MiSSConf(SP2)

Security #MiSSConcepts

Ammarit Thongthua, CISSP CISM

Who am I

<Name>

Ammarit Thongthua

Khay

Shellcodenoobx

</Name>

<Job>

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

Security #MiSSConcepts

MiS

use
understand
take


Security protection we
#Expected


MiSSConf(SP2)
Security protection
we get in
#Reality

Security by Obscurity

Security by Obscurity

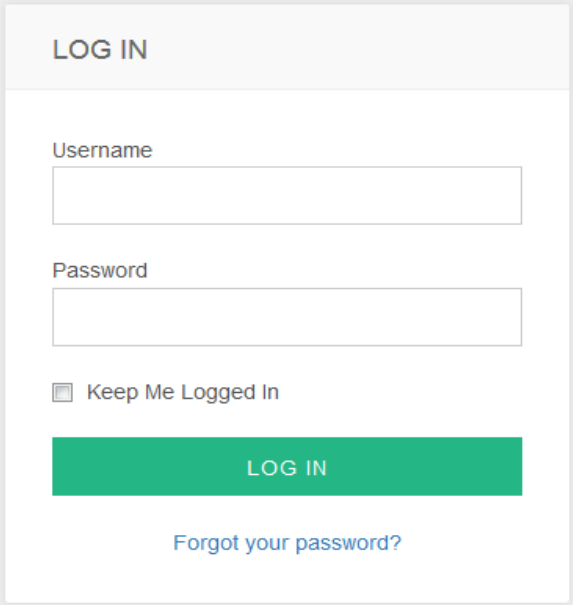
Obscurity = make nobody know or make it hard to see

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

Security by Obscurity

Path hiding

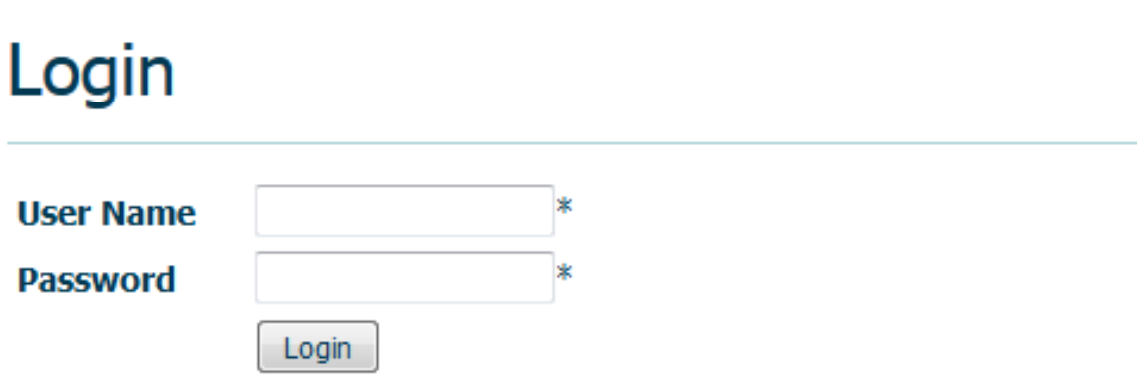
https://www.somewebsite.com/page/admin/login.aspx



