MATT SCHMIDT / EDUCATION BUG BOUNTY, COMMON VULNERABILITIES, CVE, RESPONSIBLE DISCLOSURE, VULNERABILITY

XMPie UStore Vulnerabilities Discovered

Recently during an **External Penetration Test**, Triaxiom discovered several flaws/vulnerabilities within a **commercial-off-the-shelf (COTS)** eCommerce platform called XMPie uStore. In this post, we will discuss the avenue through which Triaxiom was able to gain initial access to this application, the security flaws discovered, recommended remediation steps for those flaws, and the responsible disclosure process with the affected vendor.

Initial Access

As always, an initial vulnerability scan and **network-level testing** kicks off an External Penetration Test. During this phase, we're commonly looking for open web ports as they typically present a quick and easy identification of what is running on that port. In this case, port 80 was open on a provided target. Port 80 is most commonly associated with the HyperText Transfer Protocol (HTTP), which is used for communication

LOOKING FOR SOMETHING SPECIFIC?

JOIN OUR NEWSLETTER!

Don't be left in the dark. Enter your email below and become part of our newsletter. We promise not to spam you!

RECENT POSTS

PCI DSS v4.0 – Major Changes and Differences

XMPie uStore Vulnerabilities Discovered

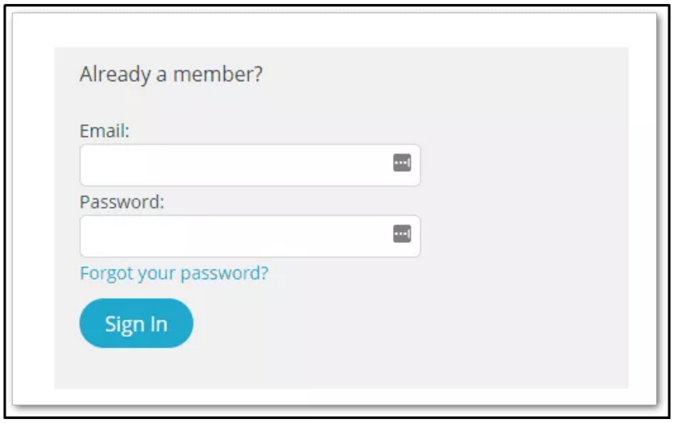
Why Security Programs Fail

CATEGORIES

Select Category

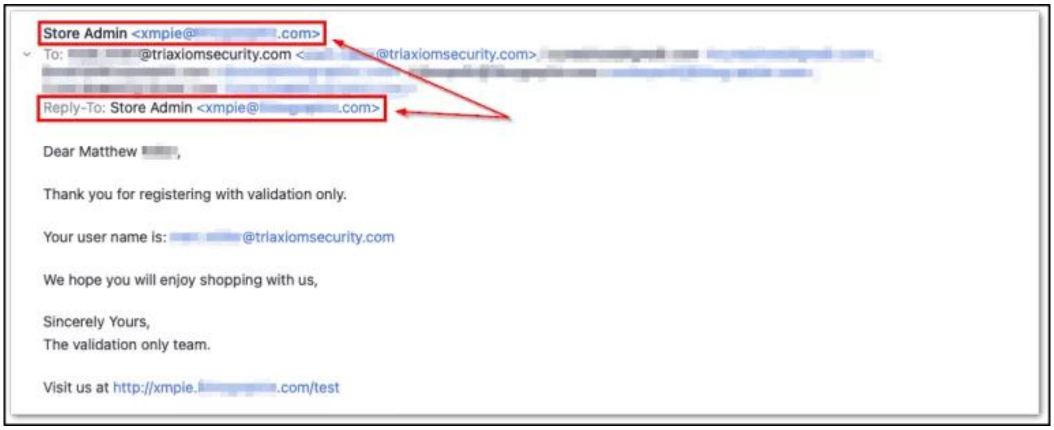
between web servers and browsers. With a web server using HTTP exposed, some more enumeration can be conducted with tools such as Nikto (a simple web application vulnerability scanner) or dirsearch (a directory brute forcing tool used to discovered content). Additionally, simply browsing to this target in a web browser will usually return some content and give us a place to start.

From here, it was quickly noted that a login interface was available. Common first steps here are to attempt default credentials (more on that below) when we identify the service. In this case, the interface needed a valid email / password combination. Without knowing what a valid email was, Triaxiom continued the enumeration process for the time being.



XMPie uStore user login interface.

While a set of credentials were unable to be guessed at this time, a registration feature was available. Triaxiom registered a new user account in an attempt to evaluate the application from an authenticated perspective. A confirmation email was sent to a Triaxiom email address which was sent from “uStore Admin”, which came in handy later on!



