acunetix WEB APPLICATION SECURITY

Acunetix Website Audit

27 August, 2018

Developer Report

Generated by Acunetix WVS Reporter (v10.5 Build 20160520)

Scan of https://dev.saskvlt.com:443/

Scan details

Scan information	
Start time	8/10/2018 8:48:11 AM
Finish time	8/10/2018 3:14:27 PM
Scan time	6 hours, 26 minutes
Profile	Default
Server information	
Responsive	True
Server banner	Apache
Server OS	Unknown
Server technologies	Java/J2EE

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	7
High	5
Medium	0
Low	2
Informational	0

Knowledge base

List of open TCP ports

Open Port 21 / ftp
Port Banner: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 07:48. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this s ...

Open Port 25 / smtp
No port banner available.

Open Port 53 / domain
No port banner available.

Open Port 80 / http
Port Banner: HTTP/1.1 200 OK
Date: Fri, 10 Aug 2018 13:48:24 GMT
Server: Apache
Last-Modified: Mon, 15 May 2017 16:28:41 GMT
Accept-Ranges: bytes
Content-Length: 111
Connection: close
Content-Type: text/html

<html><head><META HTTP-EQUIV="refresh" CONTEN ...

```
Open Port 110 / pop3
Port Banner: +OK Dovecot ready.


Open Port 143 / imap
Port Banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE
STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.


Open Port 443 / https
Port Banner: HTTP/1.1 400 Bad Request
Date: Fri, 10 Aug 2018 13:48:59 GMT
Server: Apache
Content-Length: 483
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Reque ...

Open Port 465 / smtps
No port banner available.

Open Port 587 / submission
Port Banner: 220-vps2.saskvlt.com ESMTP Exim 4.91 #1 Fri, 10 Aug 2018 07:49:15 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.


Open Port 993 / imaps
No port banner available.

Open Port 995 / pop3s
No port banner available.
```

SSL server running [443]

A TLS1 server is running on TCP port 443.

-

SSL server information:
Ciphers suported:

- TLS1_CK_RSA_WITH_AES_128_CBC_SHA(OpenSSL ciphername: AES128-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: AES(128), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA(OpenSSL ciphername: DHE-RSA-AES128-SHA, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: AES(128), Message authentication code: SHA1) - High strength
- TLS1_CK_RSA_WITH_AES_256_CBC_SHA(OpenSSL ciphername: AES256-SHA, Protocol version: TLSv1, Key Exchange: RSA, Autentication: RSA, Symmetric encryption method: AES(256), Message authentication code: SHA1) - High strength
- TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA(OpenSSL ciphername: DHE-RSA-AES256-SHA, Protocol version: TLSv1, Key Exchange: DH, Autentication: RSA, Symmetric encryption method: AES(256), Message authentication code: SHA1) - High strength
- TLS1_CK_ECDHE_RSA_WITH_AES_128_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: ECDH, Autentication: RSA, Symmetric encryption method: AES(128), Message authentication code: SHA1) - High strength
- TLS1_CK_ECDHE_RSA_WITH_AES_256_CBC_SHA(OpenSSL ciphername: n/a, Protocol version: TLSv1, Key Exchange: ECDH, Autentication: RSA, Symmetric encryption method: AES(256), Message authentication code: SHA1) - High strength

- Certificate 1:

Issuer:
    Country Name: US
    Organization Name: GeoTrust Inc.
    Organizational Unit Name: Domain Validated SSL
    Common Name: GeoTrust DV SSL CA - G3
Recipient:
    Common Name: *.saskvlt.com

Certificate version: 2
Serial number: 3aa77a148ffa7a7e4abd1eb28b53b1e3
Finger print: a841d994e2f4e23e0d09605914c60308
Algorithm ID: 1.2.840.113549.1.1.11
Valability start: Wed Mar 15 19:00:00 CDT 2017
Valability end: Sat Mar 16 18:59:59 CDT 2019
Expire in: 218 days

- Certificate 2:

