TEVORA

Case Study: Race Against Clock to Block Extortion Attempt

This case study describes how Tevora helped a large, industry-leading financial institution block an extortion attempt initiated by a skilled hacker that had identified a significant vulnerability in the institution's cyber defenses.

To protect our client's confidentiality, we'll refer to them by the fictitious name of Global Financial Institution (GFI).

The Hacker Makes Contact

A hacker based in India informed GFI that they had identified a vulnerability in GFI's systems that allowed full access to any customer account, which in turn allowed money to be transferred externally. The hacker provided data from a compromised account to demonstrate that the vulnerability was real. They then threatened to go public by posting details of the vulnerability on YouTube and Twitter unless GFI paid them $250,000 within 48 hours.

The Clock Starts Ticking: Time Left—48:00

After receiving the extortion threat, GFI reached out to Tevora and engaged us to identify the vulnerability and advise on how it could be fixed. Our Red Team of security specialists sprung into action, realizing that they had only 48 hours to complete their task—a tall order.

Time Left—46:30

Having no information about what the vulnerability might be, the Tevora team asked GFI for any evidence or logs that might provide clues about how the hacker was accessing the client's systems and customer accounts. Unfortunately, GFI had neither. We were essentially flying blind, with no information about how the hacker had obtained access to GFI customer information, or whether they had even identified a bug.

Our first instinct was to see if an employee workstation had been compromised. We challenged the hacker to obtain access to another account. When they did this successfully without accessing any previously-installed malware on an employee workstation, we ruled out the compromised workstation hypothesis.

Next, we did a vulnerability scan of the client's web server, which was unable to find any known vulnerabilities.

Time Left—36:20

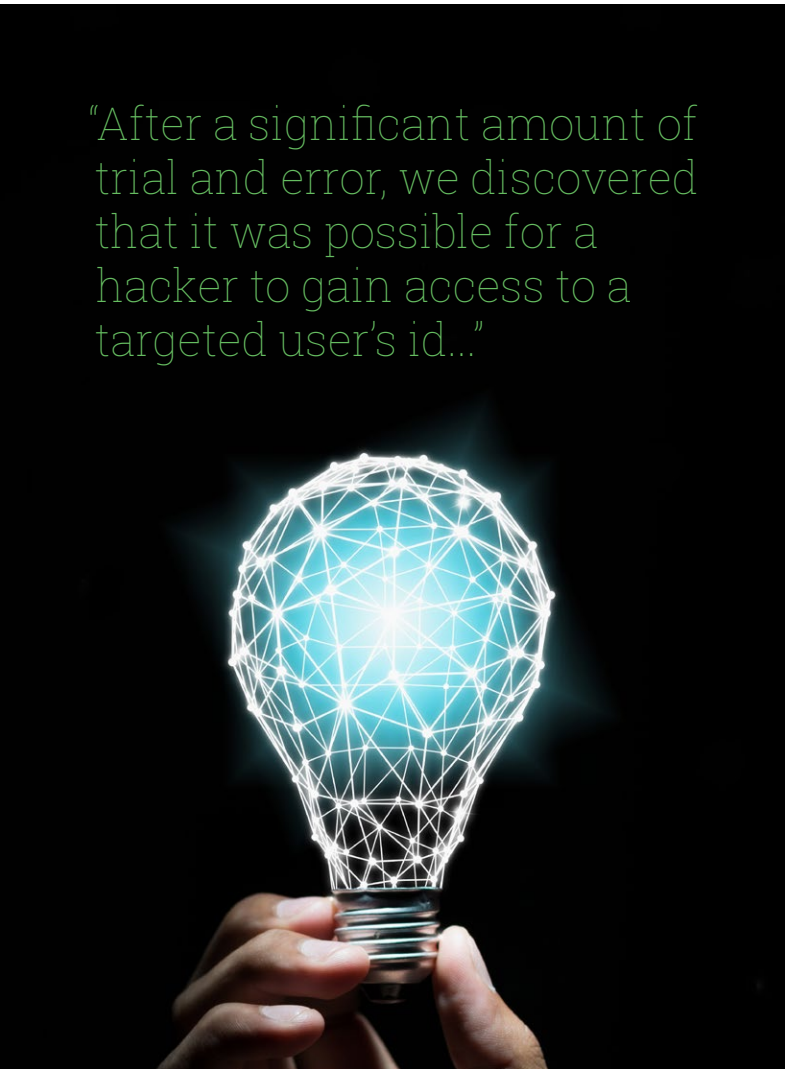
After that, we looked for flaws in web or mobile application logic, which each had different versions of business logic on the back end. After extensive exploration of this application logic, we found a flaw in the mobile app password reset workflow. If you tried to reset the password, then removed the security questions and answers, it would default and let you reset the password.

