Web Server Compromise

## Date: 2025-03-09

## Handler: Kush Patel

# Executive Summary

On 2021-02-10 at 10:00AM PST the IT Security department notified the SOC who will also be the Incident Responder about unusual behavior on one of their servers, server-a. On investigation Information Security found that an unauthorized user was present on the system. The unauthorized had a IP address of 47.75.76.54. He somehow managed to gain access to the web sever by finding the administrator credentials and logging in as the administrator and performed a session hijacking, he then got another device and logged in as the user who’s blogging his research paper and then unexpectedly had essays that were advertised by modifying the posts that included the research and replaced it by adding essays documents to the posts. After our Security Analyst will analyze the cyber attack, malicius activity and uncertaintity in the system, we will form a response plan to help combat this, and we will fix the vulnerabilities and hire more penetration testers to prevent more incidents like this happening in the future. Because of that the all of the user’s research had been lost, he would be forced to redo all his posts about this research again after we fix and change the security infrastructure of the server. We eventually found out the problem, restored the modified messages to its original state. We added some more and enhanced security features to ensure this attack doesn’t happen again

# Background

The systems that were involved were on a wide variety of systems the users were using which were an Apple Macintosh Computer, A Windows computer, an Android phone, and A Linux laptop all of which have different IP Addresses, they all accessed a web application that was called WordPress which is an web application where you can create a blog it can include a text, it can include an essay file, video file and wide variety of file types that you can share it is managed by an administrator with its credentials,there is a administrator who manages the web application and its users. The user login page is where the user can log in with their username and password, create their account, reset their password, and a wide variety of things, the administration can delete posts and change and modify different things. Anyone can send and broadcast messages to everyone and include files on those messages via blog posts. This is a blogging app that you can include anything, but when installling this app its on a HTTP protocol not HTTPS which shows this application is not secure and it lacks an SSL certificate. The wordpress app is a blog platform where you can put messages and doc files and images, The network traffic tracked normal activity on the website such as users downloading different files, whenever the website was visited by user, whenever the administrator page was visited it showed up in traffic It also includes how and when Cyber Security company of SecureTech Solutions was notified of the incident. Whenever someone find any unusual activity on the server it gets reported to the security department of the IT and find out what the problem is and what to do to fix the problem

# Timeline

2021-02-02 at 1:28PM PST –A user with the IP address of 77.88.5.21 was visited a website based on the HTTP GET message at http://yandex.com/bots

2021-02-02 at 3:53PM PST –A user with the IP address of 77.88.5.21 on the website downloaded a robot.txt file from at http://yandex.com/bots

2021-02-02 at 3:53PM PST- A user with the IP address of 130.207.188.150 visited the wordpress website and because of that it triggered a alert and notification from wp-cron.php,wp-cron showed that the site of the wordpress was visited, WPCron is usually triggered when a site receives a visit.They then tell the website that they are doing a cron task

2021-02-02 at 10:33PM PST –A user with the IP address of 77.88.5.21 on the website downloaded a robot.txt file from at http://yandex.com/bots

2021-02-03 at 12:46 AM PST- A user with the IP address of 207.46.13.236 on the website downloaded a robot.txt file from at http://www.bing.com/bingbot.htm

2021-02-03 at 05:44 AM PST- - A user with the IP address of 130.207.188.150 visited the wordpress website and because of that it triggered a alert and notification from wp-cron.php,wp-cron showed that the site of the wordpress was visited, WPCron is usually triggered when a site receives a visit.They then tell the website that they are doing a cron task

2021-02-03 at 09:32 AM PST- A user with the IP address of 47.75.76.54 accessed the website, XML cookies were sent, browser embedded clients sent some cookies

2021-02-03 at 09:32 AM PST - A user with the IP address of 47.75.76.54 accessed the website, it entered the user login page, which handles the authentication, registering, resseting password and other user handling, the login page has a form where the user can enter a username, and a password where the user can enter a password

