



اَوْنِيُوْرَسِيْتِيْ تِيْكْنُوْلُوْجِيْ مَآرَا
UNIVERSITI
TEKNOLOGI
MARA

REPORT ANALYSIS ON THE SECURITY OF TWO DOMAINS ASSIGNMENT

ITT 450 INFORMATION AND NETWORK SECURITY

INSTRUCTOR: SIR MOHD ALI

Name	Daniyana Binti Miskam
Matric	2017592341
Group	M3CS2453A

TABLE OF CONTENTS

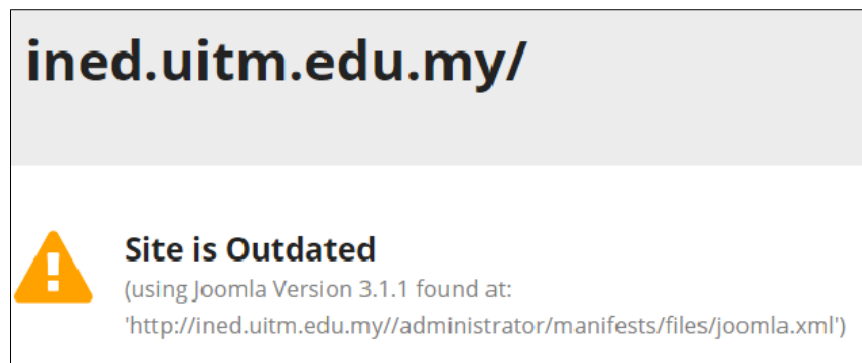
Num	Content	Pages
1.0	SUMMARY OF FINDINGS	3
1.1	Summary Findings for “ined.uitm.edu.my”	3 - 4
1.2	Summary Findings for “ultimate-guitar.com”	5 - 6
2.0	SUMMARY OF RECOMMENDATIONS	7
2.1	Summary Recommendations for " ined.uitm.edu.my”	7
2.2	Summary Recommendations for “ultimate-guitar.com”	7
3.0	DETAIL FINDINGS	8
3.1	Detail Findings and Recommendations for “ined.uitm.edu.my”	8 - 13
3.2	Detail Findings and Recommendations for “ultimate-guitar.com”	14 - 18
4.0	REFERENCES	19 - 24

1) Summary of Findings

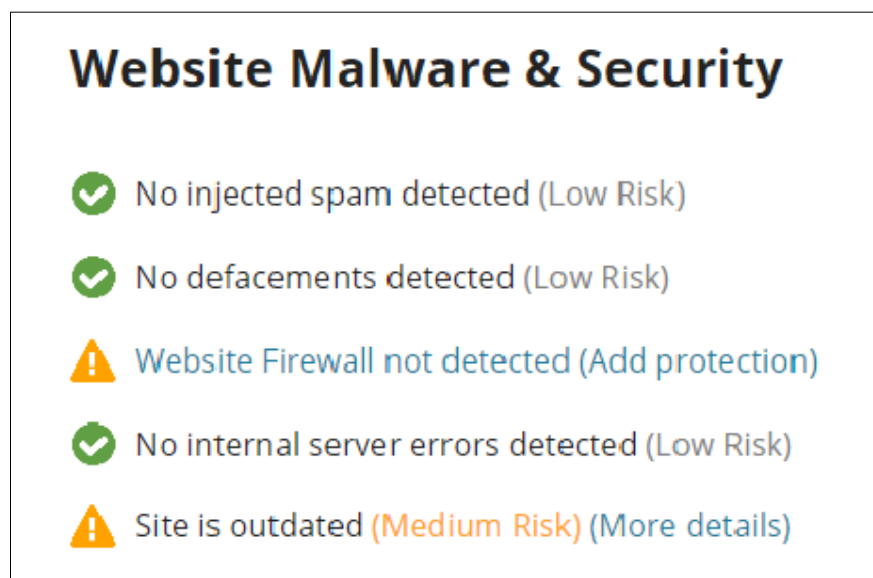
I choose “ined.uitm.edu.my” and “ultimate-guitar.com” as my two domains for this assignment. I got few of the result according to an online web scanners and using software Nmap to scan the domains. Below are the results:

1.1) Summary Findings for “ined.uitm.edu.my”:

The domain is using Joomla Version 3.1.1.



