

MiSSConf(SP2)

Security #MiSSConcepts

Ammarit Thongthua, CISSP CISM

Who am I



Name>Ammarit Thongthua
Khay
Shellcodenoobx **Shellcodenoobx Shellcodenoobx**

Senior Security Engineer (AGODA) Penetration Tester Security Consultant

</Job></Education >

B.Eng Com, ABAC M.Sci Cyber Sec Mahidol Unv.

CISSP, CISM, CSSLP, GXPN, CCNP, CEH, SEC+

</Education>

Security #MiSSConcepts

anning and statisticity and

Sector Marine

Service States of the



Security protection we #Expected

Security protection we get in #Reality MiSSConf(5P2)

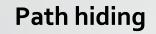


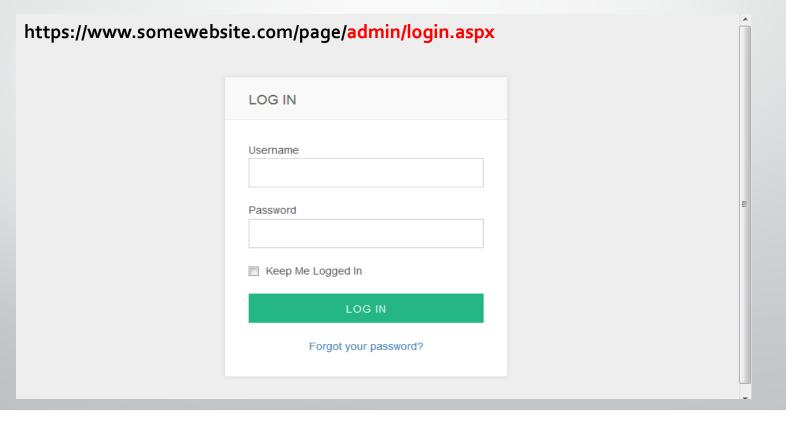
Obscurity = make nobody know or make it hard to see

• Example:

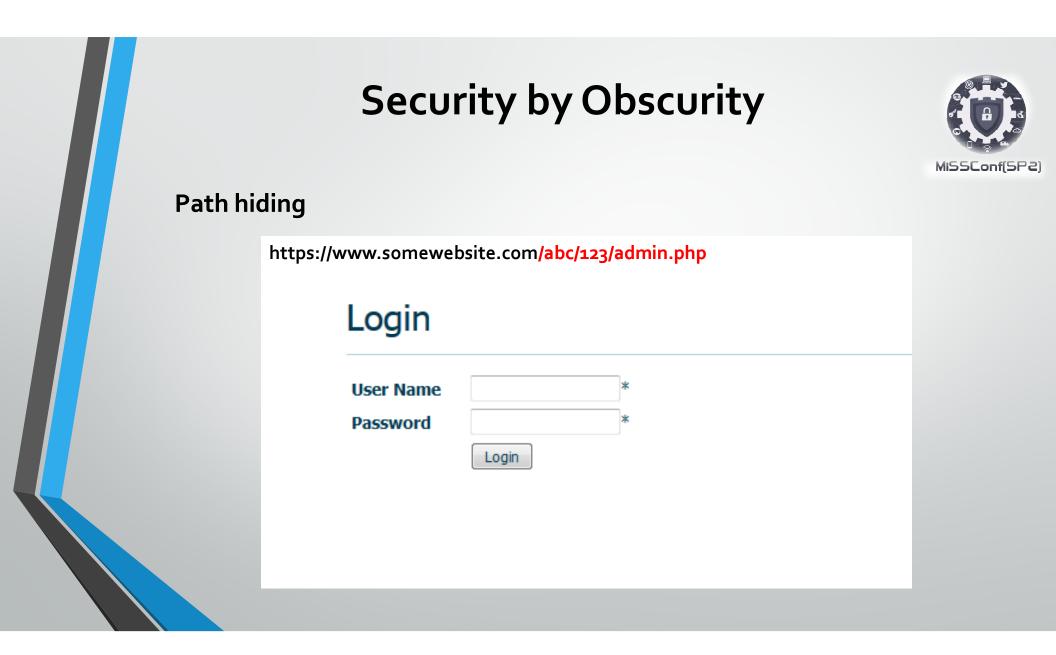
- Path hiding
- Hidden field
- Hidden/Remove object
- Change service port number
- Referrer, HTTP special Header







MiSSConf(SP2)







Path hiding

 Image: Co.th/test/session/index.php?1471600000

 Hi, admin

 Session ID : qfcdigjasmcq8ko4rtoqa3ou71

 Current Date : 20-08-2015 01:00:13

 Clear Session



Path hiding -Temp File, Back Up

Burn New folder		
Name	Date modified	Туре
_app_bin	22/1/2011 12:24 AM	File folder
🍑 _vti_pvt	27/8/2010 2:35 PM	File folder
App_Browsers	30/1/2011 8:14 AM	File folder
App_GlobalResources	27/8/2010 2:35 PM	File folder
aspnet_client	27/8/2010 2:35 PM	File folder
🍑 bin	29/1/2011 8:57 PM	File folder
wpresources	29/1/2011 8:57 PM	File folder
al global.asax	27/8/2010 2:35 PM	ASP.NET Ser
web.bak	28/11/2010 1:17 PM	BAK File
is web.config	9/3/2011 3:06 PM	XML Configu
web_2010_12_24_23_36_48.bak	24/12/2010 11:28 PM	BAK File
web_2010_12_24_23_37_06.bak	24/12/2010 11:36 PM	BAK File
web_2010_12_25_00_04_41.bak	24/12/2010 11:37 PM	BAK File