At this point, we thought, Yay! Drop the mic. Mission accomplished!

We contacted the client team and had them apply a patch, which fixed this vulnerability.

However, after the fix was applied, we challenged the hacker to compromise another account, and they were able to do it. Bummer! We had found one problem, but apparently not the only problem.

"After a significant amount of trial and error, we discovered that it was possible for a hacker to gain access to a targeted user's id..."



Time Left—24:00

At this point, we were getting pretty worried that we might not find the vulnerability in time. We still had no idea how the hacker was able to access customer accounts. We were back to the drawing board, and time was running out.

Time Left—22:35

We decided to explore all possible parts of the web application that could perform password changes, which narrowed our focus to "forgot password," "password reset in account page," and "create new account" workflows. This was time-consuming work that unfortunately yielded no results. The team was frustrated but still determined to get to the bottom of the problem.

Time Left—10:00

At this point, we shifted our focus to session management, where there are lots of opportunities for mistakes, and our testing was also, by necessity, manual and slow, which was increasingly concerning as we approached the 48-hour deadline. Our team was getting significant attention from Tevora and GFI management, which only served to heighten the tension.

The format GFI had used to reset passwords and create new accounts was complicated, with multiple pages, relying on state information in session cookies. We felt that our testing approach at this point was likely to reveal the problem but might take more time than we had.

During this phase of testing, we started noticing that there were other calls going back out to the application that weren't part of the web application itself.

Working with the client team, we discovered that they had implemented IBM Tealeaf for web analytics, which did have some logging. We asked for and obtained access to these logs, and they showed that there was activity coming from India hitting a "forgot password" page. This allowed us to narrow our focus significantly. We were at last feeling like we'd made a significant breakthrough.

Time Left—3:20

With a little over three hours to go, we were concerned, but also felt we were getting close to solving the mystery. The IBM Tealeaf logs showed access to a specific password page coming in from an IP address in India, where we knew the hacker lived. This allowed us to further narrow our

focus to just this page. After a significant amount of trial and error, we discovered that it was possible for a hacker to gain access to a targeted user's id by taking the following steps:

- Create new account, posing as legitimate new user
- Go through normal process to request password change
- Capture post request for password change
- Start reset password workflow for different (targeted) user
- Pull out the session ID
- Go back to captured post request and paste it in session ID
- Run reset password again; it will fail
- Run it yet another time; this will result in successful password change, giving hacker full access to targeted user capabilities, including ability to transfer money to external accounts of their choosing

Success!

After identifying the vulnerability in GFI's web application password reset logic, we advised the client on how to fix it. They quickly applied a patch, which successfully prevented the hacker from accessing any more client accounts. GFI was thrilled that we were able to help them quickly identify and resolve the vulnerability, allowing them to avoid paying the $250,000 ransom or suffering any reputational damage or financial losses that might have resulted from the hacker posting details about the vulnerability on YouTube and Twitter.

Lessons Learned

In addition to helping GFI identify and fix two significant vulnerabilities in their externally-facing we applications, Tevora highlighted the need for robust logging to help them diagnose future vulnerabilities or cyberattacks. We also recommended that they identify incident response resources—either in-house or externally—to be available 24/7 to respond to potential future cyberattacks.

Bug Bounty Program

For some hackers, the line between ethical/white-hat hacking and black-hat hacking is very gray. Having a Bug Bounty Program can be a great way to encourage these potentially-ethically-challenged hackers to use their skills for good by reporting vulnerabilities or bugs they have discovered to the organizations in which the weaknesses were found.

Bug Bounty Programs can offer financial rewards and/or public recognition for ethical hackers. The rewards don't necessarily need to be large dollar amounts. In some cases, small reward amounts (e.g., $100), or things like t-shirts or hats have been effective. In other cases, publishing the Bug Bounty participant's name and details of the vulnerability they identified can be a valuable way for the hacker to get the word out regarding their hacking skills, which can lead to future employment for the hacker.

The existence of a Bug Bounty program alone can be enough to make a hacker decide to report a bug to an organization rather than incur the risks associated with an extortion attempt (e.g., risks that they will get caught or that the ransom amount will not be paid).

In the GFI case, Tevora partnered with the client to implement a Bug Bounty Program, which has been successful in identifying other vulnerabilities.

We Can Help

Tevora's team of security specialists has worked with some of the world's largest companies to help them respond to extortion attempts and cyberattacks and shore up their defenses against future attacks. If you'd like to learn more about how we can help you ensure the security of your environment, just give us a call at **(833) 292-1609** or email us at **sales@tevora.com**.