



Penetration Testing Services

Identifying Vulnerabilities Before Hackers Do



www.grct.net

Summary



OUR PENETRATION TESTING SERVICES



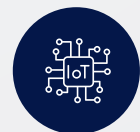
WHY ADVANCED PENETRATION?



WHY MOBILE APP SECURITY TESTING?



IMPORTANCE OF SOURCE CODE REVIEW



WHY IOT PENETRATION TESTING ?



WHY APPLICATION PENETRATION TESTING ?



Our Penetration Testing Services

1

Advanced Penetration Testing

2

Mobile App Security Testing

3

Source Code Review

4

IoT Penetration testing

5

Application Penetration Testing



WHY **ADVANCED PENETRATION TESTING?**

- **Protect Sensitive Data** Prevent unauthorized access to critical business and customer information
- **Prevent Financial Loss** Avoid costs associated with data breaches, downtime, and reputational damage
- **Ensure Compliance** Meet industry regulations like PCI DSS, ISO 27001, SOC 2, and GDPR
- **Mitigate Risks** Address vulnerabilities in application design, configuration, and code before attackers do



WHY MOBILE APP SECURITY TESTING?

01

Prevent Data Breaches

Detect and fix security vulnerabilities before attackers exploit them

02

Build Customer Trust

Secure apps enhance user confidence, driving adoption and business growth

03

Ensure Compliance

Meet regulatory requirements like PCI DSS, GDPR, HIPAA, and OWASP by implementing robust security measures





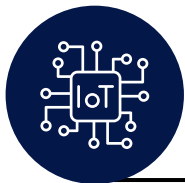
IMPORTANCE OF **SOURCE CODE** REVIEW

- **Prevent Cybersecurity Breaches** by Conducting regular source code reviews
- **Ensure Regulatory Compliance** by reviewing your application to meets industry-specific compliance standards
- **Improve Code Quality and Performance** by enhanceing your code's quality, functionality, and stability
- **Minimize Security Risks** by reviewing your source code to helps detect backdoors, insecure configurations, and other risks
- **Reduce Long-Term Costs** by fixing vulnerabilities during early developments

```
self.fingerprints = ...
self.logdups = True
self.debug = debug
self.logger = logging.getLogger(__name__)
if path:
    self.file = open(os.path.join(log_dir, 'fingerprint.log'), 'a')
    self.file.seek(0)
    self.fingerprints.update({e: r})

def request_seen(self, request):
    fp = self.request_fingerprint(request)
    if fp in self.fingerprints:
        return True
    self.fingerprints.add(fp)
    if self.file:
        self.file.write(fp + os.linesep)

def request_fingerprint(self, request):
```

WHY IOT PENETRATION TESTING ?

01

Detect Weaknesses

Uncover security gaps in hardware, software, APIs, and communication protocols

02

Protect Sensitive Data

Prevent unauthorized access and data breaches

03

Stop Cyberattacks

Secure IoT networks from hacking, tampering, and malicious threats

04

Ensure System Integrity

Test interoperability, performance, and end-to-end security across devices and cloud platforms

05

Meet Compliance Standards

Align with industry security frameworks like ISMS risk assessments





WHY APPLICATION PENETRATION TESTING ?

- **Prevent Data Breaches** Identify security loopholes before hackers do
- **Ensure Compliance** Meet regulatory requirements such as GDPR, ISO 27001, and PCI-DSS
- **Protect Customer Trust** Secure your applications to maintain brand reputation and user confidence
- **Reduce Remediation Costs** Address vulnerabilities early in the development cycle.
- **Strengthen Security Posture** Get a detailed remediation plan to improve your defense mechanisms