Store Admin <xmpie@[redacted].com>
To: [redacted]@triaxiomsecurity.com <[redacted]@triaxiomsecurity.com> [redacted]
Reply-To: Store Admin <xmpie@[redacted].com>

Dear Matthew [redacted],

Thank you for registering with validation only.

Your user name is: [redacted]@triaxiomsecurity.com

We hope you will enjoy shopping with us,

Sincerely Yours,
The validation only team.

Visit us at http://xmpie.[redacted].com/test

Registration confirmation email with valid admin email.

Remember when we mentioned using dirsearch? **Dirsearch** is a directory brute forcing tool used to discover web pages and content on the web server that isn't linked or easily discovered with normal web application usage. When analyzing the results from

MOST DISCUSSED

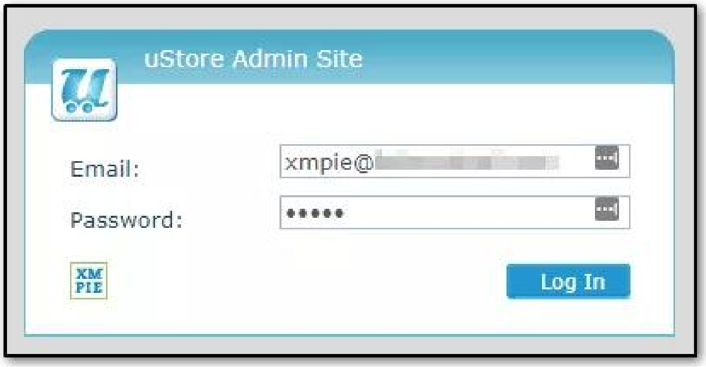
API Penetration Test Best Practice Checklist Cloud Common Vulnerabilities comparison COMPLIANCE configuration review Core Values Cost Current Events Education External Penetration Test firewall HIPAA improvement Incident Response Internal Penetration Test methodology Onsite Assessment Passphrase Passwords Password Security PCI PCI DSS PCI QSA penetration test Physical Penetration Test Problems QSA Quick Tips Regulation Remediation Report Risk ROC SAQ Security Awareness Small Business SMB Social Engineering vetting vulnerability Web Application Penetration Test wireless

LATEST TWEETS

The long-anticipated release of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 4.0 by the PCI… https://t.co/HcFP1TsLIu

6 MONTHS AGO

dirsearch, a URL was discovered which led to a separate login for an administrative portal.

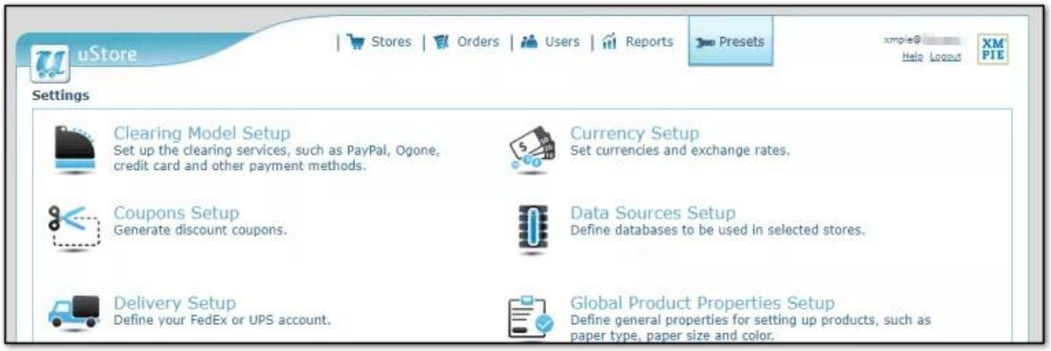

uStore Admin Site

Email: xmpie@[redacted]

Password: •••••

uStore Admin login.

With the administrator email known, since we saw it in the registration email above, the next step was identifying a valid password to login. To find the password, Triaxiom reviewed the uStore documentation (noted below) to see if there was a default password that could be tried. As luck would have it, there was. Utilizing the "uStore Admin" email from the registration confirmation and the default password listed in the XMPie uStore documentation, Triaxiom was able to successfully login to the administrative dashboard for the uStore application.



Clearing Model Setup
Set up the clearing services, such as PayPal, Ogone, credit card and other payment methods.

Currency Setup
Set currencies and exchange rates.

Coupons Setup
Generate discount coupons.

Data Sources Setup
Define databases to be used in selected stores.

Delivery Setup
Define your FedEx or UPS account.

Global Product Properties Setup
Define general properties for setting up products, such as paper type, paper size and color.

uStore administrative dashboard.

