VULNERABILITY ASSESSMENTS
VIRTUE SECURITY
ETHICAL HACKING CONSULTING
NEW YORK, NY

VIRTUE
SECURITY

APPLICATION VULNERABILITY ASSESSMENTS

Application assessments test the bounds of security controls to determine the impact a malicious user could have, including access to other user data, compromise of the server itself, and manipulation of business logic to perform unauthorized actions. Even applications used by entrusted users can be at a high risk of attack and may be vulnerable to some of the following vulnerabilities:

CROSS-SITE SCRIPTING (XSS)	SQL INJECTION	CROSS-SITE REQUEST FORGERY
PRIVILEGE ESCALATION	FORCEFUL BROWSING	COMMAND EXECUTION
URL REDIRECTION	BYPASS OF BUSINESS LOGIC	LDAP INJECTION

APPLICATIONS SUFFER FROM UNIQUE VULNERABILITIES

Applications are unique in many ways, and the vulnerabilities affecting them are no different. While there are hundreds of different attack types documented, a substantial number of vulnerabilities are always unique to each application. A manual analysis is the only true way to identify such threats that directly impact business operation.

Application security testing is a true meeting place of art and science. When sensitive business workflows blend with cutting edge technology, vulnerabilities can exist at any point in the mix. A compromise of an application can result from simple arithmetic errors or complex injection attacks; because of this application security testing requires deep technical skills as well as a creative mindset.

A UNIQUE TESTING PROCESS

Our testing process has a backbone built from industry standard methodologies including OWASP and OSSTMM. While we use a wide variety of commercial, open source, and proprietary tools to conduct our tests, nothing can replace years of experience in reverse engineering and security research. Our process is dynamic and is designed to assess the unique functions of each application.

STAGES OF AN APPLICATION VULNERABILITY ASSESSMENT

- ▶ GATHER UNNECESSARY OR SENSITIVE INFORMATION
- ▶ IDENTIFY WEAK OR BROKEN ENCRYPTION
- ▶ AUTHENTICATION AND SESSION MANAGEMENT REVIEW
- ▶ ESCALATE USER PRIVILEGES
- ▶ INPUT VALIDATION TESTING
- ▶ IDENTIFY UNIQUE LOGICAL ATTACKS
- ▶ APPLICATION FRAMEWORK AND TECHNOLOGY EVALUATION
- ▶ EVALUATE USE OF BROWSER CONTROLS

MEANINGFUL SECURITY

Our reports document all evidence required to confirm and reproduce vulnerabilities, removing false positives and allowing IT staff to take immediate action. All vulnerabilities on our reports include strategies for remediation that promote secure coding practices to reduce vulnerabilities going forward.

NETWORK PENETRATION TESTING

Penetration testing is the most effective way to identify vulnerabilities in network infrastructure. Virtue Security assessments provide the most accurate view of what an attacker sees when trying to penetrate network infrastructure. This testing combines comprehensive network scans with manual penetration testing to identify vulnerabilities across your network.

BEYOND A NETWORK SCAN

Proper tools are an essential part of network security testing, which is why we've built our manual testing process on top of industry leading products. This allows us to combine a detail oriented methodology with automated testing that scales. Our focus on research and process improvement allows us to discover more vulnerabilities than standalone products. Our testing begins where automated tools leave off.

1 ATTACK SURFACE DISCOVERY
Enumerate all protocols, ports, and services across an IP range.

2 SERVICE DETECTION
Fingerprint software and service versions for known vulnerabilities.

3 FIREWALL EVASION
Attempt to bypass firewall rules and interact with restricted services.

4 VULNERABILITY EXPLOITATION
(optional) Gain access and escalate privileges to demonstrate impact.

5 ANALYSIS
Manually review web applications, extraneous services, and perform additional testing.

6 REPORT
Prioritize vulnerabilities, document technical details, and provide remediation strategy.

REDUCE EXPOSURE AND CLOSE GAPS

Threat landscapes have changed and critical vulnerabilities are being discovered more often than ever. Vulnerabilities like Heartbleed and Shellshock have proven that widely used and trusted services are no longer immune from critical vulnerabilities. Although protecting against the unknown is challenging, risk can be mitigated by reducing the number of services exposed to the internet. We design our assessments to provide metrics that reveal exactly what is exposed to the internet, and that allow IT staff to reduce the likelihood of future security breaches.

