acunetix

Developer Report

Acunetix Security Audit

09 October 2018

Generated by Acunetix

Scan of http://192.168.3.112

Scan details

Scan information	
Start time	09/10/2018, 11:12:16
Start url	http://192.168.3.112
Host	http://192.168.3.112
Scan time	10 minutes, 23 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	16
High	0
Medium	3
Low	6
Informational	7

Alerts summary

HTML form without CSRF protection

Classification	
CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 4.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CWE	CWE-352

Affected items	Variation
/index.asp	1
/pwd.html	1

User credentials are sent in clear text

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: High Remediation Level: Workaround Report Confidence: Confirmed Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 9.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-310

Affected items	Variation

/index.asp	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693

Affected items	Variation
Web Server	1

File upload

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
/action/FileUpload	1

Login page password-guessing attack

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined

	Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CWE	CWE-307

Affected items	Variation
/login.asp	1

Session token in URL

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/C0-1x.asp	2
/C0-6x.asp	1

Content type is not specified

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined

	Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
/action/doctrl	1
/file/dbCfg.db3	1
/file/dbData.db3	1
/file/tmp/dbDat0.db3	1
/file/tmp/dbData.db3	1

Password type input with auto-complete enabled

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/index.asp	1
/pwd.html	1

Alerts details

HTML form without CSRF protection

Severity	**Medium**
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker"s choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/index.asp

Details

Form name: Login
Form action: http://192.168.3.112/login.asp
Form method: POST

Form inputs:

- Usercode [Text]
- Password [Password]

Request headers

```
GET /index.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/index.html
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/pwd.html

Details

Form name: ADDFORM
Form action: http://192.168.3.112/pwd2.asp
Form method: POST

Form inputs:

- Usercode [Hidden]
- _PwdChk [Password]
- _PwdChk2 [Password]

Request headers

```
GET /pwd.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/main.asp
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

User credentials are sent in clear text

Severity	**Medium**
Reported by module	Crawler

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

/index.asp

Details

Form name: Login
Form action: http://192.168.3.112/login.asp
Form method: POST

Form inputs:

- Usercode [Text]
- Password [Password]

Request headers

```
GET /index.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/index.html
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)
Clickjacking (http://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)
Defending with Content Security Policy frame-ancestors directive
(https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)
Frame Buster Buster (http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server
Details
Request headers

```
GET / HTTP/1.1
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

File upload

Severity	**Low**
Reported by module	Crawler

Description

This page allows visitors to upload files to the server. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

Impact

If the uploaded files are not safely checked an attacker may upload malicious files.

Recommendation

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are

not executable. If possible, rename the files that are uploaded.

Affected items

/action/FileUpload
Details
Form name: <empty> Form action: http://192.168.3.112/action/FileUpload Form method: POST Form inputs: • MAX_FILE_SIZE [Hidden] • CfgAddress [Text] • upcfgfile [File]
Request headers
`GET / HTTP/1.1`

Login page password-guessing attack

Severity	**Low**
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks (http://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)

Affected items

/login.asp
Details
The scanner tested 10 invalid credentials and no account lockout was detected.
Request headers

`POST /login.asp HTTP/1.1`
`Content-Length: 35`
`Content-Type: application/x-www-form-urlencoded`
`Referer: http://192.168.3.112`
`Host: 192.168.3.112`
`Connection: Keep-alive`
`Accept-Encoding: gzip,deflate`
`User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21`

```
Accept: */*
Password=ssPvayb9&Usercode=TyyaNVXr
```

Session token in URL

Severity	**Low**
Reported by module	Crawler

Description

This application contains a session token in the query parameters. A session token is sensitive information and should not be stored in the URL. URLs could be logged or leaked via the Referer header.

Impact

Possible sensitive information disclosure.

Recommendation

The session should be maintained using cookies (or hidden input fields).

Affected items

/C0-1x.asp

Details

http://192.168.3.112/C0-1x.asp?sid=0&itype=

Request headers

```
GET /C0-1x.asp?sid=0&itype= HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/C0-1.asp
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/C0-6x.asp

Details

http://192.168.3.112/C0-6x.asp?sid=0&tag1=0&type=3327

Request headers

```
GET /C0-6x.asp?sid=0&tag1=0&type=3327 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/C0-6.asp
Cookie: user=
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/C0-1x.asp

Details

http://192.168.3.112/C0-1x.asp?itype=3594&port=0&sid=0&tag1=1

Request headers

```
GET /C0-1x.asp?itype=3594&port=0&sid=0&tag1=1 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
```

```
Referer: http://192.168.3.112/C0-1.asp
Cookie: user=
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Content type is not specified

Severity	**Informational**
Reported by module	Crawler

Description

This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

Impact

None

Recommendation

Set a Content-Type header value for this page.

Affected items

/file/dbData.db3

Details

```
HTTP/1.1 200 OK

Date: Tue Oct  9 11:14:53 2018

Content-Length: 148480

Connection: keep-alive

Last-Modified: Sun Sep 30 16:59:07 2018
```

Request headers

```
GET /file/dbData.db3 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/omdev-file.html
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/file/tmp/dbDat0.db3

Details

```
HTTP/1.1 200 OK

Date: Tue Oct  9 11:14:54 2018

Content-Length: 14336

Connection: keep-alive

Last-Modified: Tue Oct  9 11:14:54 2018
```

Request headers

```
GET /file/tmp/dbDat0.db3 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/omdev-file.html
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/file/tmp/dbData.db3

Details