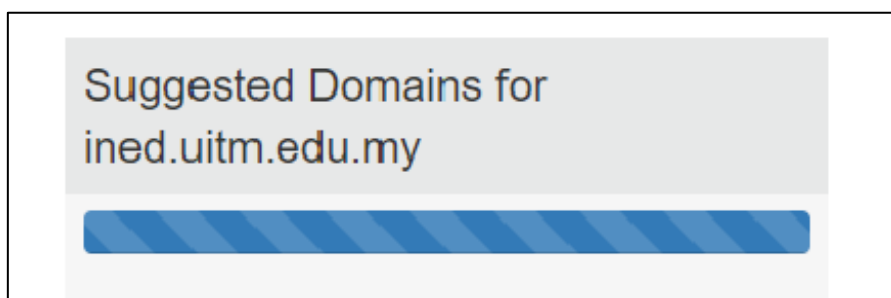
I found this by using Sucuri Website Scanner. Instead that, I also found the domain Website Firewall cannot be detected. This site is an outdated version which it can brings to medium risk.



Finally, when using Nmap in Kali Linux, I have found that this domain has several open ports such as tcp port 80, 443 and 1723.

```
Starting Nmap 6.25 ( http://nmap.org ) at 2018-05-20 07:39 UTC
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 93.95% done; ETC: 07:39 (0:00:02 remaining)
Nmap scan report for ined.uitm.edu.my (202.58.82.131)
Host is up (0.049s latency).
rDNS record for 202.58.82.131: 202-58-82-131.uitm.edu.my
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
1723/tcp  open  pptp
Nmap done: 1 IP address (1 host up) scanned in 73.36 seconds
```


The vulnerabilities that the open port can cause shall be discussed with greater details in the “Detail Findings” part of this report. Also, one thing that needs to be noted is that Who.is cannot find any data on this domain in their search libraries.





1.2) Summary Findings for “ultimate-guitar.com”:

This website is strongly secure as the scanners show that it does not have any major weaknesses.

www.ultimate-guitar.com/

**No Malware Found**
Our scanner didn't detected any malware

**Site is not Blacklisted**
9 Blacklists checked

**3**
URLs Scanned

Pages scanned: 0
Javascript files scanned: 3
Other files: 0

System running on: nginx
IP address: 205.185.216.42
[More Details](#)

However, when using Nmap, I find that it has several ports that open.

```
Starting Nmap 6.25 ( http://nmap.org ) at 2018-05-17 05:46 UTC
Nmap scan report for www.ultimate-guitar.com (205.185.216.42)
Host is up (0.023s latency).
Other addresses for www.ultimate-guitar.com (not scanned): 205.185.216.10
rDNS record for 205.185.216.42: map2.hwcdn.net
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp
Nmap done: 1 IP address (1 host up) scanned in 52.32 seconds
```

I also received some information regarding the domain by using Who.is. Some of the important information is the registrant, administrative and technician contact information.

Registrar Data

Make Private

Registrant Contact Information:

Name

Organization

Address

City

State / Province

Postal Code

Country

Phone

Email

PERFECT PRIVACY, LLC

12808 Gran Bay Parkway West

Jacksonville

FL

32258

US

+1.5707088780

qv69h3kz3u.j@networksolutionsprivateregistration.com

Administrative Contact Information:

Name

Organization

Address

City

State / Province

Postal Code

Country

Phone

Email

PERFECT PRIVACY, LLC

12808 Gran Bay Parkway West

Jacksonville

FL

32258

US

+1.5707088780

qv69h3kz3u.j@networksolutionsprivateregistration.com

Technical Contact Information:

Name

Organization

Address

City

State / Province

Postal Code

Country

Phone

Email

PERFECT PRIVACY, LLC

12808 Gran Bay Parkway West

Jacksonville

FL

32258

US

+1.5707088780

qv69h3kz3u.j@networksolutionsprivateregistration.com

Information Updated: 2018-05-13 20:18:41

Besides that, it also shows me the servers name and ip addresses. Further explanation will be done in the content of “Detail Findings”.

2) Summary of Recommendations.

Based on the result that I have receive, a few recommendations on how to improve the security of domains and decrease their risk on being hack was written. Below are some of them in a summary manner:

2.1) Summary Recommendations for “ined.uitm.edu.my”:

Update the domain to the latest version of Joomla because an attacker would try to manipulate in order to access the data in the domain. Besides that, some other recommendations are:

- Add protection firewall on the website
- Update their site to a new version regularly.