Security by Obscurity

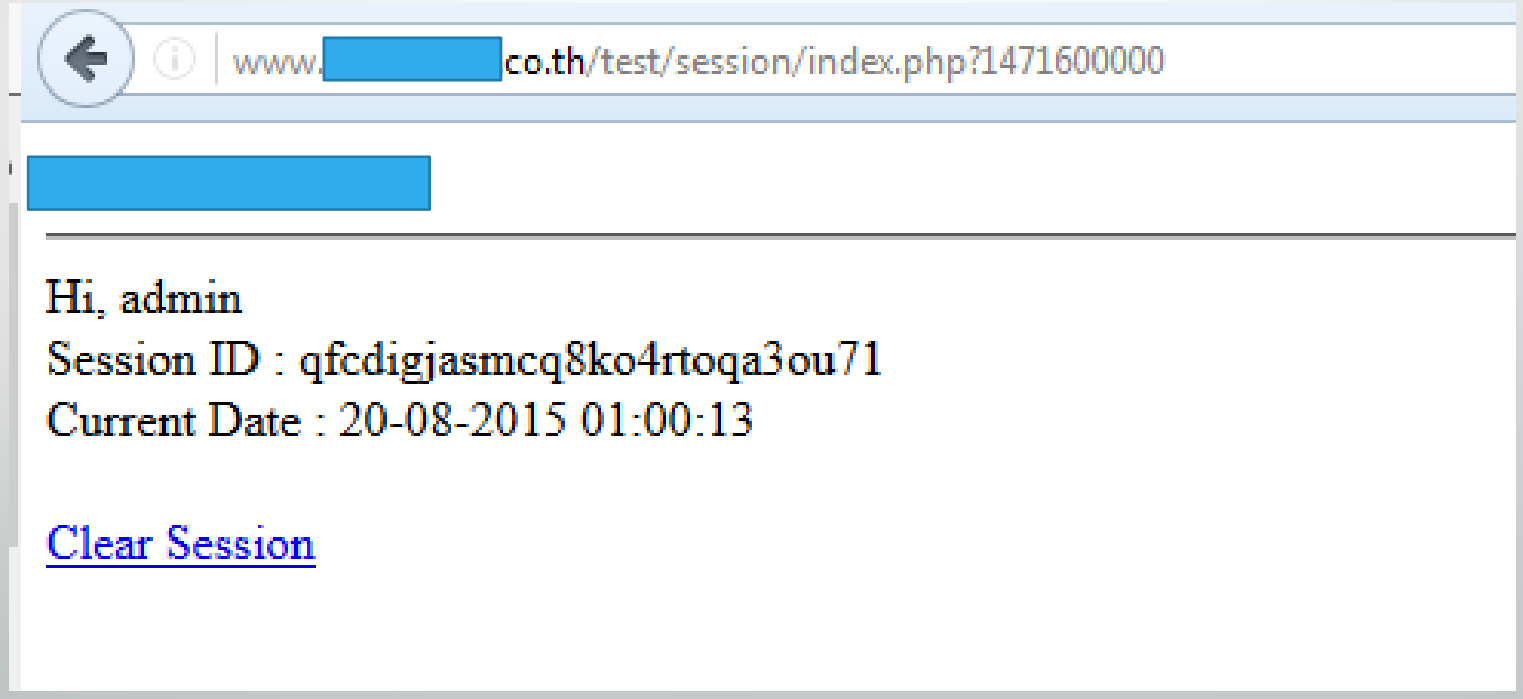
Path hiding

https://www.somewebsite.com/abc/123/admin.php



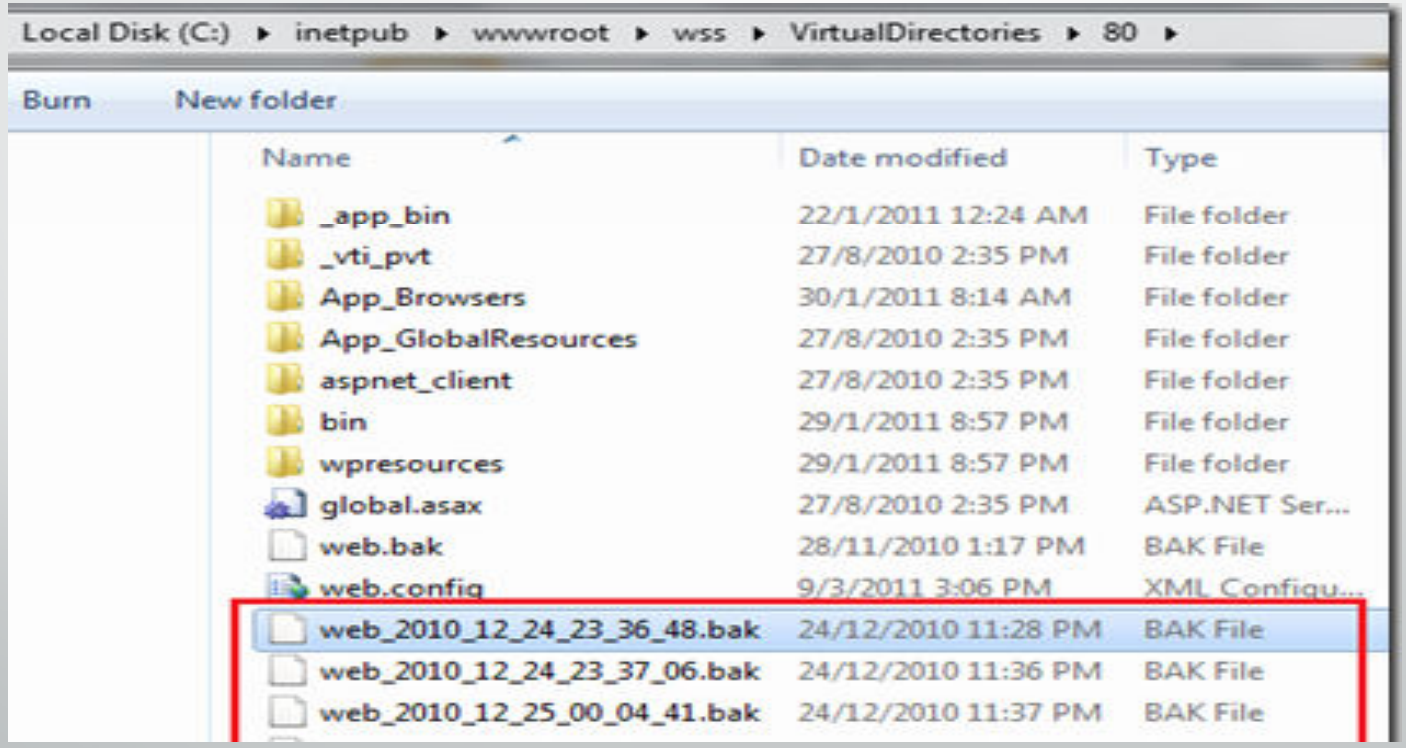
Security by Obscurity

Path hiding



Security by Obscurity

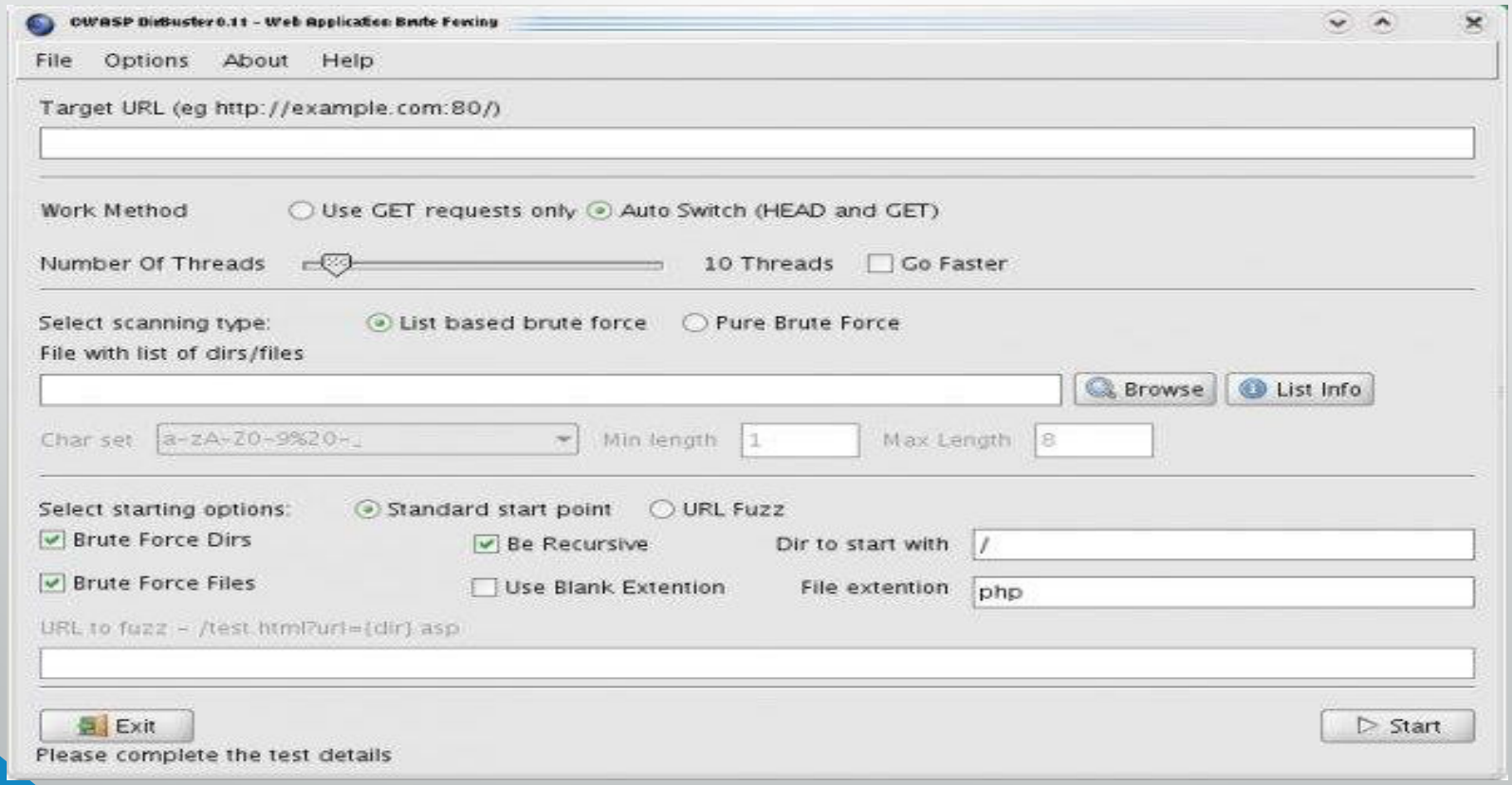
Path hiding -Temp File, Back Up



Security by Obscurity

MiSSConf(SP2)

