شرح خدمات فنی

ارزیابی امنیتی و آزمون نفوذپذیری سامانه نرم‌افزاری

مقدمه:

امنیت فضای تولید و تبادل اطلاعات (افتا)، نیازمند ارزیابی امنیتی برنامه‌های کاربردی ازجمله برنامه‌های کاربردی تحت وب[1] است. آسیب‌پذیری‌های[2] برنامه‌های کاربردی، می‌تواند منجر به نفوذ به‌کل سامانه[3] و متعاقباً سوءاستفاده از آن شود. نفوذ گر[4] با طراحی سناریوهای[5] مناسب نفوذ مبتنی بر این آسیب‌پذیری‌ها، به سامانه نفوذ نموده، سپس با ارتقای سطح دسترسی[6] خود، عواقبی جدی برای ذی‌نفعان سامانه‌ها ایجاد می‌کند. این مستند به منظور تشریح و تبیین شرح خدمات و روش کار آزمایشگاه ایریانا، برای ارائه به کارفرمایان تهیه شده است:

هزینه و زمان اجرای فرآیندهای مزبور نیز وفق چارچوب امنیتی OWASP 4.0 – 2017 و آخرین نسخه از متدلوژی‌های ارزیابی OTG, CVSS, ASVS به شرح ذیل توسط این آزمایشگاه قابل انجام خواهد بود:

قیمت پایه به ریال / سطح ارزیابی	(گواهینامه صادره از مرجع داخلی آزمایشگاه ایریانا) نام محصول نرم‌افزاری: سامانه			
جعبه خاکستری (Gray-Box)	Thick Client (C/S–Desktop)	Web Based	Mobile App (Android)	Mobile App (IOS)
سطح صفر (High Risk) OWASP Top 10 - CVSS (Automation Test Tools)				
سطح یک (Medium Risk) ASVS – L1				
سطح دو (Low Risk) ASVS - L2				
سطح سه (Minimum Risk) ASVS - L3 (Full Pack)				
زمان اجرای آزمون	**دو هفته**	**دو هفته**	**سه هفته**	**چهار هفته**

همچنین توجه کارفرمایان محترم را به نکات ذیل نیز جلب می‌نماید:

[1] Web-based Application
[2] Vulnerabilities
[3] System
[4] Attacker
[5] Scenario
[6] Privilege Escalation

۱) سطح ارزیابی امنیتی کاملاً با نظر و به انتخاب کارفرمای محترم می‌باشد ولیکن تحت هیچ شرایطی نیاز به ارائه و بررسی کد منبع برنامه (Source Code Review) توسط آزمایشگاه وجود ندارد (No White-Box Pen-Test).

۲) در فرآیند ارزیابی سامانه‌های تحت وب و برنامکها (موبایل)، نیازی به نصب سیستم در محل آزمایشگاه و ارائه هیچگونه مستندی وجود ندارد و فرآیند تست صرفاً از راه دور و از طریق یک آدرس معتبر اینترنتی (Valid-IP) همراه با دو کد کاربری و رمز عبور (ادمین/کاربرعادی) قابل انجام می‌باشد. در این حالت پس از انجام آزمون، گزارش نتایج تست بانضمام شواهد مستدل (فیلم و عکس) به کارفرما ارائه می‌گردد و در صورت عبور موفق سامانه از آزمون ذیربط، گواهینامه تائید امنیتی محصول با اعتبار یکساله صادر و ارائه خواهد شد.

۳) برای سامانه‌های تحت وب، استفاده از SSL معتبر و فعال بودن سامانه بر روی پروتکل HTTPS و همچنین غیرفعال بودن همزمان آن بر روی پروتکل HTTP کاملاً الزامی می‌باشد.

٤) فرآیند ارزیابی امنیتی، مبتنی بر چارچوب OWASP 4.0 (2017) و متدلوژی‌های ارزیابی OTG, ASVS, CVSS به همراه انواع حملات سایبری (XSS, CSRF, Brute-Force, ...) و آزمون‌های نفوذپذیری از جمله: تزریق دستورات SQL ، هک، کرک و... به صورت خودکار/دستی می‌باشد.

