HALOCK DELIVERS

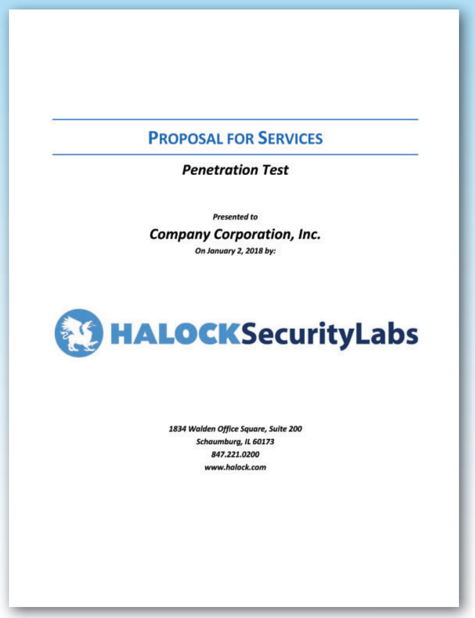
INSIGHTFUL, ACCURATE, & ACTIONABLE RESULTS

HALOCK's deliverables are second to none. Each deliverable produced contains detailed and clearly communicated information to the recipient. Every deliverable is custom written to reflect the specific results or considerations for your penetration test project. The three main artifacts produced with every penetration test include the proposal, project plan, and detailed report.

The **proposal for services** documents the context and purpose of the penetration test, goals, objectives, expectations, project activities, project management framework, scope and boundaries, fees and payment terms, methodology, sample deliverables, references, and supplemental content. There are no project assumptions in the proposal. HALOCK doesn't make assumptions ... HALOCK makes commitments. This proposal ensures all expectations are clearly defined, documented, and committed before you make any decisions.

The **project plan**, developed in close coordination with your team, documents the logistics for testing to ensure you know exactly what to expect during testing. This plan contains the scope of review from the proposal and expands upon the specific details needed to conduct high quality testing under safe and controlled conditions. The plan details the scope, scheduled preparation activities, permitted testing dates and times, all stakeholders and contact information, a role-based communication plan, connectivity and access considerations, and detailed technical documentation for each penetration test activity being performed.

The **penetration test report** is a content rich artifact containing the complete results of the penetration test including what was tested, how it was tested, when the test was performed, and what observations and recommendations should be considered. The report is structured such that it can communicate the relevant details of the engagement in a standalone format. It recaps the objectives, background, and timeline for testing. The summary of findings, intended for consumption by audiences seeking a brief but informative summary of the results, is an abbreviated overview of the results with a focus on key findings. Following the summary are the detailed results, intended for audiences more closely involved in remediation activities. Each vulnerability validated during testing is documented to ensure the audience has a clear understanding of the security weakness and the impact it presents. Detailed recommendations provide a roadmap to implementing corrective actions or countermeasures to prevent the vulnerability from being exploited. Evidence clarifying where each vulnerability was observed is included to ensure the remediation team know specifically where to apply remediation. This evidence is accompanied by visual demonstrations depicting each exploit in a step by step flow to clearly communicate impact and allow for reproduction. Finally, the report contains the complete contents of the planning materials as executed as well as supplemental content.



PROPOSAL FOR SERVICES

Penetration Test

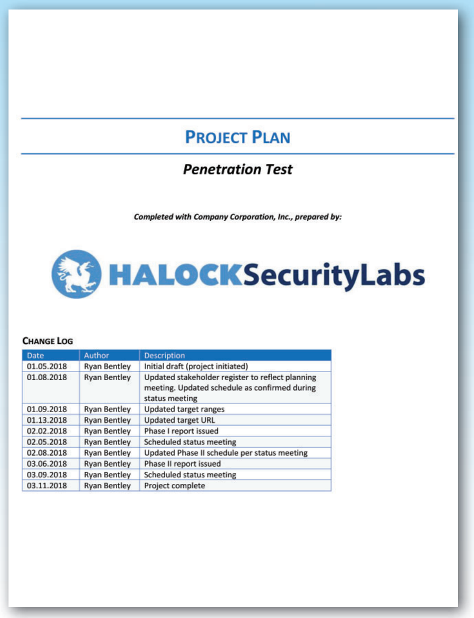
Presented to
Company Corporation, Inc.
On January 2, 2018 by:

HALOCKSecurityLabs

1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847.221.0200
www.halock.com

1. Proposal for Services

Our commitment to meet your expectations.



PROJECT PLAN

Penetration Test

Completed with Company Corporation, Inc., prepared by:

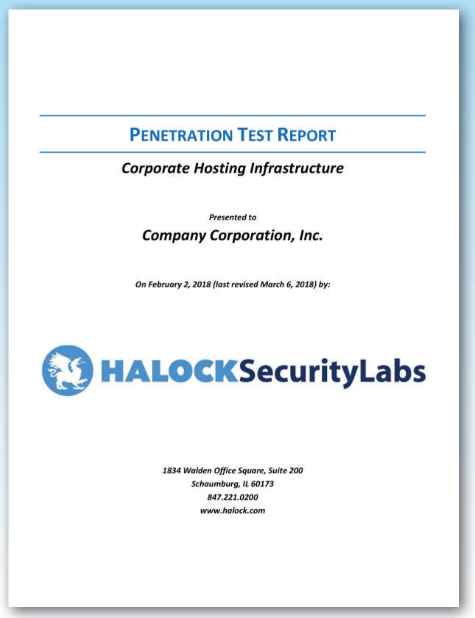
HALOCKSecurityLabs

CHANGE LOG

Date	Author	Description
01.05.2018	Ryan Bentley	Initial draft (project initiated)
01.08.2018	Ryan Bentley	Updated stakeholder register to reflect planning meeting. Updated schedule as confirmed during status meeting
01.09.2018	Ryan Bentley	Updated target ranges
01.13.2018	Ryan Bentley	Updated target URL
02.02.2018	Ryan Bentley	Phase I report issued
02.05.2018	Ryan Bentley	Scheduled status meeting
02.08.2018	Ryan Bentley	Updated Phase II schedule per status meeting
03.06.2018	Ryan Bentley	Phase II report issued
03.09.2018	Ryan Bentley	Scheduled status meeting
03.11.2018	Ryan Bentley	Project complete

2. Project Plan

Ensuring you know exactly what to expect.



PENETRATION TEST REPORT

Corporate Hosting Infrastructure

Presented to
Company Corporation, Inc.

On February 2, 2018 (last revised March 6, 2018) by:

HALOCKSecurityLabs

1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847.221.0200
www.halock.com

3. Penetration Test Report

Comprehensive, accurate, and actionable results you can use.

