گزارش ارزیابی : PIHUNTER

شناسه سند : ۲۲-۱۲۱۱۴۰۰

مقدمه

این گزارش، در تاریخ [۱۴۰۳/۰۹/۰۲] توسط تیم امنیت سایبری پی هانتر به منظور ارزیابی امنیتی و آزمون نفوذ برنامه‌های کاربردی مجموعه .... ارائه شده است. هدف از این تست، شناسایی آسیب‌پذیری‌ها و نقاط ضعف در سیستم‌های مجموعه .... به منظور بهبود امنیت و حفاظت از اطلاعات کاربران می‌باشد.

تست نفوذ به عنوان یک ابزار کلیدی در ارزیابی امنیت، به ما این امکان را می‌دهد تا با شبیه‌سازی حملات سایبری، نقاط ضعف موجود را شناسایی کرده و راهکارهای عملی برای رفع آن‌ها ارائه دهیم. نتایج این گزارش شامل تحلیل‌های دقیق، یافته‌ها و پیشنهادات بهبود خواهد بود که به مجموعه ..... در تقویت زیرساخت‌های امنیتی‌اش کمک خواهد کرد.

اطلاعات سند		
نام پروژه	پروژه تست و نفوذ	
اطلاعات سند	تاریخ تهیه سند	۱۴۰۳/۰۹/۰۲
	تهیه کننده سند	مهدی مرادلو
	تعداد صفحات	۱۰۱
متدلوژی و نوع آزمون	OWASP WSTG V4.2	
روش آزمون	Grey Box Testing	
بالاترین سطح دسترسی	.....	
حساب کاربری استفاده شده در این آزمون	شماره همراه	.....
	ایمیل	.....
	حساب بانکی	.....
محل انجام تست	محل انجام تست در محل پیمانکار، از طریق اینترنت	
محیط مورد آزمون	محیط عملیاتی	
آدرس IP آزمونگر	.....	