۵) شرایط و نحوه پرداخت هزینه‌ها، به شرح می‌باشد:

a. پرداخت ۱۰۰٪ قیمت پایه قبل از شروع دور اول ارزیابی (تست اولیه)
b. پرداخت ۷۵٪ قیمت پایه قبل از شروع دور دوم ارزیابی (تست ثانویه) به صورت مازاد و در صورت نیاز
c. پرداخت ۵۰٪ قیمت پایه قبل از شروع دور سوم (چهارم و...) ارزیابی به صورت مازاد و در صورت نیاز

تبصره: پس از انجام آزمون اولیه، گزارش نتایج تست بانضمام شواهد مستدل (فیلم و عکس) به کارفرما ارائه میگردد. طبیعتاً چنانچه در این فاز، سیستم با موفقیت از آزمونهای مربوطه عبور نماید، در همین مرحله گواهینامه مزبور صادر و ارائه می‌گردد و نیازی به تست دوم و پرداخت هزینه مازاد نخواهد بود.

در غیر این صورت، هر زمان که با اعلام رسمی کارفرما، نسخه جدید (سامانه اصلاح شده) آماده تست مجدد شد، مرحله بعدی ارزیابی (با شرایط پرداختی فوق) جهت صدور گواهینامه به اجرا در می‌آید.

٦) در هر یک از فازها (مراحل) ارزیابی، در صورت عدم موفقیت سیستم در عبور از آزمون مربوطه، هزینه تکرار فاز بعدی آزمون، بر اساس مفاد مندرج در بند ۵ به صورت جداگانه (مازاد) می‌بایست پرداخت گردد.

۷) در انتهای کار یک فقره فاکتور قطعی و نهایی مشتمل بر ۹٪ مالیات بر ارزش افزوده (همراه با گواهی معتبر) با موضوع "فروش تست پلن، تست شیت و تست ریپورت سامانه ..." به کارفرما ارائه خواهد شد که برابر با کل مبالغ پرداختی توسط کارفرما بدون هرگونه کسوراتی می‌باشد.

۸) از آنجائیکه گواهینامه صادره کاملاً محصول محور است (با ذکر دقیق نام سامانه و شماره ورژن)، لذا درصورت وجود مجموعه‌ای از زیرسامانه‌ها در قالب یک سامانه جامع با اسم تجاری مستقل، فرآیند آزمون بصورت کاملاً یکپارچه، جامع، پیوسته و همزمان اجرا خواهد شد مشروط به آنکه کل سامانه از یک فرم و فرآیند واحد جهت ورود به سامانه استفاده نمایند **(SSO : Single Sign on)**. در غیر این صورت، هر سامانه جداگانه و مستقل محسوب خواهد شد.

۹) جمع‌بندی نهایی و خلاصه نتایج تست نفوذپذیری، وفق جدول ذیل به کارفرما ارائه خواهد شد:

برنامه‌های کاربردی رومیزی و کلاینت/سرور ویندوز	CVSS	رتبه‌بندی	نتیجه
Invalidated input	۰,۰	–	–
Weak authentication & session management	۰,۰	–	–
Critical data in files & registry	۰,۰	–	–
Sensitive data in memory	۰,۰	–	–
Impersonating a high privilege user	۰,۰	–	–
Mitigating risks	۰,۰	–	–
برنامه‌های کاربردی تحت وب	**CVSS**	**رتبه‌بندی**	**نتیجه**
آزمون جمع‌آوری اطلاعات	۰,۰	–	–
آزمون پیکربندی و مدیریت استقرار	۰,۰	–	–
آزمون مدیریت هویت	۰,۰	–	–
آزمون اصالت‌سنجی	۰,۰	–	–
آزمون مجازشماری	۰,۰	–	–
آزمون مدیریت نشست	۰,۰	–	–
آزمون اعتبارسنجی داده‌ها	۰,۰	–	–
آزمون مدیریت خطاها	۰,۰	–	–
آزمون رمزنگاری	۰,۰	–	–
آزمون منطق کسب‌وکار	۰,۰	–	–
آزمون سمت مشتری	۰,۰	–	–
برنامک‌های موبایل (Android / IOS)	**CVSS**	**رتبه‌بندی**	**نتیجه**
آزمون معماری طراحی و مدلسازی تهدید	۰,۰	–	–
آزمون حافظه داده‌ای و حریم شخصی	۰,۰	–	–
آزمون رمزنگاری	۰,۰	–	–
آزمون احراز هویت و مدیریت نشست	۰,۰	–	–
آزمون ارتباطات شبکه‌ای	۰,۰	–	–

آزمون تعامل بسترهای نرم‌افزاری	۰,۰	–	–
آزمون مهندسی معکوس روی برنامک	۰,۰	–	–
آزمون کیفیت کد	۰,۰	–	–
آزمون دستکاری کد	۰,۰	–	–
آزمون عملکردهای اضافی	۰,۰	–	–

