acunetix WEB APPLICATION SECURITY

Acunetix Website Audit

15 April, 2010

Detailed Scan Report

Generated by Acunetix WVS Reporter (v6.0 Build 20081124)

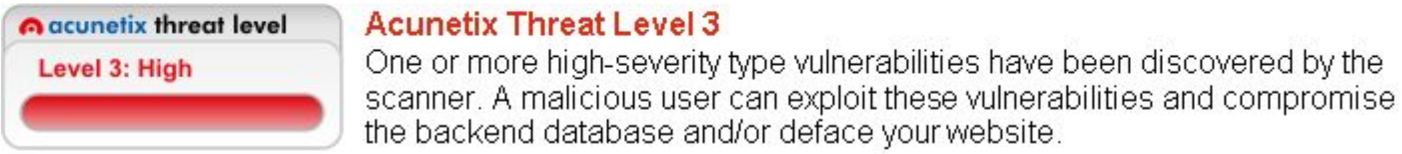
Scan of http://www.webcredito.des:80/Pages/login.aspx

Scan details

Scan information	
Starttime	15/04/2010 11:07:52
Finish time	15/04/2010 11:15:12
Scan time	7 minutes, 20 seconds
Profile	default

Server information	
Responsive	True
Server banner	Microsoft-IIS/6.0
Server OS	Windows
Server technologies	ASP,ASP.NET,Perl,mod_ssl,mod_perl,mod_python,OpenSSL,JRun

Threat level



Acunetix Threat Level 3

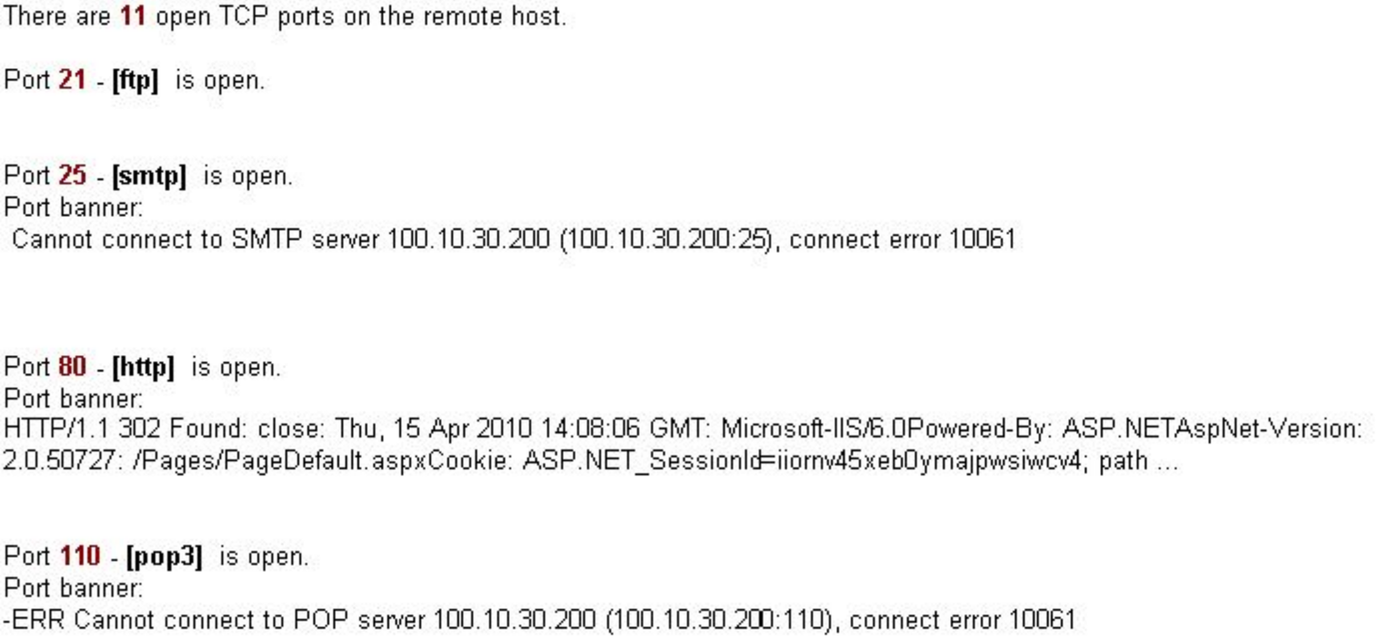
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	15
High	2
Medium	0
Low	1
Informational	12

