گزارش آسیب‌پذیری‌های امنیتی – Penetration Test Report

تاریخ انجام تست: 2025/09/24

تست کننده: nimazerobit

هدف: جیم اسپید | jimspeed.com

---

1. Weak Signup Form Validation & Missing Server-Side Phone/Email Verification

Severity: High

OWASP Category: A01 – Broken Access Control

توضیحات:

در فرآیند ثبت نام پنل کاربری، هیچ **Server-Side Validation** مناسبی برای شماره موبایل و ایمیل اعمال نشده است. کاربر می‌تواند با وارد کردن تنها یک کاراکتر به عنوان شماره موبایل و ایمیل، حساب جدید ایجاد کند.

علاوه بر این، مکانیزم **OTP Verification** برای شماره موبایل عملا بلا استفاده است، چرا که میتوان با ارسال درخواست مستقیم به API ثبت نام بدون تایید کردن شماره موبایل در سایت ثبت نام کرد.

همچنین میتوان با این آسیب پذیری اطلاعات کاربری اشخاص دیگر مانند (ایمیل، شماره موبایل، نام کامل و رمز عبور را با ارسال درخواست به API ثبت نام بدون داشتن رمز عبور قبلی تغییر داد.

مراحل تست (Steps to Reproduce):

1. بررسی درخواست های ارسال شده در مرورگر
2. بررسی کد های جاوا اسکریپت و ارسال دستی درخواست ثبت نام به API
3. مشاهده عدم وجود Server-Side Validation و OTP Verification در API ثبت نام
4. تغییر اطلاعاتی مثل ایمیل و رمز عبور و ارسال مجدد درخواست و مشاهده عدم بررسی وجود اکانت توسط سرور و تغییر اطلاعات اکانت به جای پیغام خطا

Penetration Test Report

```
POST /wp-json/jimspeed/v1/linking/weblink/init HTTP/1.1
Host: jimspeed.com
Content-Type: application/json
{
    "website_user_id": "pentest",
    "username_site": "pentest",
    "email": "pentest",
    "phone": "pentest",
    "fullname": "pentest",
    "password": "pentest"
}
```

اثر امنیتی (Impact):

1. ایجاد اکانت های جعلی (Fake Accounts) بدون محدودیت
2. حذف لایه احراز هویت اولیه کاربران و کاهش قابلیت ردیابی
3. امکان تغییر اطلاعات اکانت ها فقط با داشتن نام کاربری

راهکار (Recommendation):

1. پیاده‌سازی **Server-Side Validation** برای فرمت وارد شده برای شماره موبایل و ایمیل
2. الزام ارسال و تایید **OTP Verification** قبل از ایجاد اکانت یا ادغام با API ثبت نام
3. بررسی وجود مقادیری مثل نام کاربری، ایمیل و شماره موبایل در دیتابیس و تایید یونیک بودن آنها در API ثبت نام
4. استفاده از Captcha های امن برای API ثبت نام جهت کنترل حملات Brute Force

2. Authentication Bypass via Username Only

Severity: ***Critical***

OWASP Category: A07 – Identification and Authentication Failures

توضیحات:

در بخش ورود به اکانت، بعد از ارسال درخواست به API ورود صرفا اطلاعاتی مثل نام کاربری، ایمیل، شماره موبایل و نام کامل دریافت می شود و هیچ **Authentication Token** جهت احراز هویت کاربر دریافت نمی شود و در ادامه با درخواست به API مرتبط با دریافت اطلاعات حساب کاربر میتوان صرفا با ارسال نام کاربری تمام اطلاعات حساب را دریافت کرد. این موضوع منجر به **Account Takeover** و **Account Spoofing** برای هر اکانت در این سیستم می‌شود.

مراحل تست (Steps to Reproduce):

1. ورود به اکانت و بررسی درخواست های مرورگر برای دریافت اطلاعات کاربر
2. بررسی درخواست و عدم مشاهده هیچ گونه Authentication Token جهت تایید هویت واقعی کاربر
3. ارسال مجدد درخواست با تغییر پارامتر نام کاربری و مشاهده دریافت کامل اطلاعات اکانت

اثر امنیتی (Impact):

1. دسترسی کامل غیرمجاز به اکانت کاربران
2. امکان دسترسی به اطلاعات حساس، تغییر تنظیمات و..
3. ریسک بالای Data Breach و نقض حریم خصوصی کاربران

راهکار (Recommendation):

1. الزام ورود رمز عبور و بررسی آن بر اساس الگوریتم‌های امن
2. ثبت دقیق رویداد های ورود به سیستم و تلاش های ناموفق (Security Logging)
3. استفاده از Captcha های امن برای API ورود جهت کنترل حملات Brute Force
4. استفاده از سیستم توکن امن مثل JWT Token یا سایر گزینه ها جهت احراز هویت کاربر

---

3. User Information Disclosure via Mobile Number

Severity: ***Critical***

OWASP Category: A01 – Broken Access Control

توضیحات:

با ارسال یک درخواست به API مربوط به فراموشی رمز عبور و وارد کردن شماره موبایل در پارامتر مربوطه بدون ارسال هیچ گونه کد تاییدی اطلاعات کامل کاربر شامل نام کاربری، ایمیل، شماره موبایل و نام کامل را باز می گرداند.

مراحل تست (Steps to Reproduce):

1. ارسال درخواست فراموشی رمز عبور و بررسی درخواست های ارسال شده در مرورگر
2. مشاهده اطلاعات اکانت در پاسخ API مربوطه قبل از ارسال کد تایید

Penetration Test Report

```
POST /wp-json/jimspeed/v1/webauth/check-phone HTTP/1.1
Host: jimspeed.com
Content-Type: application/json
{
    "phone":"pentest"
}
```

اثر امنیتی (Impact):

1. دسترسی کامل غیرمجاز به اکانت کاربران
2. ریسک بالای Data Breach و نقض حریم خصوصی کاربران
3. افزایش ریسک حمله Account Takeover و Account Spoofing با استفاده از داده های افشا شده

راهکار (Recommendation):

1. جلوگیری از ارسال اطلاعات حساس اکانت قبل از بررسی کد تایید شماره موبایل

اسکریپت پایتون مرتبط با تست و بررسی هر کدام از این آسیب پذیری ها در صورت درخواست برای شما ارسال می شود.

با تشکر 🙏