☑ **شرط اخذ گواهی تائیدیه امنیتی محصول (با اعتبار یکساله) آنست که:**

- **برای سامانه‌های رومیزی و کلاینت/سروری؛ از مجموع ۶ مورد فوق، حداقل ۴ مورد سبز رنگ (قبول) و حداکثر ۲ مورد زرد رنگ (کم خطر) باشد.**
- **برای سامانه‌های تحت وب و موبایل؛ از مجموع ۱۱ مورد فوق، حداقل ۶ مورد سبز رنگ (قبول) و حداکثر ۵ مورد زرد رنگ (کم خطر) باشد.**

ساختار موارد آزمون

بر اساس مدل اجرایی، از روشگان OWASP Mobile Security Testing Guide، موارد آزمون در این گزارش، می‌تواند در ارتباط با یک یا چند مورد آزمون از روشگان اصلی بوده؛ و نیز به یک یا چند کلاس مربوط باشد. همچنین هر مورد آزمون در این گزارش حاوی بخش‌های زیر است:

- **نام آزمون**[۷]: در این بخش عنوان موارد آزمون مشخص می‌شود.
- **شرح آزمون**[۸]: در این بخش، شرحی از کنترل‌های مورد ارزیابی و آسیب‌پذیری‌های مرتبط با هر مورد آزمون، ارائه می‌شود.
- **نتیجه آزمون**[۹]: در بخش، نتیجه هر آزمون، با یکی از ۴حالت زیر مشخص می‌شود:
  - **قبول**: به این معنی است که محصول مورد ارزیابی، مورد آزمون را برآورده کرده است.
  - **مردود**: به این معنی است که محصول مورد ارزیابی این مورد آزمون را برآورده نکرده است.
  - **ناموجود**: به معنی آن است که این آزمون به هر دلیلی ازجمله درخواست کارفرما و یا عدم وجود عملکرد مربوطه در محصول مورد ارزیابی، انجام‌نشده است
  - **نامشخص**: به معنی آن است که این آزمون به هر دلیلی ازجمله عدم کارکرد صحیح عملکرد مربوطه در محصول مورد ارزیابی و یا عدم وجود دسترسی کافی برای انجام آزمون، انجام‌نشده است.
- **رتبه‌بندی خطر:** در این بخش رتبه‌بندی کمی CVSS[۱۰] برای هر مورد آزمون، بر اساس نسخه‌ی ۳/۱ ارائه می‌شود.

[7] Test Case

[8] Description

[9] Status

[10] Common Vulnerability Scoring System

- **شواهد آزمون**[11]: در این بخش، توضیح نتایج و دلایل احتمالی مربوط به وضعیت آزمون و راه‌کارهای سطح بالایی به‌منظور راهنمایی مخاطب در درک بهتر مورد آزمون و برطرف نمودن ایرادات احتمالی به‌صورت مختصر ارائه می‌شود. همچنین اثبات نتایج به‌دست‌آمده در هر مورد آزمون، به‌صورت تصویر یا عکس و یا ارجاع به پرونده‌های دیگر ارائه می‌شود.

CVSS v3.1

رتبه‌بندی آسیب‌پذیری[12]های کشف‌شده بر اساس بانک اطلاعاتی CVE[13] طبقه‌بندی می‌گردد. در این بانک اطلاعاتی، از سیستم ارزش‌گذاری CVSS استفاده شده است. به‌منظور محاسبه‌ی CVSS V3.1، می‌توان از محاسبه‌گری که توسط موسسه ملی استاندارد و تکنولوژی ایالات‌متحده[14] در آدرس زیر فراهم آمده است استفاده نمود:

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

در نگاشت کمی به کیفی این رتبه‌بندی، آسیب‌پذیری‌های **بحرانی** (Critical)، **پرخطر**(High)، **خطرناک**(Medium) و **کم‌خطر**(Low)، مطابق با جدول ۱ زیر با رنگ‌های متفاوت مشخص‌شده‌اند.

درنهایت نیازمندی‌های امنیتی براساس چک لیست OWASP تطبیق داده شده و در بخش نتایج گزارش آورده می‌شود:

جدول ۱: راهنمای رتبه‌بندی CVSS نسخه‌ی ۳/۱

رتبه‌بندی آسیب پذیری	بازه‌ی امتیاز CVSS 3.1
بحرانی	9.0 - 10
پرخطر	7.0 – 8.9
خطرناک	4.0 – 6.9
کم‌خطر	0.1 – 3.9
قبول	0.0

[11] Evidence

[12] Bug

[13] Common Vulnerabilities and Exposure

[14] National Institute of Standards and Technology (NIST)