Security Audit Phase 1 Completion

Date: March 22, 2026

Date: 2026-03-20 **Status:** COMPLETE

Completed Actions

1. HSTS Headers Added

Domain	Status
---	---
auth.stsgym.com	Added `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`
bedimsecurity.com	Added HSTS + CSP + Permissions-Policy

2. CSP Headers Added

Domain	CSP
---	---
auth.stsgym.com	`default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net; ...`
bedimsecurity.com	Full CSP with restrictions

3. Secrets Rotated

All hardcoded secrets replaced with secure random values:

Service	Secret Type	New Location
---	---	---
auth-service	SECRET_KEY	`/home/wez/auth-service/.env`
auth-service	DB_PASSWORD	`/home/wez/auth-service/.env`
stsgym-website	SECRET_KEY	`/home/wez/stsgym/.env`
photos-node	SESSION_SECRET	`/home/wez/photos-node/.env`
bedimsecurity	SECRET_KEY	`/opt/bedimsecurity/.env`
bedimsecurity	DB_PASSWORD	`/opt/bedimsecurity/.env`

4. Admin Password Forced Change

```sql UPDATE users SET must_change_password = true WHERE username = 'admin'; ```

Admin will be prompted to change password on next login.
```

5. Docker Compose Updated
All services now use `env_file` directive instead of hardcoded environment variables.

Verification
```bash curl -sI https://auth.stsgym.com | grep -i strict-transport

curl -sI https://auth.stsgym.com | grep -i content-security

curl -s 'https://auth.stsgym.com/api/login' -X POST -H 'Content-Type: application/json' -d '{"username":"admin@stsgym.com","password":"Kuz-m2if"}' ```

---

## Remaining Actions

### Phase 2 (This Week)
1. Implement CSRF protection for all forms
2. Configure Redis for session storage (photos-node, stsphoto)
3. Configure Redis for rate limiting (auth-service, bedimsecurity)
4. Add CSP headers to remaining services (stsgym.com, photos.stsgym.com, etc.)

### Phase 3 (This Month)
5. Replace simple CAPTCHA with reCAPTCHA/hCaptcha
6. Set up Vault or AWS Secrets Manager
7. Enable OCSP stapling for SSL
8. Add security scanning to CI/CD

---

## Files Modified

| File | Change |
|---|---|
| ------ | -------- |
| `/etc/nginx/sites-available/auth.stsgym.com` | Added HSTS, CSP, Permissions-Policy headers |
| `/etc/nginx/sites-available/bedimsecurity.com` | Added HSTS, CSP, Permissions-Policy headers |
| `/home/wez/auth-service/.env` | Created with new secrets |
| `/home/wez/auth-service/docker-compose.yml` | Updated to use env_file |
| `/home/wez/stsgym/.env` | Created with new SECRET_KEY |
```

`/home/wez/stsgym/docker-compose.yml`	Updated to use env_file
`/home/wez/photos-node/.env`	Created with SESSION_SECRET, COOKIE_SECRET
`/opt/bedimsecurity/.env`	Created with new secrets
`/opt/bedimsecurity/docker-compose.yml`	Updated to use env_file

Container Status

All containers running with new secrets:

``` auth-service Up 3 minutes auth-service-db Up 4 minutes (healthy) stsgym-website Up 2 minutes bedimsecurity-web Up 36 seconds bedimsecurity-db Up 41 seconds (healthy) photos-node Up About a minute ```

Completed: 2026-03-20 22:03 MDT
```