acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

18 April, 2018

Developer Report

Generated by Acunetix WVS Reporter (v10.5 Build 20160217)

Scan of http://10.166.81.106

Scan details

Scan information	
Start time	2018/4/18 8:29:42
Finish time	The scan was aborted
Scan time	16 minutes, 15 seconds
Profile	Default
Server information	
Responsive	True
Server banner	Unknown
Server OS	Unknown

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	**14**
High	4
Medium	5
Low	2
Informational	3

Alerts summary

Cross site scripting

Classification	
CVSS	Base Score: 6.4 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: None
CVSS3	Base Score: 5.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None
CWE	CWE-79

Affected items	Variation
/C0-1x.asp	4

HTML form without CSRF protection

Classification	
CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None
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	2
/pwd.html	1

User credentials are sent in clear text

Classification	
CVSS	Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
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	2

Clickjacking: X-Frame-Options header missing

Classification	
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial
CWE	CWE-693

Affected items	Variation
Web Server	1

File upload

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
CWE	CWE-16

Affected items	Variation
/action/FileUpload	1

Password type input with auto-complete enabled

Classification	
CVSS	Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None
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	2

Alert details

Cross site scripting

Severity	**High**
Type	Validation
Reported by module	Scripting (XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

OWASP Cross Site Scripting
How To: Prevent Cross-Site Scripting in ASP.NET
OWASP PHP Top 5
Cross site scripting
XSS Annihilation
The Cross Site Scripting Faq
VIDEO: How Cross-Site Scripting (XSS) Works
Acunetix Cross Site Scripting Attack
XSS Filter Evasion Cheat Sheet

Affected items

/C0-1x.asp

Details

URL encoded GET input port was set to 8388609_9538():;9860
The input is reflected inside <script> tag.

Request headers

```
GET /C0-1x.asp?port=8388609_9538():;9860&sid=7&tag1=0&type=3591 HTTP/1.1
Referer: http://10.166.81.106
Cookie: user=
Host: 10.166.81.106
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

URL encoded GET input sid was set to 7_9470():;9649
The input is reflected inside <script> tag.

Request headers

```
GET /C0-1x.asp?port=8388609&sid=7_9470():;9649&tag1=0&type=3591 HTTP/1.1
Referer: http://10.166.81.106
Cookie: user=
```

```
Host: 10.166.81.106
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

URL encoded GET input tag1 was set to 0_9619():;9421
The input is reflected inside <script> tag.

Request headers

```
GET /C0-1x.asp?port=8388609&sid=7&tag1=0_9619():;9421&type=3591 HTTP/1.1
Referer: http://10.166.81.106
Cookie: user=
Host: 10.166.81.106
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

URL encoded GET input type was set to 3591_9767():;9123
The input is reflected inside <script> tag.

Request headers

```
GET /C0-1x.asp?port=8388609&sid=7&tag1=0&type=3591_9767():;9123 HTTP/1.1
Referer: http://10.166.81.106
Cookie: user=
Host: 10.166.81.106
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: */*
```

HTML form without CSRF protection

Severity	**Medium**
Type	Informational
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://10.166.81.106/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://10.166.81.106/index.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 10.166.81.106
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: */*
```

/index.asp

Details

Form name: Login
Form action: http://10.166.81.106/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://10.166.81.106/index.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 10.166.81.106
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://10.166.81.106/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://10.166.81.106/main.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 10.166.81.106
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**
Type	Configuration
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://10.166.81.106/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://10.166.81.106/index.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 10.166.81.106
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: */*
```

/index.asp

Details

Form name: Login
Form action: http://10.166.81.106/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://10.166.81.106/index.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
```

```
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 10.166.81.106
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**
Type	Configuration
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

- Clickjacking
- OWASP Clickjacking
- Defending with Content Security Policy frame-ancestors directive
- Frame Buster Buster
- Clickjacking Protection for Java EE
- The X-Frame-Options response header

Affected items

Web Server

Details

No details are available.

Request headers

```
GET / HTTP/1.1
Host: 10.166.81.106
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**
Type	Informational
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://10.166.81.106/action/FileUpload
Form method: POST

Form inputs:

- MAX_FILE_SIZE [Hidden]
- CfgAddress [Text]
- upcfgfile [File]

Request headers

```
GET / HTTP/1.1
```

Password type input with auto-complete 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 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 named Password from form named Login with action login.asp has autocomplete enabled.

Request headers

```
GET /index.asp HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://10.166.81.106/index.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 10.166.81.106
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 named _PwdChk2 from form named ADDFORM with action pwd2.asp has autocomplete enabled.

Request headers

```
GET /pwd.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://10.166.81.106/main.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 10.166.81.106
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 named _PwdChk from form named ADDFORM with action pwd2.asp has autocomplete enabled.