Default Credentials

Upon discovering a login portal, one of the very first steps a **Penetration Tester** or malicious hacker will usually take is to attempt default credentials (admin/admin, admin/password, etc.). While it seems obvious to change these credentials immediately upon deploying a new application, it is not uncommon to gain unauthorized access to a web application via default credentials. Further, many applications ship with default credentials in place and do not require administrators to change them immediately during the installation or deployment process. In the case of this assessment, the same was true for the uStore application. Below is an excerpt from the XMPie Knowledge Base detailing default credentials after install:

We are hiring! Come join our already awesome team and help make a difference securing organizations. Focus for this… https://t.co/3ofuZQNHPV

10 MONTHS AGO

Web App Series: Now that we have covered the ins and outs of web app penetration testing, we are going to shift gea… https://t.co/hTplgbKdgS

11 MONTHS AGO

Follow Us on Twitter

> By default, when uStore is installed, the admin username and password are both “admin”. Your uStore is a publicly accessible website, so you should change the default admin login credentials as soon as possible to ensure that access to the uStore Back Office is secure.
>
> *https://help.xmpie.com/KBA/0052/0052_Configuring_initial_settings_after_uStore_installation.htm*

It should be noted that the above instructions do advise to change the default credentials as soon as possible. While this advice is good, it would likely be better to have the application generate a unique set of strong credentials in the first place, or require administrators to change their password on first login to the administration panel.

Administrator Access to Raw SQL Queries

This next security issue is an unintended consequence of a built-in feature. The XMPie uStore application allows for administrators to set events which are triggered on predefined actions, or generate reports from custom SQL statements. Because of this, Triaxiom was able to successfully run SQL queries and pull sensitive information from the client’s database, including password hashes, customer information, and decryption keys. The images below demonstrate the impact of this feature.

Custom SQL query to retrieve the ‘Users’ table.

Fetching usernames and password hashes from database.

This feature should be removed entirely, or have careful consideration of who has access to it. Additionally, restrictions should be placed on the commands which can be executed and the databases / tables that can be accessed from it.

Persistent XSS

The final vulnerability we will cover is **Persistent Cross-Site Scripting (XSS)**. Persistent XSS vulnerabilities occur when a user can submit input to an application which then gets stored and rendered by the application in an unsafe manner. This can be exploited through JavaScript code that is included in user input which is stored within the application and then viewed/rendered somewhere. When detonated, this malicious input executes code in the client's browser to steal cookies, gain remote control over their host, redirect their browser to an attacker controlled website, or perform some other type of unwanted action on their behalf.

Triaxiom discovered two locations where Persistent XSS vulnerabilities were present in the application, but there are likely other locations that are vulnerable, as well. Exploitation is fairly simple:

1. Authenticate into the application as an Administrator.

2. Go to User Setup and select a victim.

3. Insert code in either the first name or last name field. The proof-of-concept code using this example was <script>alert("XSS")</script>.

Vulnerable input fields when editing a user.

XSS alert executing.

While the above image is a very rudimentary proof-of-concept (PoC), a real-world attacker would utilize a more malicious payload. Triaxiom recommends always utilizing proper escaping techniques whenever displaying user input to prevent it from executing. Additionally, utilize proper input validation to filter for XSS attacks on both the client-side and server-side. A Web Application Firewall (WAF) could also be considered to provide some defense in depth against this attack.

Responsible Disclosure

Upon discovering security concerns / vulnerabilities on software during a penetration test, Triaxiom then goes through the **responsible disclosure process** to ensure the vendor is fully aware of the issue. During this phase, we work closely with the vendor and allow them to work on any fixes or patches during this time. Typically vendors are receptive to hearing about security concerns and swiftly address any discovered issues. After initial correspondence, the point-of-contact with XMPie stopped replying to Triaxiom Security's inquiries and attempts to address the issues discovered. While communication with the point-of-contact was lost, it is possible the security issues were still fixed, as the **release notes** from January 18th, 2022 mention “a few low and medium” (*debatable on the severity*) security risks have been fixed.

This blog post and discovered vulnerabilities were a collaborative effort between Matthew Hier and Matt Schmidt of Triaxiom Security.

Matt Schmidt

Matt is a security engineer at Triaxiom Security. He holds a BS in Information Technology and currently has his OSCP, CRT, eWPT, and Security+ certifications. You can find him on Twitter @rumhamstuff.

Why Security Programs Fail

PCI DSS v4.0 – Major Changes and Differences

LATEST TWEETS

As development techniques and technology change, there are changes in the trends for the types of vulnerabilities u… https://t.co/wxDZ9BPXZR

1 YEAR AGO

We are hiring! We are looking for a Senior Security Consultant and a Junior Penetration Tester. #infosecjobs… https://t.co/Dg2jmNxOu0

1 YEAR AGO

Follow Us on Twitter