Knowledge base

List of open TCP ports



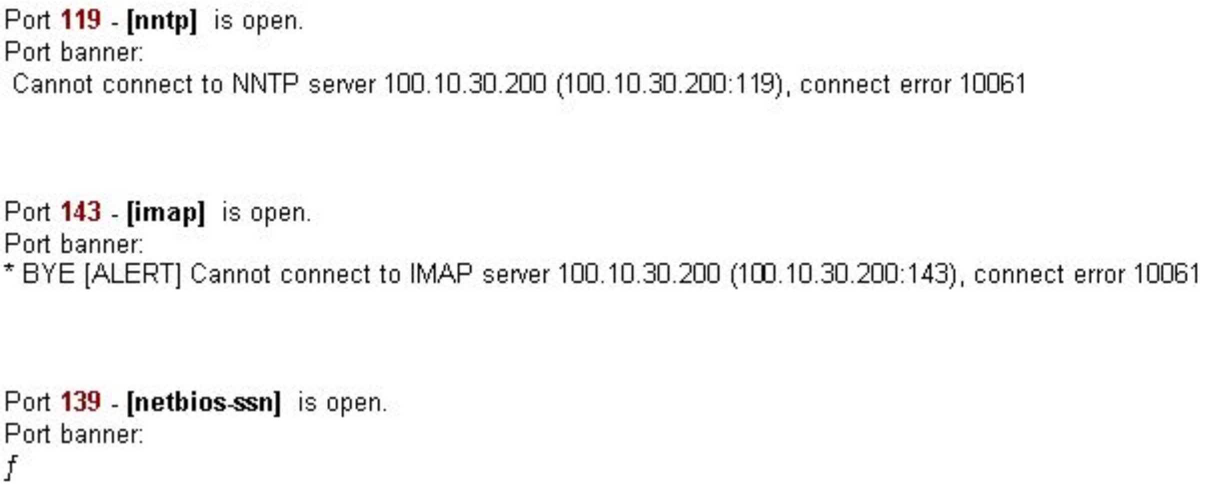
There are **11** open TCP ports on the remote host.

Port **21** - **[ftp]** is open.

Port **25** - **[smtp]** is open.
Port banner:
Cannot connect to SMTP server 100.10.30.200 (100.10.30.200:25), connect error 10061

Port **80** - **[http]** is open.
Port banner:
HTTP/1.1 302 Found: close: Thu, 15 Apr 2010 14:08:06 GMT: Microsoft-IIS/6.0Powered-By: ASP.NETAspNet-Version: 2.0.50727: /Pages/PageDefault.aspxCookie: ASP.NET_SessionId=iiornv45xeb0ymajpwsiwcv4; path ...

Port **110** - **[pop3]** is open.
Port banner:
-ERR Cannot connect to POP server 100.10.30.200 (100.10.30.200:110), connect error 10061

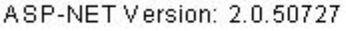


Port **119** - **[nntp]** is open.
Port banner:
Cannot connect to NNTP server 100.10.30.200 (100.10.30.200:119), connect error 10061

Port **143** - **[imap]** is open.
Port banner:
* BYE [ALERT] Cannot connect to IMAP server 100.10.30.200 (100.10.30.200:143), connect error 10061

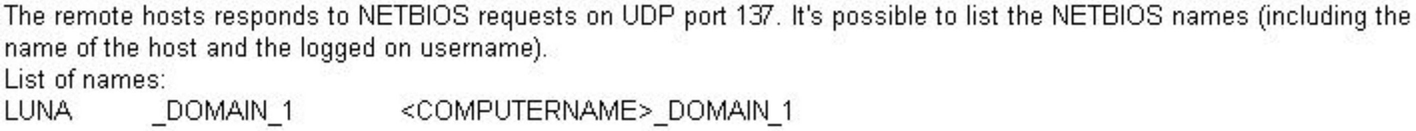
Port **139** - **[netbios-ssn]** is open.
Port banner:
ƒ

ASP-NET



ASP-NET Version: 2.0.50727

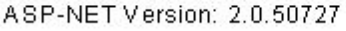
NETBIOS names



The remote hosts responds to NETBIOS requests on UDP port 137. It's possible to list the NETBIOS names (including the name of the host and the logged on username).
List of names:

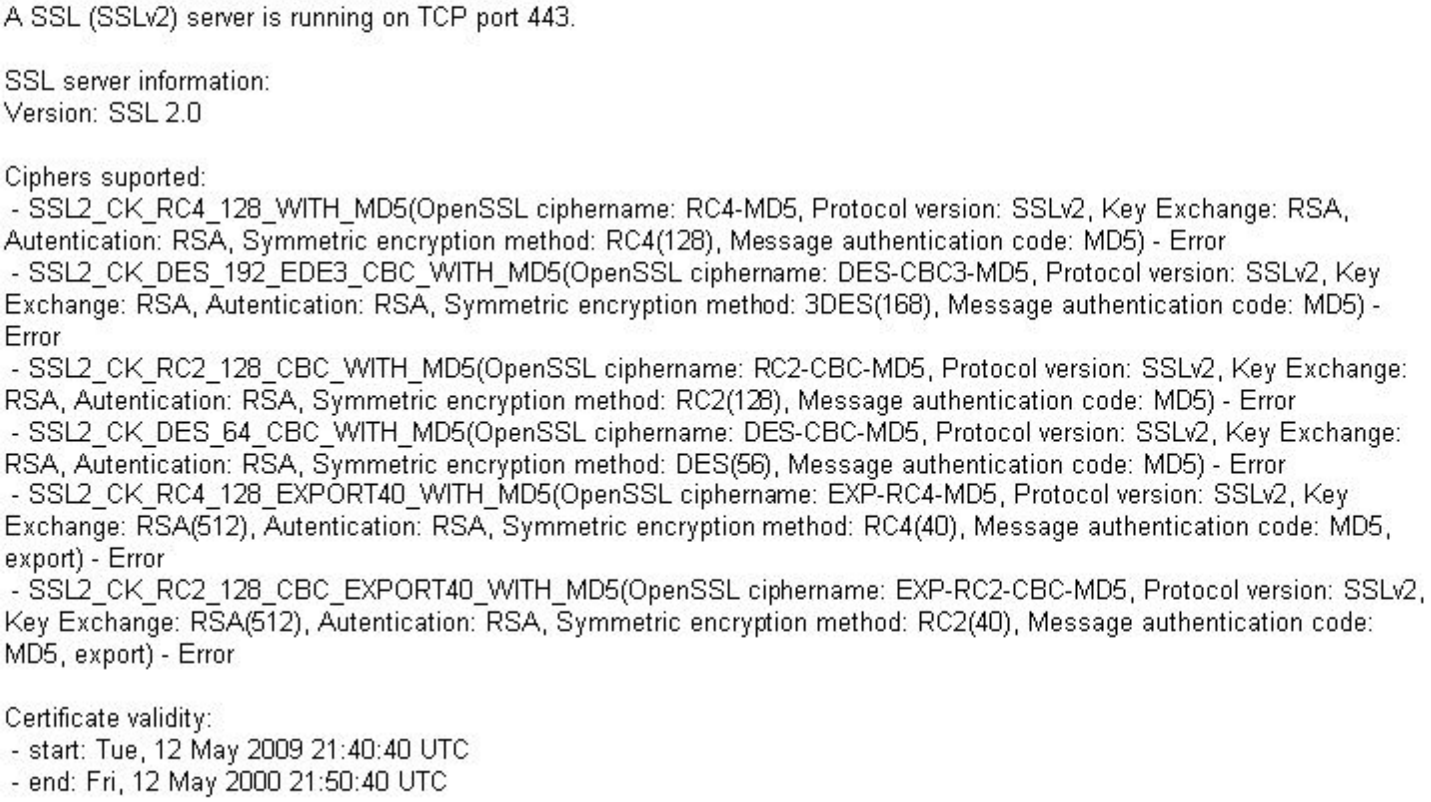
LUNA	_DOMAIN_1	<COMPUTERNAME>_DOMAIN_1

ASP-NET



ASP-NET Version: 2.0.50727

SSL server running [443]



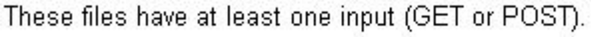
A SSL (SSLv2) server is running on TCP port 443.