PiHUNTER

فهرست مطالب

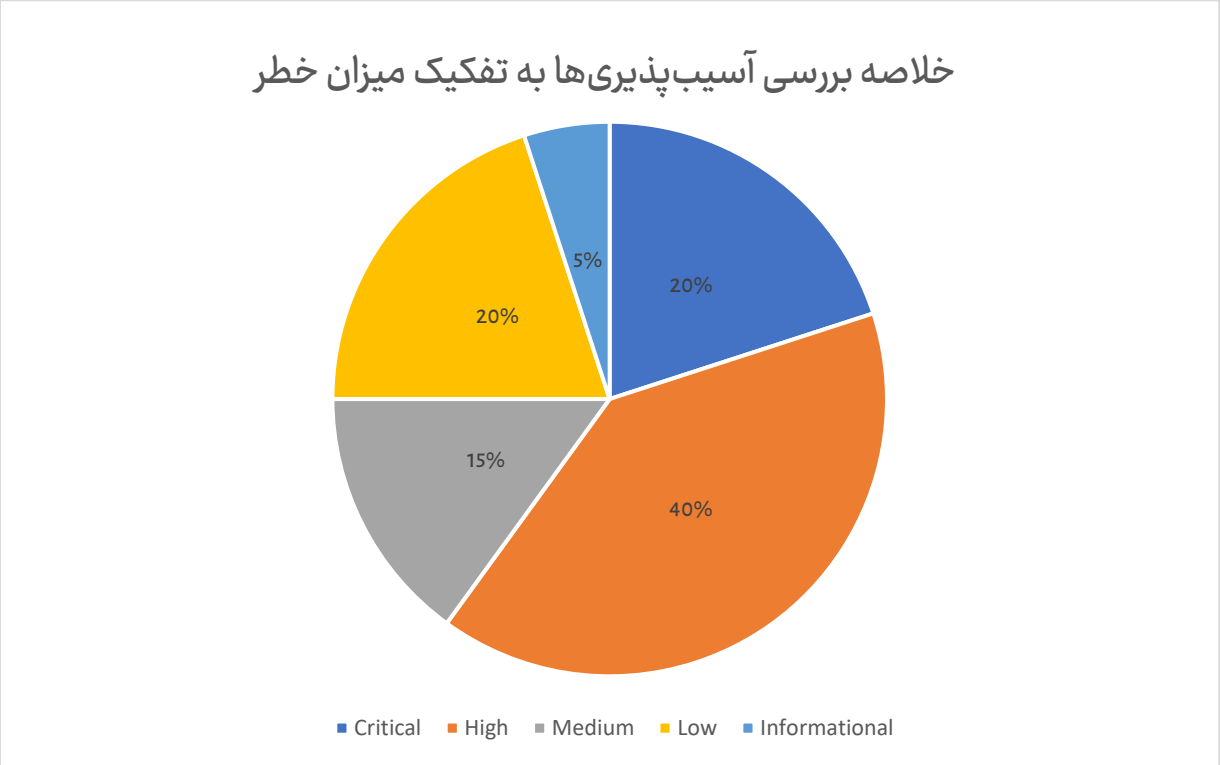
PIHUNTER

گزارش مدیریتی

در این بخش به بررسی آماری آسیب‌پذیری‌های یافت‌شده در قالب یک گزارش مدیریتی پرداخته می‌شود. وضعیت سامانه در برابر هر یک از موارد بررسی‌شده در آزمون، در قالب یک جدول گزارش شده است. در انتها نیز نظر کارشناسی گروه ارزیابی امنیتی و آزمون نفوذ پی هانتر در مورد وضعیت امنیتی کاربردی برنامه شما ارائه شده است.

بررسی آماری آسیب پذیری های سامانه

در این بخش، خلاصه‌ای از آسیب‌پذیری‌های یافت‌شده در پروژه تست و نفوذ شما، به تفکیک شدت خطر آسیب‌پذیری‌ها، ارائه شده است.



نظر کارشناسان تست نفوذ:

.....

ابزار های مورد استفاده در پروژه تست و نفوذ	
Nuclei	ابزاری برای اسکن هدفمند بر اساس الگوهای آسیب‌پذیری‌های کشف شده است.
Nmap	ابزاری برای پویش شبکه و سرویس است.
SQLmap	ابزای برای شناسایی نقاط ضعف مرتبط با تزریق پایگاه داده و ایجاد دسترسی در وب‌سرور از طریق حملات تزریق پایگاه داده است.
Acunetix	پویش‌گری تخصصی برای ارزیابی آسیب‌پذیری‌های مرتبط با برنامه‌های کاربردی تحت .وب است
Metasploit	نرم‌افزار تخصصی آزمون نفوذ بر روی سکوها، سیستم‌عامل‌ها و کتابخانه‌ها است.
DirSearch/ katana	جستجوگر تمام‌خودکار برای اجرای حملات خزش در وب‌سایت و شناسایی موارد مخفی است.
dalfox	ابزاری برای کشف URL های آسیب‌پذیر در سامانه است.
corsy	ابزاری برای کشف آسیب‌پذیری‌های CROS در سامانه است.
subjs	ابزاری برای آنالیز و بررسی حملات بر روی فایل‌ها JavaScript است.
broken-link-checker	ابزاری برای تشخیص منابعی که از سایت‌های دیگر فراخوانی شده‌اند و دچار مشکل شده اند است.
pihunt	ابزار اختصاصی تیم پی هانتر برای شناسایی اتوماتیک آسیب پذیری ها .
Burp Suite	یک ابزار جامع تست نفوذ وب است که برای شناسایی و بهره‌برداری از آسیب‌پذیری‌های امنیتی در برنامه‌های وب استفاده می‌شود

جمع بندی و خلاصه آسیب پذیری ها

در جدول زیر، خلاصهٔ نتایج ارزیابی امنیتی و آزمون نفوذ سامانهٔ «.....» ارائه شده است. جزئیات مربوط به این موارد آزمون شامل توصیف، علت و شواهد اثبات، علت وقوع آسیب‌پذیری و راهکارهای امن‌سازی در فصل بعد به تفصیل آمده است

[جدول فهرست آسیب پذیری ها]