Issuer:
    Country Name: US
    Organization Name: GeoTrust Inc.
    Common Name: GeoTrust Global CA
Recipient:
    Country Name: US
    Organization Name: GeoTrust Inc.
    Organizational Unit Name: Domain Validated SSL
    Common Name: GeoTrust DV SSL CA - G3

Certificate version: 2
Serial number: 023a73
Finger print: 6f1b445d7084fe973df5afe4e8875d9c
Algorithm ID: 1.2.840.113549.1.1.11
Valability start: Wed Jun 11 17:02:59 CDT 2014
Valability end: Fri May 20 17:02:59 CDT 2022
Expire in: 1379 days

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	Variations
/claim/step1.html	2

Cross site scripting (verified)

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	Variations
/claim/step1.html	3

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	Variations
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	Variations
/claim/step2.html	1

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

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

Affected items

/claim/step1.html

Details

POST (multipart) input address was set to test<WDI8NO>2XJRS[!+!]</WDI8NO>
The input is reflected inside a text element.

Request headers

```
POST /claim/step1.html HTTP/1.1
Content-Length: 1888
Content-Type: multipart/form-data; boundary=-----Boundary_OMPWDMVHHR
Referer: https://dev.saskvlt.com:443/
Cookie: sessions=31882vd08664v5q2gtrbm065n2v8hr7k
Host: dev.saskvlt.com
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: */*

-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="address"

test<WDI8NO>2XJRS[!+!]</WDI8NO>
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="city"
```

```
test
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="csrf_token_name"

32ff5a9af3132459802811327de777f8
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="email"

cindy@2webdesign.com
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="file1"

1
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="file1_name"

1
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="file1_size"

1
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="file1_type"

1
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="file2_name"

1
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="file2_size"

1
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="file2_type"

1
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="file3_name"

1
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="file3_size"

1
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="file3_type"

1
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="fname"

test
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="lname"

test
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="phone"

3068501234
-------Boundary_OMPWDMVHHR
Content-Disposition: form-data; name="postal"

s9s9s9
-------Boundary_OMPWDMVHHR
Conte ...
```

/claim/step1.html

Details

POST (multipart) input city was set to test<WROLU1>QUGR9[!+!]</WROLU1>
The input is reflected inside a text element.

Request headers

```
POST /claim/step1.html HTTP/1.1
Content-Length: 1888
Content-Type: multipart/form-data; boundary=-----Boundary_MOFYKIHYQG
Referer: https://dev.saskvlt.com:443/
Cookie: sessions=31882vd08664v5q2gtrbm065n2v8hr7k
Host: dev.saskvlt.com
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: */*

-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="address"

test
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="city"

test<WROLU1>QUGR9[!+!]</WROLU1>
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="csrf_token_name"

32ff5a9af3132459802811327de777f8
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="email"

cindy@2webdesign.com
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="file1"

1
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="file1_name"

1
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="file1_size"

1
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="file1_type"

1
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="file2_name"

1
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="file2_size"

1
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="file2_type"

1
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="file3_name"

1
```

```
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="file3_size"

1
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="file3_type"

1
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="fname"

test
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="lname"

test
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="phone"

3068501234
-------Boundary_MOFYKIHYQG
Content-Disposition: form-data; name="postal"

s9s9s9
-------Boundary_MOFYKIHYQG
Conte ...
```

Cross site scripting (verified)

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

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

Affected items

/claim/step1.html

Details

POST (multipart) input address was set to test"onmouseover=CLz0(9348)"
The input is reflected inside a tag parameter between double quotes.