Dirbuster



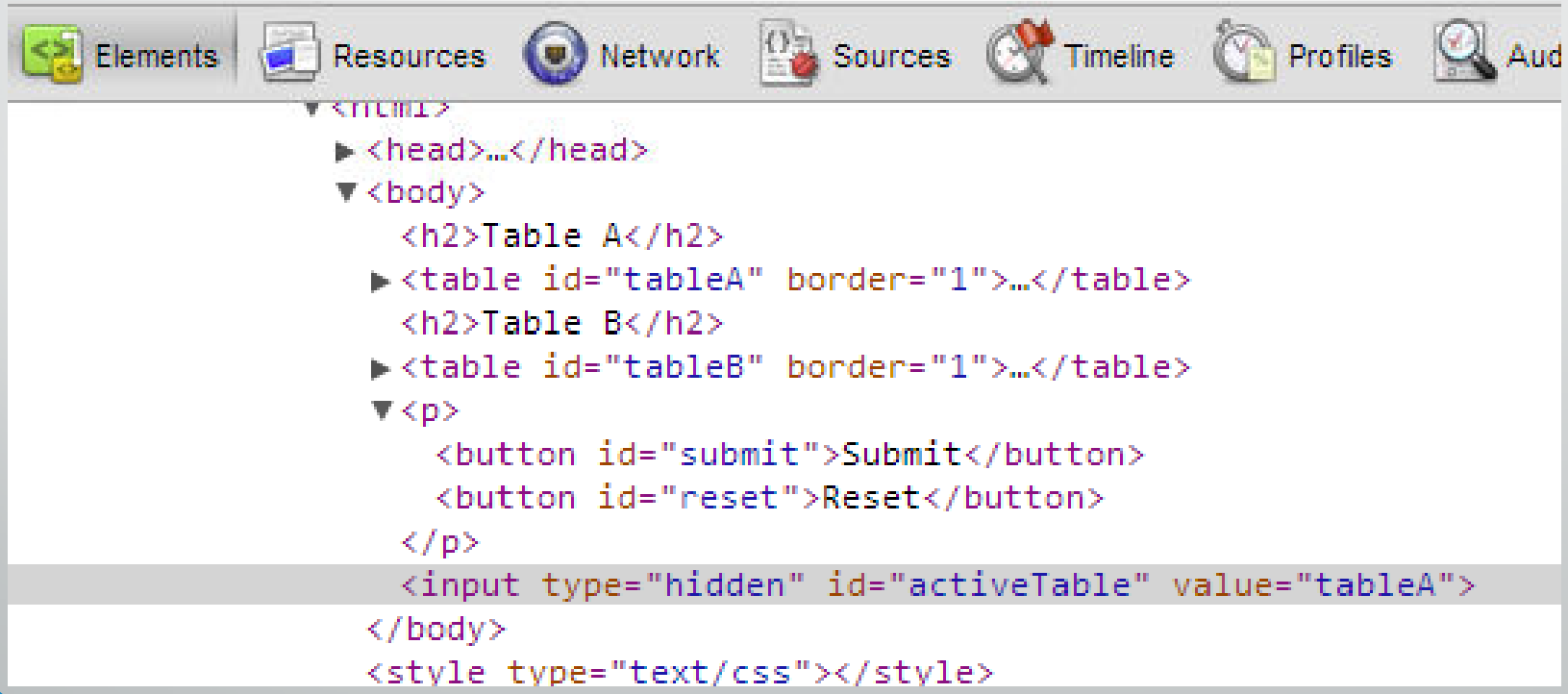
Security by Obscurity

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

Security by Obscurity

Hidden filed



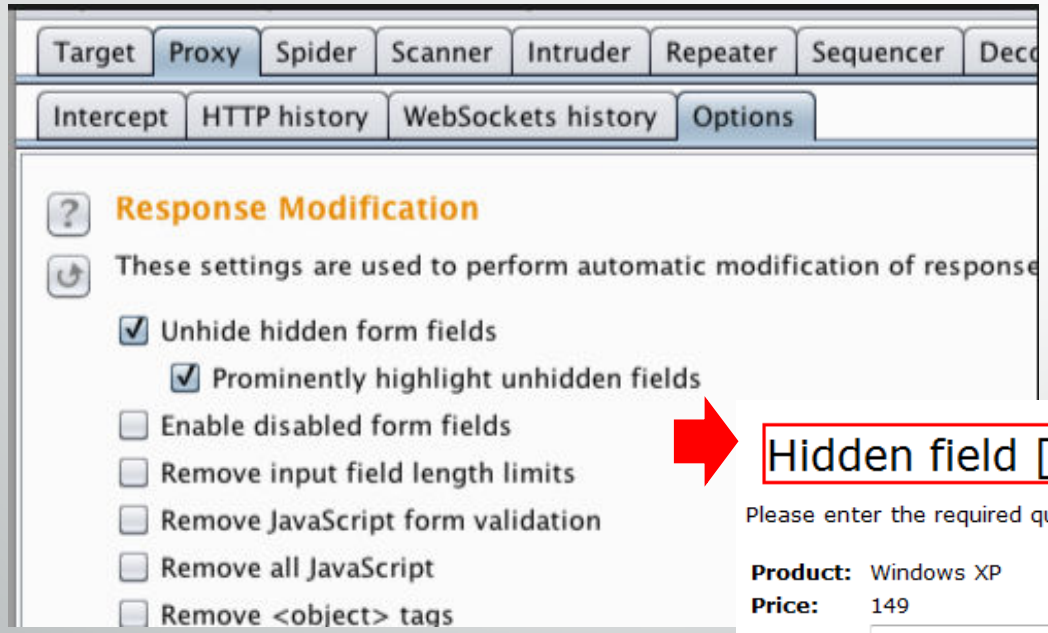
Security by Obscurity

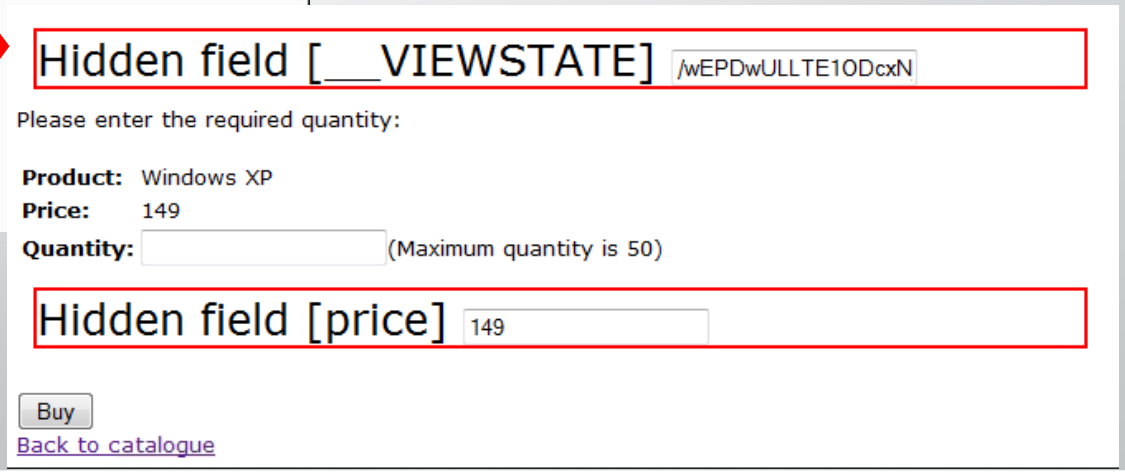
Hidden filed

```
<tr>
    <td height="30"> </td>
    <td align="left">
        <input id="login" name="login" value="login" type="submit">
        <input id="usertype" name="usertype" value="user" type="hidden">
        <input id="path" name="path" value="" type="hidden">
    </td>
</tr>
<tr>
</tbody>
```

Security by Obscurity

Hidden filed





Security by Obscurity

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;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.67.136/WebGoat/attack?Screen=1554&menu=
Cookie: remember_token=PNkIxJ3DG8iXL0F4vrAWBA; acopendivids=sw
PHPSESSID=0l8fof1nkg5333kq6pckk47hn0;
_cyclone_session=BAh7B0kiD3Nlc3Npb25faWQGOgZFRkkiJTBlYjc2YjdjZ
vSi9hQTBGclVjeFZYQ3cvVkQzSmtLRnp5Z3ZvMkdTRHA5TTQzcFE9BjsARg%3D
JSESSIONID=1ED3891622C69A1B110F4BC57D1204E1;
_railsgoat_session=BAh7B0kiD3Nlc3Npb25faWQGOgZFRkkiJTk2ZGMxY2I
FEyWU9USGhUVUV3d3RSWWpDL0tlZEJaUXJpdU5HSnMxWllCTGw5L1E9BjsARg%
Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 35