2021-02-03 at 09:32 AM PST - A user with the IP address of 47.75.76.54 potentially performed a attacked by putting in “?author=1” in the link of the webpage, it could be a brute force attack given that in the form there is no author id in the form only a username id and a password id which shows that, it was all because of a default username the attacker managed to figure out the login, it was also an attempt to enumerate the administrators username, it looks like a SQL injection attack but there is no form with the id of author in the code of the wp-login, there is an id called loginForm, it just shows user\_pass for password and user\_login for login

2021-02-03 at 09:32 AM PST – Based on the request of “GET /author/admin/” it showed that the user with the IP address of 47.75.76.54 who was the attacker was able to successfully log in as the administrator via brute force attack

2021-02-03 from 09:32 AM to 09:42 AM- After the attacker successfully logged into the system he consistently performed some attacks, he as the the administrator was able to log into the system and send cookies consistently again and again for 10 minutes straight, he continued to post and fill and send out so many XML contents again and again for 10 minutes straight

2021-02-03 at 10:04 AM- A user with the IP address of 77.88.5.21 on the website downloaded a robot.txt file from at http://yandex.com/bots

2021-02-03 at 05:44 PM- A user with the IP address of 130.207.188.150 visited the wordpress website and because of that it triggered a alert and notification from wp-cron.php,wp-cron showed that the site of the wordpress was visited, WPCron is usually triggered when a site receives a visit. They then tell the website that they are doing a cron task

2021-02-04 at 11:43 AM- A user with the IP address of 130.207.188.150 visited the wordpress website and because of that it triggered a alert and notification from wp-cron.php,wp-cron showed that the site of the wordpress was visited, WPCron is usually triggered when a site receives a visit.They then tell the website that they are doing a cron task

2021-02-04 at 12:53 PM- A user with the IP address of 40.88.21.235 accessed a website on firefox at http://duckduckgo.com

2021-02-04 at 02:23 PM-A user with the IP address of 72.167.247.190 accessed wp-content/themes/paper-and-glue//timthumb.php?src=http://img.youtube.com.dollhousedelight.com/.mods/bbb.php, which showed that he is trying to set an image and given that there was a 404 request not found the image didn’t exist

2021-02-04 at 03:46 PM- A user with the IP address of 66.249.70.26 accessed a website on firefox at http://yandex.com/bots and downloaded robot.txt

2021-02-05 at 04:38 AM- A user with the IP address of 66.249.70.26 logged onto the computer and opened the computer

2021-02-05 at 04:38 AM- A user with the IP address of 130.207.188.150 visited the wordpress website and because of that it triggered a alert and notification from wp-cron.php,wp-cron showed that the site of the wordpress was visited, WPCron is usually triggered when a site receives a visit.They then tell the website that they are doing a cron task

2021-02-05 at 09:12 AM- A user with the IP address of 72.167.34.8 accessed /wp-content/plugins/wordpress-gallery-plugin/bbb.php and wrote in the send form with the message “like gecko” five times

2021-02-05 at 09:12 AM- A user with the IP address of 72.167.31.2 accessed /wp-content/plugins/wordpress-gallery-plugin/bbb.php and wrote in the send form with the message“” seven times, which could be the plug ins he was installing before the attack happened

2021-02-05 at 05:18 PM- A user with the IP address of 51.210.124.177 accessed wp-includes/wpconfig.bak.php?act=ul HTTP/1.1" 403 431 "www.google.com" "Mozlila/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Moblie Safari/537.36" which showed that it was trying to change and configure that part of the website

2021-02-06 at 10:57AM PST –A user with the IP address of 66.249.70.28 on the website downloaded a robot.txt file from at http://yandex.com/bots

2021-02-06 at 03:16PM PST- A user with the IP address of 93.158.161.13 accessed the wordpress software at the website

2021-02-06 from 11:39PM PST to 11:40PM PST- A user with the IP address of 157.75.167.23 filled out a form at /wp-content/plugins/wordpress-gallery-plugin/bbb.php, which showed he was trying to make sure he was in the clear to perform any other messages