Request headers

```
POST /claim/step1.html HTTP/1.1
Content-Length: 1885
Content-Type: multipart/form-data; boundary=-----Boundary_JQYTRLCPBG
Referer: https://dev.saskvlt.com:443/
Cookie: sessions=31882vd08664v5q2gtrbm065n2v8hr7k
Host: dev.saskvlt.com
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: */*

-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="address"

test"onmouseover=CLz0(9348)"
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="city"

test
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="csrf_token_name"
```

```
32ff5a9af3132459802811327de777f8
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="email"

cindy@2webdesign.com
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="file1"

1
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="file1_name"

1
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="file1_size"

1
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="file1_type"

1
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="file2_name"

1
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="file2_size"

1
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="file2_type"

1
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="file3_name"

1
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="file3_size"

1
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="file3_type"

1
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="fname"

test
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="lname"

test
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="phone"

3068501234
-------Boundary_JQYTRLCPBG
Content-Disposition: form-data; name="postal"

s9s9s9
-------Boundary_JQYTRLCPBG
Content- ...
```

/claim/step1.html

Details

POST (multipart) input city was set to test"onmouseover=CLz0(9162)"
The input is reflected inside a tag parameter between double quotes.

Request headers

```
POST /claim/step1.html HTTP/1.1
Content-Length: 1885
Content-Type: multipart/form-data; boundary=-----Boundary_GHQWFYQCRF
Referer: https://dev.saskvlt.com:443/
Cookie: sessions=31882vd08664v5q2gtrbm065n2v8hr7k
Host: dev.saskvlt.com
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: */*

-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="address"

test
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="city"

test"onmouseover=CLz0(9162)"
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="csrf_token_name"

32ff5a9af3132459802811327de777f8
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="email"

cindy@2webdesign.com
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="file1"

1
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="file1_name"

1
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="file1_size"

1
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="file1_type"

1
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="file2_name"

1
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="file2_size"

1
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="file2_type"

1
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="file3_name"

1
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="file3_size"
```

```
1
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="file3_type"

1
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="fname"

test
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="lname"

test
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="phone"

3068501234
-------Boundary_GHQWFYQCRF
Content-Disposition: form-data; name="postal"

s9s9s9
-------Boundary_GHQWFYQCRF
Content- ...
```

/claim/step1.html

Details

POST (multipart) input email was set to cindy@2webdesign.com"onmouseover=CLz0(9934)"
The input is reflected inside a tag parameter between double quotes.

Request headers

```
POST /claim/step1.html HTTP/1.1
Content-Length: 1885
Content-Type: multipart/form-data; boundary=-----Boundary_RXSUXVYWBW
Referer: https://dev.saskvlt.com:443/
Cookie: sessions=31882vd08664v5q2gtrbm065n2v8hr7k
Host: dev.saskvlt.com
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: */*

-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="address"

test
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="city"

test
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="csrf_token_name"

32ff5a9af3132459802811327de777f8
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="email"

cindy@2webdesign.com"onmouseover=CLz0(9934)"
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="file1"

1
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="file1_name"

1
```

```
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="file1_size"

1
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="file1_type"

1
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="file2_name"

1
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="file2_size"

1
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="file2_type"

1
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="file3_name"

1
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="file3_size"

1
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="file3_type"

1
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="fname"

test
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="lname"

test
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="phone"

3068501234
-------Boundary_RXSUXVYWBW
Content-Disposition: form-data; name="postal"

s9s9s9
-------Boundary_RXSUXVYWBW
Content- ...
```

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
The X-Frame-Options response header

Affected items

Web Server

Details

No details are available.

Request headers

```
GET / HTTP/1.1
Cookie: sessions=31882vd08664v5q2gtrbm065n2v8hr7k
Host: dev.saskvlt.com
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

/claim/step2.html

Details

Form name: <empty>
Form action: https://dev.saskvlt.com/claim/step2.html
Form method: POST

Form inputs:

- csrf_token_name [Hidden]
- act [Hidden]
- claim_id [Hidden]
- fname [Hidden]
- lname [Hidden]
- address [Hidden]
- phone [Hidden]
- city [Hidden]
- province [Hidden]
- postal [Hidden]
- prizeamount [Hidden]
- ticketamount [Hidden]
- ticketno [Hid ... (line truncated)

Request headers