QTY=1&SUBMIT=Purchase&Price=10
```

Security by Obscurity

Disabled

```
<body 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="ค้นหา" dir="auto" type="text" autocomplete="off" aria-autocomplete="true" aria-controls="searchSuggestionTable" expanded="false" placeholder="ค้นหา" Disabled=""/>
        <input id="searchSubmit" value="" onclick="onSearchSubmit(event)" aria-label="ค้นหา" type="button" Disabled="Disabled"/>
      <table id="searchSuggestionTable" class="contentSearchSuggestionTable" role="presentation" hidden="">
    </div>
    <div id="snippetContainer">
```

Security by Obscurity

Hidden/Remove object

UNSUCCESSFULLY

ไม่สามารถบันทึกข้อมูลได้ ::ปิดการรับสมัคร

สมัครลงทะเบียน

1.กรอกข้อมูลส่วนตัว (Personal information)

ชื่อ (Name)*

นามสกุล (Surname)*

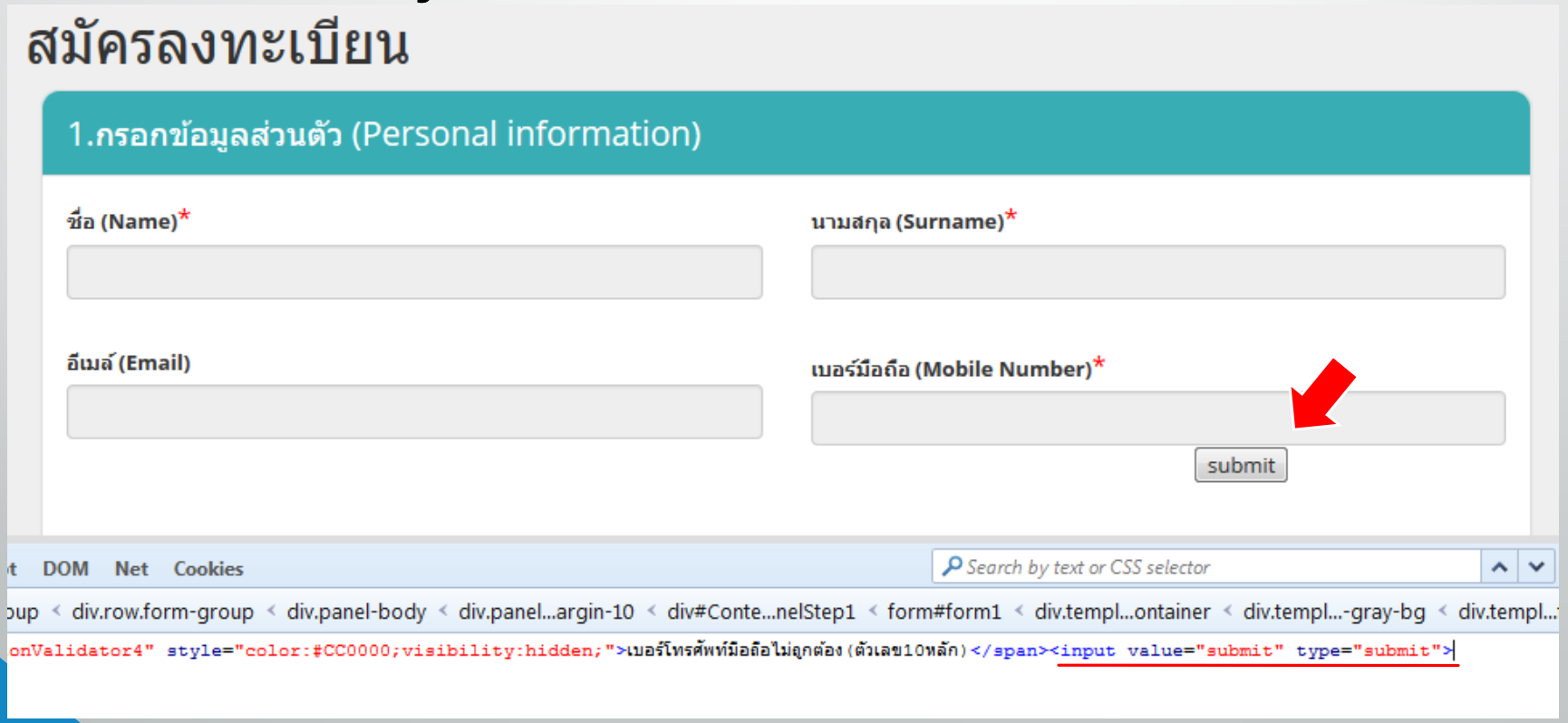
อีเมล์ (Email)

เบอร์มือถือ (Mobile Number)*

Security by Obscurity

MiSSConf(SP2)

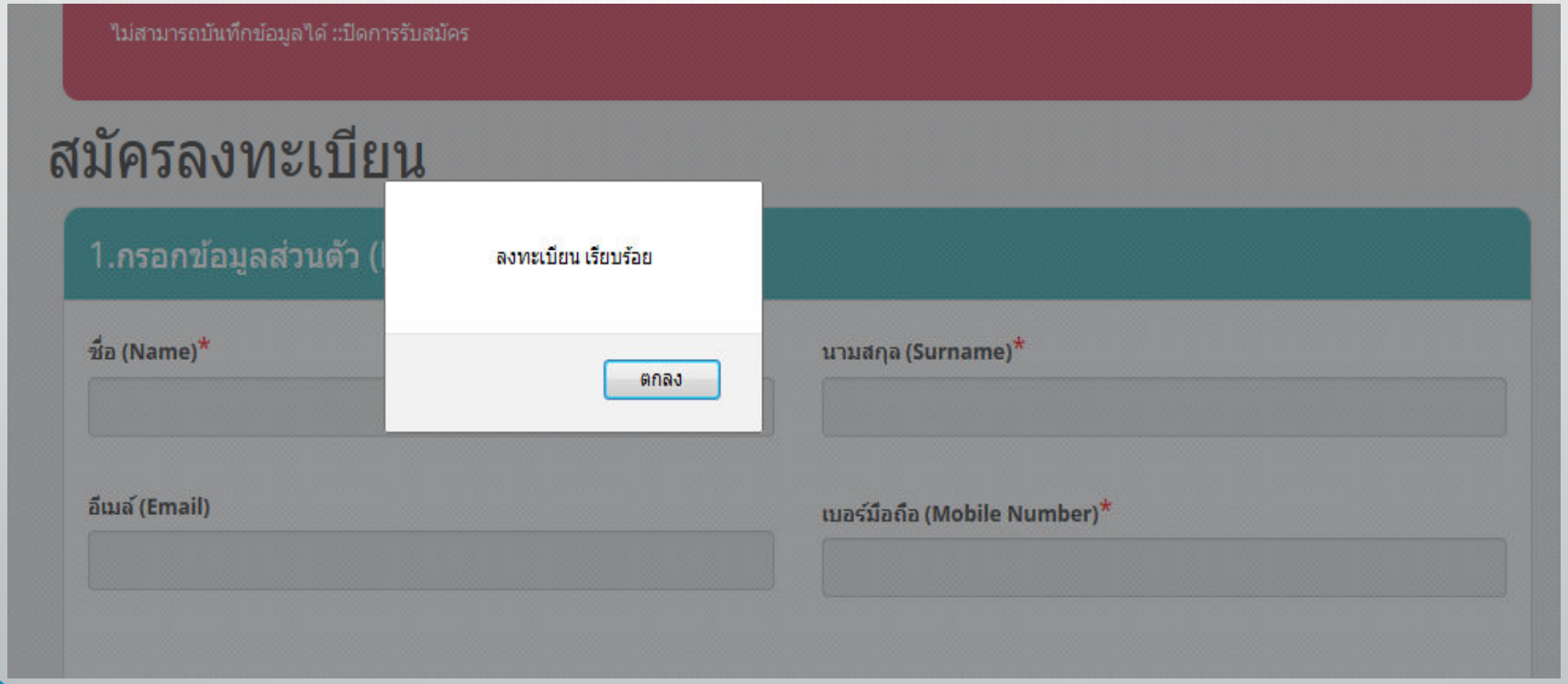
Hidden/Remove object



Security by Obscurity

MiSSConf(SP2)

Hidden/Remove object



Security by Obscurity

Change service port number

```
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 01:07:18] "GET /Downloads/ HTTP/1.1" 200 -
127.0.0.1 - - [19/Nov/2016 01:07:32] "GET /Downloads/VMInjector-master/ HTTP/1.1" 200 -
127.0.0.1 - - [19/Nov/2016 01:07:35] "GET /Downloads/VMInjector-master/vminjector/ HTTP/1.1" 200 -
```

Security by Obscurity

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
5432/tcp open  postgresql PostgreSQL DB
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:\0Fpostmaster\.c\0L1955\0RProcessStartupPacket\0\0");
```

Security by Obscurity

HTTP Referrer

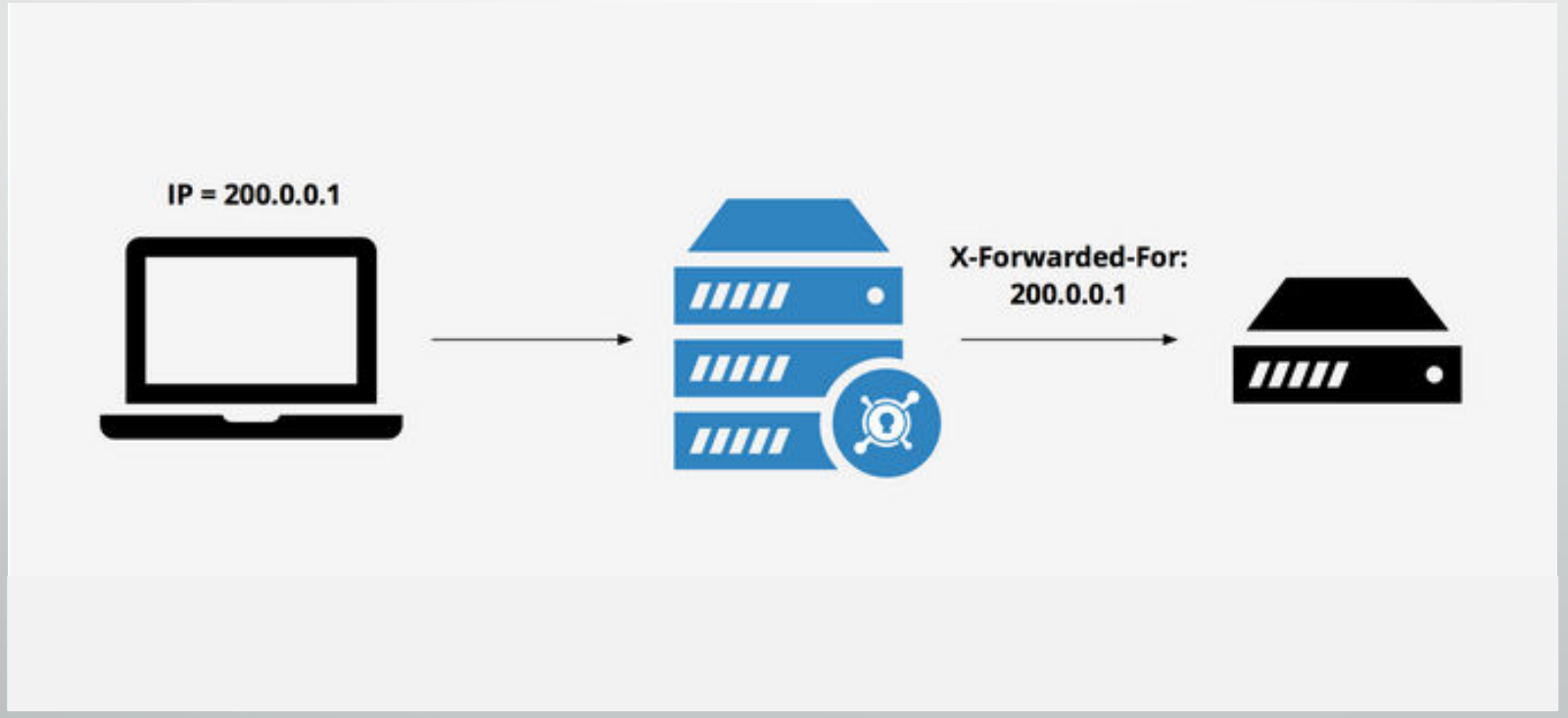
Raw | Headers | Hex

```
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
```

