a long filename argument to the gettransbitmap CGI program. ***Solution:*** Incomplete. |
| OSVDB-4301 | ***Problem:*** Netwin WebNews 1.1k CGI program includes several default usernames and cleartext passwords that cannot be deleted by the administrator, which allows remote attackers to gain privileges via the username/password combinations (1) testweb/newstest, (2) alwn3845/imaptest, (3) alwi3845/wtest3452, or (4) testweb2/wtest4879. ***Solution:*** Incomplete. |
| OSVDB-11740 | ***Problem:*** Buffer overflow in (1) foxweb.dll and (2) foxweb.exe of Foxweb 2.5 allows remote attackers to execute arbitrary code via a long URL (PATH_INFO value). ***Solution:*** Incomplete. |
| ***Cross Site Scripting* (XSS)** | |
| OSVDB-2878 | ***Problem:*** MoinMoin contains two flaws that allows a remote cross site scripting attack. This flaw exists because the application does not validate two variables upon submission. This could allow a user to create a specially crafted URL that would execute arbitrary code in a user's |

| | |
|---|---|
| | browser within the trust relationship between the browser and the server, leading to a loss of integrity.<br>***Solution:***<br>Upgrade to version 1.1 or higher, as it has been reported to fix this vulnerability. |
| OSVDB-5689 | ***Problem:***<br>Namazu contains a flaw that allows a remote cross site scripting attack. This flaw exists because the application does not validate 'lang' parameter upon submission to the 'namazu.cgi' script. This could allow a user to create a specially crafted URL that would execute arbitrary code in a user's browser within the trust relationship between the browser and the server, leading to a loss of integrity.<br>***Solution:***<br>Upgrade to version 2.0.8 or higher, as it has been reported to fix this vulnerability. |
| OSVDB-19772 | ***Problem:***<br>Cross-site scripting (XSS) vulnerability in Hyper NIKKI System (HNS) Lite before 0.9 and HNS before 2.10-pl2 allows remote attackers to inject arbitrary web script or HTML.<br>***Solution:*** Incomplete. |
| OSVDB-21365 | ***Problem:***<br>CGI Online Worldweb Shopping (COWS) contains a flaw that allows a remote cross-site scripting (XSS) attack. This flaw exists because the application does not validate the malicious code contained within HTML tags upon submission to the compatible.cgi script. This may allow a user to create a specially crafted URL that would execute arbitrary script code in a user's browser within the trust relationship between their browser and the server.<br>***Solution:***<br>The vendor has discontinued this product and therefore has no patch or upgrade that mitigates this problem. It is recommended that an alternate software package be used in its place. |
| ***Cross Site Tracing* (XST)** | |
| OSVDB-877 | ***Problem:***<br>RFC compliant web servers support the TRACE HTTP method, which contains a flaw that may lead to an unauthorized information disclosure. The TRACE method is used to debug web server connections and allows the client to see what is being received at the other end of the request chain. Enabled by default in all major web servers, a remote attacker may abuse the HTTP TRACE functionality, i.e. cross-site scripting (XSS), which will disclose sensitive configuration information resulting in a loss of confidentiality.<br>***Solution:***<br>If the TRACE method is not essential for your site, disable it in the web server configuration. Consult your documentation or vendor for detailed instructions on how to accomplish this. |
| ***Directory Traversal*** | |
| OSVDB-2511 | ***Problem:***<br>SITEBUILDER v1.4 may allow retrieval of any file. With a valid username and password, request:<br>/<CGIDIR>/sbcgi/sitebuilder.cgi?username=<user>&password=<password>&selectedpage=../../../../../../../../../../etc/passwd<br>***Solution:*** Incomplete. |
| OSVDB-2695 | ***Problem:***<br>My Photo Gallery pre 3.6 contains multiple vulnerabilities including directory traversal, unspecified vulnerabilities and remote management interface access.<br>***Solution:***<br>Upgrade to version 3.6 or higher, as it has been reported to fix this vulnerability. |
| OSVDB-38580 | ***Problem:*** |