2.2) Summary Recommendations for “ultimate-guitar.com”:

For this domain, the website also has to update the domain to the latest version of Joomla. Next, keep their domain information in secret on who.is because an attacker can use the information there to attack their server. Besides that, other recommendations are:

- Add protection firewall on the website
- Update their site to a new version regularly.
- Close the unnecessary open ports.
- Manage the open ports correctly.
- Update the domain operating system to the latest version.

3) Detail Findings.

3.1) Detail Findings and Recommendations for “ined.uitm.edu.my” Domain:

Information Gained About Domain:

Website= [https:// ined.uitm.edu.my](https://ined.uitm.edu.my)


Site report for ined.uitm.edu.my

Lookup another URL: Share: [f](#) [t](#) [in](#) [g+](#) [Y](#) [e5](#)

Background


Site title	iNED - Institute of Neo Education - Home Anjung	Date first seen	March 2006
Site rank		Primary language	English
Description	uitm part time distance learning program through lms vle iclass mooc openlearning digital content		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10 <div></div>		

Network

Site	https://ined.uitm.edu.my	Netblock Owner	Universiti Teknologi MARA
Domain	uitm.edu.my	Nameserver	ns2.uitm.edu.my
IP address	202.58.82.131	DNS admin	postmaster@salam.uitm.edu.my
IPv6 address	Not Present	Reverse DNS	202-58-82-131.uitm.edu.my
Domain registrar	mynic.net.my	Nameserver organisation	whois.mynic.net.my
Organisation	Universiti Teknologi MARA, Pusat Sistem Maklumat Bersepadu Tkt 5, Bangunan Menara, Universiti Teknologi MARA40450 Shah Alam Selangor, Malaysia	Hosting company	uitm.edu.my
Top Level Domain	Malaysia (.edu.my)	DNS Security Extensions	unknown
Hosting country	 MY		

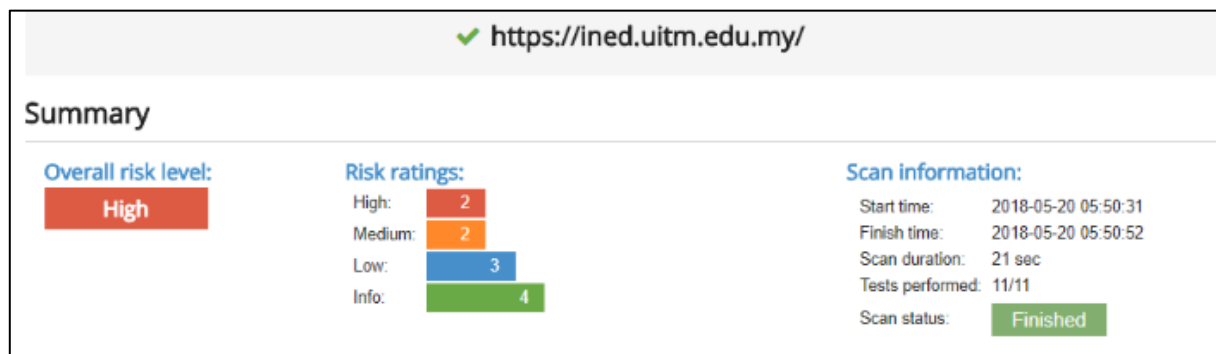
SSL/TLS

SSLv3/POODLE	This site does not support the SSL version 3 protocol. More information about SSL version 3 and the POODLE vulnerability.		
Heartbleed	The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable. This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. More information about Heartbleed detection.		
Assurance	Domain validation		
Organisation	Not Present	Common name	*.uitm.edu.my
State	Not Present	Country	Not Present
Organisational unit	Domain Control Validated; PositiveSSL Wildcard	Subject Alternative Name	*.uitm.edu.my, uitm.edu.my
Validity period	From Aug 24 2016 to Aug 24 2019 (36 months)	Matches hostname	Yes
Server	Apache	Public key algorithm	rsaEncryption
Protocol version	TLSv1.2	Public key length	4096