Security by Obscurity

MiSSConf(SP2)

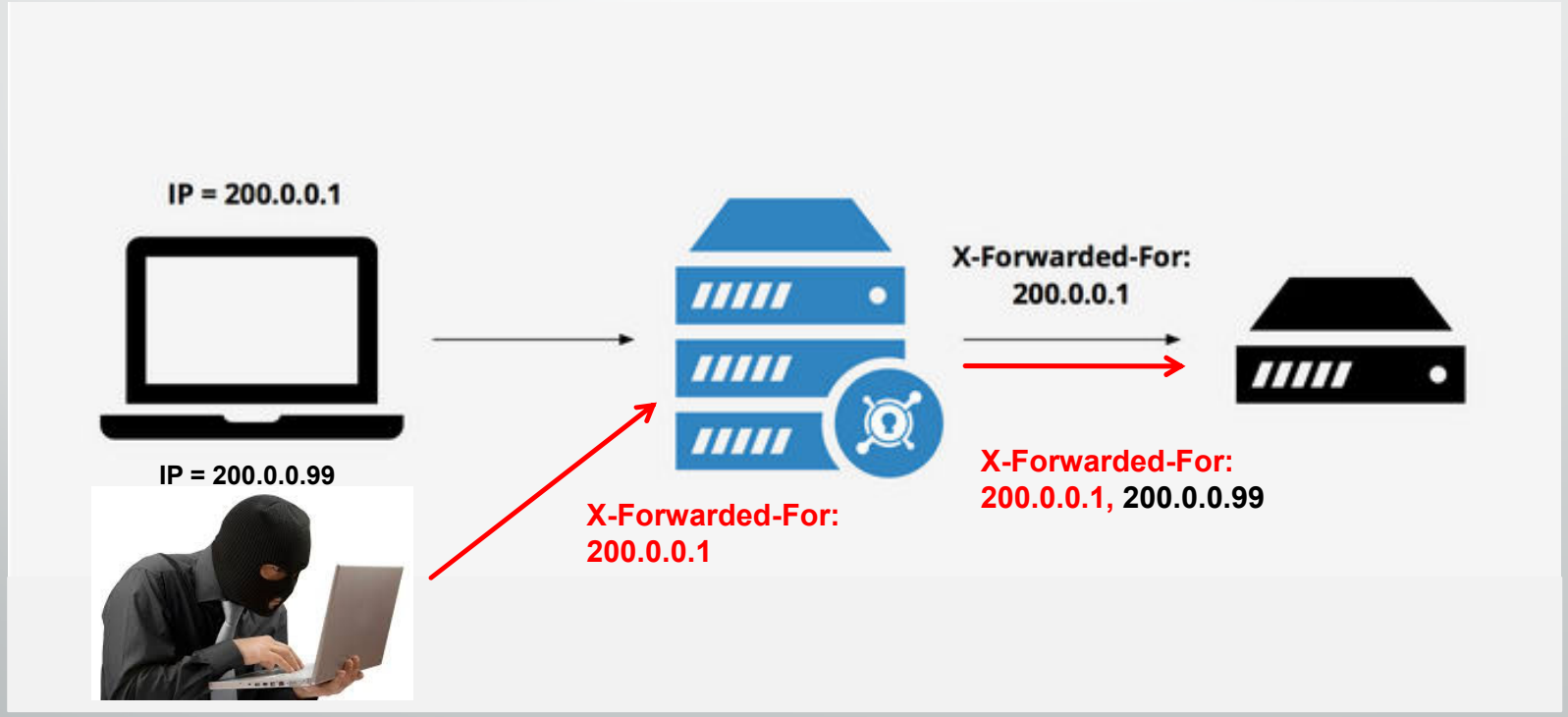
HTTP special Header



Security by Obscurity

MiSSConf(SP2)