Dirbuster

OWASP DieBuster 0.1 t - Web Applicati	on Brite Ferriny	••	×
File Options About Help			
Target URL (eg http://exampl	e.com:80/)		
Work Method 🛛 🔾 Use	GET requests only 💿 Auto Switch (HEAD and GET)		
Number Of Threads 🖂 🖂 🖂	10 Threads 🗌 Go Faster		
Select scanning type: (List based brute force O Pure Brute Force		
File with list of dirs/files			
	S. Br	rowse 🕕 🚺 List Info	
Char set [a-zA-Z0-9%20+]	★ Min length 1 Max Length 8]	
Select starting options:) Standard start point 🔿 URL Fuzz		
Brute Force Dirs	Be Recursive Dir to start with /		
Brute Force Files	Use Blank Extention File extention php		
URL to fuzz - /test.html?url={	dir) asp		
			I
Exit		D Sta	rt
Please complete the test detai	15		

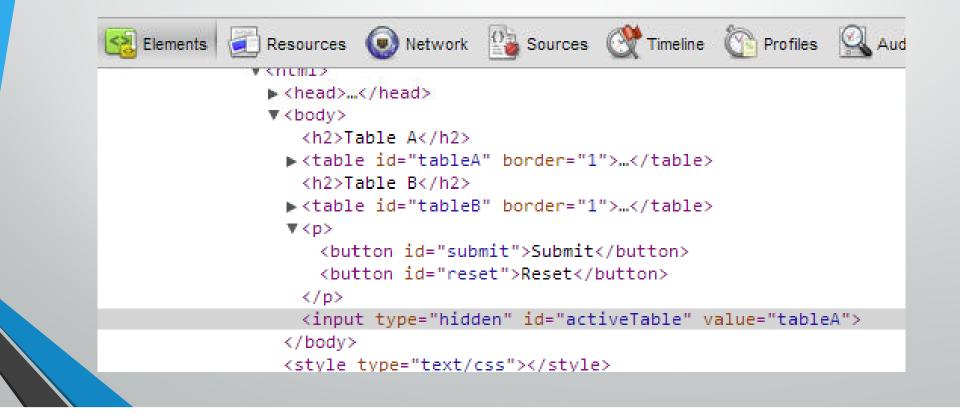
Dirbuster

- Prepare path dictionary
 - Basic : /admin , /test, /abc, /xyz
 - Well known : /administrator /manager, /wp-admin, /console
 - Advance : /admin-path, /
- Temp File, Back Up
 - Path + .zip , .rar , .bak
 - Ex; /admin
 - http://testsite.com/admin.zip
 - http://testsite.com/admin.rar
 - http://testsite.com/admin.bak



MiSSConf(SP2)

Hidden filed





MiSSConf(SP2)

Hidden filed

	Repeater Sequencer Deco
Intercept HTTP history WebSockets history	Options
Response Modification	
These settings are used to perform automat	tic modification of response
🗹 Unhide hidden form fields	
🗹 Prominently highlight unhidden field	ds
Enable disabled form fields	
Remove input field length limits	Hidden field [VIEWSTATE] /WEPDWULLTE10DCXN
Remove JavaScript form validation	Please enter the required quantity:
Remove all JavaScript	Product: Windows XP
Remove <object> tags</object>	Price: 149
	Quantity: (Maximum quantity is 50)
	Hidden field [price] 149
	Buy
	Back to catalogue



Hidden filed

User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5 1 like Mac OS Safari/7534.48.3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9, Accept-Language: en-GB, en; g=0.5 Accept-Encoding: gzip, deflate Referer: http://172.16.67.136/WebGoat/attack?Screen=1554&menu= Cookie: remember token=PNkIxJ3DG8iXL0F4vrAWBA; acopendivids=sw PHPSESSID=018fof1nkq5333kq6pckk47hn0; cyclone session=BAh7B0kiD3Nlc3Npb25faWQGOqZFRkkiJTBlYjc2YjdjZ vSi9hQTBGclVjeFZYQ3cvVkQzSmtLRnp5Z3ZvMkdTRHA5TTQzcFE9BjsARq%3D JSESSIONID=1ED3891622C69A1B110F4BC57D1204E1; railsgoat session=BAh7B0kiD3Nlc3Npb25faWQGOqZFRkkiJTk2ZGMxY2I FEyWU9USGhUVUV3d3RSWWpDL0tl2EJaUXJpdU5HSnMxWllCTGw5L1E9BjsARq% Authorization: Basic Z3Vlc306Z3Vlc30= Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 35

QTY=1&SUBMIT=Purchase Price=10



Disabled

- dir="ltr">
 - <div class="spacer"> </div>
 - div id="topSection">
 - <div id="brandLogo"> </div>
 - div id="searchIconAndTextContainer">
 - <div id="searchIcon"> </div>
 - <input id="searchText" name="q" value="" maxlength="256" aria-label="ค่ำค้น</pre>
 - W1" dir="auto" type="text" autocomplete="off" aria-autocomplete="true" aria-controls="searchSuggestionTable"
 expanded="false" placeholder="Aux1" Disabled=""/>
 - <input id="searchSubmit" value="" onclick="onSearchSubmit(event)" aria-label="@u
 - wi" type="button" Disabled="Disabled"/>
 - 🗄
 - </div>
 - div id="snippetContainer">