بررسی ساختار هر آزمون

عنوان گزارش آسیب پذیری	
وضعیت	**شدت آسیب پذیری**
--	--
cvss v3 vector	**cvss v3 Score**
--	--
روش شناسایی آسیب پذیری	**قابلیت شناسایی در سطح**
--	--
مسیر های آسیب پذیر	
--	
علت و شواهد اثبات آسیب پذیری	
--	
فایل کامل درخواست	**فایل اثبات و مراحل بهره برداری**

--	--
راه کارهای امن سازی	
--	

وضعیت آزمون:

- **Passed** به معنی عدم وجود آسیب‌پذیری مرتبط با مورد آزمون در سامانه می‌باشد.
- **Failed** به معنی وجود آسیب‌پذیری مرتبط با مورد آزمون در سامانه می‌باشد.
- **Not Accessible** به معنی عدم امکان بررسی مورد آزمون با توجه به دسترسی‌های موجود (جعبه خاکستری) می‌باشد. در این حالت، آسیب‌پذیری موضوعیت دارد، اما امکان دسترسی به عملکرد مربوطه با توجه به سطوح دسترسی آزمون میسر نبوده و به همین دلیل این مورد آزمون بررسی نشده است.
- **Not Applicable** به معنی عدم وجود عملکرد مرتبط با این مورد آزمون در سامانه می‌باشد. لذا مورد آزمون در سامانه موضوعیت ندارد.

شدت آسیب پذیری ها :

در ارزیابی آسیب‌پذیری‌ها، شدت آسیب‌پذیری‌ها به چهار دسته تقسیم می‌شود:

- **بحرانی (Critical) :** آسیب‌پذیری‌های بحرانی نیاز به پاسخ فوری دارند و بهره‌برداری از آن‌ها می‌تواند به افزایش سطح دسترسی بر روی سیستم قربانی و داده‌های حساس منجر شود. این آسیب‌پذیری‌ها تأثیر مستقیم بر کنترل‌های نظارتی و دسترسی به اطلاعات حساس دارند.
- **زیاد (High) :** آسیب‌پذیری‌هایی با رتبه‌بندی شدت زیاد نیاز به رفع فوری دارند. بهره‌برداری از آن‌ها می‌تواند دسترسی مهاجم به سیستم یا داده‌های حساس را فراهم کند، هرچند که دسترسی به میزبان‌های دیگر در آن محیط ممکن نیست.

- **متوسط (Medium):** آسیب‌پذیری‌هایی با شدت متوسط نیازمند بررسی و رفع در زمان کوتاه هستند. این آسیب‌پذیری‌ها ممکن است به مهاجم اجازه دهند به داده‌های حساس دسترسی پیدا کنند یا در صورت ترکیب با دیگر آسیب‌پذیری‌ها، سناریوهای پیچیده‌تری را ایجاد کنند.
- **پایین (Low):** آسیب‌پذیری‌های با شدت پایین ممکن است اطلاعاتی را به کاربران غیرمجاز نشت دهند، اما در حال حاضر تهدیدی جدی برای کسب‌وکار سامانه محسوب نمی‌شوند. این آسیب‌پذیری‌ها تنها ممکن است به نشت اطلاعات اضافی منجر شوند و به فرد نفوذگر در طراحی حملات هدفمند کمک کنند.
- **اطلاعاتی (Informational):** آسیب‌پذیری‌هایی که تنها به نشت اطلاعات اضافی منجر می‌شوند و به نفوذگر در طراحی حملات هدفمند یاری می‌رسانند.

CVSS:

cvss یک استاندارد امتیازدهی به آسیب‌پذیری وجود دارد که شرکت پی هانتر در راستای بررسی میزان خطر هر آسیب‌پذیری از آخرین نسخهٔ آن (نسخهٔ 3) استفاده می‌کند. در این نسخه از این سازوکار، 8 پارامتر بررسی شده تا امتیاز نهایی که عددی بین صفر تا ده می‌باشد، محاسبه گردد. طبیعی است که هر چه عدد به سمت ده نزدیک‌تر شود، به معنی بالاتر بودن شدت آسیب‌پذیری است.