HTTP special Header



Security by Obscurity

HTTP special Header

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
```

Security by Obscurity

HTTP special Header Example

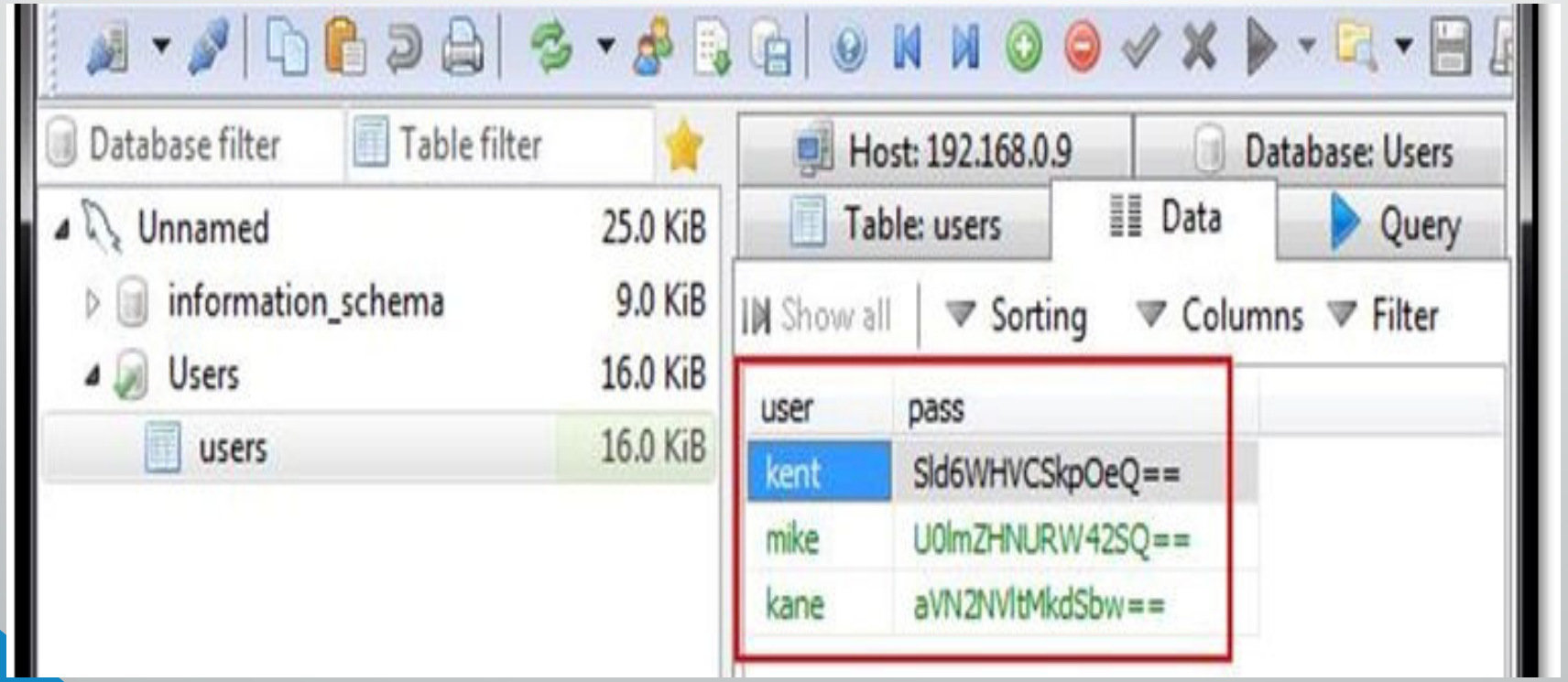
Header name	What it means
x-forwarded-for	Originating IP of a client connection to the server
x-forwarded-host	Origination host name
x-forwarded-server	Originating server name
x-wap-profile	A reference to the user-agent profile as specified.
x-imsi	The imsi number. Identifies the end user.
x-msisdn	The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

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

Encode = Encrypt ?

Encode != Encrypt

- **BASE 64 password in database**

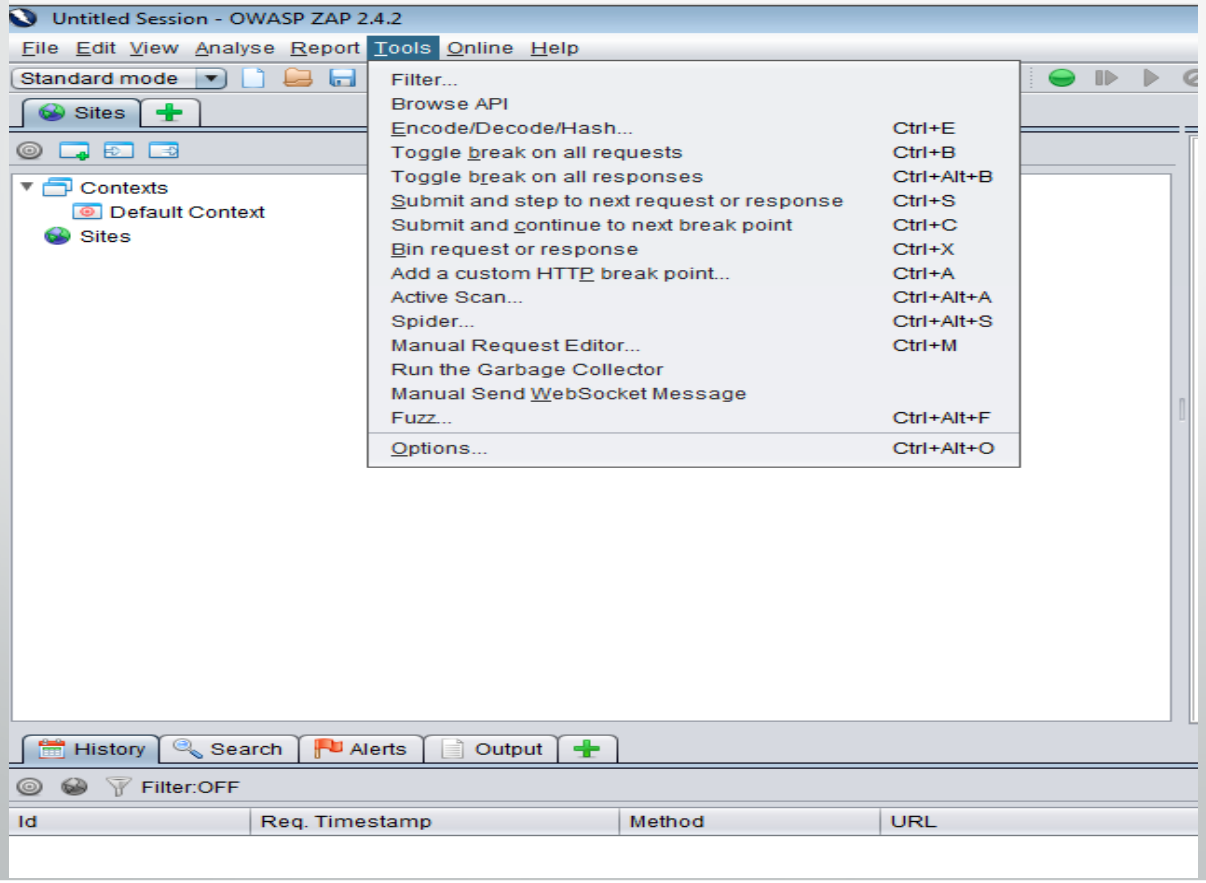


Encode != Encrypt

- **BASE 64 password Cookie**

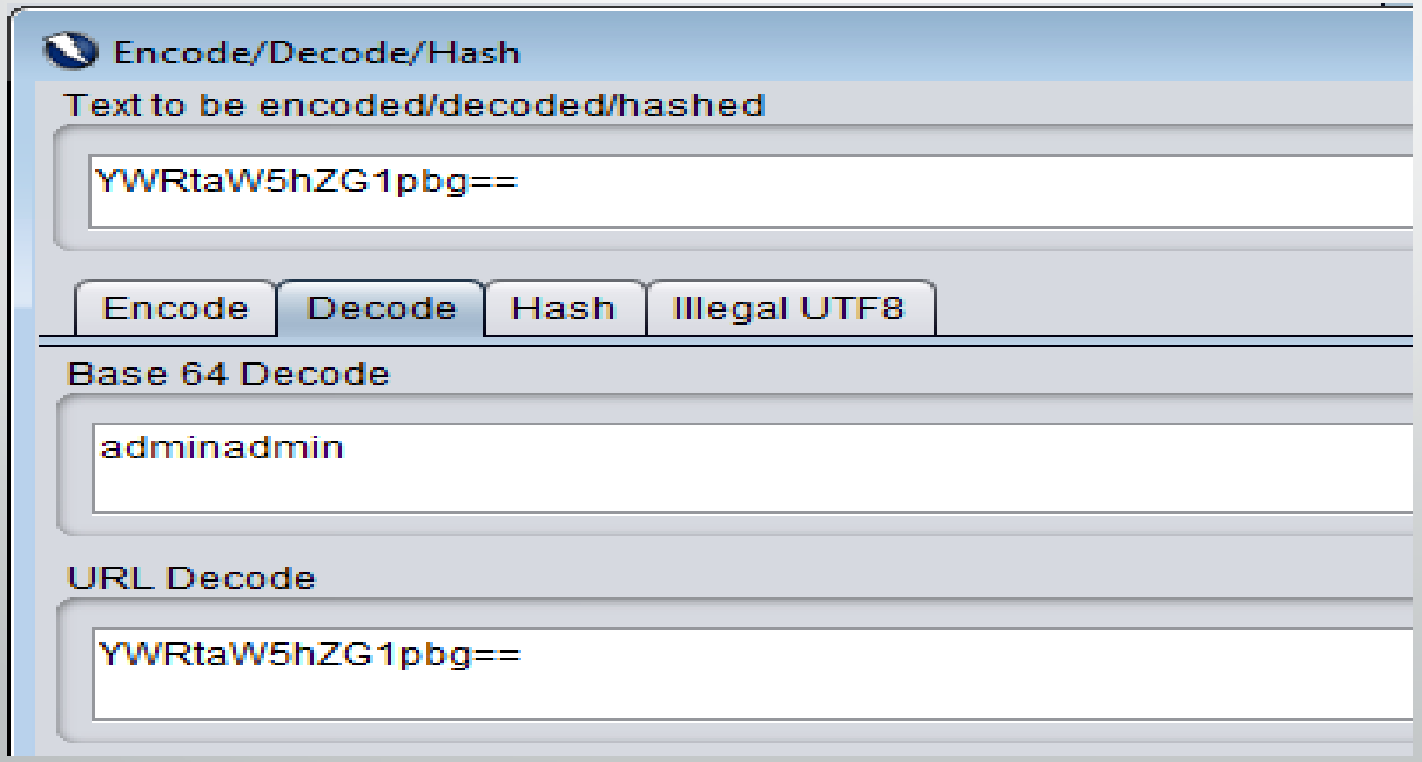
```
POST /cgi-bin/index.cgi HTTP/1.1
Host: [redacted]:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0
Iceweasel/31.8.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://[redacted]:8080/cgi-bin/html/login.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=[redacted]; 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