Protocol version	TLSv1.2	Public key length	4096
Certificate check	ok	Signature algorithm	sha256WithRSAEncryption
Serial number	0x349ad7928a20fddfa60ed8c468ff8ad8	Cipher	ECDHE-RSA-AES128-GCM-SHA256
Version number	0x02	Perfect Forward Secrecy	Yes
Next Protocol Negotiation	Not Present	Supported TLS Extensions	RFC4366 server name, RFC5746 renegotiation info, RFC4492 EC point formats, RFC5077 session ticket, RFC6520 heartbeat
Issuing organisation	COMODO CA Limited	Issuer common name	COMODO RSA Domain Validation Secure Server CA
Issuer unit	Not Present	Issuer location	Salford
Issuer country	GB	Issuer state	Greater Manchester
Certificate Revocation Lists	http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl	Certificate Hash	J3Wp5HKuNQLWYfH6wpM0uF084Qo
Public Key Hash	be67e99ea35f625746b748af834f337db2724c43a3dafa951affb39b7495d992		
OCSP servers	http://ocsp.comodoca.com - 100% uptime in the past 24 hours 		
OCSP stapling	No response received		

Open Ports= TCP port 80-HTTP, TCP port 443-HTTPS, TCP port 1723-PPTP

Risk Rating



Vulnerabilities found for server-side software

	CVSS	CVE	Summary	Affected software
●	10.0	CVE-2012-2688	Unspecified vulnerability in the <code>_php_stream_scandir</code> function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."	PHP 5.3.3
●	10.0	CVE-2012-2376	Buffer overflow in the <code>com_print_typeinfo</code> function in PHP 5.4.3 and earlier on Windows allows remote attackers to execute arbitrary code via crafted arguments that trigger incorrect handling of COM object VARIANT types, as exploited in the wild in May 2012.	PHP 5.3.3
●	10.0	CVE-2011-3268	Buffer overflow in the <code>crypt</code> function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.	PHP 5.3.3
●	7.5	CVE-2014-9427	<code>sapi/cgi/cgi_main.c</code> in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when <code>mmap</code> is used to read a <code>.php</code> file, does not properly consider the mapping's length during processing of an invalid file that begins with a <code>#</code> character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from <code>php-cgi</code> process memory by leveraging the ability to upload a <code>.php</code> file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.	PHP 5.3.3
●	7.5	CVE-2013-6420	The <code>asn1_time_to_time_t</code> function in <code>ext/openssl/openssl.c</code> in PHP before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7 does not properly parse (1) <code>notBefore</code> and (2) <code>notAfter</code> timestamps in X.509 certificates, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted certificate that is not properly handled by the <code>openssl_x509_parse</code> function.	PHP 5.3.3

Analysis

The result that I received is Joomla is an outdated version of 3.6.5. These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation

Upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Exploits found for server-side software

Exploit name	Affected software
PHP 5.3.3 - 'ibase_gen_id()' Off-by-One Overflow	PHP 5.3.3
PHP 5.3.3 - NumberFormatter::getSymbol Integer Overflow	PHP 5.3.3
PHP 5.3.3/5.2.14 - ZipArchive::getArchiveComment Null Pointer Dereference	PHP 5.3.3

Analysis

An attacker could use these exploits to gain unauthorized access to the application, steal confidential data or affect the availability of the system

Recommendation

Upgrade the affected software to the latest version in order to remediate the vulnerabilities targeted by these exploits.

Insecure HTTP cookies

Cookie Name	Flags missing
9e84326430eb32d4db3905fe97262ad7	Secure

Analysis

Since the Secure flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation

Reconfiguring the web server in order to set the flag(s) Secure to all sensitive cookies.

Directory listing is enabled

https://ined.uitm.edu.my/templates/yoo_balance/warp/js/
https://ined.uitm.edu.my/templates/yoo_balance/js/
https://ined.uitm.edu.my/cache/widgetkit/







Analysis

An attacker can see the entire structure of files from the affected URL. It is often the case that sensitive files are 'hidden' among public files in that location and attackers can use this vulnerability to access them.

Recommendation

Reconfiguring the web server in order to deny directory listing and verify that there are no sensitive files at the mentioned URLs..