Hidden/Remove object

UNSUCCESSFULLY

ไม่สามารถบันทึกข้อมูลได้ ::ปิดการรับสมัคร

สมัครลงทะเบียน

1.กรอกข้อมูลส่วนตัว (Personal information)	
ชื่อ (Name)*	นามสกุล (Surname) [*]
อีเมล์ (Email)	เบอร์มือถือ (Mobile Number) [*]



MiSSConf(SP2)



1.กรอกข้อมูลส่วนตัว (Personal information)		
ชื่อ (Name)*	นามสกุล (Surname) [*]	
อีเมล์ (Email)	ເນລຣ໌ນົລຄືລ (Mobile Number)*	
DOM Net Cookies	Search by text or CSS selector	~ ~
up < div.row.form-group < div.panel-body < div.panelargin-10 < div#Conte	nelStep1 < form#form1 < div.templontainer < div.templgray-bg <	div.templ
nValidator4" style="color:#CC0000;visibility:hidden;">เบอร์โทรศัพท์มือถือไ	ไม่ถูกต้อง(ตัวเลข10หลัก) <td><u>×</u></td>	<u>×</u>



ม <mark>ัครลงทะเบียน</mark> 1.กรอกข้อมูลส่วนตัว (I	ลงทะเบียน เรียบร้อย		
ชื่อ (Name)*	ตกลง	นามสกุล (Surname)*	
อีเมล์ (Email)		เบอร์มือถือ (Mobile Number)*	

MiSSConf(5P2)



C:\Users\ShellCodeNoobx>python -m SimpleHTTPServer 8888 Serving HTTP on 0.0.0.0 port 8888 ... 127.0.0.1 - [19/Nov/2016 01:07:13] "GET / HTTP/1.1" 200 -127.0.0.1 - [19/Nov/2016 01:07:14] code 404, message File not found 127.0.0.1 - [19/Nov/2016 01:07:14] "GET /favicon.ico HTTP/1.1" 404 -127.0.0.1 - [19/Nov/2016 01:07:14] code 404, message File not found 127.0.0.1 - [19/Nov/2016 01:07:14] "GET /favicon.ico HTTP/1.1" 404 -127.0.0.1 - [19/Nov/2016 01:07:14] "GET /favicon.ico HTTP/1.1" 404 -127.0.0.1 - [19/Nov/2016 01:07:14] "GET /favicon.ico HTTP/1.1" 200 -127.0.0.1 - [19/Nov/2016 01:07:32] "GET /Downloads/ HTTP/1.1" 200 -127.0.0.1 - [19/Nov/2016 01:07:32] "GET /Downloads/UMInjector-master/ HTTP/1.1" 200 -