Encode != Encrypt

- **BASE 64 decode by zap proxy**



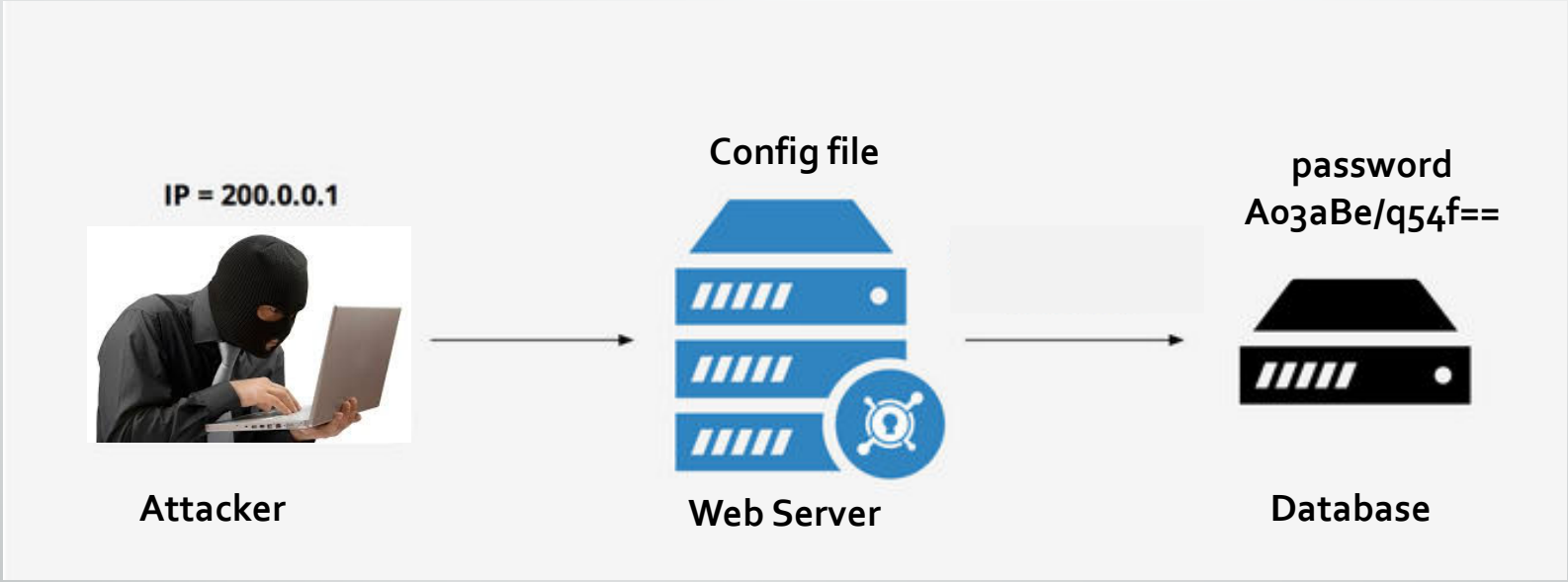
Is self developed encryption algorithm more secure ?
(Nobody know)

Weak hashing algorithm

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

Encrypted password ?

Encrypted Password ?



Password hashing ?

Weak hashing algorithm

Select: webapp_user

Select data Show structure Alter table New item

Select | Search | Sort | Limit: 50 | Text length: 100 | Action: Select

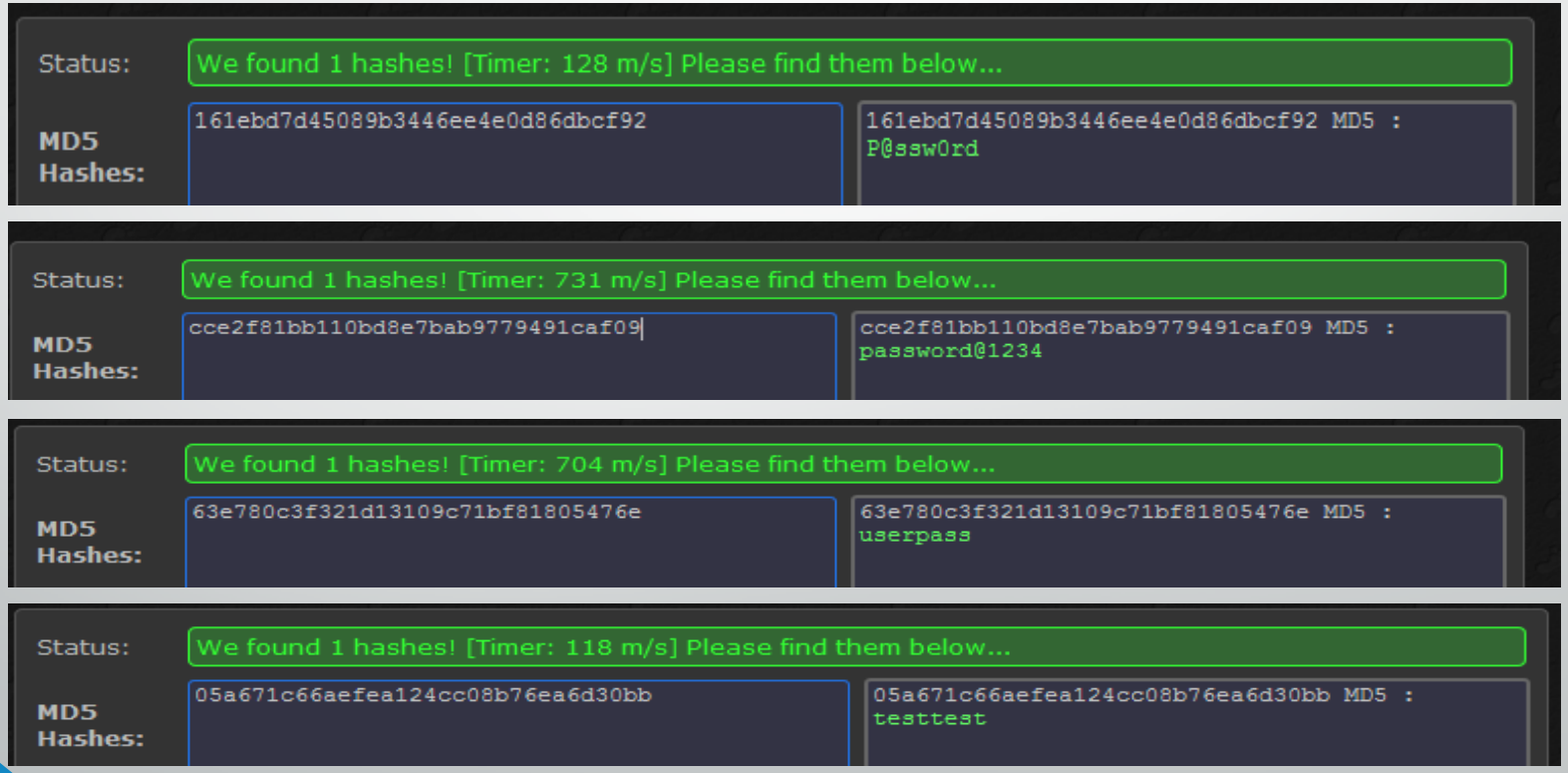
```
SELECT * FROM `webapp_user` LIMIT 50 (0.001 s) Edit
```

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 rows) whole result

Weak hashing algorithm

MiSSConf(SP2)



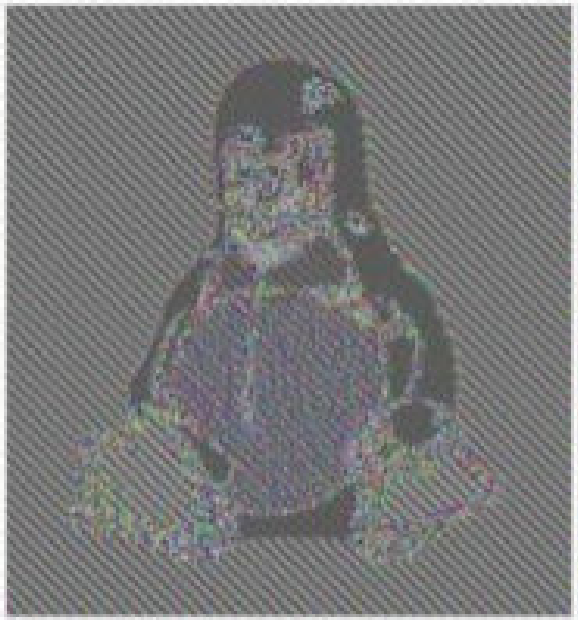
Encrypt data with secure algorithm is OK.
No more need to concern

Encryption

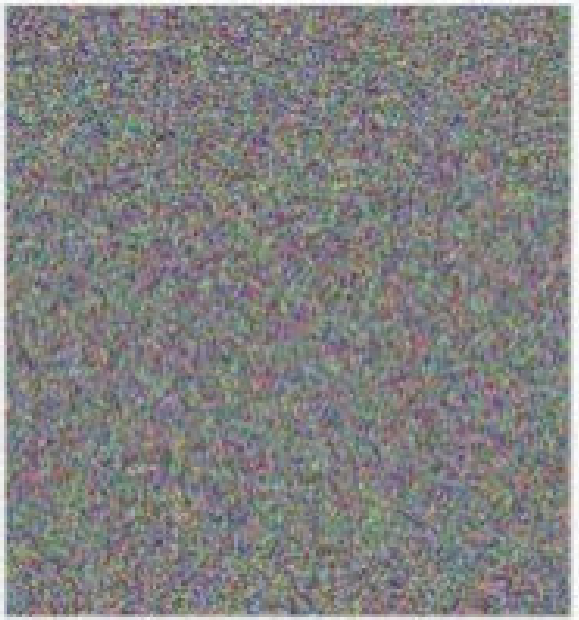
More things to concern for the encryption

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

Original image



Encrypted using ECB mode



Modes other than ECB result in pseudo-randomness

ECB mode weakness in real case ?