2021-02-06 from 11:41PM PST- A user with the IP address of 157.75.167.23 entered the login page and based on the link it said http://10.128.25.182/wp-login.php?loggedout=true&wp\_lang=en\_US which showed that no user was logged in and the attacker was preparing to log in with the credentials he got from the session hijacking days ago , he then logged in as an administrator and started to tamper with the posts, forms, and other messages, the loggedout=true shows that no user was logged in and it prompted for the username and password

2021-02-06 from 11:41PM PST to 11:46 PM PST- A user with the IP address of 157.75.167.23 started to do some unknown and malcious activty, he then added some directories to the url of wp/admin such as “/admin-ajax.php”, “edit.php”,”index.php”, it then showed a duck saying “may the duck bring you luck”, and then when it is at edit.php it shows the id of post\_type in the edit.php?post\_type=page" which shows that the post type is a page that contains a essay which shows that the attacked must have found the password of the user who posted his rearch, it showed that the post was changed from a chat blog to an essay page when that attacker was able to log into the administration page via brute force attack he found the list of users he decided to use the credentials of the user who initially did the research post after he did the post and plug in, the post\_type=”page” indicates that the essay was being posted/advertise, he also accessed edit.php in which he decided to edit the post

2021-02-06 at 11:43PM PST-A user with the IP address of 157.75.167.23 started to some other activity like modify, edit or edit some of the other posts made by the user while on the admin page in which he used it to change the user research blog to essays that were being advertised, the attacker changed all the reached related blogs and posts to advertised essays, the post.php file manages all the posts actions and other things related to the post in which the administration can based on the change to the url, the url part of post.php?post=1&action=edit indicates that the essay is edited, based on the action=edit, it showed that the attacker modified some of the posts already made by the users especially the user who was blogging his research

2021-02-07 at 3:45AM PST- A user with the IP address of 130.207.188.150 visited the wordpress website and because of that it triggered a alert and notification from wp-cron.php,wp-cron showed that the site of the wordpress was visited, WPCron is usually triggered when a site receives a visit. They then tell the website that they are doing a cron task

2021-02-07 at 11:58AM PST- A user with the IP address of of 77.88.5.21, accessed the website of http://yandex.com/bots

2021-02-07 at 05:41PM PST- A user with the IP address of of 216.244.66.233, accessed the website http://www.opensiteexplorer.org/dotbot

2021-02-08 at 04:32AM PST- A user with the IP address of 130.207.188.150 visited the wordpress website and because of that it triggered a alert and notification from wp-cron.php,wp-cron showed that the site of the wordpress was visited, WPCron is usually triggered when a site receives a visit. They then tell the website that they are doing a cron task

2021-02-08 at 04:32AM PST- A user with a IP address of 207.46.13.228 visited the website http://www.bing.com/bingbot.htm

2021-02-09 at 02:07PM PST- A user with the IP address of 130.207.188.150 visited the wordpress website and because of that it triggered a alert and notification from wp-cron.php,wp-cron showed that the site of the wordpress was visited, WPCron is usually triggered when a site receives a visit. They then tell the website that they are doing a cron task

2021-02-09 at 05:07PM PST- The user who blogged his research filed a complaint with the support team of wordpress that his research chat and messages were gone and instead modified and replaced by essays that were advertised

2021-02-10 at 10:00 AM PST- The Security Analyst of SecureTechSolutions was notified about the report and started to analyze the incident

2021-02-10 from 10:00 AM PST to 05:00PM PST- The Security Analyst started to find some vulnerabilities in the software, found out what was the problem, reported huge details of what was going on and trying to decide on how to respond to this incident and what measures to take in the future

2021-02-11 from 08:00AM PST to 08:30AM PST – The IT Specialists blocked the specific users with the IP address of 157.75.167.23 and 47.75.76.54 to prevent further access

2021-02-11 from 09:00AM PST to 09:00PM PST- – The developers implemented login attempt limitations in which they only have three attempts to logged in or else they are locked out for 5 minutes for first attempt after the three attempts and the lock out time increases progressively after each failed attempt

2021-02-11 from 09:30PM PST to 11:30PM PST– The IT specialists blocked the User Enumeration requests via GET and POST methods to prevent attackers from identifying valid usernames

2021-02-12 from 04:00 AM PST to 12:00PM PST- The IT specialists resetted all administrator and user passwords immediately, the developers started to implementing hashing and salting on all stored passwords with a hashing algorithm so the attacker can’t see the password or try to find it.