1. PROPOSAL FOR SERVICES Our commitment to meet your expectations.

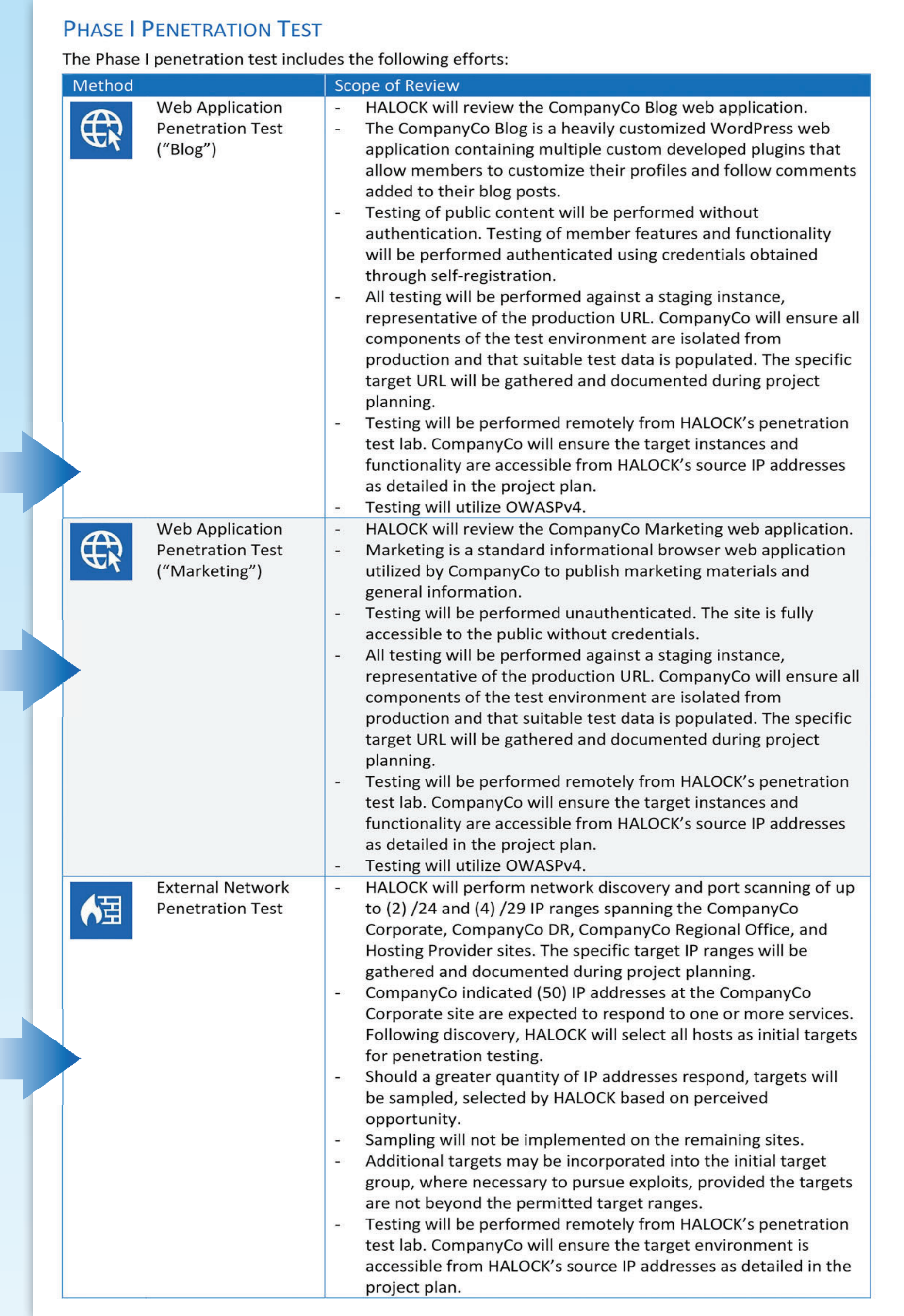
The proposal for services, as depicted below, details the scope and boundaries, project background, deliverables, activities, methodology, and other pertinent content.

SCOPE AND BOUNDARIES

To ensure the penetration test methodologies are applied where intended, the proposal scope and boundaries commit the defined scope of review. Each component of testing is detailed and noted with any unique or customized requirements that were defined.

For example, this penetration test included two phases, an initial comprehensive review followed by a remediation verification test. The first phase depicted here is a defined as a comprehensive baseline review, specifically targeted two key web applications and the internet facing infrastructure.

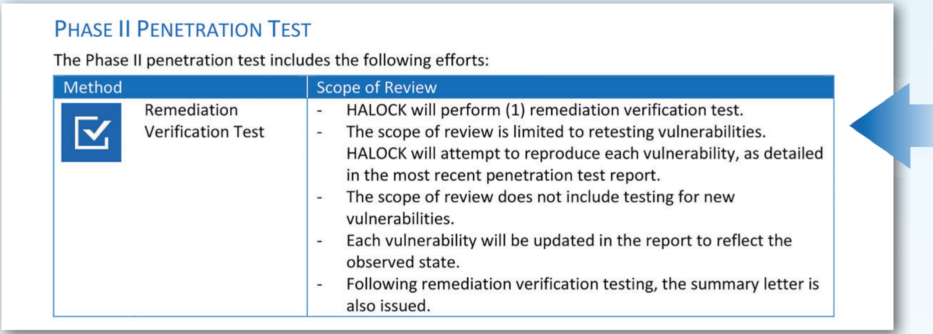
The basis for all planning conducted before testing is built upon the scope and boundaries as the foundation, ensure that any decisions to be made regarding targets, quantities, sampling methodologies, test origins, and related considerations are agreed to by decision makers early in the process.



Phase I Penetration Test

The Phase I penetration test includes the following efforts:

Method	Scope of Review
Web Application Penetration Test (“Blog”)	- HALOCK will review the CompanyCo Blog web application. - The CompanyCo Blog is a heavily customized WordPress web application containing multiple custom developed plugins that allow members to customize their profiles and follow comments added to their blog posts. - Testing of public content will be performed without authentication. Testing of member features and functionality will be performed authenticated using credentials obtained through self-registration. - All testing will be performed against a staging instance, representative of the production URL. CompanyCo will ensure all components of the test environment are isolated from production and that suitable test data is populated. The specific target URL will be gathered and documented during project planning. - Testing will be performed remotely from HALOCK’s penetration test lab. CompanyCo will ensure the target instances and functionality are accessible from HALOCK’s source IP addresses as detailed in the project plan. - Testing will utilize OWASPv4.
Web Application Penetration Test (“Marketing”)	- HALOCK will review the CompanyCo Marketing web application. - Marketing is a standard informational browser web application utilized by CompanyCo to publish marketing materials and general information. - Testing will be performed unauthenticated. The site is fully accessible to the public without credentials. - All testing will be performed against a staging instance, representative of the production URL. CompanyCo will ensure all components of the test environment are isolated from production and that suitable test data is populated. The specific target URL will be gathered and documented during project planning. - Testing will be performed remotely from HALOCK’s penetration test lab. CompanyCo will ensure the target instances and functionality are accessible from HALOCK’s source IP addresses as detailed in the project plan. - Testing will utilize OWASPv4.
External Network Penetration Test	- HALOCK will perform network discovery and port scanning of up to (2) /24 and (4) /29 IP ranges spanning the CompanyCo Corporate, CompanyCo DR, CompanyCo Regional Office, and Hosting Provider sites. The specific target IP ranges will be gathered and documented during project planning. - CompanyCo indicated (50) IP addresses at the CompanyCo Corporate site are expected to respond to one or more services. Following discovery, HALOCK will select all hosts as initial targets for penetration testing. - Should a greater quantity of IP addresses respond, targets will be sampled, selected by HALOCK based on perceived opportunity. - Sampling will not be implemented on the remaining sites. - Additional targets may be incorporated into the initial target group, where necessary to pursue exploits, provided the targets are not beyond the permitted target ranges. - Testing will be performed remotely from HALOCK’s penetration test lab. CompanyCo will ensure the target environment is accessible from HALOCK’s source IP addresses as detailed in the project plan.



Phase II Penetration Test

The Phase II penetration test includes the following efforts:

Method	Scope of Review
Remediation Verification Test	- HALOCK will perform (1) remediation verification test. - The scope of review is limited to retesting vulnerabilities. HALOCK will attempt to reproduce each vulnerability, as detailed in the most recent penetration test report. - The scope of review does not include testing for new vulnerabilities. - Each vulnerability will be updated in the report to reflect the observed state. - Following remediation verification testing, the summary letter is also issued.