ECB block shuffler

AES 128-bit ECB Mode

mobile_num=0899999999 [MR. A]

C17D95754A5B0C2B5711AD1E9E74ACFC2C8FE56BE20D6138613D77B60DEB5B22

mobile_num=0899966666 [MR. B]

C17D95754A5B0C2B5711AD1E9E74ACFC78F664431DFB0AFDC05FD8C0084C96ED

mobile_num=0866666666 [MR. C]

B1E564C90CAB46B381FB95DCC325F58D78F664431DFB0AFDC05FD8C0084C96ED

ECB block shuffler

AES 128-bit ECB Mode

mobile_num=0899999999

C17D95754A5B0C2B5711AD1E9E74ACFC2C8FE56BE20D6138613D77B60DEB5B22

mobile_num=0899966666

C17D95754A5B0C2B5711AD1E9E74ACFC78F664431DFB0AFDC05FD8C0084C96ED

mobile_num=0866666666

B1E564C90CAB46B381FB95DCC325F58D78F664431DFB0AFDC05FD8C0084C96ED

mobile_num=0866699999 **[MR. X]**

B1E564C90CAB46B381FB95DCC325F58D2C8FE56BE20D6138613D77B60DEB5B22

ECB block shuffler

mobile_num=0866699999 [MR. X]

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

data=B1E564C90CAB46B381FB95DCC325F58D2C8FE56BE20D6138613D77B60DEB5B22

ECB block shuffler

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


```
<table>
  <thead>
  <tbody id="creditCardContainer">
    <tr class="creditcard_item
    selected" data-ccdetail="rOIgEtYV5C8GQTe7HGNYKs/E6eewF1WfsHIuzW8V9Mc=" data-cardtypeid="2"
      <td class="card-type">
      <td class="card-name">
          <span>AMMARIT </span>
          <span>THONGTHUA </span>
      </td>
      <td class="card-number">8124</td>
      <td class="card-expiry">05/19</td>
```

Replay Attack

Raw | Headers | Hex

```
GET / HTTP/1.1
Host: www.somewebsite.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; W0W64; 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
Upgrade-Insecure-Requests: 1

data-ccdetail=r0TgETYves34dfdDeDAEr86YKs/E6eewF1WfsHIuzW8V9Mc==&CardName=AMMARIT%20TH0NGTHUA&Card-Expiry=05/19&amount=12000
```

Other Security #MiSSConcepts

Authentication Check at on load

- Tamper Data and reject

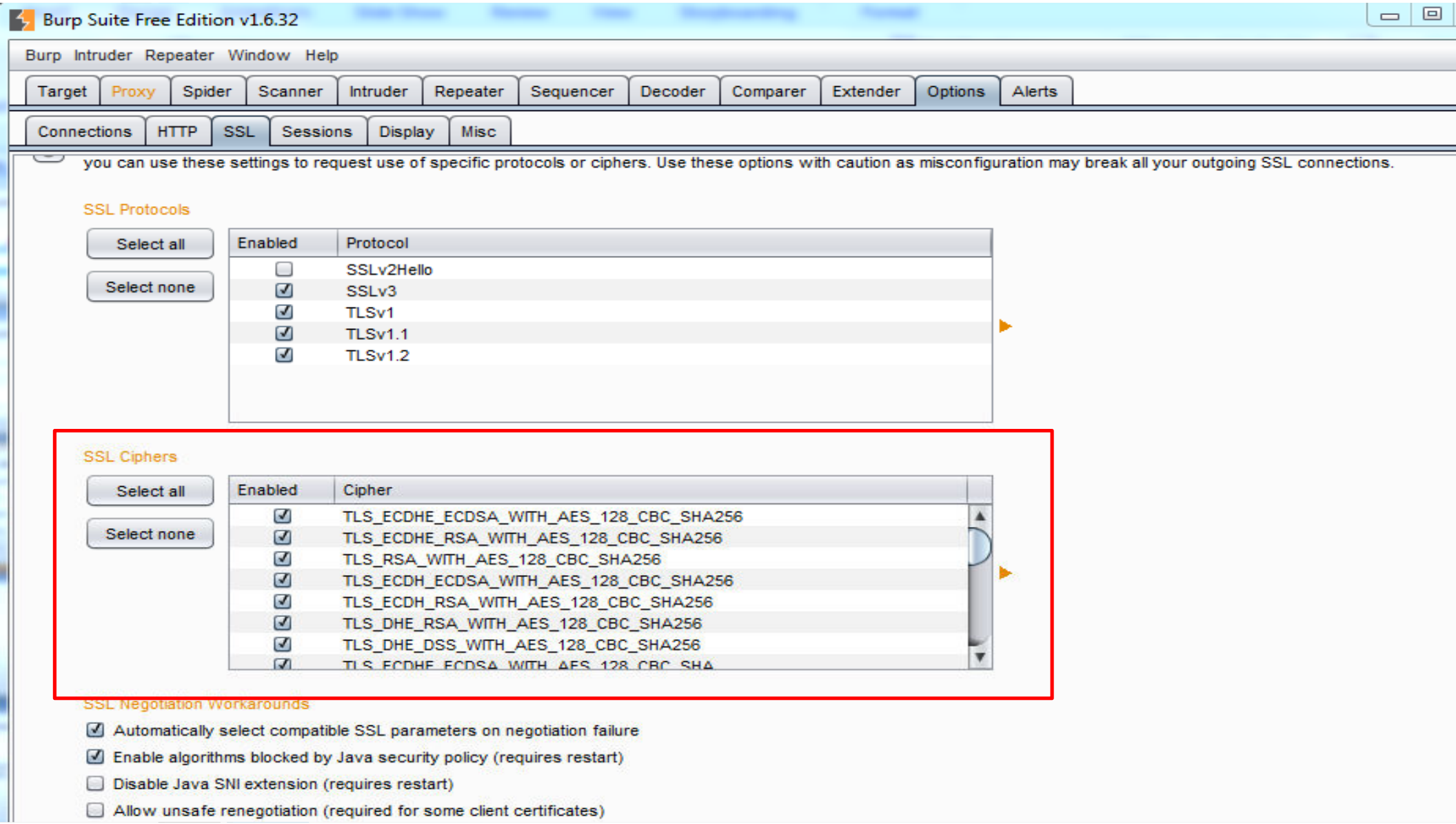
Cookie Expired date is work

- Cookie Editor

Protection by WAF is sufficient

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

HTTPS is sufficient


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Connections HTTP SSL Sessions Display Misc
you can use these settings to request use of specific protocols or ciphers. Use these options with caution as misconfiguration may break all your outgoing SSL connections.
SSL Protocols
Select all
Select none
Enabled
Protocol
SSLv2Hello
SSLv3
TLSv1
TLSv1.1
TLSv1.2
SSL Ciphers
Select all
Select none
Enabled
Cipher
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
SSL Negotiation Workarounds
Automatically select compatible SSL parameters on negotiation failure
Enable algorithms blocked by Java security policy (requires restart)
Disable Java SNI extension (requires restart)
Allow unsafe renegotiation (required for some client certificates)

Other Security #MiSSConcepts

No vulnerability found in VA/Pentest = Secured

Conclusion

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


MiSSConf(SP2)


ThankYou
Tack
Kop
Salamat
Merci
Hvala
Xie
kun
Gra
Diolch
Kiitos
Sheun
umesc
Shnorhakalutiun
Kasih
Mamnoon
Todah
Shokriya
Spaas
Mul
Ačі
Ngiyabonga
Gamsahapnida
Dank
Takk
Cam
Dankie
Kruthagnathalu
Arigatou
Dhonnobaad
Asante
Dhan
daa
Hain
ederim
Dhanyavad
Khopjai
krap
Grazzi
raibh
Gracias
Nandree
Gomapsupnida
Terima
Enkosi
Danke
dank
Kun
Shukriya
Dakujem
Waad
Dhanyavaadaalu
Dekuju/Dekujeme
Te ekkür
Dziękuję
Shokran
Grazie
Falemindierit
Go
Or
al
Dhanyavaad
Blagodariya
Kyrie
Euxaristo