2021-02-12 from 12:00 PM PST to 2:00PM PST- The company was coming up with strong password polcies and requiring a time when every user has to change their password

2021-02-12 from 03:00 PM PST to 8:00PM PST- The IT specialists and Developers decided to enable Multi Factor Authentication to add an extra layer of security

2021-02-12 from 12:00 AM PST to 11:59PM PST- IT Support Specialists remove any suspicious or unauthorized plugins installed during the attacks, they review all the server logs, access logs, or error logs, for any suspicious or unauthorized activity and logins and we monitor unusual login attempts from unknown IP addresses

2021-02-13 from 04:00 AM PST to 06:00AM PST- IT Support Specialists forced logout of all users and required authentication to prevent any session hijacking from happening

2021-02-13 from 06:00 AM PST to 02:00PM PST- Cyber Security Specialists, Developers, and IT Specialists enabled HTTPS by installing an SSL certificate to encrypt communications and prevent any man in the middle attacks from happening and implemented firewalls, the developers implement encryption on the communications, IT specialists went through the process of implementing the firewalls, and Cyber Security Specialists did the process of enabling the HTTPS and getting the certificates of the SSL and configured the security features on the networks

2021-02-13 from 02:00 PM PST to 04:00PM PST- IT Specialists and Developers restricted admin access to certain and limited IP addresses

2021-02-13 from 04:00 PM PST to 09:00PM PST- Developers implemented rate limiting to block users from sending messages at an very high rate

2021-02-13 from 09:00 PM PST to 11:00PM PST-The IT Specialists installled a security plugin to detect or block any threats from happening proactively

2021-02-14 to 2021-02-20(8:00AM PST to 8:00PM PST) - The company’s IT security team(Cyber Security Specialists) then conducted one of its first security audit to find any vulnerabilities and strengthen its defenses

2021-02-20 to 2021-03-04(8:00AM PST to 8:00PM PST)- The IT specialists were in the process of manually recovering the original blog posts/messages of the original modified messages given that there was no backup, it took longer for the IT specialists to recover the message due to a lack of backups

2021-03-05 from 12:00 AM PST to 11:59PM PST – The SOC the created this incident plan report to report the incident, its findings, actions we took, and financial impact

2021-03-06 from 12:00 AM PST to 11:59PM PST – The company mandated all employees and users of the wordpress platform to take cyber security training course for one week on their own time

2021-03-07 at 12:00 AM PST - Everything in this web application was changed and updated after the fixes were made