SSL server information:
Version: SSL 2.0

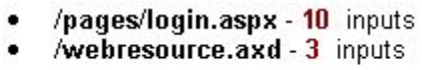
Ciphers suported:
- SSL2_CK_RC4_128_WITH_MD5(OpenSSL ciphername: RC4-MD5, Protocol version: SSLv2, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: RC4(128), Message authentication code: MD5) - Error
- SSL2_CK_DES_192_EDE3_CBC_WITH_MD5(OpenSSL ciphername: DES-CBC3-MD5, Protocol version: SSLv2, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: 3DES(168), Message authentication code: MD5) - Error
- SSL2_CK_RC2_128_CBC_WITH_MD5(OpenSSL ciphername: RC2-CBC-MD5, Protocol version: SSLv2, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: RC2(128), Message authentication code: MD5) - Error
- SSL2_CK_DES_64_CBC_WITH_MD5(OpenSSL ciphername: DES-CBC-MD5, Protocol version: SSLv2, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: DES(56), Message authentication code: MD5) - Error
- SSL2_CK_RC4_128_EXPORT40_WITH_MD5(OpenSSL ciphername: EXP-RC4-MD5, Protocol version: SSLv2, Key Exchange: RSA(512), Autentication: RSA, Symmetric encryption method: RC4(40), Message authentication code: MD5, export) - Error
- SSL2_CK_RC2_128_CBC_EXPORT40_WITH_MD5(OpenSSL ciphername: EXP-RC2-CBC-MD5, Protocol version: SSLv2, Key Exchange: RSA(512), Autentication: RSA, Symmetric encryption method: RC2(40), Message authentication code: MD5, export) - Error

Certificate validity:
- start: Tue, 12 May 2009 21:40:40 UTC
- end: Fri, 12 May 2000 21:50:40 UTC

List of files with inputs



These files have at least one input (GET or POST).



- **/pages/login.aspx** - **10** inputs
- **/webresource.axd** - **3** inputs

Alerts summary

SSL 2.0 deprecated protocol

Affects	Variations
Server	1

SSL certificate invalid date

Affects	Variations
Server	1

SMB null session

Affects	Variations
Server	1

GHDB: Typical login page

Affects	Variations
/pages/login.aspx	7

Password type input with autocomplete enabled

Affects	Variations
/pages/login.aspx	4

Windows Terminal Services server running

Affects	Variations
Server	1

Alert details

SSL 2.0 deprecated protocol

Severity	**High**
Type	Configuration
Reported by module	Scripting

Description

The remote service encrypts traffic using an old deprecated protocol with known weaknesses.

Impact

An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

Recommendation

Disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.

Affected items

Server
Details
The SSL server (port: 443) encrypts traffic using an old deprecated protocol (SSL 2.0) with known weaknesses.

SSL certificate invalid date

Severity	**High**
Type	Configuration
Reported by module	Scripting

Description

SSL certificate is either expired or not valid yet.

Impact

The SSL certificate is not valid.

Recommendation

Please verify you certificate validity period and in case regenare the certificate.

Affected items

Server
Details
The SSL certificate (port 443) is expired. The cerificate validity period is: Tue, 12 May 2009 21:40:40 UTC to Fri, 12 May 2000 21:50:40 UTC

SMB null session

Severity	**Low**
Type	Configuration
Reported by module	Scripting

Description

It's possible to establish a NULL session to this host. A null session is a session established with a server when no credentials are supplied. Use of null sessions, however, can expose information to an anonymous user that could compromise security on a system.

Impact

Possible sensitive information disclosure.

Recommendation

It's recommended to disallow null sessions to the fullest extent possible.

Affected items

Server

Details

The SMB server is running on TCP port 445. Security mode: user

GHDB: Typical login page

Severity	**Informational**
Type	Informational
Reported by module	GHDB - Google hacking database

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.

Category : Pages containing login portals

This is a typical login page. It has recently become a target for SQL injection. Comsec's article at http://www.governmentsecurity.org/articles/SQLinjectionBasicTutorial.php brought this to my attention.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

Affected items

/pages/login.aspx

Details

We found
inurl:login.asp

Request

```
GET /pages/login.aspx?ReturnUrl=%2fpages%2flogout.aspx HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
Referer: http://www.webcredito.des/pages/logout.aspx
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
```

```
Connection: close
Date: Thu, 15 Apr 2010 14:07:57 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
```

/pages/login.aspx

Details

We found
inurl:login.asp

Request

```
GET /pages/login.aspx?ReturnUrl=/pages/logout.aspx HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
Referer: http://www.webcredito.des/pages/login.aspx
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Connection: close
Date: Thu, 15 Apr 2010 14:07:57 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 12898
```

/pages/login.aspx

Details

We found
inurl:login.asp

Request

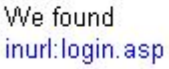
```
POST /pages/login.aspx HTTP/1.0
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Content-Length: 685
Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
Referer: http://www.webcredito.des/pages/login.aspx
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Connection: close
Date: Thu, 15 Apr 2010 14:07:57 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 12771
```