MANAGE THE INSIDER THREAT

The concept of an external perimeter is rapidly vanishing. BYOD, phishing emails, and IoT devices are increasing the exposure of internal networks more than ever. What was once viewed as a safe haven is now one of the most challenging assets to secure. An internal penetration test is the first step to close vulnerabilities that would allow an attacker to gain a foothold inside your network. In a large organization, security incidents can no longer be prevented, but they can be mitigated and responded to. Protecting internal infrastructure is a top priority in today's most security driven institutions.

SYSTEM HARDENING

A system configuration review evaluates server or workstation security settings with widely adopted and trusted standards. This is an essential process for hardening critical servers as well as deploying a "gold image" for user workstations. By creating hardened baselines, vulnerabilities can be identified and fixed before being deployed hundreds of times across an organization. This process saves substantial cost in vulnerability remediation over time and creates a strong foundation for users and applications. System hardening is also a core principle of defense in depth strategies. Host systems are a vital layer of security and cannot be overlooked in any sustainable security process.

USER ACCOUNT POLICIES	SYSTEM AUDITING	INTERNAL SYSTEM FUNCTIONS
NETWORK SECURITY	USER PERMISSIONS	SYSTEM LOGGING

MOBILE APPLICATION ASSESSMENT

The power of mobile platforms has changed the way we use applications today. But with great power comes great risk, and the mobile world faces many new security challenges. Mobile applications are often vulnerable to a number of attack vectors and can vary wildly in nature. Mobile security testing requires deep understanding of application security as well as the core mobile platform itself. The Virtue Mobile Methodology was built to consider this new range of attack vectors and ensure mobile applications remain resilient to many attack scenarios.

- **ABUSE OF UNDERLYING API**
- **BYPASSING CLIENT SIDE CONTROLS**
- **MISUSE OF PLATFORM FEATURES**
- **THREATS FROM MALICIOUS APPLICATIONS ON THE DEVICE**
- **ATTACKS ON SERVER-SIDE COMPONENTS**
  (SQL Injection, CSRF, XSS, weak authentication)
- **INSECURE DATA STORAGE**
  (lost or stolen device)

WIRELESS ASSESSMENT

A Wireless Vulnerability Assessment will determine if an attacker can penetrate, eavesdrop, or inject data into a wireless network. This assessment examines the strength and configuration of the wireless infrastructure as well as client configuration on all radio frequencies. Specialty WiFi cards along with spectrum analyzers are used in "war walks" to physically locate any unauthorized rogue wireless hardware. Virtue Security also utilizes an in house GPU cluster capable of cracking WPA2 pre-shared keys several thousand times faster than a desktop computer.

VIRTUE SECURITY

ABOUT US

The strength of Virtue Security delivers comprehensive assessments that quantify and prioritize real world risk. By demonstrating, documenting, and remediating vulnerabilities Virtue Security delivers solutions that fulfill covered entities and business associates security and regulatory objectives.

Penetration testing is far more than a job for our team; it's a craft that we live, breathe, and take great pride in. We believe in going beyond common scare tactics to provide realistic security assessments that educate, remediate, and provide forward thinking strategic advice.

We understand that security landscapes are always changing; and we constantly adapt our testing methods to challenge emerging threats. Headquartered in New York City, Virtue Security is a research driven team and an active contributor to some of the most influential security working groups.

CONTACT

Elliott Frantz
Founder / CEO
elliott.frantz@virtuesecurity.com
347-826-3330

Frank McLaughlin
Director Business Development
fcm@virtuesecurity.com
617-939-9278

VULNERABILITY ASSESSMENTS
VIRTUE SECURITY
ETHICAL HACKING CONSULTING
NEW YORK, NY