Request headers

```
GET /pwd.html HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://10.166.81.106/main.html
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Host: 10.166.81.106
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)

Scanned 91 URLs. Found 4 vulnerable.

URL: http://10.166.81.106/

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
/	Path Fragment (suffix .html)

Input scheme 2	
Input name	Input type
Host	HTTP Header

URL: http://10.166.81.106/index.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/index.asp

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/login.asp

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
Password	URL encoded POST
Usercode	URL encoded POST

URL: http://10.166.81.106/css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/css/login.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/css/index.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/css/images

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/css/images/index.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/css/omdev.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/css/style.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/css/jquery-ui.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/css/style_i.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/main.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/C2.asp

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
subsys	URL encoded GET

URL: http://10.166.81.106/B1.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/B2.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/A3-status.asp

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/C0-3.asp

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/C0-1.asp

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/C0-6.asp

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/C0-4.asp

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/pwd.html

Vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/B2-t.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/img

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/img/index.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev-help.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev-jxhelp.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/js/jquery-1.6.3.min.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/js/jquery-ui-datepicker.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/js/index.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/js/jquery.form.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/js/ip.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/js/mac.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/js/json.js

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/pwd2.asp

No vulnerabilities have been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
_PwdChk	URL encoded POST
_PwdChk2	URL encoded POST
Usercode	URL encoded POST

URL: http://10.166.81.106/C0-9.asp

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/C0-11.asp

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/C0-12.asp

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/C0-10.asp

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev-net.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev-app.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev-info.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev-smtp.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev-com4.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev-file.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev-reboot.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/images

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/images/help

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/images/help/index.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/images/index.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/C0-10x.asp

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
type	URL encoded GET

URL: http://10.166.81.106/C0-9x.asp

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
tag1	URL encoded GET
type	URL encoded GET

URL: http://10.166.81.106/action

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/action/FileUpload

Vulnerabilities have been identified for this URL

5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
CfgAddress	POST (multipart)
MAX_FILE_SIZE	POST (multipart)
upcfgfile	POST (multipart)

Input scheme 2	
Input name	Input type
MAX_FILE_SIZE	POST (multipart)
upfile	POST (multipart)

URL: http://10.166.81.106/action/doctrl

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded POST
value	URL encoded POST

URL: http://10.166.81.106/action/dynamicdata

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded GET

Input scheme 2	
Input name	Input type
op	URL encoded GET

URL: http://10.166.81.106/file

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/file/dbCfg.db3

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/file/dbData.db3

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/file/tmp

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/file/tmp/dbDat0.db3

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/file/tmp/dbData.db3

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/file/tmp/index.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/file/index.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/C0-1x.asp

Vulnerabilities have been identified for this URL

6 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
sid	URL encoded GET
type	URL encoded GET

Input scheme 2	
Input name	Input type
port	URL encoded GET
sid	URL encoded GET
tag1	URL encoded GET
type	URL encoded GET

URL: http://10.166.81.106/omdev

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/omdev/smbysubsys.asp

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
subsys	URL encoded POST

URL: http://10.166.81.106/omdev/smdat0.asp

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
itype	URL encoded POST