The scope and boundaries continues through Phase II, detailing a follow up engagement to verify remediation effectiveness.

1. PROPOSAL FOR SERVICES Our commitment to meet your expectations.

BACKGROUND

Understanding your business is a critical first step in understanding the most appropriate scope and methodology for your penetration test. The background captures this context, establishing the drivers, intent, and purpose of the penetration test.

DELIVERABLES

The deliverables you can expect to receive are committed and visually depicted directly in the proposal, including samples, so you know what you will receive following testing. You will find detailed examples of these reports later in this document.

FINANCIAL INVESTMENT

With a well-defined and carefully crafted scope established, HALOCK commits the financial investment as a fixed fee. The fees are itemized for transparency along with payment terms dependent on the completion of milestones. This approach ensures the cost meets your budget.

PROJECT ACTIVITIES

Your penetration test engagement is closely planned and coordinated. To ensure you know what to expect, the project management phases are customized and committed directly in the proposal. The project activities define each phase and milestone to ensure you have confidence the penetration test will be performed under safe and controlled conditions and that you will know what to expect even before the testing process begins.

PENETRATION TEST METHODOLOGY

Penetration testing is not a linear approach, but rather an interactive process. As HALOCK progresses through each phase of testing, additional information is gathered, knowledge of the environment is gained, and new attack scenarios are identified. Information gathered through each phase of testing is fed back into the reconnaissance phase for additional analysis and to pursue exploits.

The proposal documents the complete penetration test methodology, including the activities involved in each phase of testing. Key actions taken, such as how exploits are pursued, as detailed to ensure the approach is consistent with your expectations. The methodology detailed in the proposal further defines the specific methodology for each selected area of review. HALOCK's penetration test procedures, processes, and related activities are directly tied to this committed methodology to ensure each member of the project team is performing the penetration test in a consistent, coordinated, and repeatable manner.

SUPPLEMENTAL CONTENT

The supplemental content included provides additional supporting information. An overview of HALOCK is provided to demonstrate your penetration test is being performed by a provider with deep experience in this field. References are provided so you can discuss their experiences with HALOCK and be comfortable in HALOCK's capabilities and reputation for excellence.

HALOCK'S PENETRATION TEST TEAM

HALOCK's dedicated penetration test team possesses the experience and training you can count on. Combined with the experience of having performed thousands of successful penetration tests, the team maintains expert credentials and knowledge that is required to expertly test and advise.

TERMS AND CONDITIONS

When unique terms and conditions apply to a penetration test, they are defined in advance. These primarily related to ensuring planning can be conducted, establish certain access requirements, and commit that the scope and pricing will not be altered unless requested and approved.

2. PROJECT PLAN Ensuring you know exactly what to expect.

The **project plan**, developed prior to testing, includes the project background, schedule, stakeholders, communication plan, and detailed planning for each effort included in the scope of review.

BACKGROUND

As you include additional individuals in penetration test planning, it is important the **background** from the proposal carries through to the project plan for continuity and context.

Testing Method	Description
Web Application Penetration Test	Based on the sensitivity or value of a web application, an in-depth review is appropriate. HALOCK's approach to assessing web applications provides a flexible framework for comprehensively identifying and evaluating technical vulnerabilities.
External Network Penetration Test	External network penetration tests differ from automated vulnerability scans in that efforts are focused on exploiting weaknesses with the intent of gaining access to the environment. They are performed remote to the environment to simulate an external attack and include testing of networks, hosts, and responding services.
Remediation Verification Test	Remediation verification testing validates identified vulnerabilities have been successfully remediated, providing confirmation corrective measures have been implemented in a manner that prevents exploitation.

PROJECT SCHEDULE

All key activities are detailed in the **project schedule**. This schedule includes all key activities, permitted dates and times, and upcoming events. This allows you to coordinate internally and preserves history after testing has completed.

Event	Date(s)	Time(s)
Project Scope Definition Meeting	01.01.2018	10:00-11:30
Project Scope Review Meeting	01.03.2018	13:00-13:45
Project Initiated	01.05.2018	09:00
Project Planning Meeting	01.08.2018	11:00-11:45
Phase I Web Application Penetration Test Fieldwork	01.22.2018-01.26.2018	07:00-19:00
Phase I External Network Penetration Test Fieldwork	01.29.2018-01.31.2018	07:00-19:00
Report Issued	02.02.2018	14:00
Status Meeting	02.08.2018	14:00-15:00
Phase II Remediation Verification Test	03.05.2018	07:00-19:00
Report Issued	03.06.2018	17:00
Summary Letter Issued	03.06.2018	17:00
Status Meeting	03.11.2018	14:00-15:00
Project Closed	03.11.2018	17:00

STAKEHOLDER REGISTER

Everyone involved in the project planning and execution is documented in the **stakeholder register**, including their roles and involvement. This allows all involved to know who to contact for what purposes, and ensures the reports are issued only to those authorized to receive it.

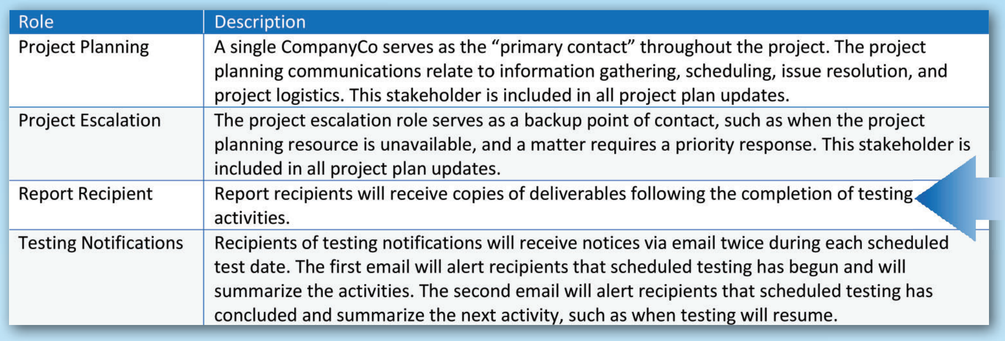
COMPANY CORPORATION, INC.

Name	Involvement	Email	Phone
Jane Doe	Project Planning Report Recipient Testing Notifications	jdoe@localhost.com	555.555.1001
John Smith	Project Escalation Report Recipient Testing Notifications	jsmith@localhost.com	555.555.1002
Help Desk	Testing Notifications	helpdesk@localhost.com	N/A
IT Operations	Testing Notifications	it@localhost.com	N/A

HALOCK SECURITY LABS

Name	Involvement	Email	Phone
Cathy Manager	Project Manager	cmanager@halock.com	555.555.2001
John Tester	Project Team	jtester@halock.com	555.555.2002
Frank Tester	Project Team	ftester@halock.com	555.555.2003
Alice Tester	Project Team	atester@halock.com	555.555.2004

2. PROJECT PLAN Ensuring you know exactly what to expect.



Role	Description
Project Planning	A single CompanyCo serves as the “primary contact” throughout the project. The project planning communications relate to information gathering, scheduling, issue resolution, and project logistics. This stakeholder is included in all project plan updates.
Project Escalation	The project escalation role serves as a backup point of contact, such as when the project planning resource is unavailable, and a matter requires a priority response. This stakeholder is included in all project plan updates.
Report Recipient	Report recipients will receive copies of deliverables following the completion of testing activities.
Testing Notifications	Recipients of testing notifications will receive notices via email twice during each scheduled test date. The first email will alert recipients that scheduled testing has begun and will summarize the activities. The second email will alert recipients that scheduled testing has concluded and summarize the next activity, such as when testing will resume.