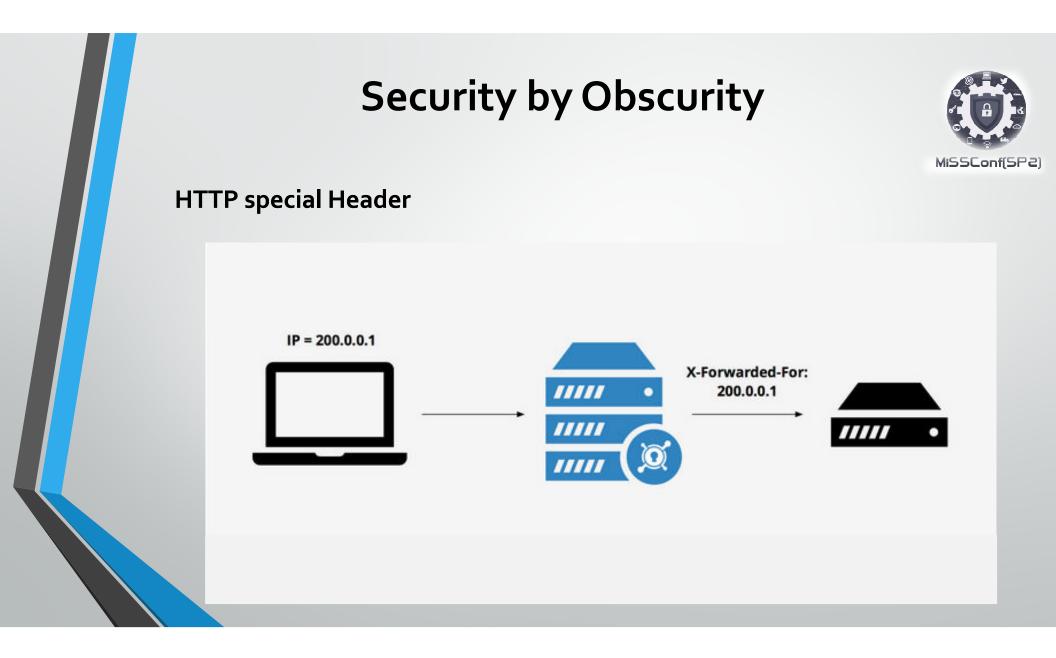
Change service port number

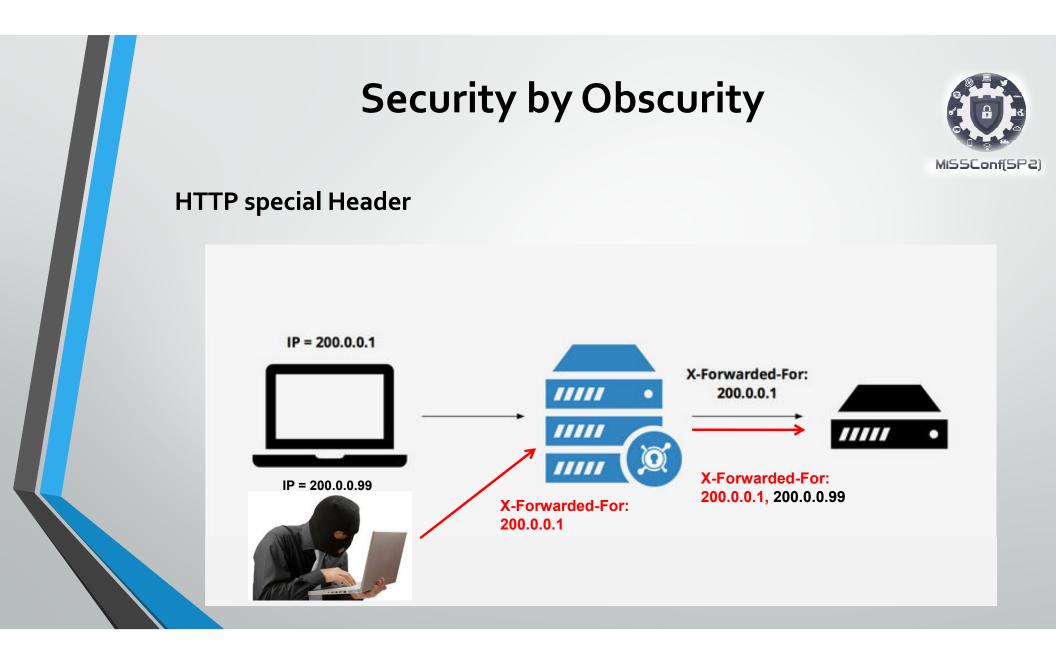
root@kali:~# nmap -p 1-65535 -Pn 127.0.0.1 -A
Starting Nmap 6.49BETA4 (https://nmap.org) at 2016-10-09 13:46 ICT mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
servers Nmap scan report for localhost (127.0.0.1)
Host is up (0.000028s latency). Not shown: 65533 closed ports
PORT STATE SERVICE VERSION
8888/tcp open http SimpleHTTPServer 0.6 (Python 2.7.9)
_http-methods: No Allow or Public header in OPTIONS response (status code 501) _http-server-header: SimpleHTTP/0.6 Python/2.7.9
_http-title: Directory listing for / 1 service unrecognized despite returning data. If you know the service/version,
cgi-bin/submit.cgi?new-service : SF-Port5432-TCP:V=6.49BETA4%I=7%D=10/9%Time=57F9E7C2%P=x86 64-pc-linux-gnu
SF:%r(SMBProgNeg,85,"E\0\0\0\x84SFATAL\0C0A000\0Munsupported\x20frontend\x SF:20protocol\x2065363\.19778:\x20server\x20supports\x201\.0\x20to\x203\.0
SF:\OFpostmaster\.c\OL1955\ORProcessStartupPacket\0\0");



HTTP Referrer

Raw Headers Hex
GET / HTTP/1.1
Host: www.somewebsite.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: th-TH,th;q=0.8,en-US;q=0.6,en-GB;q=0.4,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referrer: https://www.somewebsite.com/login.aspx?user=1234
Upgrade-Insecure-Requests: 1





MiSSConf(SP2)



Request

Raw Hex

GET /customer.php HTTP/1.1 Host: www.somewebsite.com X-Forwarded-For: 200.0.0.1 Accept: */* User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.118 Safari/537.36 Accept-Language: en-US,en;q=0.8,de;q=0.6,ja;q=0.4 Connection: close



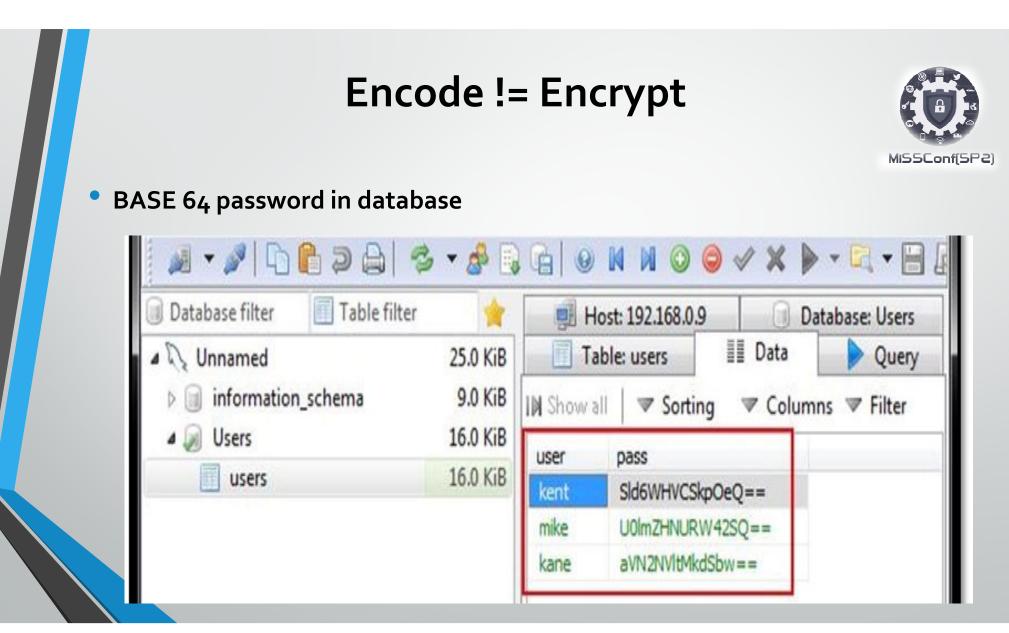
HTTP special Header Example

Header name What it means

x-forwarded-for
x-forwarded-host
x-forwarded-server
x-forwarded-server
x-forwarded-server
X-imsi
x-imsi
x-msisdn
Originating IP of a client connection to the server
Origination host name
Origination server name
A reference to the user-agent profile as specified.
The imsi number. Identifies the end user.
The end users phone number

Ref: https://mobiforge.com/design-development/useful-x-headers

Encode = Encrypt ?