Server software and technology found

Software / Version	Category
 Apache	Web Servers
 PHP 5.3.3	Programming Languages
 Joomla	CMS
 Twitter Bootstrap	Web Frameworks
 Google Analytics UA	Analytics
 jQuery	JavaScript Frameworks

Analysis

An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation

Eliminate the information which permit the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Missing HTTP security headers

HTTP Security Header	Header Role	Status
X-Frame-Options	Protects against Clickjacking attacks	Not set
X-XSS-Protection	Mitigates Cross-Site Scripting (XSS) attacks	Not set
Strict-Transport-Security	Protects against man-in-the-middle attacks	Not set
X-Content-Type-Options	Prevents possible phishing or XSS attacks	Not set

Analysis

- Because the X-Frame-Options header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent.
- The X-XSS-Protection HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.
- The HTTP Strict-Transport-Security header instructs the browser not to load the website via plain HTTP connection but always use HTTPS. Lack of this header exposes the application users to the risk of data theft or unauthorized modification in case the attacker implements a man-in-the-middle attack and intercepts the communication between the user and the server.

- The HTTP X-Content-Type-Options header is addressed to Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation

- Add the X-Frame-Options HTTP response header to every page that you want to be protected against Clickjacking attacks.
- Setting the X-XSS-Protection header to "X-XSS-Protection: 1; mode=block".
- Setting the Strict-Transport-Security header.
- Setting the X-Content-Type-Options header to "X-Content-Type-Options: nosniff".

Robots.txt file found

<https://ined.uitm.edu.my/robots.txt>

Analysis

There is no particular security risk in having a robots.txt file. However, this file is often misused to try to hide some web pages from the users. This should not be done as a security measure because these URLs can easily be read from the robots.txt file.

Recommendation

Remove the entries from robots.txt which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).


- ✓ **Communication is secure**
- ✓ **No security issue found regarding client access policies**
- ✓ **No password input found (auto-complete test)**
- ✓ **No password input found (clear-text submission test)**

3.2) Detail Findings and Recommendations for “ultimate-guitar.com” Domain:


Information Gained About Domain:

Website= <https://www.ultimate-guitar.com>

Background			
Site title	ULTIMATE GUITAR TABS. 1,100,000 songs catalog with free Chords, Guitar Tabs, Bass Tabs, Ukulele Chords and Guitar Pro Tabs!	Date first seen	November 1999
Site rank	5707	Primary language	English
Description	Your #1 source for chords, guitar tabs, bass tabs, ukulele chords, guitar pro and power tabs. Comprehensive tabs archive with over 1,100,000 tabs! Tabs search engine, guitar lessons, gear reviews, rock news and forums!		
Keywords	guitar tabs, bass tabs, tab, tablature, tabs, chords, ukulele, ukulele chords, guitar pro, guitar archive, power tab, sheet music, free guitar tabs, forums, reviews, lessons, metallica, nirvana, u2, led zeppelin, ultimate guitar, ug, ultimate-guitar.com		
Netcraft Risk Rating [FAQ]	0/10 		

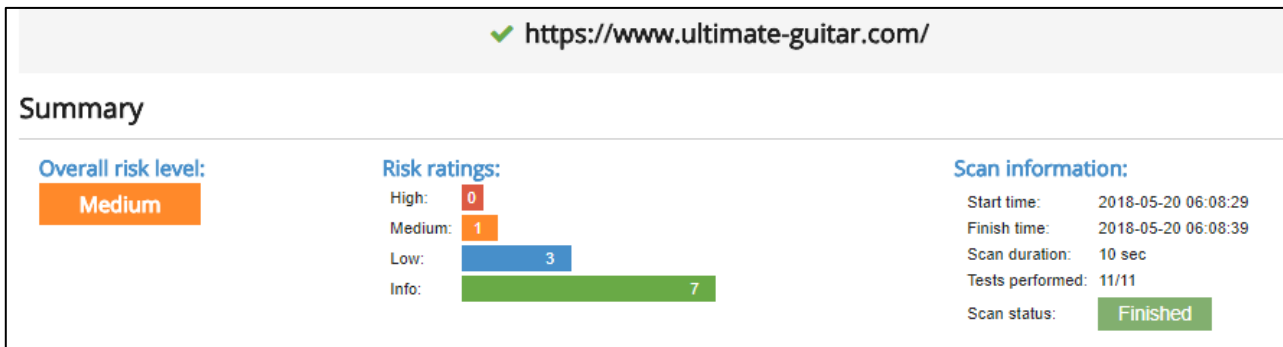
Network			
Site	https://www.ultimate-guitar.com	Netblock Owner	Highwinds Network Group, Inc.
Domain	ultimate-guitar.com	Nameserver	dns0.zoneedit.com
IP address	205.185.216.42	DNS admin	zone@zoneedit.com
IPv6 address	Not Present	Reverse DNS	map2.hwcdn.net
Domain registrar	unknown	Nameserver organisation	whois.easydns.com
Organisation	unknown	Hosting company	Highwinds
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	 US		