# Findings

The web application was running its normal activity as usual where the users of the application would access different website and log in, the IP address of 130.207.188.150, whos responsible for managing the visits on the application called wp-cron.php to trigger a alert that someone accessed the web application, wp-cron.php is a WordPress task scheduler that runs when the site is visited. it also detected other usual activity like various users with different IP address accessed the robot.txt file which was usual activity they did both before and after the attack, when the attacker entered the log in page he then performed some kind of brute force attack, to login in as the administrator by adding in “?author=1” at the link of the webpage login url and because of it he was successfully able to log in as the administrator and then found a bunch of users and got their credentials and usernames and modified their message, I know for sure that this wasn’t in SQL injection attack because there was no author attribute in the form nor the wordpress sql file which showed it was a brute force attack, it was a user enumeration attack with the help of a brute force method because the attacker tried to put in“?author=1” to see if the attack was successful and it was successful on the first attempt, based on the to much post methods of xmlrpc.php in the same time page, which tells that there is a brute force attack Attackers can increment the number (?author=2, ?author=3, etc.) to enumerate multiple users which could have also been a brute force attack with user enumeration. The attacker then later logged in to the web application as the administrator on the device he performed the user enumeration attack via brute force. When the attacker performed the user enumeration, the default admin ID was 1 and because of this the attacker brute force its way into the attack, he managed to also use the network tab via inspect when he accessed it on the browser,after he found the admin account id, he then performed a brute force attack to find the username and password in which he eventually found it, after that he sent to much XML cookies which showed that he was implementing a brute force attack by linearly searching through the possible usernames and passwords to make sure it is a valid password and after that let some normal and usual activity happen for a period of time such as a other user sending a blog with a message “like gecko” 5 times, the user whos research blog will get modified and changed with advertised essay papers, he then installed a few plug ins and after the attacker logged out of the device he performed the cyber attack, the attacker then logged into a new device to login in as the administrator from the credentials he found and when he logged in as amin, and when he was in the administrator page, he then went to the edit page of the website which was the edit.php?post\_type=page",which showed that the attacker changed the blogged research information on that page, there was a message that included some reach information and as the administrator who has the power to modify or change any messages. He did some other activity like modify, edit or edit some of the other posts made by the user while on the admin page in which he used it to change the user research blog to essays that were being advertised, the attacker changed all the reached related blogs and posts to advertised essays, the post.php file manages all the posts actions and other things related to the post in which the administration can based on the change to the url, the url part of post.php?post=1&action=edit indicates that the essay is edited, based on the action=edit, it showed that the attacker modified some of the posts already made by the users especially the user who was blogging his research. Because of the user modifying all the posts after he implemented a brute force attack to find the log in information on the page and logged in as the administrator to modify the posts he performed a session hijacking along with a man in the middle attack in which he intercepted the rearch blogs and modified and altered its contents by replacing its reach blog message with its advertised essay files, the web application was insecure because it was on HTTP not HTTPS, which showed that it wasn’t secure, since the attacker was on /wp-admin/aadmin-ajx.php the attackers usually often exploit these endpoints to perform brute-force attacks in which they find information, the end points of /edit.php,/post.php are attempts and access to modify the content in which the attacker did, the attacker attempted to exploit the admin-ajax.php to bypass encryption, it did the user enumeration to perform the attack, the presence of admin-related pages showed that the attacker performed a man in the middle attack and altered the contents of the post made by previous users, he exploited the admin-ajax.php to perform a brute force attack, the HTTP 405 showed that the XML RPC requests were blocked and the attacker tried to exploit it but failed. The user had 27 blogs related to his research that was modified by the attacker. Based on the to much xmlrpc.php post requests sent to much at the time, the attacker was trying implement a brute force attack. When I looked in a SQL file, we noticed that passwords were encoded with the function “utf8mb4\_unicode\_ci”, which is good but not strong enough because the attacker could translate it easily, so we need to hash and salt the passwords to make it harder for the attacker to crack the hash and encoded password during a brute force attack

# Actions Taken

Some actions that we need to take are block the suspicious users with the ip addresses of 157.75.167.23 and 47.75.76.54, we should also limit the number of attempts the user logs into the system lets say if they attempt to log in more than 3 times they are unable to log in or use the application for 5 minutes and if they do it again we slowly increase the time from 5 minutes to 10 minutes, we should also block the user enumeration requests by GET or POST. We also need to create a response plan in which we have to reset all administrator and user passwords immediately, we need to salt and hash all of our passwords in the database in order to prevent the attacker from finding the password, it just encodes and decodes the password which isn’t enough because hackers can find and translate the password easily, so we need to use a hashing algorithm to store our passwords, we also need to require all users to have strong passwords that are long, complex, and unique, we need the users to change their passwords every 4 years. We also need to enable multi factor authentication, since there were no backups available it costed us so much money so we need to install and create backups for every user, we must remove any suspicious or unauthorized plugins installed by the attacks, we must review all server logs like the access logs and error logs for any unauthorized access attempts.We must look for unusual log in attempts from any unknown IP Address, we must all log out and force re authentication to prevent any hijacked sessions. We also must enable HTTPS by installing an SSL certificate, we must encrypt and decrypt all the communications and prevent the MITM attacks. We also must restrict admin access like /wp-admin to certain IP addresses, we also must implement rate limiting to prevent the attacker or anyone sending messages at a fast rate, we should only limit access to admin-ajax to authenticated users. We also must install a security plugin to detect and block threats, we must include regular backups we also must do some more security audits because of this incident. The initial audit will take 6 days ,12 hours for each day and will be done by the cyber security specialists(pentesters, soc, ethical hackers, etc) The IT specialists then had to manually recover and restore the modify the data by looking at the logs because there were no backups installed prior to the incident. It took 8 hours to identify the lost content by checking the access logs. They also had to check the browser history to search for cached versions, when manually rewriting the blog posts each research rakes like 3 hours to restore it to its original form, they also must make final revisions and proofread and ensure the proper structure. They have to rewrite it based on the old access logs, notes, or memory. We also had to configure the routers and switches with security features to make it more secure. We need to limit access to the certain API endpoints to authenticated users which would reduce the surfaces and degree of the attack