COMMUNICATION PLAN

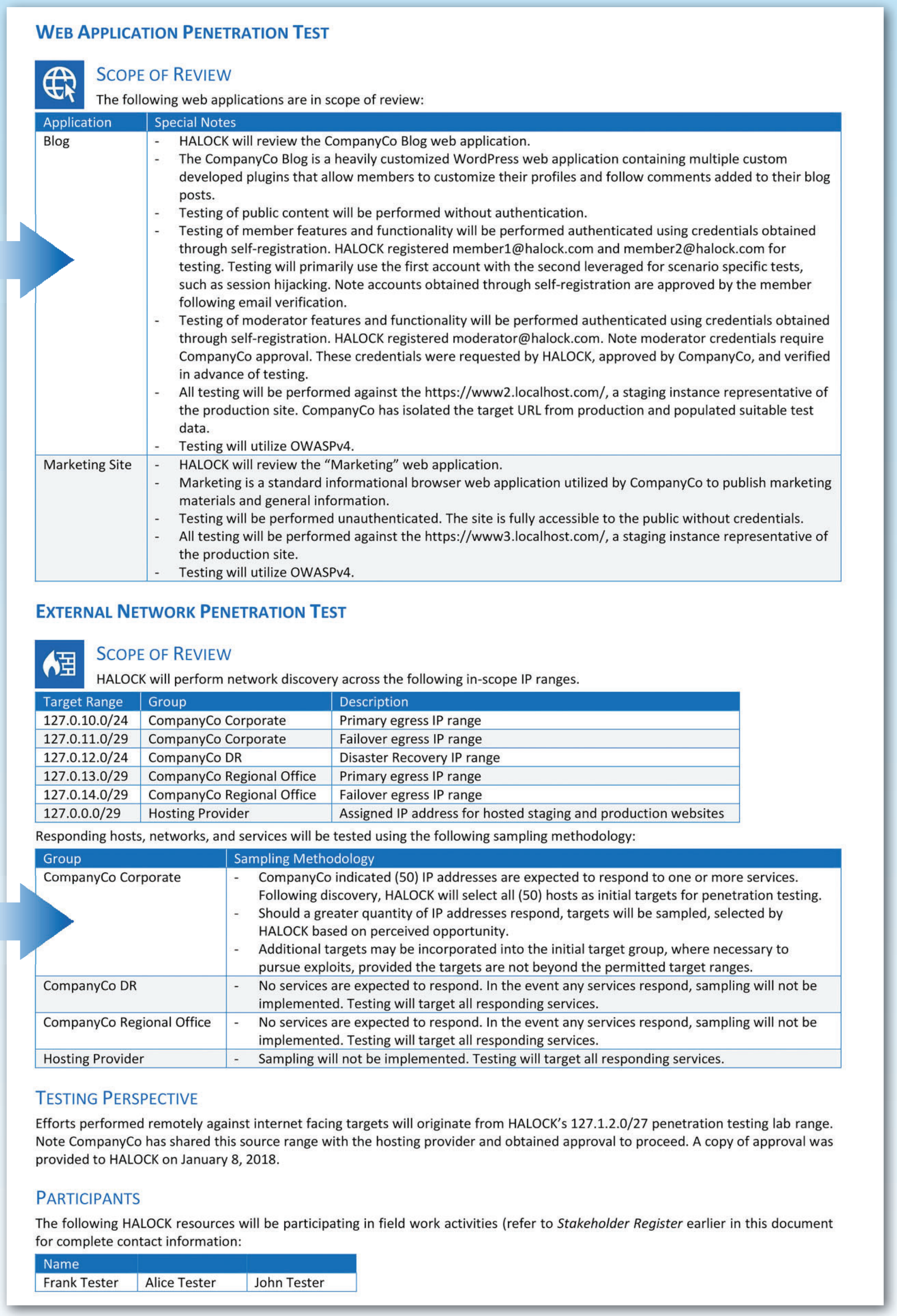
Project stakeholder roles are defined in the communication plan and can be revised to reflect any unique communication considerations.

DETAILED PLANNING

The detailed planning expands upon the scope of review defined in the proposal. Specific test details, activities, documentation, or other dependencies are identified, gathered, and verified before any testing begins. This ensures testing is highly productive, adheres to the schedule, and avoids any disruptive last-minute needs.

DETAILED PLANNING (continued)

The detailed planning also captures the most current information as well as information that was not necessarily available during scope definition. For example, the scope of review may have defined the sites and number of networks to be targeted, but the project plan expands upon that to ensure the exact target networks are included, none are overlooked, and sampling thresholds are fine tuned.



Web Application Penetration Test

Scope of Review

The following web applications are in scope of review:

Application	Special Notes
Blog	- HALOCK will review the CompanyCo Blog web application. - The CompanyCo Blog is a heavily customized WordPress web application containing multiple custom developed plugins that allow members to customize their profiles and follow comments added to their blog posts. - Testing of public content will be performed without authentication. - Testing of member features and functionality will be performed authenticated using credentials obtained through self-registration. HALOCK registered member1@halock.com and member2@halock.com for testing. Testing will primarily use the first account with the second leveraged for scenario specific tests, such as session hijacking. Note accounts obtained through self-registration are approved by the member following email verification. - Testing of moderator features and functionality will be performed authenticated using credentials obtained through self-registration. HALOCK registered moderator@halock.com. Note moderator credentials require CompanyCo approval. These credentials were requested by HALOCK, approved by CompanyCo, and verified in advance of testing. - All testing will be performed against the https://www2.localhost.com/, a staging instance representative of the production site. CompanyCo has isolated the target URL from production and populated suitable test data. - Testing will utilize OWASPv4.
Marketing Site	- HALOCK will review the “Marketing” web application. - Marketing is a standard informational browser web application utilized by CompanyCo to publish marketing materials and general information. - Testing will be performed unauthenticated. The site is fully accessible to the public without credentials. - All testing will be performed against the https://www3.localhost.com/, a staging instance representative of the production site. - Testing will utilize OWASPv4.

External Network Penetration Test

Scope of Review

HALOCK will perform network discovery across the following in-scope IP ranges.

Target Range	Group	Description
127.0.10.0/24	CompanyCo Corporate	Primary egress IP range
127.0.11.0/29	CompanyCo Corporate	Failover egress IP range
127.0.12.0/24	CompanyCo DR	Disaster Recovery IP range
127.0.13.0/29	CompanyCo Regional Office	Primary egress IP range
127.0.14.0/29	CompanyCo Regional Office	Failover egress IP range
127.0.0.0/29	Hosting Provider	Assigned IP address for hosted staging and production websites

Responding hosts, networks, and services will be tested using the following sampling methodology:

Group	Sampling Methodology
CompanyCo Corporate	- CompanyCo indicated (50) IP addresses are expected to respond to one or more services. Following discovery, HALOCK will select all (50) hosts as initial targets for penetration testing. - Should a greater quantity of IP addresses respond, targets will be sampled, selected by HALOCK based on perceived opportunity. - Additional targets may be incorporated into the initial target group, where necessary to pursue exploits, provided the targets are not beyond the permitted target ranges.
CompanyCo DR	- No services are expected to respond. In the event any services respond, sampling will not be implemented. Testing will target all responding services.
CompanyCo Regional Office	- No services are expected to respond. In the event any services respond, sampling will not be implemented. Testing will target all responding services.
Hosting Provider	- Sampling will not be implemented. Testing will target all responding services.

Testing Perspective

Efforts performed remotely against internet facing targets will originate from HALOCK’s 127.1.2.0/27 penetration testing lab range. Note CompanyCo has shared this source range with the hosting provider and obtained approval to proceed. A copy of approval was provided to HALOCK on January 8, 2018.