| | |
|---|---|
| | c32web.exe in McMurtrey/Whitaker Cart32 before 6.4 allows remote attackers to read arbitrary files via the ImageName parameter in a GetImage action, by appending a NULL byte (%00) sequence followed by an image file extension, as demonstrated by a request for a ".txt%00.gif" file. NOTE: this might be a directory traversal vulnerability.<br>***Solution:***<br>Upgrade to version 3.6 or higher, as it has been reported to fix this vulnerability. |
| ***Execute via Remote*** | |
| OSVDB-237 | ***Problem:***<br>websendmail in Webgais 1.0 allows a remote user to access arbitrary files and execute arbitrary code via the receiver parameter ($VAR_receiver variable).<br>***Solution:*** Incomplete. |
| OSVDB-756 | ***Problem:***<br>The dbm and shm session cache code in mod_ssl before 2.8.7-1.3.23, and Apache-SSL before 1.3.22+1.46, does not properly initialize memory using the i2d_SSL_SESSION function, which allows remote attackers to use a buffer overflow to execute arbitrary code via a large client certificate that is signed by a trusted Certificate Authority (CA), which produces a large serialized session.<br>***Solution:*** Incomplete. |
| OSVDB-2717 | ***Problem:***<br>Les Visiteurs contains a flaw that may allow a remote attacker to execute arbitrary commands or code. The issue is due to the 'new-visitor.inc.php' script not properly sanitizing user input supplied to the 'lvc_include_dir' parameter. This may allow an attacker to include a file from a third-party remote host that contains commands or code that will be executed by the vulnerable script with the same privileges as the web server.<br>***Solution:***<br>Currently, there are no known workarounds or upgrades to correct this issue. However, Matthieu Peschaud has released an unofficial patch to address this vulnerability. As with all third-party solutions, ensure they come from a reliable source and are permitted under your company's security policy. |
| OSVDB-2873 | ***Problem:***<br>RNN Guestbook's gbadmin.cgi script only asks for authentication when attempting to access the main admin page. If an attacker provides a specific QUERY_STRING with the gbadmin.cgi request, the script will not require authentication. This allows a remote attacker to have full administrative control over the guestbook system.<br>***Solution:***<br>Currently, there are no known upgrades or patches to correct this issue. It is possible to correct the flaw by disabling all access to the guestbook scripts until a patch or upgrade is made available. |
| OSVDB-4854 | ***Problem:***<br>Virgil CGI Scanner contains a flaw that allows a remote attacker to gain remote access. The issue is due to the "virgil.cgi" script not properly validating user input to several variables. By providing a specially crafted URI a remote attacker can spawn a shell on a random port. The shell will be available for a short time but run with the same privileges as the web server.<br>***Solution:*** Incomplete. |
| OSVDB-6192 | ***Problem:***<br>Duma Photo Gallery System may allow remote users to write to any file on the system. See http://b0iler.eyeonsecurity.net for details. This could not be remotely tested.<br>***Solution:*** Incomplete. |
| OSVDB-6661 | ***Problem:*** |

| | |
|---|---|
| | Ion-P allows remote file retrieval.<br>***Solution:*** Incomplete. |
| OSVDB-54034 | ***Problem:***<br>This CGI may be vulnerable to remote execution by sending 8000 x 'a' characters (check to see if you get a 500 error message)<br>***Solution:*** Incomplete. |
| ***Injection*** | |
| OSVDB-13981 | ***Problem:***<br>May be vulnerable to command injection. viralator CGI script in Viralator 0.9pre1 and earlier allows remote attackers to execute arbitrary code via a URL for a file being downloaded, which is insecurely passed to a call to wget.<br>***Solution:***<br>Upgrade to version 0.9pre2 or higher, as it has been reported to fix this vulnerability. |
| OSVDB-59031 | ***Problem:***<br>Uninets StatsPlus 1.25 from http://www.uninetsolutions.com/stats.html may be vulnerable to command/script injection by manipulating HTTP_USER_AGENT or HTTP_REFERER.<br>***Solution:*** Incomplete. |
| ***Password*** | |
| OSVDB-13978 | ***Problem:***<br>ibillpm.pl in iBill password management system generates weak passwords based on a client's MASTER_ACCOUNT, which allows remote attackers to modify account information in the .htpasswd file via brute force password guessing.<br>***Solution:*** Incomplete. |