/pages/login.aspx

Details



We found
inurl:login.asp

Request

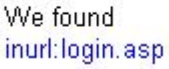
```
POST /pages/login.aspx?ReturnUrl=/pages/logout.aspx HTTP/1.0
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Content-Length: 685
Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
Referer: http://www.webcredito.des/pages/login.aspx
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Connection: close
Date: Thu, 15 Apr 2010 14:07:58 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 12804
```

/pages/login.aspx

Details



We found
inurl:login.asp

Request

```
POST /pages/login.aspx?ReturnUrl=/pages/logout.aspx HTTP/1.0
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Content-Length: 694
Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
Referer: http://www.webcredito.des/pages/login.aspx
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
```

```
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

Response

```
HTTP/1.1 200 OK
Connection: close
Date: Thu, 15 Apr 2010 14:07:58 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 12804
```

/pages/login.aspx

Details

We found
inurl:login.asp

Request

```
GET /pages/login.aspx HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Cookie: {postponed}={postponed}
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Connection: close
Date: Thu, 15 Apr 2010 14:07:57 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc; path=/; HttpOnly
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 12865
```

/pages/login.aspx

Details

We found
inurl:login.asp

Request

```
POST /pages/login.aspx HTTP/1.0
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Content-Length: 694
Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
```

```
Referer: http://www.webcredito.des/pages/login.aspx
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

Response

```
HTTP/1.1 200 OK
Connection: close
Date: Thu, 15 Apr 2010 14:07:57 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 12771
```

Password type input with autocomplete enabled

Severity	**Informational**
Type	Informational
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure

Recommendation

The password autocomplete should be disabled in sensitive applications.
To disable autocomplete, you may use a code similar to:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

Affected items

/pages/login.aspx

Details

Password type input named **ctl00$Formulario$txtContrasenia** from form named **aspnetForm** with action **login.aspx** has autocomplete enabled.

Request

```
POST /pages/login.aspx HTTP/1.0
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Content-Length: 694
Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
Referer: http://www.webcredito.des/pages/login.aspx
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm

(line truncated)
...FEkZlY2hhIGRlIFRyYWJham86IB4HVmlzaWJsZWhkZAIJDw8WAh8BaGRkAhEPDxYCHwAFEUluaWNpbyBkZSB
```

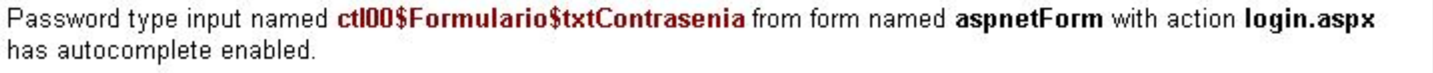
```
TZXNpw7NuZGQCEw9kFgICAw8PFgIfAWhkFgYCAQ8QZGQWAGQCAw8QZGQWAGQCBQ8QZGQWAGQCFQ8PFgIfAAUIdi4
gNC4xMTBkZGQXHj%2FQJq1Nfg2SBZzPBn%2BirquCqQ%3D%3D&__EVENTVALIDATION=%2FwEWBQLB59fkCALi9p
74CAKizqWsDQKa1cx8AvWLvckFIHPZ0sfSqi%2FLAvrb%2Bu1Kmn8y80c%3D&ctl00%24Formulario%24txtCod
Usuario=&ctl00%24Formulario%24txtContrasenia=&ctl00%24Formulario%24btnCambiarClave=Camb
```

Response

```
HTTP/1.1 200 OK
Connection: close
Date: Thu, 15 Apr 2010 14:07:57 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 12771
```

/pages/login.aspx

Details



Password type input named **ctl00$Formulario$txtContrasenia** from form named **aspnetForm** with action **login.aspx** has autocomplete enabled.

Request

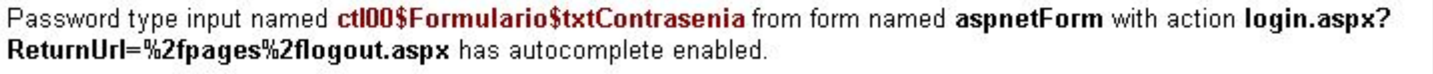
```
GET /pages/login.aspx HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Cookie: {postponed}={postponed}
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
```

Response

```
HTTP/1.1 200 OK
Connection: close
Date: Thu, 15 Apr 2010 14:07:57 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc; path=/; HttpOnly
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 12865
```

/pages/login.aspx

Details



Password type input named **ctl00$Formulario$txtContrasenia** from form named **aspnetForm** with action **login.aspx?ReturnUrl=%2fpages%2flogout.aspx** has autocomplete enabled.