Participants

The following HALOCK resources will be participating in field work activities (refer to *Stakeholder Register* earlier in this document for complete contact information:

Name		
Frank Tester	Alice Tester	John Tester

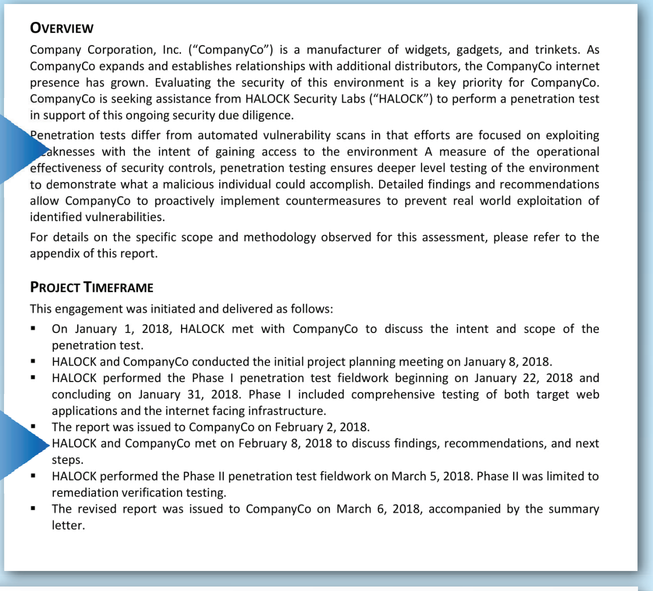
3. PENETRATION TEST REPORT Comprehensive, accurate, and actionable results you can use.

The **penetration test report**, as depicted below, is a content rich document containing the complete results of the test in both summary and detailed formats. The report documents the background and timing of the test, complete results of identified vulnerabilities, demonstrations of the exploits performed, and supplemental content.

OVERVIEW AND PROJECT TIMEFRAME

The **background and timing** of the penetration test are details important to understanding the context of the findings and recommendations. Any drivers, such as compliance requirements or boundaries, allow the reader to understand why the test was performed. The timeline provides a historical record of when the test was scoped, planned, conducted, and delivered. These provide attestation of the dates work was performed and when remediation began, details required for regulatory due dates or other requirements containing deadlines.

In the example depicted below, the organization conducted a penetration test for due diligence purposes, evaluating if their rapid growth has potentially introduced vulnerabilities into the environment.



OVERVIEW

Company Corporation, Inc. ("CompanyCo") is a manufacturer of widgets, gadgets, and trinkets. As CompanyCo expands and establishes relationships with additional distributors, the CompanyCo internet presence has grown. Evaluating the security of this environment is a key priority for CompanyCo. CompanyCo is seeking assistance from HALOCK Security Labs ("HALOCK") to perform a penetration test in support of this ongoing security due diligence.

Penetration tests differ from automated vulnerability scans in that efforts are focused on exploiting weaknesses with the intent of gaining access to the environment A measure of the operational effectiveness of security controls, penetration testing ensures deeper level testing of the environment to demonstrate what a malicious individual could accomplish. Detailed findings and recommendations allow CompanyCo to proactively implement countermeasures to prevent real world exploitation of identified vulnerabilities.

For details on the specific scope and methodology observed for this assessment, please refer to the appendix of this report.

PROJECT TIMEFRAME

This engagement was initiated and delivered as follows:

- On January 1, 2018, HALOCK met with CompanyCo to discuss the intent and scope of the penetration test.
- HALOCK and CompanyCo conducted the initial project planning meeting on January 8, 2018.
- HALOCK performed the Phase I penetration test fieldwork beginning on January 22, 2018 and concluding on January 31, 2018. Phase I included comprehensive testing of both target web applications and the internet facing infrastructure.
- The report was issued to CompanyCo on February 2, 2018.
- HALOCK and CompanyCo met on February 8, 2018 to discuss findings, recommendations, and next steps.
- HALOCK performed the Phase II penetration test fieldwork on March 5, 2018. Phase II was limited to remediation verification testing.
- The revised report was issued to CompanyCo on March 6, 2018, accompanied by the summary letter.

INDEX OF VULNERABILITIES AND EXPLOITS

The **index of vulnerabilities and exploits** section also includes a complete list of all vulnerabilities, indexed and grouped by severity, as well as a listing of the exploit steps. This section provides the reader with a snapshot of the complete results. Below we can see the organization conducted scope definition and project planning in early January before proceeding to Phase I testing of the web applications and internet facing infrastructure in late January. The report was issued a few days following testing and was followed by a meeting to review results and discuss next steps. Following remediation, a subsequent remediation verification test was performed in March, producing an updated detailed deliverable and a summary letter for sharing with external audiences.