SSL/TLS			
SSLv3/POODLE	<p>This site does not support the SSL version 3 protocol.</p> <p>More information about SSL version 3 and the POODLE vulnerability.</p>		
Heartbleed	<p>The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.</p> <p>This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. More information about Heartbleed detection.</p>		
Assurance	Organisation validation		
Organisation	Ultimate Guitar USA LLC	Common name	*.ultimate-guitar.com
State	California	Country	US
Organisational unit	PremiumSSL Wildcard	Subject Alternative Name	*.ultimate-guitar.com, ultimate-guitar.com
Validity period	From Oct 14 2015 to Oct 13 2018 (35 months, 4 weeks, 2 days)	Matches hostname	Yes
Server	unknown	Public key algorithm	rsaEncryption
Protocol version	TLSv1.2	Public key length	2048
Certificate check	ok	Signature algorithm	sha256WithRSAEncryption

Serial number	0x4dc80d63797d19584553d87d72f7b619	Cipher	ECDHE-RSA-AES128-GCM-SHA256
Version number	0x02	Perfect Forward Secrecy	Yes
Next Protocol Negotiation	Not Present	Supported TLS Extensions	RFC4366 server name, RFC5746 renegotiation info, RFC4492 EC point formats, RFC5077 session ticket, RFC4366 status request
Issuing organisation	COMODO CA Limited	Issuer common name	COMODO RSA Organization Validation Secure Server CA
Issuer unit	Not Present	Issuer location	Salford
Issuer country	GB	Issuer state	Greater Manchester
Certificate Revocation Lists	http://crl.comodoca.com/COMODORSAArganizationValidationSecureServerCA.crl	Certificate Hash	kTSZHey7ftsSDgN/IL7fwhgrY94
Public Key Hash	0b17ef44d14dd1301dc0b1f3228b5e0e156bda5639ed4497fb02844d0d229acc		
OCSP servers	http://ocsp.comodoca.com - 100% uptime in the past 24 hours 		
OCSP stapling response	Certificate valid		
OCSP data generated	May 19 13:44:26 2018 GMT	OCSP data expires	May 26 13:44:26 2018 GMT

Open Ports= TCP port 21-FTP, TCP port 80-HTTP, TCP port 443-HTTPS, TCP port 554-RTSP, TCP port 1723-PPTP

Risk Rating



Insecure HTTP cookies

Cookie Name	Flags missing
_pro_abVar	Secure, HttpOnly
static_cache_key_v2	Secure, HttpOnly
_csrf	Secure








Analysis

- Since the Secure flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.
- Lack of the HttpOnly flag permits the browser to access the cookie from client-side scripts (ex. JavaScript, VBScript, etc). This can be exploited by an attacker in conjunction with a Cross-Site Scripting (XSS) attack in order to steal the affected cookie. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation

Reconfiguring the web server in order to set the flag(s) Secure, HttpOnly to all sensitive cookies.

Server software and technology found

Software / Version	Category
 Nginx	Web Servers
 webpack	Build CI Systems
 Prebid	Advertising Networks
 Google Font API	Font Scripts
 Google Tag Manager	Tag Managers
 React	JavaScript Frameworks
 Yandex.Metrika	Analytics

Analysis

An attacker could use this information to mount specific attacks against the identified software type and version

Recommendation

Eliminate the information which permit the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Missing HTTP security headers

HTTP Security Header	Header Role	Status
X-Frame-Options	Protects against Clickjacking attacks	Not set
X-XSS-Protection	Mitigates Cross-Site Scripting (XSS) attacks	Not set
Strict-Transport-Security	Protects against man-in-the-middle attacks	Not set
X-Content-Type-Options	Prevents possible phishing or XSS attacks	Not set

Analysis

- Because the X-Frame-Options header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack.
- The X-XSS-Protection HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

- The HTTP Strict-Transport-Security header instructs the browser not to load the website via plain HTTP connection but always use HTTPS. Lack of this header exposes the application users to the risk of data theft or unauthorized modification in case the attacker implements a man-in-the-middle attack and intercepts the communication between the user and the server.
- The HTTP X-Content-Type-Options header is addressed to Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation

- Add the X-Frame-Options HTTP response header to every page that you want to be protected against Clickjacking attacks.
- Setting the X-XSS-Protection header to "X-XSS-Protection: 1; mode=block".
- Setting the Strict-Transport-Security header.
- Setting the X-Content-Type-Options header to "X-Content-Type-Options: nosniff".