Encode != Encrypt



BASE 64 password Cookie

POST /cgi-bin/index.cgi HTTP/1.1 Host: :8080 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Icewease/31.8.0 Accept: text/html,application/xhtml+xml,application/xml;g=0.9,*/*;g=0.8 Accept-Language: en-US,en;g=0.5 Accept-Encoding: gzip, deflate Referer: http:// :8080/cai-bin/html/loain.html Cookie: qnap_admin_style=default; nas_lang=ENG; nas_tree_x=240; nas_tree_y=370; nas save u=1; nas u=YWRtaW4=; nas address= ; nas save p=1; nas_a=WVdSdGFXND0=: nas_p=YWRtaW5hZG1pbg== Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 12

sid=5rfrajax

Encode != Encrypt



Standard mode 💌 📄 😓 🔚	Tools Online Help		1:	 D
Sites Sites Contexts Default Context Sites	Filter Browse API Encode/Decode/Hash Toggle break on all requests Toggle break on all responses Submit and step to next request or response Submit and continue to next break point Bin request or response Add a custom HTTP break point Active Scan Spider Manual Request Editor Run the Garbage Collector Manual Send WebSocket Message Fuzz Options	Ctrl+E Ctrl+Alt+B Ctrl+Alt+B Ctrl+S Ctrl+C Ctrl+X Ctrl+A Ctrl+Alt+A Ctrl+Alt+S Ctrl+Alt+S Ctrl+Alt+F Ctrl+Alt+O		
🛗 History 🔍 Search 🏴 A	Ierts 📋 Output 🕂			

Encode != Encrypt

BASE 64 decode by zap proxy

🔇 Encode/Decode/Hash

Text to be encoded/decoded/hashed

YWRtaW5hZG1pbg==

Encode Decode Hash Illegal UTF8

Base 64 Decode

adminadmin

URL Decode

YWRtaW5hZG1pbg==



Is self developed encryption algorithm more secure ? (Nobody know)

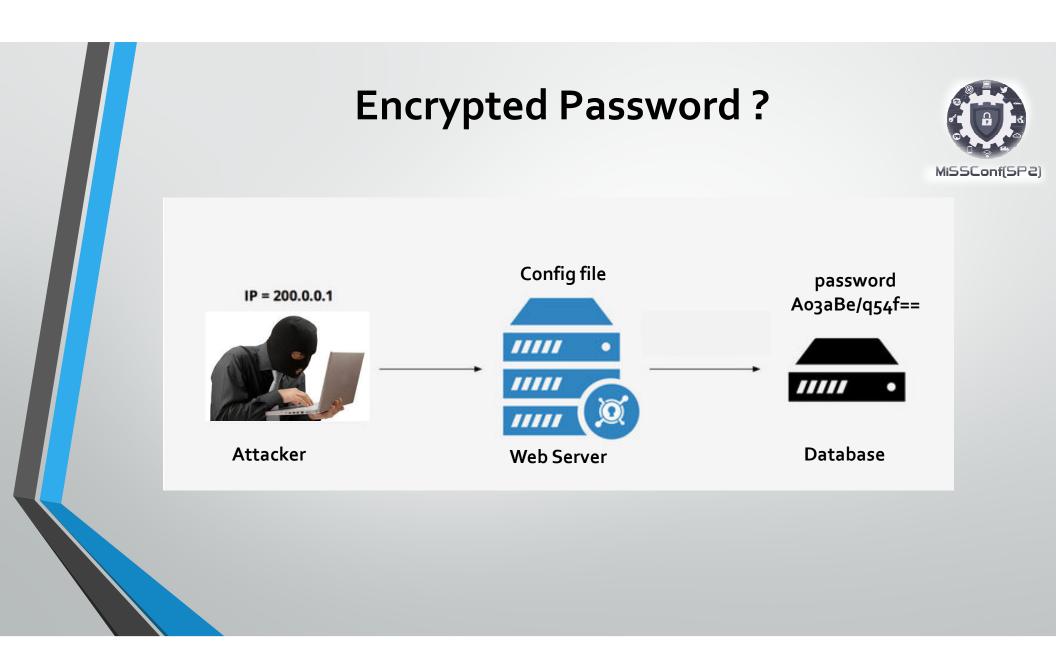
Weak hashing algorithm



Example

- Shift-bit + Add letter GD + Fake Pad (==)
- Password = QGDbGDtGDtGDxGDpGDsGDe==
 - Remove GD => Obttxpse
 - Shift back => Password

Encrypted password?



Password hashing?