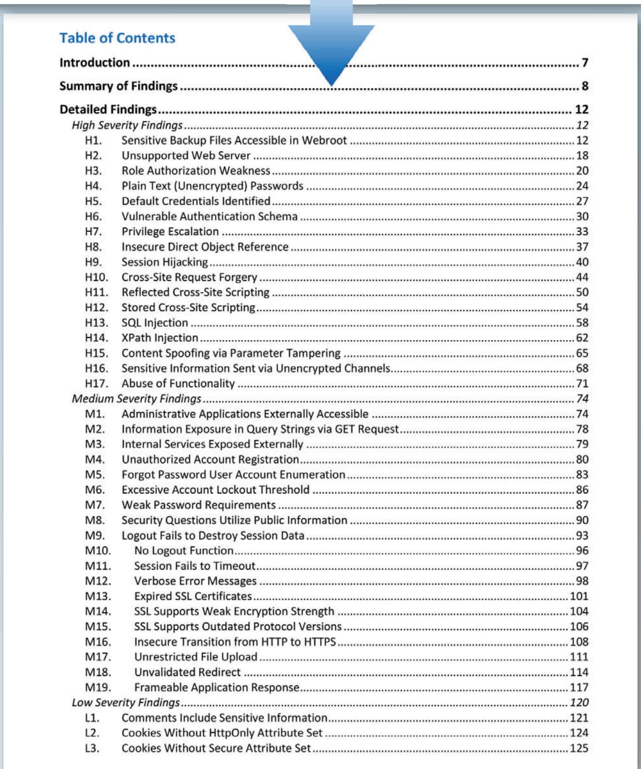


Table of Contents

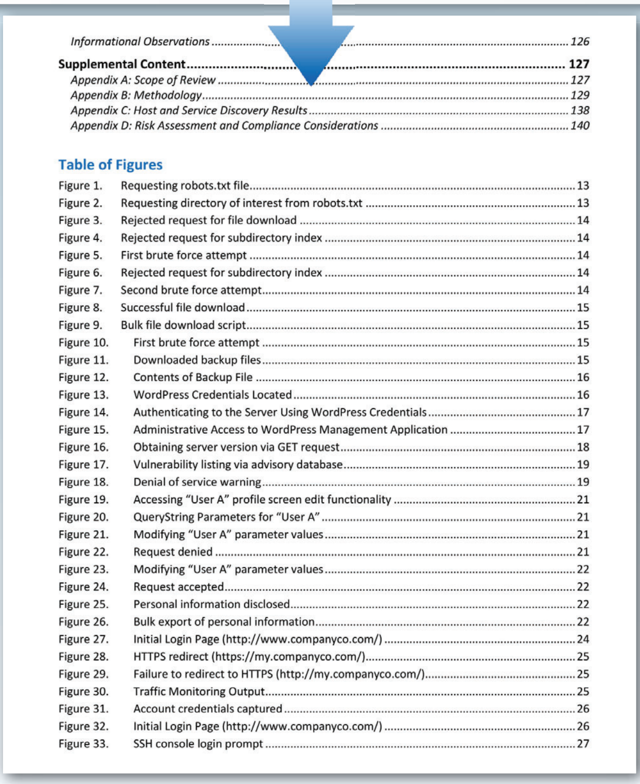


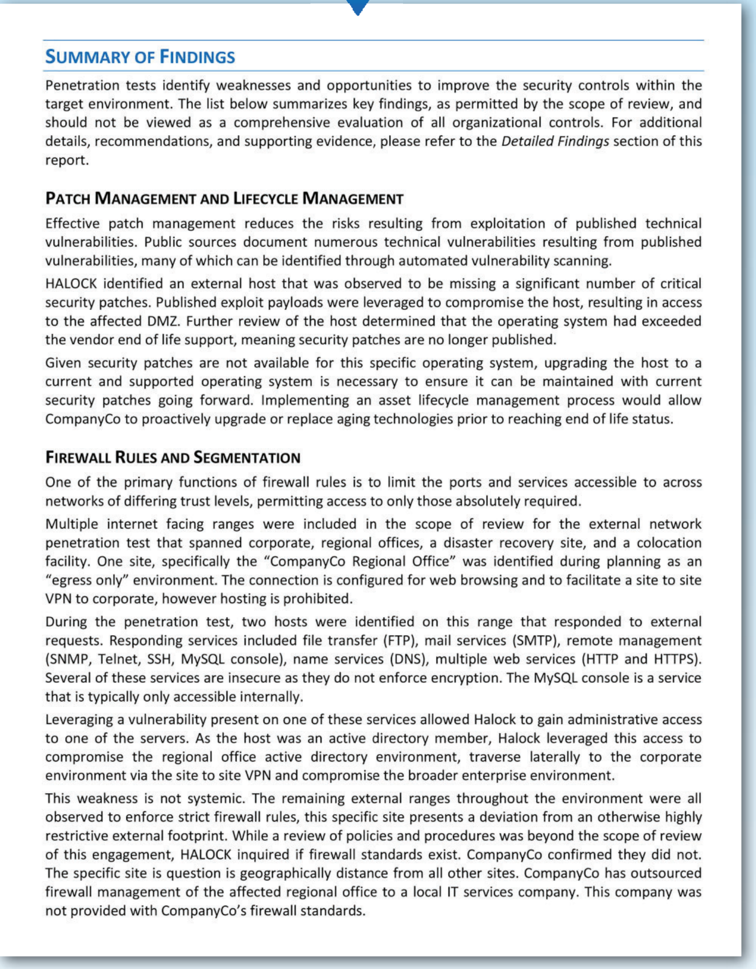
Table of Figures

3. PENETRATION TEST REPORT

Comprehensive, accurate, and actionable results you can use.

SUMMARY OF FINDINGS

The **summary of findings** is an abridged roll up of the complete detail found later in the report. This section groups key findings by topic, discusses common or recurring issues observed during testing, and notes other pertinent information. Intended primarily for audiences that are interested in an "at a glance" overview, the summary of findings also is commonly leveraged by teams presenting to executive audiences. In the images below, the first two pages of the summary are depicted. The primary topics discussed include key findings and common issues, specifically focusing on the impact of exploits derived from weaknesses in patch management, network segmentation, configuration management, and authentication. For most reports, this section contains 2-3 pages of content, but does vary based on the volume of vulnerabilities observed as well as the size and scope of the engagement itself.



Summary of Findings

Penetration tests identify weaknesses and opportunities to improve the security controls within the target environment. The list below summarizes key findings, as permitted by the scope of review, and should not be viewed as a comprehensive evaluation of all organizational controls. For additional details, recommendations, and supporting evidence, please refer to the *Detailed Findings* section of this report.

Patch Management and Lifecycle Management

Effective patch management reduces the risks resulting from exploitation of published technical vulnerabilities. Public sources document numerous technical vulnerabilities resulting from published vulnerabilities, many of which can be identified through automated vulnerability scanning.

HALOCK identified an external host that was observed to be missing a significant number of critical security patches. Published exploit payloads were leveraged to compromise the host, resulting in access to the affected DMZ. Further review of the host determined that the operating system had exceeded the vendor end of life support, meaning security patches are no longer published.

Given security patches are not available for this specific operating system, upgrading the host to a current and supported operating system is necessary to ensure it can be maintained with current security patches going forward. Implementing an asset lifecycle management process would allow CompanyCo to proactively upgrade or replace aging technologies prior to reaching end of life status.

Firewall Rules and Segmentation

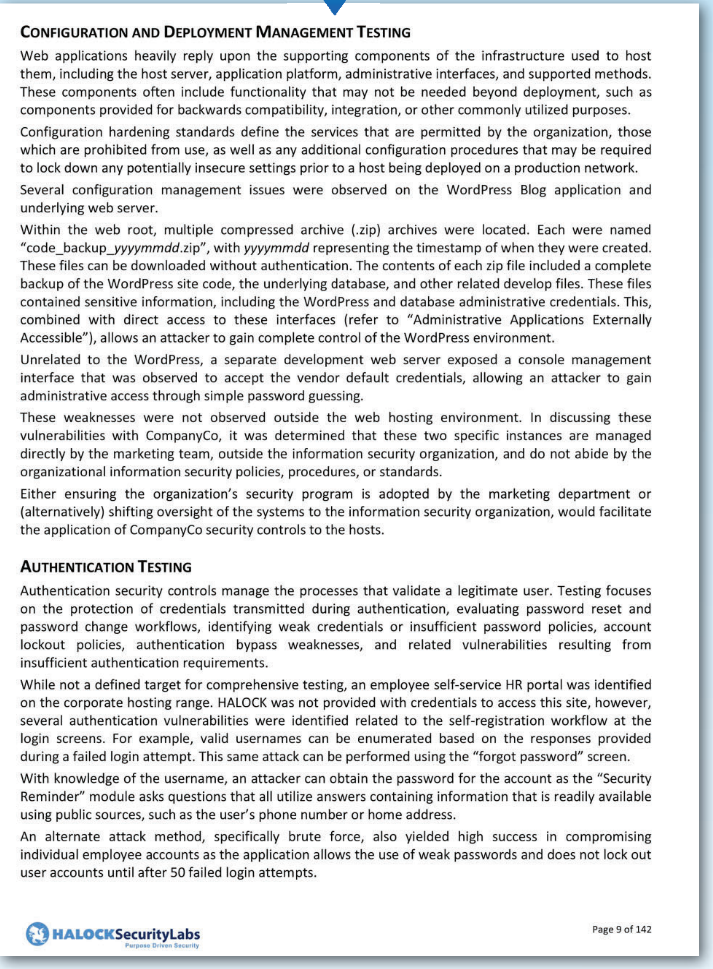
One of the primary functions of firewall rules is to limit the ports and services accessible to across networks of differing trust levels, permitting access to only those absolutely required.

Multiple internet facing ranges were included in the scope of review for the external network penetration test that spanned corporate, regional offices, a disaster recovery site, and a colocation facility. One site, specifically the "CompanyCo Regional Office" was identified during planning as an "egress only" environment. The connection is configured for web browsing and to facilitate a site to site VPN to corporate, however hosting is prohibited.

During the penetration test, two hosts were identified on this range that responded to external requests. Responding services included file transfer (FTP), mail services (SMTP), remote management (SNMP, Telnet, SSH, MySQL console), name services (DNS), multiple web services (HTTP and HTTPS). Several of these services are insecure as they do not enforce encryption. The MySQL console is a service that is typically only accessible internally.