Robots.txt file found

<https://www.ultimate-guitar.com/robots.txt>

Analysis

There is no particular security risk in having a robots.txt file. However, this file is often misused to try to hide some web pages from the users. This should not be done as a security measure because these URLs can easily be read from the robots.txt file.

Recommendation

Remove the entries from robots.txt which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

- ✓ **No vulnerabilities found for server-side software**
- ✓ **No exploits found for server-side software**
- ✓ **Communication is secure**
- ✓ **No security issue found regarding client access policies**
- ✓ **Directory listing not found (quick scan)**
- ✓ **No password input found (auto-complete test)**
- ✓ **No password input found (clear-text submission test)**

4) References.

(i) Nmap Scans (via Kali LINUX)

- **Normal Scans**

ined.uitm.edu.my

```
Starting Nmap 6.25 ( http://nmap.org ) at 2018-05-20 07:39 UTC
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 93.95% done; ETC: 07:39 (0:00:02 remaining)
Nmap scan report for ined.uitm.edu.my (202.58.82.131)
Host is up (0.049s latency).
rDNS record for 202.58.82.131: 202-58-82-131.uitm.edu.my
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 73.36 seconds
```

ultimate-guitar.com

```
Starting Nmap 6.25 ( http://nmap.org ) at 2018-05-17 05:46 UTC
Nmap scan report for www.ultimate-guitar.com (205.185.216.42)
Host is up (0.023s latency).
Other addresses for www.ultimate-guitar.com (not scanned): 205.185.216.10
rDNS record for 205.185.216.42: map2.hwcdn.net
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 52.32 seconds
```

▪ Stealth Scans

ined.uitm.edu.my

```
root@kali:~# nmap -sS ined.uitm.edu.my

Starting Nmap 6.25 ( http://nmap.org ) at 2018-05-20 07:39 UTC
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 93.95% done; ETC: 07:39 (0:00:02 remaining)
Nmap scan report for ined.uitm.edu.my (202.58.82.131)
Host is up (0.049s latency).
rDNS record for 202.58.82.131: 202-58-82-131.uitm.edu.my
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 73.36 seconds
```

ultimate-guitar.com

```
root@kali:~# nmap -sS www.ultimate-guitar.com

Starting Nmap 6.25 ( http://nmap.org ) at 2018-05-17 05:46 UTC
Nmap scan report for www.ultimate-guitar.com (205.185.216.42)
Host is up (0.023s latency).
Other addresses for www.ultimate-guitar.com (not scanned): 205.185.216.10
rDNS record for 205.185.216.42: map2.hwcdn.net
Not shown: 995 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 52.32 seconds
```

■ Operating System Type Scan

ined.uitm.edu.my (success)

```
root@kali:~# nmap -O ined.uitm.edu.my

Starting Nmap 6.25 ( http://nmap.org ) at 2018-05-20 10:28 UTC
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 51.00% done; ETC: 10:29 (0:00:14 remaining)
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 72.30% done; ETC: 10:29 (0:00:11 remaining)
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.25% done; ETC: 10:29 (0:00:11 remaining)
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.75% done; ETC: 10:29 (0:00:14 remaining)
Nmap scan report for ined.uitm.edu.my (202.58.82.131)
Host is up (0.074s latency).
rDNS record for 202.58.82.131: 202-58-82-131.uitm.edu.my
Not shown: 933 filtered ports, 62 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp
Device type: general purpose
Running (JUST GUESSING): Linux 2.4.X (90%), Microsoft Windows 7 (90%)
OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/o:microsoft:windows_7::enterprise
Aggressive OS guesses: DD-WRT v24-sp2 (Linux 2.4.37) (90%), Microsoft Windows 7
Enterprise (90%)
```

ultimate-guitar.com (failed)


```
root@kali:~# nmap -O www.ultimate-guitar.com

Starting Nmap 6.25 ( http://nmap.org ) at 2018-05-17 06:06 UTC
Nmap scan report for www.ultimate-guitar.com (205.185.216.42)
Host is up (0.00043s latency).
Other addresses for www.ultimate-guitar.com (not scanned): 205.185.216.10
rDNS record for 205.185.216.42: map2.hwcdn.net
All 1000 scanned ports on www.ultimate-guitar.com (205.185.216.42) are filtered
Too many fingerprints match this host to give specific OS details


OS detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 12.39 seconds
```