پارامترهای مرتبط به همراه توضیحات مختصر در جدول زیر آمده است:

کلاس	نام پارامتر	توضیحات
Exploitability Metrics	Attack Vector	محلی که بهره برداری از آسیب پذیری امکان پذیر است.
	Attack Complexity	میزان سختی بهره برداری از آسیب پذیری
	Privileges Required	میزان دسترسی که نفوذگر برای بهره برداری از آسیب پذیری نیاز دارد
	User Interaction	بررسی اینکه جهت بهره برداری از آسیب پذیری ایا نیاز به تعامل قربانی هست یا خیر

	Scope	آیا با بهره برداری از آسیب پذیری ، محدودهٔ آزمون تغییر میکند یا خیر
Impact Metrics	Confidentiality	میزان تأثیر آسیب پذیری بر روی محرمانگی سامانه
	Integrity	میزان تأثیر آسیب پذیری بر روی یکپارچگی سامانه
	Availability	میزان تأثیر آسیب پذیری بر روی دسترس پذیری سامانه

همچنین مقادیر ممکن برای هر یک از پارامترها در جدول زیر آمده است:

کلاس	نام پارامتر	مقادیر ممکن
Exploitability Metrics	Attack Vector [AV]	Network (AV:N)
		Adjacent (AV:A)
		Local (AV:L)
		Physical (AV:P)
	Attack Complexity [AC]	Low (AC :L)
		High (AC:H)
	Privileges Required [PR]	None (PR:N)
		Low (PR:L)
		High (PR:H)
	User Interaction [UI]	None (UI:N)
		Required (UI:R)
	Scope [S]	Unchanged (S:U)
		Changed (S:C)
Impact Metrics	Confidentiality [C]	None (C:N)
		Low (C:L)

		High (C:H)
	Integrity [I]	None (I:N)
		Low (I:L)
		High (I:H)
	Availability [A]	None (A:N)
		Low (A :L)
		High (A:H)

در انتها، در مورد هر آسیب‌پذیری، پس از تعیین مقادیر مربوط به هر پارامتر، محاسبات مشخصی صورت گرفته که به دلیل پیچیدگی، توضیحات در این مستند نیامده است. پس از محاسبه، دو پارامتر زیر در جدول قرار داده می‌شود:

- Score(امتیاز): امتیاز محاسبه‌شده بر اساس پارامترهای مقداردهی‌شده.
- Summary (خلاصه): خلاصه‌ای از مقادیر مربوط به هر یک از پارامترها که از طریق جدول 11 قابل کدگشایی است.

روش شناسایی آسیب پذیری :

در این بخش نحوه یافتن آسیب پذیری توسط تیم پی هانتر مشخص شده است که شامل موارد زیر است:

- به صورت دستی توسط کارشناسان پروژه
- توسط ابزارهای عمومی
- توسط ابزارهای توسعه داده شده تیم پی هانتر

قابلیت شناسایی در سطح

- جعبه سیاه
- جعبه خاکستری(کاربر مدیر)

- جعبه خاکستری(کاربر غیر مدیر)

مسیر های آسیب پذیر

مسیر هایی که آسیب پذیری در آن رخ داده در این قسمت قرار می گیرد

علت و شواهد اثبات

در این بخش، علت وقوع آسیب‌پذیری‌ها به همراه مراحل شناسایی آن‌ها توسط گروه ارزیابی امنیتی و آزمون نفوذ پی هانتر، به طور دقیق توضیح داده خواهد شد. این توضیحات شامل دلایل اثباتی و شواهد مربوطه، از جمله توضیحات و عکس‌های مربوطه، با جزئیات کافی ارائه می‌شود.

فایل کامل درخواست

درخواست ارسالی در یک فایل متنی ذخیره شده و نام فایل در این بخش قرار می گیرد

فایل اثبات و مراحل بهره برداری

فایل تصویری و مراحل بازآفرینی آسیب پذیری در این بخش قرار می گیرد

راهکار های امن سازی

در این بخش، راهکار های برطرف سازی آسیب پذیری و شیوه آن بیان می شود.