# Financial Impact

|  |  |
| --- | --- |
| Item | Cost |
| This section documents the financial impact of the incident | $10 |
| IT Specialist Labor1 | $19,850 |
| Developer Labor2 | $4,340 |
| Cyber Security Specialist Labor3 | $10,400 |
| Data Recovery4 | $7,371 |
| SSL Certificate and HTTPS Setup Costs5 | $2,500 |
| Firewall Costs6 | $4,000 |
| MFA Costs7 | $180 |
| Security Plugin Costs8 | $477 |
| IT Security Audit Costs9 | $26,500 |
| Data Backup Costs10 | $141,000 |
| Customer Service Support Ticket11 | $16 |
| Incident Report Cost | $10 |
| Total | $216,654 |

1. We must first hire IT Specialists to recover the data and fix everything else and it’s the labor they are doing and number of hours for every problem they have to be paid $100 hourly fixing the problem in the midst of a cyber-attack, the IT specialists spent 0.5 hour blocking the suspicious and malicious IP addresses, it took 2 hours for the IT Specialists to block user enumeration GET and POST Requests, it took 8 hours for the IT Specialists to reset all the users usernames and passwords, it took 5 hours for IT specialists to enable two factor authentication, it took 24 hours for IT to remove any suspicious and unauthorized plugins and read through all the user logs, access logs, and manual logs to find any suspicious activity, it took 2 hours for the IT specialists to force log out all the users and reauthenticate them, it took 8 hours for the IT specialists to enable the HTTPS, install the SSL certificate and implement the firewalls, it took 2 hours for the IT specialists to restrict the admin access to certain IP addresses, it took 3 hours for the IT specialists to implement security plugins, it took 12 days(12 hours each day) which totaled to a 144 hours for the IT specialists to manually recover the data and restore it to its original state, it took a total of 198.5 hours of IT Specialist Labor, $100 \* 198.5 hours = $19,850 total
2. We also must have hour developers change and fix all the code in the system, we also need to program and make are current programs more secure and fix all the broken code , and because of this cyber attack the developers would have to be paid $140 an hour for fixing the damages of the cyber attack since the pay of the developer is 1.4 times higher than an IT specialist, it took 12 hours for the developers to implement logic log in attempts and limits and lockouts, it took 8 hours for the developers to hash and salt the passwords with a hashing algorithm, it took 4 hours for the developers implement encryption on the communications, it took 2 hours for the developers to implement restriction logic of certain ip addresses on the wp-admin page, it took 5 hours for the developers to implement the rate limiting logic. It took a total of 31 hours, $140 \* 31 hours = $4,340
3. We also must have cyber security professionals to analyze the damages done from the cyber attack, implement more secure solutions, change the security of the networks, perform the security audit, set up the SSL certificate, make the protocols more secure, and because of this cyber attack the cyber security specialists would have to be paid $130 an hour for fixing the damages of the cyber attack since the pay of the the cyber security specialists is 1.3 times higher than an IT specialists, it took 8 hours for enabling the HTTPS and obtaining the certificates of the SSL, manging the firewalls, configuring the security measures on the networks, then spent 6 days(12 hours on each day) a total of 72 hours performing a security audit doing a variety of things on that security audit related to cyber security, it took a total of 80 hours for the cyber security specialists to do some work, $130 \* 80 hours = $10,400
4. there are logs, we can check the log version history, and cached content and compared both the original and modified message, so each message would cost on average $273 to repair and restore so 27 messages\* $273 = $7,371
5. We must purchase an SSL certificate, it costs $500 per year per certificate and given that so much was modified we need to maintain the certificate for at least 5 years so it would be 5 years \* $500 = $2,500
6. The cost of implementing a firewall in this type of software and the business that manages the software costs $4,000
7. The cost of implementing MFA is $3 per month and lets say we’ll need to maintain it for at least 5 years, 5 \* 12 = 60 months. 60 months \* $3 = $180
8. We also need to install strong and secure security plugings to provide real-time updates, on average a plug in costs $95.43 per year and if we want to have them for 5 years, it would cost $95.43 \* 5 years = $477.14
9. An IT Security Audit costs on average of $26,500, because the pentesters have to purchase ethical hacking tools which cost so much money, they also need specialized tools to look for the vulnerabilities, they need those tools for vulnerability scanning, penetration testing, and risk analysis, the scope of the audit, legal compliance, etc
10. It costs 3 dollars per GB to back up data and given that an average small business uses like 47 TB a year. 47 TB per year \* 1000 GB \* $3 = $141,000
11. Average cost of customer service support ticket is $16.00