Weak hashing algorithm



					MIDSC
Se	elect:	weba	pp_use	r	
S	ect dat	Search			Text length Action I00 Select
	Modify	user_id	group_id	username	password
	edit	1	1	administrator	161ebd7d45089b3446ee4e0d86dbcf92
	edit	2	2	admin	cce2f81bb110bd8e7bab9779491caf09
	edit	8	2	user001	63e780c3f321d13109c71bf81805476e
	edit	9	2	user002	63e780c3f321d13109c71bf81805476e
	edit	11	2	test	05a671c66aefea124cc08b76ea6d30bb
(5 r	ows) [whole re	acult		

Weak hashing algorithm



Status:	We found 1 hashes! [Timer: 128 m/s] Please find t	them below
MD5 Hashes:	161ebd7d45089b3446ee4e0d86dbcf92	161ebd7d45089b3446ee4e0d86dbcf92 MD5 : P@ssw0rd
Status:	We found 1 hashes! [Timer: 731 m/s] Please find t	hem below
MD5 Hashes:	cce2f81bb110bd8e7bab9779491caf09	cce2f81bb110bd8e7bab9779491caf09 MD5 : password@1234
Status:	We found 1 hashes! [Timer: 704 m/s] Please find t	hem below
MD5 Hashes:	63e780c3f321d13109c71bf81805476e	63e780c3f321d13109c71bf81805476e MD5 : userpass
Status:	We found 1 hashes! [Timer: 118 m/s] Please find	them below
MD5 Hashes:	05a671c66aefea124cc08b76ea6d30bb	05a671c66aefea124cc08b76ea6d30bb MD5 : testtest

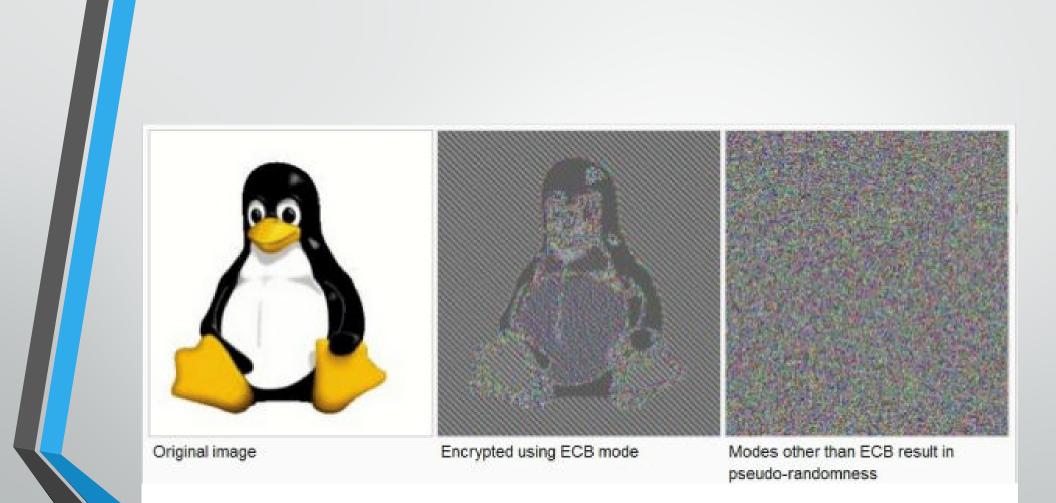
Encrypt data with secure algorithm is OK. No more need to concern

Encryption



More things to concern for the encryption

- Implementation
- Key length (bits)
- Mode (ECB, CBC, OFB, CFB)



ECB mode weakness in real case ?



AES 128-bit ECB Mode mobile_num=0899999999 [MR. A] C17D95754A5B0C2B5711AD1E9E74ACFC2C8FE56BE20D6138613D77B60DEB5B222 mobile_num=0899966666 [MR. B] C17D95754A5B0C2B5711AD1E9E74ACFC78F664431DFB0AFDC05FD8C0084C96ED mobile_num=0866666666 [MR. C] B1E564C90CAB46B381FB95DCC325F58D78F664431DFB0AFDC05FD8C0084C96ED



AES 128-bit ECB Mode



mobile_num=0866699999 [MR. X]

https://fitnessxx.com/cutomer.php?

data=B1E564C90CAB46B381FB95DCC325F58D2C8FE56BE20D6138613D77B60DEB5B22



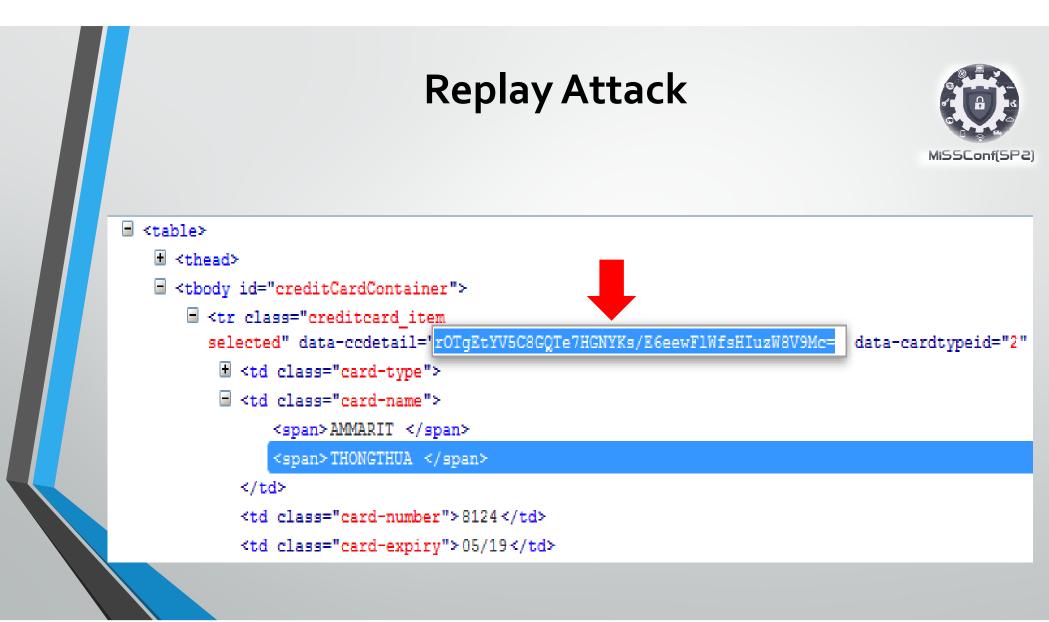
Payload Options [ECB block shuffler]

This payload type can be used to shuffle blocks of ciphertext in ECB-encrypted data, so a same cipher and key, to provide additional blocks for shuffling into the original data.

