acunetix

# Developer Report

Acunetix Security Audit

10 October 2018

Generated by Acunetix

# Scan of http://192.168.3.112

## Scan details

| Scan information | |
|---|---|
| Start time | 10/10/2018, 10:23:36 |
| Start url | http://192.168.3.112 |
| Host | http://192.168.3.112 |
| Scan time | 47 minutes, 14 seconds |
| Profile | Full Scan |

### 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 | 22 |
|---|---|
| High | 7 |
| Medium | 0 |
| Low | 10 |
| Informational | 5 |

## Alerts summary

### Blind SQL Injection

| Classification | |
|---|---|
| CVSS2 | Base Score: 6.8<br>Access Vector: Network_accessible<br>Access Complexity: Medium<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: Partial<br>Availability Impact: Partial<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CVSS3 | Base Score: 10.0<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Changed<br>Confidentiality Impact: High<br>Integrity Impact: High<br>Availability Impact: None |
| CWE | CWE-89 |

| Affected items | Variation |
|---|---|
| /login.asp | 1 |
| /omdev/smtype.asp | 1 |

### Cross site scripting

| Classification | |
|---|---|
| CVSS2 | Base Score: 6.4<br>Access Vector: Network_accessible<br>Access Complexity: Low<br>Authentication: None<br>Confidentiality Impact: Partial<br>Integrity Impact: Partial<br>Availability Impact: None<br>Exploitability: Not_defined<br>Remediation Level: Not_defined<br>Report Confidence: Not_defined<br>Availability Requirement: Not_defined<br>Collateral Damage Potential: Not_defined<br>Confidentiality Requirement: Not_defined<br>Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CVSS3 | Base Score: 5.3<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: None<br>Integrity Impact: Low<br>Availability Impact: None |
| CWE | CWE-79 |

| Affected items | Variation |
|---|---|

| | |
|---|---|
| /C0-1x.asp | 4 |
| /omdev/smbysubsys.asp | 1 |

### Clickjacking: X-Frame-Options header missing

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

| Affected items | Variation |
|---|---|
| Web Server | 1 |

### File upload

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

| Affected items | Variation |
|---|---|
| /action/FileUpload | 1 |

### Session token in URL

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

| | |
|---|---|
| | Integrity Requirement: Not_defined<br>Target Distribution: Not_defined |
| CVSS3 | Base Score: 7.5<br>Attack Vector: Network<br>Attack Complexity: Low<br>Privileges Required: None<br>User Interaction: None<br>Scope: Unchanged<br>Confidentiality Impact: High<br>Integrity Impact: None<br>Availability Impact: None |
| CWE | CWE-200 |

| Affected items | Variation |
|---|---|
| /A3-769.asp | 1 |
| /C0-1x.asp | 3 |
| /C0-3x.asp | 1 |
| /C0-4x.asp | 1 |
| /C0-6x.asp | 1 |
| /C2-0.asp | 1 |

**Content type is not specified**

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

## Alerts details

## Blind SQL Injection

| | |
|---|---|
| Severity | **High** |
| Reported by module | Scripting (Blind_Sql_Injection.script) |

### Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

### Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

### Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

### References

Acunetix SQL Injection Attack (http://www.acunetix.com/websitesecurity/sql-injection.htm)
VIDEO: SQL Injection tutorial (http://www.acunetix.com/blog/web-security-zone/video-sql-injection-tutorial/)
OWASP Injection Flaws (http://www.owasp.org/index.php/Injection_Flaws)
How to check for SQL injection vulnerabilities (http://www.acunetix.com/websitesecurity/sql-injection2/)
SQL Injection Walkthrough (http://www.securiteam.com/securityreviews/5DP0N1P76E.html)
OWASP PHP Top 5 (http://www.owasp.org/index.php/PHP_Top_5)

### Affected items

**/login.asp**

Details

URL encoded POST input **Usercode** was set to **-1' OR 3*2*1=6 AND 000216=000216 --**

Tests performed:

- -1' OR 2+216-216-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+216-216-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+216-216) -- => **FALSE**
- -1' OR 3*2>(0+5+216-216) -- => **FALSE**
- -1' OR 2+1-1-1=1 AND 000216=000216 -- => **TRUE**
- -1' OR 000216=000216 AND 3+1-1-1=1 -- => **FALSE**
- -1' OR 3*2=5 AND 000216=000216 -- => **FALSE**
- -1' OR 3*2=6 AND 000216=000216 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000216=000216 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000216=000216 -- => **TRUE**

Original value: **e**

Request headers

```
POST /login.asp HTTP/1.1
Content-Length: 67
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://192.168.3.112
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=&Usercode=-1'%20OR%203*2*1=6%20AND%20000216=000216%20--%20
```

**/omdev/smtype.asp**

Details

URL encoded POST input **type** was set to **-1 OR 3*2*1=6 AND 000927=000927 --**

Tests performed:

- -1 OR 2+927-927-1=0+0+0+1 -- => **TRUE**
- -1 OR 3+927-927-1=0+0+0+1 -- => **FALSE**
- -1 OR 3*2<(0+5+927-927) -- => **FALSE**
- -1 OR 3*2>(0+5+927-927) -- => **FALSE**
- -1 OR 2+1-1-1=1 AND 000927=000927 -- => **TRUE**
- -1 OR 000927=000927 AND 3+1-1-1=1 -- => **FALSE**
- -1 OR 3*2=5 AND 000927=000927 -- => **FALSE**
- -1 OR 3*2=6 AND 000927=000927 -- => **TRUE**
- -1 OR 3*2*0=6 AND 000927=000927 -- => **FALSE**
- -1 OR 3*2*1=6 AND 000927=000927 -- => **TRUE**