Leveraging a vulnerability present on one of these services allowed Halock to gain administrative access to one of the servers. As the host was an active directory member, Halock leveraged this access to compromise the regional office active directory environment, traverse laterally to the corporate environment via the site to site VPN and compromise the broader enterprise environment.

This weakness is not systemic. The remaining external ranges throughout the environment were all observed to enforce strict firewall rules, this specific site presents a deviation from an otherwise highly restrictive external footprint. While a review of policies and procedures was beyond the scope of review of this engagement, HALOCK inquired if firewall standards exist. CompanyCo confirmed they did not. The specific site is question is geographically distance from all other sites. CompanyCo has outsourced firewall management of the affected regional office to a local IT services company. This company was not provided with CompanyCo's firewall standards.



Configuration and Deployment Management Testing

Web applications heavily reply upon the supporting components of the infrastructure used to host them, including the host server, application platform, administrative interfaces, and supported methods. These components often include functionality that may not be needed beyond deployment, such as components provided for backwards compatibility, integration, or other commonly utilized purposes.

Configuration hardening standards define the services that are permitted by the organization, those which are prohibited from use, as well as any additional configuration procedures that may be required to lock down any potentially insecure settings prior to a host being deployed on a production network.

Several configuration management issues were observed on the WordPress Blog application and underlying web server.

Within the web root, multiple compressed archive (.zip) archives were located. Each were named "code_backup_*yyyymmdd*.zip", with *yyyymmdd* representing the timestamp of when they were created. These files can be downloaded without authentication. The contents of each zip file included a complete backup of the WordPress site code, the underlying database, and other related develop files. These files contained sensitive information, including the WordPress and database administrative credentials. This, combined with direct access to these interfaces (refer to "Administrative Applications Externally Accessible"), allows an attacker to gain complete control of the WordPress environment.

Unrelated to the WordPress, a separate development web server exposed a console management interface that was observed to accept the vendor default credentials, allowing an attacker to gain administrative access through simple password guessing.

These weaknesses were not observed outside the web hosting environment. In discussing these vulnerabilities with CompanyCo, it was determined that these two specific instances are managed directly by the marketing team, outside the information security organization, and do not abide by the organizational information security policies, procedures, or standards.

Either ensuring the organization's security program is adopted by the marketing department or (alternatively) shifting oversight of the systems to the information security organization, would facilitate the application of CompanyCo security controls to the hosts.

Authentication Testing

Authentication security controls manage the processes that validate a legitimate user. Testing focuses on the protection of credentials transmitted during authentication, evaluating password reset and password change workflows, identifying weak credentials or insufficient password policies, account lockout policies, authentication bypass weaknesses, and related vulnerabilities resulting from insufficient authentication requirements.

While not a defined target for comprehensive testing, an employee self-service HR portal was identified on the corporate hosting range. HALOCK was not provided with credentials to access this site, however, several authentication vulnerabilities were identified related to the self-registration workflow at the login screens. For example, valid usernames can be enumerated based on the responses provided during a failed login attempt. This same attack can be performed using the "forgot password" screen.

With knowledge of the username, an attacker can obtain the password for the account as the "Security Reminder" module asks questions that all utilize answers containing information that is readily available using public sources, such as the user's phone number or home address.

An alternate attack method, specifically brute force, also yielded high success in compromising individual employee accounts as the application allows the use of weak passwords and does not lock out user accounts until after 50 failed login attempts.

HALOCKSecurityLabs Purpose Driven Security

Page 9 of 142

3. PENETRATION TEST REPORT

Comprehensive, accurate, and actionable results you can use.

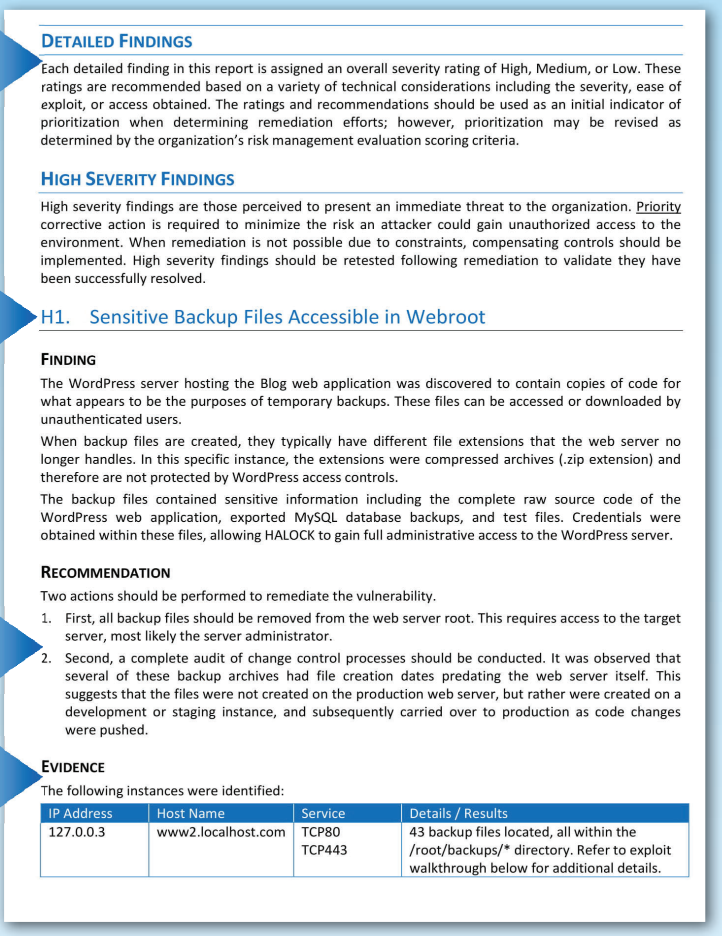
DETAILED FINDINGS: HIGH SEVERITY

The **detailed findings** report the complete results of the pen test, grouped by severity and indexed for reference.

DETAILED FINDINGS: H1

In this first example finding, rated as a high severity vulnerability, the report details the presence of backup files located in the web root of a target web application. The finding begins with a narrative describing the vulnerability as well as the impact of the exploit achieved resulting from the presence of the security flaw. This is followed by recommendations that, if implemented, would remediate the vulnerability and prevent its exploitation. Finally, an evidence table is included that lists specifically where the vulnerability was observed.

In this example, we see that only one occurrence was observed, with the evidence table detailing the IP address, website URL, service(s), and directory location. This information is critical to remediation teams as it allows them to understand exactly what the vulnerability is, why the impact warrants a high severity rating, how to resolve the issue, and where to do so.



Detailed Findings

Each detailed finding in this report is assigned an overall severity rating of High, Medium, or Low. These ratings are recommended based on a variety of technical considerations including the severity, ease of exploit, or access obtained. The ratings and recommendations should be used as an initial indicator of prioritization when determining remediation efforts; however, prioritization may be revised as determined by the organization's risk management evaluation scoring criteria.

High Severity Findings

High severity findings are those perceived to present an immediate threat to the organization. Priority corrective action is required to minimize the risk an attacker could gain unauthorized access to the environment. When remediation is not possible due to constraints, compensating controls should be implemented. High severity findings should be retested following remediation to validate they have been successfully resolved.

H1. Sensitive Backup Files Accessible in Webroot

Finding

The WordPress server hosting the Blog web application was discovered to contain copies of code for what appears to be the purposes of temporary backups. These files can be accessed or downloaded by unauthenticated users.

When backup files are created, they typically have different file extensions that the web server no longer handles. In this specific instance, the extensions were compressed archives (.zip extension) and therefore are not protected by WordPress access controls.