Encrypted data to shuffle:	 Base value of payload position 							
	Specific string:							
Format of original data:	Literal value							
	 Encoded as ASCII hex 							
Block size (usually 8 or 16):	16							
Additional encrypted strings – optional								
Paste								
Load								

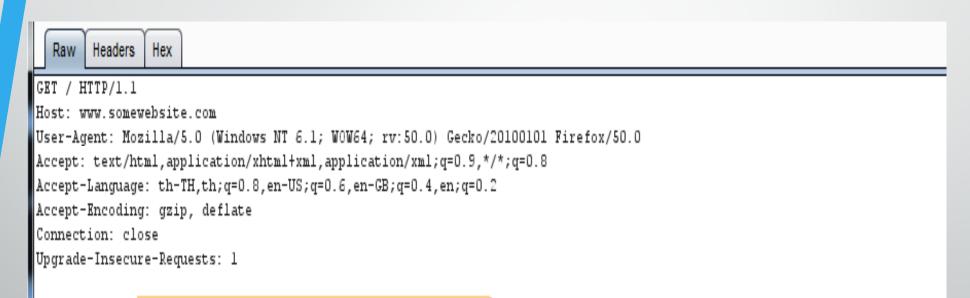
Is encrypted data secured when secure algorithm and Mode?

Yes, But



Replay Attack





data-ccdetail=<mark>r0TgETYves34dfdDeDAEr86YKs/E6eewF1WfsH1uzW8V9Mc==</mark>&CardName=AMMARIT%20TH0NGTHUA&Card-Expiry=05/19&amount=12000

Other Security #MiSSConcepts

Authentication Check at on load

-Tamper Data and reject

Cookie Expired date is work

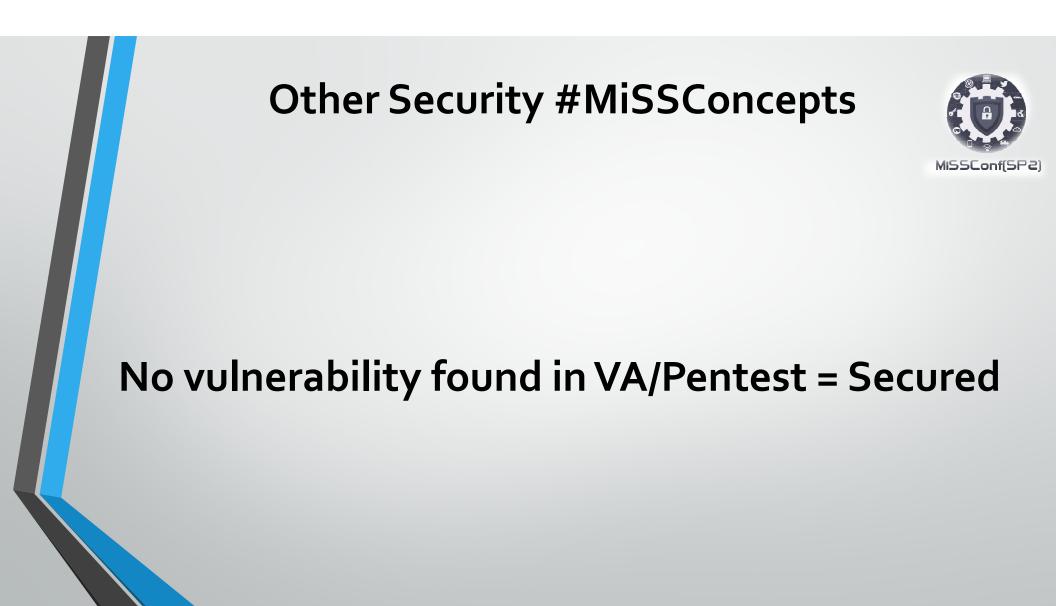
-Cookie Editor

Protection by WAF is sufficient

- -Evasion (Ex; admin';--)
- -Unsupported SSL cipher suite
- -Pollution technique
- -WAFWooF Input validate
- **HTTPS** is sufficient