Original value: **NaN**

Request headers

```
POST /omdev/smtype.asp HTTP/1.1
Content-Length: 112
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://192.168.3.112
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: */*
insval=e,NaN,'e','e',e,e,6,'e',e,e,e,e,e,e,9&op=ins2&tag1=e&type=-1%20OR%203*2*1=6%20AND%200
00927=000927%20--%20
```

## Cross site scripting

| | |
|---|---|
| Severity | **High** |
| 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

Acunetix Cross Site Scripting Attack (http://www.acunetix.com/websitesecurity/cross-site-scripting.htm)
VIDEO: How Cross-Site Scripting (XSS) Works (http://www.acunetix.com/blog/web-security-zone/video-how-cross-site-scripting-xss-works/)
The Cross Site Scripting Faq (http://www.cgisecurity.com/xss-faq.html)
OWASP Cross Site Scripting (http://www.owasp.org/index.php/Cross_Site_Scripting)
XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
Cross site scripting (http://en.wikipedia.org/wiki/Cross-site_scripting )
OWASP PHP Top 5 (http://www.owasp.org/index.php/PHP_Top_5)
How To: Prevent Cross-Site Scripting in ASP.NET (http://msdn.microsoft.com/en-us/library/ms998274.aspx)

### Affected items

**/omdev/smbysubsys.asp**

Details

URL encoded POST input **subsys** was set to **3'"()&%<acx><ScRiPt >0UOE(9459)</ScRiPt>**

Request headers

```
POST /omdev/smbysubsys.asp HTTP/1.1
Content-Length: 53
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.3.112
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: */*
subsys=3'"()%26%25<acx><ScRiPt%20>0UOE(9459)</ScRiPt>
```

**/C0-1x.asp**

Details

URL encoded GET input **itype** was set to **35949891"{+![$]`}9065**

The input is reflected inside a <script> tag between double quotes.

Request headers

```
GET /C0-1x.asp?itype=35949891"{%2b![%24]`}9065&port=8388615&sid=8&tag1=1 HTTP/1.1
Referer: http://192.168.3.112
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

URL encoded GET input **port** was set to **83886159230"{+![$]`}9136**

The input is reflected inside a <script> tag between double quotes.

Request headers

```
GET /C0-1x.asp?itype=3594&port=83886159230"{%2b![%24]`}9136&sid=8&tag1=1 HTTP/1.1
Referer: http://192.168.3.112
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

URL encoded GET input **sid** was set to **89507"{+![$]`}9346**

The input is reflected inside a <script> tag between double quotes.

Request headers

```
GET /C0-1x.asp?itype=3594&port=8388615&sid=89507"{%2b![%24]`}9346&tag1=1 HTTP/1.1
Referer: http://192.168.3.112
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

URL encoded GET input **tag1** was set to **19451"{+![$]`}9846**

The input is reflected inside a <script> tag between double quotes.

Request headers

```
GET /C0-1x.asp?itype=3594&port=8388615&sid=8&tag1=19451"{%2b![%24]`}9846 HTTP/1.1
Referer: http://192.168.3.112
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: */*
```

## 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><br>Form action: http://192.168.3.112/action/FileUpload<br>Form method: POST<br><br>Form inputs: |

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

Request headers

```
GET / HTTP/1.1
```

## 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: */*
```

**/A3-769.asp**

Details

http://192.168.3.112/A3-769.asp?sid=6

Request headers

```
GET /A3-769.asp?sid=6 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/C2.asp?subsys=3
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: */*
```

**/C2-0.asp**

Details

http://192.168.3.112/C2-0.asp?itype=769&sid=6

Request headers

```
GET /C2-0.asp?itype=769&sid=6 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/C2.asp?subsys=3
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: */*
```

**/C0-3x.asp**

Details

http://192.168.3.112/C0-3x.asp?itype=769&port=1048578&sid=6

Request headers

```
GET /C0-3x.asp?itype=769&port=1048578&sid=6 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/C0-3.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=8388615&sid=8&tag1=1

Request headers

```
GET /C0-1x.asp?itype=3594&port=8388615&sid=8&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: */*
```

**/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: */*
```

**/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: */*
```

**/C0-4x.asp**

Details

http://192.168.3.112/C0-4x.asp?itype=256&sid=7

Request headers

```
GET /C0-4x.asp?itype=256&sid=7 HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://192.168.3.112/C0-4.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/dbCfg.db3**

Details

```
HTTP/1.1 200 OK

Date: Wed Oct 10 10:32:59 2018

Content-Length: 66560

Connection: keep-alive

Last-Modified: Tue Oct  9 16:25:20 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: */*
```

**/file/dbData.db3**

Details

```
HTTP/1.1 200 OK

Date: Wed Oct 10 10:32:59 2018

Content-Length: 321536

Connection: keep-alive

Last-Modified: Wed Oct 10 10:16:49 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: Wed Oct 10 10:32:59 2018

Content-Length: 24576

Connection: keep-alive

Last-Modified: Wed Oct 10 10:32:58 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: Wed Oct 10 10:33:00 2018

Content-Length: 41984

Connection: keep-alive

Last-Modified: Wed Oct 10 10:32:51 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: */*
```

**/action/doctrl**

Details

```
HTTP/1.1 200 OK

Date: Wed Oct 10 10:48:38 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: */*
```

## Scanned items (coverage report)

http://192.168.3.112/
http://192.168.3.112/A3-769.asp
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/C0-3x.asp
http://192.168.3.112/C0-4.asp
http://192.168.3.112/C0-4x.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/C2-0.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/almx.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