```
GET / HTTP/1.1
```

Scanned items (coverage report)

Scanned 51 URLs. Found 2 vulnerable.

URL: https://dev.saskvlt.com/
No vulnerabilities have been identified for this URL
8 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
/[*]/<s>.html	Path Fragment (suffix .html)
/<s>/[*].html	Path Fragment (suffix .html)

Input scheme 2	
Input name	Input type
/[*].html	Path Fragment (suffix .html)

Input scheme 3	
Input name	Input type
/[*]/<s>/<n>_<s>	Path Fragment
/<s>/[*]/<n>_<s>	Path Fragment
/<s>/<s>/[*]_<s>	Path Fragment
/<s>/<s>/<n>_[*]	Path Fragment

Input scheme 4	
Input name	Input type
Host	HTTP Header

URL: https://dev.saskvlt.com/pages
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/winners.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/contact.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/media_release.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/responsible_gaming.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/legal.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/submit_by_mail.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/submit_claim_online.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/private_policy.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/rules_of_operations.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/submit_at_payout_centers.html

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/media_release

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/media_release/12_million_vlt_jackpot_awarded_in_saskatoon

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/pages/contact

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/public/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/css/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/css/skin.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/css/style.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/css/media.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/css/slider.css

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/images/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/images/arrow

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/js/
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/js/responsiveslides.min.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/js/jquery.jcarousel.min.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/js/custom.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/default/js/jquery-megajackpots-meters-2.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/validator/
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/validator/css/
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/validator/css/validationEngine.jquery.css
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/validator/js/
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/validator/js/languages/
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/validator/js/languages/jquery.validationEngine-en.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/validator/js/jquery.validationEngine.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/js/
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/public/js/jquery.mask.min.js
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/common
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/common/contact_form.html
No vulnerabilities have been identified for this URL
5 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
comments	POST (multipart)
csrf_token_name	POST (multipart)
email	POST (multipart)
name	POST (multipart)
phone	POST (multipart)

URL: https://dev.saskvlt.com/ckfinder/
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/ckfinder/userfiles/
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/ckfinder/userfiles/images/
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/ckfinder/userfiles/files/
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/claim.html
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/claim
No vulnerabilities have been identified for this URL
No input(s) found for this URL

URL: https://dev.saskvlt.com/claim/step1.html
Vulnerabilities have been identified for this URL
21 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
address	POST (multipart)
city	POST (multipart)
csrf_token_name	POST (multipart)
email	POST (multipart)
file1	POST (multipart)
file1_name	POST (multipart)
file1_size	POST (multipart)
file1_type	POST (multipart)
file2_name	POST (multipart)
file2_size	POST (multipart)
file2_type	POST (multipart)
file3_name	POST (multipart)
file3_size	POST (multipart)
file3_type	POST (multipart)
fname	POST (multipart)

lname	POST (multipart)
phone	POST (multipart)
postal	POST (multipart)
province	POST (multipart)
ticketamount	POST (multipart)
ticketno	POST (multipart)

URL: https://dev.saskvlt.com/claim/step2.html

Vulnerabilities have been identified for this URL

29 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
act	POST (multipart)
address	POST (multipart)
city	POST (multipart)
claim_id	POST (multipart)
csrf_token_name	POST (multipart)
email	POST (multipart)
file1	POST (multipart)
file1_name	POST (multipart)
file1_size	POST (multipart)
file1_type	POST (multipart)
file2	POST (multipart)
file2_name	POST (multipart)
file2_size	POST (multipart)
file2_type	POST (multipart)
file3	POST (multipart)
file3_name	POST (multipart)
file3_size	POST (multipart)
file3_type	POST (multipart)
fname	POST (multipart)
lname	POST (multipart)
phone	POST (multipart)
postal	POST (multipart)
prizeamount	POST (multipart)
province	POST (multipart)
ticketamount	POST (multipart)
ticketno	POST (multipart)
uploadBtn1	POST (multipart)
uploadBtn2	POST (multipart)
uploadBtn3	POST (multipart)

URL: https://dev.saskvlt.com/cgi-bin/

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/home

No vulnerabilities have been identified for this URL

No input(s) found for this URL

URL: https://dev.saskvlt.com/utility/

No vulnerabilities have been identified for this URL

No input(s) found for this URL