Intruder Repeate	r Window He	lp												
get Proxy Spi	der Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts					
nections HTTP	SSL Sess	ions Displa	y Misc											
you can use the	se settings to re	equest use of	f specific pro	otocols or ciphe	ers. Use the	se options wi	th caution as	s misconfig	juration ma	y break a	all your ou	utgoing SSL	_ connectio	ns.
SSL Protocols														
Select all	Enabled	Protocol												
		SSLv2Hel	io]					
Select none		SSLv3												
	 ✓ 	TLSv1												
		TLSv1.1												
		TLSv1.2												
SSL Ciphers														
SSL Ciphers	Enabled	Cipher												
SSL Ciphers Select all		Cipher TLS ECDH	IE ECDSA V	WITH AES 128	3 CBC SHA2	256								
<u></u>		TLS_ECDH		VITH_AES_128 H_AES_128 C				4						
Select all		TLS_ECDH TLS_ECDH	IE_RSA_WIT	VITH_AES_128 H_AES_128_C 128_CBC_SH4	BC_SHA256									
Select all		TLS_ECDH TLS_ECDH TLS_RSA_	IE_RSA_WIT WITH_AES_	H_AES_128_C	BC_SHA256 A256	3								
Select all) 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	TLS_ECDH TLS_ECDH TLS_RSA_ TLS_ECDH TLS_ECDH	IE_RSA_WIT _WITH_AES_ I_ECDSA_W I_RSA_WITH	H_AES_128_C 128_CBC_SHA ITH_AES_128_ L_AES_128_CE	BC_SHA256 A256 CBC_SHA25 BC_SHA256	3								
Select all) 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	TLS_ECDH TLS_ECDH TLS_RSA_ TLS_ECDH TLS_ECDH TLS_DHE_	IE_RSA_WIT _WITH_AES_ I_ECDSA_W I_RSA_WITH _RSA_WITH_	H_AES_128_C 128_CBC_SHA ITH_AES_128_ I_AES_128_CE AES_128_CBC	BC_SHA256 A256 CBC_SHA25 BC_SHA256 C_SHA256	3								
Select all	 	TLS_ECDH TLS_ECDH TLS_RSA_ TLS_ECDH TLS_ECDH TLS_DHE_ TLS_DHE_	IE_RSA_WIT _WITH_AES_ I_ECDSA_W I_RSA_WITH _RSA_WITH_ _DSS_WITH_	H_AES_128_C 128_CBC_SHA ITH_AES_128_ I_AES_128_CBC AES_128_CBC AES_128_CBC	BC_SHA256 A256 CBC_SHA256 C_SHA256 C_SHA256 C_SHA256	3								
Select all) 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	TLS_ECDH TLS_ECDH TLS_RSA_ TLS_ECDH TLS_ECDH TLS_DHE_ TLS_DHE_	IE_RSA_WIT _WITH_AES_ I_ECDSA_W I_RSA_WITH _RSA_WITH_ _DSS_WITH_	H_AES_128_C 128_CBC_SHA ITH_AES_128_ I_AES_128_CE AES_128_CBC	BC_SHA256 A256 CBC_SHA256 C_SHA256 C_SHA256 C_SHA256	3								
Select all	9 9 9 9 9 9 9 9 9 9 9	TLS_ECDH TLS_ECDH TLS_RSA_ TLS_ECDH TLS_ECDH TLS_DHE_ TLS_DHE_	IE_RSA_WIT _WITH_AES_ I_ECDSA_W I_RSA_WITH _RSA_WITH_ _DSS_WITH_	H_AES_128_C 128_CBC_SHA ITH_AES_128_ I_AES_128_CBC AES_128_CBC AES_128_CBC	BC_SHA256 A256 CBC_SHA256 C_SHA256 C_SHA256 C_SHA256	3								
Select all Select none	V V V V V Workarounds	TLS_ECDH TLS_ECDH TLS_RSA_ TLS_ECDH TLS_ECDH TLS_DHE_ TLS_DHE_ TLS_ECDH	IE_RSA_WIT WITH_AES_ I_ECDSA_W I_RSA_WITH RSA_WITH_ DSS_WITH_ IE_ECDSA_V	H_AES_128_C 128_CBC_SH/ ITH_AES_128_ I_AES_128_CB AES_128_CBC AES_128_CBC AES_128_CBC MITH_AES_128	EBC_SHA256 A256 CBC_SHA256 C_SHA256 C_SHA256 C_SHA256 C_SHA256 C_SHA256 CBC_SHA	3								
Select all Select none	V V V V V V V V V V V V V V V V V V V	TLS_ECDH TLS_ECDH TLS_RSA_ TLS_ECDH TLS_ECDH TLS_DHE_ TLS_DHE_ TLS_ECDH	IE_RSA_WIT WITH_AES_ I_ECDSA_W I_RSA_WITH RSA_WITH_ DSS_WITH_ IE_ECDSA_W	H_AES_128_C 128_CBC_SHA ITH_AES_128_ I_AES_128_CB AES_128_CBC AES_128_CBC MITH_AES_128 egotiation failur	EBC_SHA256 A256 CBC_SHA256 C_SHA256 C_SHA256 C_SHA256 C_SHA256 C_SHA256 CBC_SHA	3								
Select all Select none SSL Negotiation Automatically Enable algor	V V V V V V V V V V V V V V V V V V V	TLS_ECDH TLS_ECDH TLS_RSA_ TLS_ECDH TLS_ECDH TLS_DHE_ TLS_DHE_ TLS_ECDH	IE_RSA_WIT WITH_AES_ I_ECDSA_W I_RSA_WITH_ RSA_WITH_ DSS_WITH_ IE_ECDSA_W IMMETERS on n	H_AES_128_C 128_CBC_SHA ITH_AES_128_ I_AES_128_CB AES_128_CBC AES_128_CBC MITH_AES_128 egotiation failur	EBC_SHA256 A256 CBC_SHA256 C_SHA256 C_SHA256 C_SHA256 C_SHA256 C_SHA256 CBC_SHA	3								



Conclusion



- Secure by design
- Put the right solutions to the right jobs
- Security Source code review
- Perform regular vulnerability assessment / penetration test