- ***Medium*** → mendesak untuk ditangani

| | |
|---|---|
| OSVDB-28 | ***Problem:***<br>This host is running the Squid Proxy server 'cachemanager' CGI. The cache manager CGI program, by default, contains no restricts or access permissions. With a malformed request, an intruder can use this script to launch port scans from the server.<br>***Solution:***<br>If you are not using the system as a Squid WWW Proxy/Cache server, then uninstall the package by executing: '/etc/rc.d/init.d/squid stop ; rpm -e squid'. If you want to continue using the Squid proxy server software, take the following restrict access to the manager interface: 'mkdir /home/httpd/protected-cgi-bin', 'mv /home/httpd/cgi- bin/cachemgr.cgi /home/httpd/protected-cgi-bin/', and add the following directives to /etc/httpd/conf/access.conf and srm.conf: (Add the following to access.conf ) order deny,allow deny from all allow from localhost AllowOverride None Options ExecCGI (Add the following to srm.conf) ScriptAlias /protected-cgi- bin/ /home/httpd/protected-cgi-bin/ |
| OSVDB-319 | ***Problem:***<br>Sambar may allow anonymous email to be sent from any host via this CGI.<br>***Solution:*** Incomplete. |
| OSVDB-4663 | ***Problem:***<br>Super GuestBook 1.0 from lasource.r2.ru stores the admin password in a plain text file.<br>***Solution:*** Incomplete. |
| OSVDB-9332 | ***Problem:***<br>This script (part of UnixWare WebTop) may have a local root exploit. It is also a system admin script and should be protected via the web.<br>***Solution:***<br>The vendor has released a patch to address this vulnerability. |

❖ ***Low*** → tidak terlalu mendesak untuk ditangani

| | |
|---|---|
| - | ***Problem:***<br>PHP/5.2.17 appears to be outdated (current is at least 5.4.26)<br>***Solution:***<br>Upgrade PHP to version 5.4.26. |
| OSVDB-142 | ***Problem:***<br>PowerPlay Web Edition may allow unauthenticated users to view pages.<br>***Solution:*** Incomplete. |
| OSVDB-596<br>OSVDB-17111 | ***Problem:***<br>The DCShop installation allows credit card numbers to be viewed remotely. See dcscripts.com for fix information.<br>***Solution:*** Incomplete. |
| OSVDB-3092 | ***Problem:***<br>A potentially interesting file, directory or CGI was found on the web server. While there is no known vulnerability or exploit associated with this, it may contain sensitive information which can be disclosed to unauthenticated remote users, or aid in more focused attacks.<br>***Solution:***<br>If the file or directory contains sensitive information, remove the files from the web server or password protect them. |
| OSVDB-11871 | ***Problem:***<br>MondoSearch 4.4 may allow source code viewing by requesting MsmMask.exe?mask=/filename.asp where 'filename.asp' is a real ASP file.<br>***Solution:*** Incomplete. |

- Oleh karena banyaknya *vulnerability* yang ditemukan pada web server dan setelah dilakukan *crosscheck* menggunakan web www.osvdb.org ternyata banyak *vulnerability* yang belum diketahui solusinya, maka penulis menyarankan untuk meng-*uninstall* aplikasi-aplikasi yang tidak diperlukan, sehingga dapat meminimalisir celah keamanan pada server tersebut.
- Selain itu, perlu dilakukan penutupan port/*service* pada web server yang tidak diperlukan oleh www.uii.ac.id. Idealnya yang dibuka hanya port TCP 80 dan port lain yang mendukung berjalannya *website* tersebut, misalnya TCP 21 (FTP) dan protokol ICMP (untuk keperluan *troubleshoot* server).
- Perlu diberlakukan *firewall rule* (iptables) pada web server untuk membatasi akses pengguna dari dan ke server, serta mengatur trafik yang diizinkan untuk masuk ke server dan keluar dari server.

**b. Saran untuk perbaikan *website***

- Dari hasil nikto -h www.uii.ac.id, ditemukan *vulnerability* dan ditemukan port-port yang masih terbuka. Maka saran perbaikan terhadap *website* www.uii.ac.id adalah sebagai berikut:
  - ❖ Melakukan perbaikan sistem dan navigasi yang ada pada antarmuka situs web.
  - ❖ Perbaikan yang dilakukan dengan memberikan keamanan supaya penyerang tidak bisa mengakses ke server secara ilegal, misalnya dengan menutup port/*service* yang tidak diperlukan.

- Perlu dilakukan evaluasi terhadap celah keamanan web server, misalnya dengan pengujian (*pentest*) secara berkala (per 3 atau 6 bulan) untuk memeriksa kerentanan yang ada pada web server.
- Dari hasil pengujian, maka perlu dilakukan perbaikan, misalnya melakukan *update* kernel sistem operasi dan versi aplikasi ke *stable release* dan melakukan *patching* apabila ditemukan celah keamanan (*security hole*) pada aplikasi.