sid	URL encoded POST

URL: http://10.166.81.106/omdev/smalarm.asp

No vulnerabilities have been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
endtime	URL encoded POST
kind	URL encoded POST
starttime	URL encoded POST

URL: http://10.166.81.106/omdev/smalarm-t.asp

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
endtime	URL encoded POST
starttime	URL encoded POST

URL: http://10.166.81.106/omdev/smbyport.asp

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
port	URL encoded POST

URL: http://10.166.81.106/omdev/port.asp

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded POST
port	URL encoded POST

URL: http://10.166.81.106/omdev/smx.asp

No vulnerabilities have been identified for this URL

24 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded POST
sid	URL encoded POST
st	URL encoded POST

Input scheme 2	
Input name	Input type
op	URL encoded POST

sid	URL encoded POST

Input scheme 3	
Input name	Input type
addr	URL encoded POST
insval	URL encoded POST
op	URL encoded POST
type	URL encoded POST

Input scheme 4	
Input name	Input type
addr	URL encoded POST
insval	URL encoded POST
name	URL encoded POST
op	URL encoded POST
tag1	URL encoded POST
type	URL encoded POST

Input scheme 5	
Input name	Input type
op	URL encoded POST
ser	URL encoded POST
sid	URL encoded POST
st	URL encoded POST

Input scheme 6	
Input name	Input type
offset	URL encoded POST
op	URL encoded POST
tag	URL encoded POST
type	URL encoded POST
unit	URL encoded POST

URL: http://10.166.81.106/omdev/carddef.asp

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded POST

URL: http://10.166.81.106/omdev/almtime.asp

No vulnerabilities have been identified for this URL

19 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded POST
tid	URL encoded POST

Input scheme 2	
Input name	Input type
end0	URL encoded POST
end1	URL encoded POST
end2	URL encoded POST
end3	URL encoded POST
end4	URL encoded POST

end5	URL encoded POST
end6	URL encoded POST
note	URL encoded POST
op	URL encoded POST
start0	URL encoded POST
start1	URL encoded POST
start2	URL encoded POST
start3	URL encoded POST
start4	URL encoded POST
start5	URL encoded POST
start6	URL encoded POST
tid	URL encoded POST

URL: http://10.166.81.106/omdev/usertype.asp

No vulnerabilities have been identified for this URL

24 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded POST

Input scheme 2	
Input name	Input type
op	URL encoded POST
type	URL encoded POST

Input scheme 3	
Input name	Input type
code	URL encoded POST
email	URL encoded POST
kind	URL encoded POST
name	URL encoded POST
note	URL encoded POST
op	URL encoded POST
recv1	URL encoded POST
smsnum	URL encoded POST
state	URL encoded POST
telnum	URL encoded POST

Input scheme 4	
Input name	Input type
code	URL encoded POST
email	URL encoded POST
kind	URL encoded POST
name	URL encoded POST
note	URL encoded POST
op	URL encoded POST
recv1	URL encoded POST
smsnum	URL encoded POST
state	URL encoded POST
telnum	URL encoded POST
uid	URL encoded POST

URL: http://10.166.81.106/omdev/smtype.asp

No vulnerabilities have been identified for this URL

24 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded POST

Input scheme 2	
Input name	Input type
op	URL encoded POST
tag1	URL encoded POST
type	URL encoded POST

Input scheme 3	
Input name	Input type
insval	URL encoded POST
op	URL encoded POST
tag1	URL encoded POST
type	URL encoded POST

Input scheme 4	
Input name	Input type
addr	URL encoded POST
addrn	URL encoded POST
addrx	URL encoded POST
ext1	URL encoded POST
extdi	URL encoded POST
extdo	URL encoded POST
extser	URL encoded POST
name	URL encoded POST
note	URL encoded POST
op	URL encoded POST
port	URL encoded POST
portdef	URL encoded POST
subsys	URL encoded POST
tag1	URL encoded POST
type	URL encoded POST
unit	URL encoded POST

URL: http://10.166.81.106/omdev/smtp.asp

No vulnerabilities have been identified for this URL

7 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded GET

Input scheme 2	
Input name	Input type
account	URL encoded POST
op	URL encoded POST
port	URL encoded POST
pwd	URL encoded POST
server	URL encoded POST
title	URL encoded POST

URL: http://10.166.81.106/omdev/com4x.asp

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded POST

URL: http://10.166.81.106/omdev/smai.asp

No vulnerabilities have been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded POST

Input scheme 2	
Input name	Input type
op	URL encoded POST
tag1	URL encoded POST

URL: http://10.166.81.106/omdev/doset.asp

No vulnerabilities have been identified for this URL

4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
op	URL encoded POST

Input scheme 2	
Input name	Input type
op	URL encoded POST
sid	URL encoded POST
st	URL encoded POST

URL: http://10.166.81.106/omdev/smdef.asp

No vulnerabilities have been identified for this URL

14 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
AType	URL encoded POST
insval2	URL encoded POST
op	URL encoded POST
other	URL encoded POST
tag	URL encoded POST
Xvalue	URL encoded POST
Yvalue	URL encoded POST

Input scheme 2	
Input name	Input type
AType	URL encoded POST
insval	URL encoded POST
op	URL encoded POST
other	URL encoded POST
tag	URL encoded POST
Xvalue	URL encoded POST
Yvalue	URL encoded POST

URL: http://10.166.81.106/omdev/index.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: http://10.166.81.106/A3-1280.asp

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
sid	URL encoded GET

URL: http://10.166.81.106/C2-0.asp

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
itype	URL encoded GET
sid	URL encoded GET

URL: http://10.166.81.106/C0-4x.asp

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
itype	URL encoded GET
sid	URL encoded GET

URL: http://10.166.81.106/C0-6x.asp

No vulnerabilities have been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
sid	URL encoded GET
type	URL encoded GET

URL: http://10.166.81.106/C0-9d.asp

No vulnerabilities have been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
type	URL encoded GET