(ii) Netcraft Site Report (toolbar.netcraft.com/site_report)

ined.uitm.edu.my









Site report for ined.uitm.edu.my




Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map

Lookup another URL:

Share:      

Background

Site title	INED - Institute of Neo Education - Home Anjung	Date first seen	March 2006
Site rank		Primary language	English
Description	uitm part time distance learning program through lms vle iclass mooc openlearning digital content		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10 		

ultimate-guitar.com



Site report for www.ultimate-guitar.com



Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Lookup another URL:

Share:      

Background

Site title	ULTIMATE GUITAR TABS. 1,100,000 songs catalog with free Chords, Guitar Tabs, Bass Tabs, Ukulele Chords and Guitar Pro Tabs!	Date first seen	November 1999
Site rank	5707	Primary language	English
Description	Your #1 source for chords, guitar tabs, bass tabs, ukulele chords, guitar pro and power tabs. Comprehensive tabs archive with over 1,100,000 tabs! Tabs search engine, guitar lessons, gear reviews, rock news and forums!		
Keywords	guitar tabs, bass tabs, tab, tablature, tabs, chords, ukulele, ukulele chords, guitar pro, guitar archive, power tab, sheet music, free guitar tabs, forums, reviews, lessons, metallica, nirvana, u2, led zeppelin, ultimate guitar, ug, ultimate-guitar.com		
Netcraft Risk Rating [FAQ]	0/10 		

(iii) who.is Information

ultimate-guitar.com (success)

who.is

Search for domains or IP addresses...

Q

Premium Domains

Transfer

Features

ultimate-guitar.com

whois information

WhoisHistoryDNS RecordsDiagnostics

cache expires in and 0 seconds ↺

Registrar Info

Name	NETWORK SOLUTIONS, LLC.
Whois Server	whois.networksolutions.com
Referral URL	http://networksolutions.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires On	2018-10-13
Registered On	1999-10-13
Updated On	2017-12-16

Name Servers

NS.ULTIMATE-GUITAR.COM	178.18.22.155
NS1.ZONEEDIT.COM	45.77.82.193
NS7.ZONEEDIT.COM	139.162.196.199

Similar Domains

ultim-8.com | ultim-8.info | ultim-aid.com | ultim-blog.com | ultim-debrid.com | ultim-ed.com | ultim-eight.com | ultim-eyes.com | ultim-eyes.net | ultim-eyes.org | ultim-hd.net | ultim-ld.nl | ultim-image.eu | ultim-kacho.com | ultim-kyojo.com | ultim-lexperience.com | ultim-lexperience.fr | ultim-media.com | ultim-medias.com | ultim-paradise.net |

Registrar Data

Make Private

Registrant Contact Information:

Name	PERFECT PRIVACY, LLC
Organization	
Address	12808 Gran Bay Parkway West
City	Jacksonville
State / Province	FL
Postal Code	32258
Country	US
Phone	+1.5707088700
Email	qv69h3kz3u.j@networksolutionsprivateregistration.com

Administrative Contact Information:

Name	PERFECT PRIVACY, LLC
Organization	
Address	12808 Gran Bay Parkway West
City	Jacksonville
State / Province	FL
Postal Code	32258
Country	US
Phone	+1.5707088700
Email	qv69h3kz3u.j@networksolutionsprivateregistration.com

Technical Contact Information:

Name	PERFECT PRIVACY, LLC
Organization	
Address	12808 Gran Bay Parkway West
City	Jacksonville
State / Province	FL
Postal Code	32258
Country	US
Phone	+1.5707088700
Email	qv69h3kz3u.j@networksolutionsprivateregistration.com

Information Updated: 2018-05-13 20:18:41

who.is

click away. Register your .COM domain for **only \$7.99.**

Start your search

Use promo code **NAME799**

name.com
Limit one discounted .COM registration per customer.

Site Status

Status	Inactive
Server Type	

Suggested Domains for ined.uitm.edu.my