# Lessons Learned

This section is not optional.

## Successes

* One thing I learned from this is that we need to look at the link to see if the attacker has put something suspicious or malicious in the link to determine if it is malicious or safe, you need to analyze the link
* I also found out the attacker did a user enumeration and was able to detect it quickly all because of the network logs and in the link it was
* We also prevented the attacker from gaining access to the admin page due to restricting the admin page to a certain IP addresses
* We also must pay attention to the url in order to find the attack, we were able to detect the action early and find out what type it was and we also were able to inform the user and everyone else of the session hijacking within 72 hours based on the General Data Privacy Regulation
* There were execessive XML-RPC requests which showed that we were able to identify that the attacker brute forced its way to finding the admin’s credentials
* In the midst of any cyber attack we should immediately reset all the user and administrator passwords and hash and salt the passwords with an hashing algorithm
* The server logs helped me identify the problem in the server and I looked at the patterns in the sever log to determine if it is unusual, malicious, or normal activity
* I also learned that we should only limit certain end points of websites to certain IP addresses
* We need to implement rate limiting on logic attempts and sending messages to prevent any brute force attacks or the chatting system to crash which would lead an open hole for the attackers
* We also learned that we need to have implemented backups to help us quickly restore the data to its original state, because it would save us so much money in labor costs and the tools used to recover the data
* I also learned that on top of damages done to the information ,there would be labor costs due to the time it will take for them to fix and repair everything in the server
* We were able to learn that we need to make sure not to install plugins immediately we have to make sure that they are safe and secure plug ins
* We were also able to identify the attack based on the access logs, the access logs helped us a lot in determining the type of attack, recovering the old data before it got modified, but it made the data recovery slower because we didn’t have any backups

## Opportunities for Improvement

**Issue:** One thing we could’ve done was that we should scan and analyze the plugin for any malware

**Recommendation:** We can perform a malware analysis on the plug to see if it is free of any viruses or any other malicious software that way it can be safer for it use.

**Action Item Owner:** The malware analyst should be responsible for performing the malware analysis of the plugin and determine if it is safe or not, and if it is not safe they should remove the plugin

**Issue:** Another thing we could’ve done was that we should’ve looked for the automation and bots in the system

**Recommendation:** We could’ve looked at any IP addresses that are public and commonly used in other companies and try to verify the IP address if an actual human being or an robot,

**Action Item Owner:** The SOC will be responsible for identifying if there is are any humans or robots

**Issue:** Another thing we could’ve done was that we should’ve added turing tests to our software to prevent any robot or automation