```
HTTP/1.1 200 OK

Date: Tue Oct  9 11:14:54 2018

Content-Length: 3072

Connection: keep-alive

Last-Modified: Tue Oct  9 11:04:30 2018
```

Request headers

```
GET /file/tmp/dbData.db3 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/omdev-file.html
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/file/dbCfg.db3

Details

```
HTTP/1.1 200 OK

Date: Tue Oct  9 11:14:54 2018

Content-Length: 59392

Connection: keep-alive

Last-Modified: Wed Sep  5 07:51:20 2018
```

Request headers

```
GET /file/dbCfg.db3 HTTP/1.1
```

```
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/omdev-file.html
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/action/doctrl

Details

```
HTTP/1.1 200 OK

Date: Tue Oct  9 11:21:31 2018

Connection: keep-alive

Content-Length: 2
```

Request headers

```
GET /action/doctrl HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/B1.html
Cookie: user=
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Password type input with auto-complete enabled

Severity	**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 auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:

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

Affected items

/index.asp

Details

Password type input(s): **Password** from form named **Login** with action **login.asp** have autocomplete enabled.

Request headers

```
GET /index.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/index.html
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/pwd.html

Details

Password type input(s): **_PwdChk,_PwdChk2** from form named **ADDFORM** with action **pwd2.asp** have autocomplete enabled.

Request headers

```
GET /pwd.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/main.asp
Host: 192.168.3.112
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Scanned items (coverage report)

http://192.168.3.112/
http://192.168.3.112/A3-status.asp
http://192.168.3.112/action
http://192.168.3.112/action/doctrl
http://192.168.3.112/action/dynamicdata
http://192.168.3.112/action/FileUpload
http://192.168.3.112/action/Operate
http://192.168.3.112/B1.html
http://192.168.3.112/B2-t.html
http://192.168.3.112/B2.html
http://192.168.3.112/C0-1.asp
http://192.168.3.112/C0-10.asp
http://192.168.3.112/C0-10x.asp
http://192.168.3.112/C0-11.asp
http://192.168.3.112/C0-12.asp
http://192.168.3.112/C0-1x.asp
http://192.168.3.112/C0-3.asp
http://192.168.3.112/C0-4.asp
http://192.168.3.112/C0-6.asp
http://192.168.3.112/C0-6x.asp
http://192.168.3.112/C0-9.asp
http://192.168.3.112/C0-9x.asp
http://192.168.3.112/C2.asp
http://192.168.3.112/css
http://192.168.3.112/css/images
http://192.168.3.112/css/images/index.html
http://192.168.3.112/css/index.html
http://192.168.3.112/css/jquery-ui.css
http://192.168.3.112/css/login.css
http://192.168.3.112/css/omdev.css
http://192.168.3.112/css/style.css
http://192.168.3.112/css/style_i.css
http://192.168.3.112/favicon.ico
http://192.168.3.112/file
http://192.168.3.112/file/dbCfg.db3
http://192.168.3.112/file/dbData.db3
http://192.168.3.112/file/index.html
http://192.168.3.112/file/tmp
http://192.168.3.112/file/tmp/dbDat0.db3
http://192.168.3.112/file/tmp/dbData.db3
http://192.168.3.112/file/tmp/index.html
http://192.168.3.112/images
http://192.168.3.112/images/help
http://192.168.3.112/images/help/index.html
http://192.168.3.112/images/index.html
http://192.168.3.112/img
http://192.168.3.112/img/index.html
http://192.168.3.112/index.asp
http://192.168.3.112/index.html
http://192.168.3.112/js
http://192.168.3.112/js/index.html
http://192.168.3.112/js/ip.js
http://192.168.3.112/js/jquery-1.6.3.min.js
http://192.168.3.112/js/jquery-ui-datepicker.js
http://192.168.3.112/js/jquery.form.js
http://192.168.3.112/js/json.js
http://192.168.3.112/js/mac.js
http://192.168.3.112/js/qrcode.js
http://192.168.3.112/login.asp
http://192.168.3.112/main.asp
http://192.168.3.112/main.html
http://192.168.3.112/omdev
http://192.168.3.112/omdev-app.html
http://192.168.3.112/omdev-com4.html
http://192.168.3.112/omdev-file.html
http://192.168.3.112/omdev-help.html
http://192.168.3.112/omdev-info.html

http://192.168.3.112/omdev-jxhelp.html
http://192.168.3.112/omdev-net.html
http://192.168.3.112/omdev-reboot.html
http://192.168.3.112/omdev-smtp.html
http://192.168.3.112/omdev.html
http://192.168.3.112/omdev/almtime.asp
http://192.168.3.112/omdev/carddef.asp
http://192.168.3.112/omdev/com4x.asp
http://192.168.3.112/omdev/doset.asp
http://192.168.3.112/omdev/index.html
http://192.168.3.112/omdev/port.asp
http://192.168.3.112/omdev/smai.asp
http://192.168.3.112/omdev/smalarm-t.asp
http://192.168.3.112/omdev/smalarm.asp
http://192.168.3.112/omdev/smbyport.asp
http://192.168.3.112/omdev/smbysubsys.asp
http://192.168.3.112/omdev/smdat0.asp
http://192.168.3.112/omdev/smdef.asp
http://192.168.3.112/omdev/smtp.asp
http://192.168.3.112/omdev/smtype.asp
http://192.168.3.112/omdev/smx.asp
http://192.168.3.112/omdev/usertype.asp
http://192.168.3.112/pwd.html
http://192.168.3.112/pwd2.asp