Request

```
GET /pages/login.aspx?ReturnUrl=/pages/logout.aspx HTTP/1.0
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
Referer: http://www.webcredito.des/pages/login.aspx
```

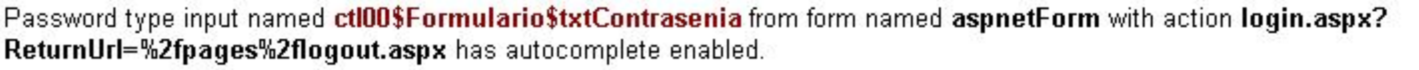
```
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
```

Response

```
HTTP/1.1 200 OK
Connection: close
Date: Thu, 15 Apr 2010 14:07:57 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 12898
```

/pages/login.aspx

Details



Password type input named **ctl00$Formulario$txtContrasenia** from form named **aspnetForm** with action **login.aspx?ReturnUrl=%2fpages%2flogout.aspx** has autocomplete enabled.

Request

```
POST /pages/login.aspx?ReturnUrl=/pages/logout.aspx HTTP/1.0
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.webcredito.des
Content-Length: 694
Cookie: ASP.NET_SessionId=evwxm045dau4dzew32l4i2jc
Connection: Close
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Pragma: no-cache
Acunetix-aspect-queries: filelist;aspectalerts
Referer: http://www.webcredito.des/pages/login.aspx
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm

(line truncated)
...FEkZlY2hhIGRlIFRyYWJham86IB4HVmlzaWJsZWhkZAIJDw8WAh8BaGRkAhEPDxYCHwAFEUluaWNpbyBkZSBT
ZXNpw7NuZGQCEw9kFgICAw8PFgIfAWhkFgYCAQ8QZGQWAGQCAw8QZGQWAGQCBQ8QZGQWAGQCFQ8PFgIfAAUIdi4g
NC4xMTBkZGQXHj%2FQJq1Nfg2SBZzPBn%2BirquCqQ%3D%3D&__EVENTVALIDATION=%2FwEWBQLB59fkCALi9p7
4CAKizqWsDQKa1cx8AvWLvckFIHPZ0sfSqi%2FLAvrb%2Bu1Kmn8y80c%3D&ctl00%24Formulario%24txtCodU
suario=&ctl00%24Formulario%24txtContrasenia=&ctl00%24Formulario%24btnCambiarClave=Cambia
r%20Clave&ctl00%24Formulario%24btnLogin=Ingresar%20al%20Sistema
```

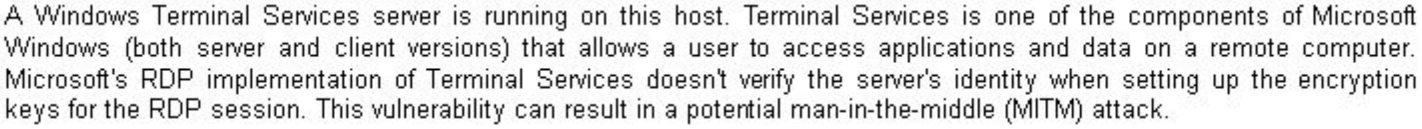
Response

```
HTTP/1.1 200 OK
Connection: close
Date: Thu, 15 Apr 2010 14:07:58 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 12804
```

Windows Terminal Services server running

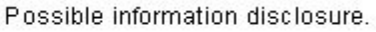
Severity	**Informational**
Type	Configuration
Reported by module	Scripting

Description



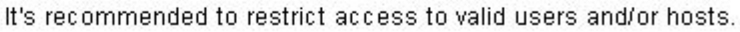
A Windows Terminal Services server is running on this host. Terminal Services is one of the components of Microsoft Windows (both server and client versions) that allows a user to access applications and data on a remote computer. Microsoft's RDP implementation of Terminal Services doesn't verify the server's identity when setting up the encryption keys for the RDP session. This vulnerability can result in a potential man-in-the-middle (MITM) attack.

Impact



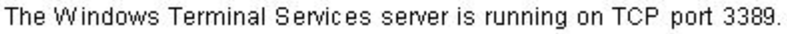
Possible information disclosure.

Recommendation



It's recommended to restrict access to valid users and/or hosts.

Affected items

Server
Details
 The Windows Terminal Services server is running on TCP port 3389.