**Recommendation:** We can add software that asks before log in attempt if they are human or a user by taking a quiz to similar to Completely Automated Public Turing, we need to make sure if it is human or not and if it is not human then we deny them access to the application

**Action Item Owner:** The Cyber Security Software Developers and other Developers of this company will be responsible for developing and writing the code for the Turing tests to prevent the Robots from gaining access to the system

**Issue:** Another thing we could’ve done was implementing Sanctions screening

**Recommendation:** We should verify names, identities, and other information of the designated users and entities on this software to make sure that legitimate users can access it, and anyone with no criminal record can be a legitimate user

**Action Item Owner:** The IT Specialists and Blue Team will be the ones responsible for checking to see if there are legitimate users, if there are any illegitimate users or users with criminal records, they can prevent the users from accessing this software

**Issue:** Another thing we could’ve done was adding a real time monitoring system with security alerts

**Recommendation:** We need to develop a real time monitoring system with security alerts, because it could help detect the attacks earlier and as soon as the attack happens, as soon as there is a malicious activity warnings will pop up everywhere in the business and they can try to stop the attack before it does more damage

**Action Item Owner:** All the Cyber Security Specialists, IT Specialists, and Developers should develop and work on the real time monitoring system with security alerts to test that something malicious happened and when it happens we can immediately try to stop and prevent the current attack or any future attacks from happening.

**Issue:** Another thing we could’ve done was that we could’ve limited the amount of the same HTTP POST requests can be sent for the same action

**Recommendation:** We could’ve had the Network Engineers implemented rate limiting on the networks, and configure the networks to send limited messages at a time

**Action Item Owner:** The Network Engineer should be responsible for configuring the systems and networks to implement a limited amount of traffic to be sent from network to network and limit the number of packets.

# Sources

*What is the average cost of hiring a cyber security expert for an individual or small business (not government)?*. Quora. (n.d.). <https://www.quora.com/What-is-the-average-cost-of-hiring-a-cyber-security-expert-for-an-individual-or-small-business-not-government>

*How much should your SMB budget for cybersecurity?*. business.com. (n.d.). <https://www.business.com/articles/smb-budget-for-cybersecurity/>

Casey.crane. (2021, July 9). *How much does an SSL / HTTPS certificate cost?*. Comodo SSL Resources. <https://comodosslstore.com/resources/how-much-does-an-ssl-https-certificate-cost/>

*Network firewall price: Comparing security costs*. Fortinet. (n.d.). <https://www.fortinet.com/products/network-firewall-pricing#:~:text=Firewall%20Security%20Price,ongoing%20maintenance%20of%20the%20firewall>

10, L. U. M. (2025, March 10). *Top 10 multi-factor authentication software solutions for 2021 - spiceworks*. Spiceworks Inc. <https://www.spiceworks.com/it-security/identity-access-management/articles/top-10-multi-factor-authentication-software-solutions/>

says, L. I. P. (2024, June 11). *9+ best wordpress security plugins to shield your website*. WordPress Tutorial Videos by WP101®. <https://wp101.com/best-wordpress-security-plugins/>

Krishna, A., & Ananda Krishna                              Ananda Krishna is the co-founder & CTO of Astra Security. (2025a, January 7). *How much does an IT security audit cost?*. Astra Security. <https://www.getastra.com/blog/security-audit/it-security-audit-cost/>

Optimalnetwork. (2022, May 10). *How much does data backup cost for small business? - optimal networks: Managed IT services: Washington D.C.* Optimal Networks | Managed IT Services | Washington D.C. - The Premium Provider of IT Services for Legal, Associations, and Consulting Firms. <https://www.optimalnetworks.com/how-much-does-data-backup-cost-for-small-business/>

*How much digital data does an average digital user generate per day and per year?*. Quora. (n.d.-a). <https://www.quora.com/How-much-digital-data-does-an-average-digital-user-generate-per-day-and-per-year>

22, A., & Kidd, C. (2019, August 22). *Cost per ticket: The Ultimate Service Desk Metric*. BMC Blogs. https://www.bmc.com/blogs/cost-per-ticket/