The backup files contained sensitive information including the complete raw source code of the WordPress web application, exported MySQL database backups, and test files. Credentials were obtained within these files, allowing HALOCK to gain full administrative access to the WordPress server.

Recommendation

Two actions should be performed to remediate the vulnerability.

1. First, all backup files should be removed from the web server root. This requires access to the target server, most likely the server administrator.
2. Second, a complete audit of change control processes should be conducted. It was observed that several of these backup archives had file creation dates predating the web server itself. This suggests that the files were not created on the production web server, but rather were created on a development or staging instance, and subsequently carried over to production as code changes were pushed.

Evidence

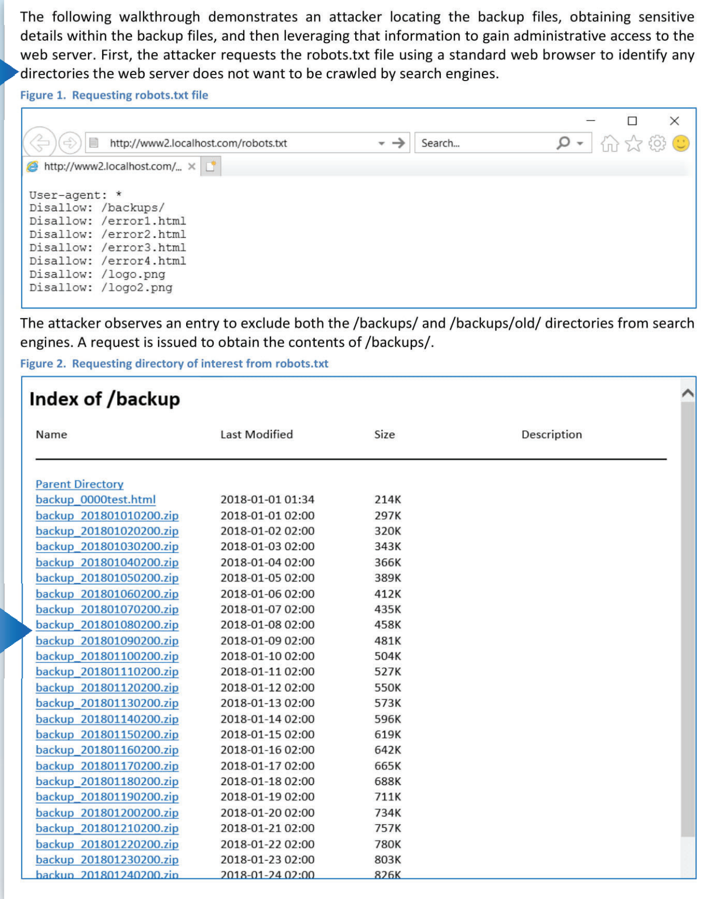
The following instances were identified:

IP Address	Host Name	Service	Details / Results
127.0.0.3	www2.localhost.com	TCP80 TCP443	43 backup files located, all within the /root/backups/* directory. Refer to exploit walkthrough below for additional details.

EXPLOIT DEMONSTRATION

As this specific vulnerability was fully exploited, the finding also includes an **exploit demonstration**. Documenting the walkthrough is a critical reporting element for several reasons. First, it clearly establishes, step by step and screen by screen, how to perform the exploit. Validating successful remediation requires the tester attempt to reproduce the exploit. If the vulnerability cannot be reproduced, the procedures in the walkthrough ensure this can be relied upon as confirmation of remediation. Additionally, especially in the case of complex exploits, a visual and content rich depiction can provide remediation teams with a very clear and detailed understanding of how the exploit works, what to address, and a full understanding of the impact it represents.

The example provided here begins with the early stages of the attack, namely identifying the presence of a "robots" file that could prove useful to an attacker at the reconnaissance stage of an attack. It is worth noting that an automated scan would end this thread at this point, simply reporting on the presence of the robots file, typically a low severity or informational finding, without further determining the impact.



The following walkthrough demonstrates an attacker locating the backup files, obtaining sensitive details within the backup files, and then leveraging that information to gain administrative access to the web server. First, the attacker requests the robots.txt file using a standard web browser to identify any directories the web server does not want to be crawled by search engines.

Figure 1. Requesting robots.txt file

http://www2.localhost.com/robots.txt
Search...
http://www2.localhost.com/...

```
User-agent: *
Disallow: /backups/
Disallow: /error1.html
Disallow: /error2.html
Disallow: /error3.html
Disallow: /error4.html
Disallow: /logo.png
Disallow: /logo2.png
```

The attacker observes an entry to exclude both the /backups/ and /backups/old/ directories from search engines. A request is issued to obtain the contents of /backups/.

Figure 2. Requesting directory of interest from robots.txt

Index of /backup

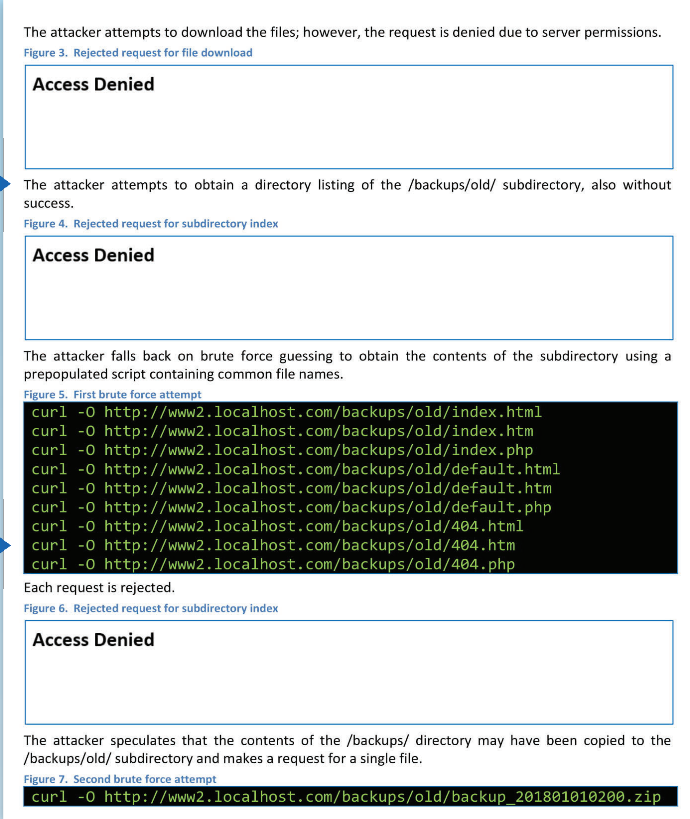
Name	Last Modified	Size	Description
Parent Directory			
backup_0000test.html	2018-01-01 01:34	214K	
backup_201801010200.zip	2018-01-01 02:00	297K	
backup_201801020200.zip	2018-01-02 02:00	320K	
backup_201801030200.zip	2018-01-03 02:00	343K	
backup_201801040200.zip	2018-01-04 02:00	366K	
backup_201801050200.zip	2018-01-05 02:00	389K	
backup_201801060200.zip	2018-01-06 02:00	412K	
backup_201801070200.zip	2018-01-07 02:00	435K	
backup_201801080200.zip	2018-01-08 02:00	458K	
backup_201801090200.zip	2018-01-09 02:00	481K	
backup_201801100200.zip	2018-01-10 02:00	504K	
backup_201801110200.zip	2018-01-11 02:00	527K	
backup_201801120200.zip	2018-01-12 02:00	550K	
backup_201801130200.zip	2018-01-13 02:00	573K	
backup_201801140200.zip	2018-01-14 02:00	596K	
backup_201801150200.zip	2018-01-15 02:00	619K	
backup_201801160200.zip	2018-01-16 02:00	642K	
backup_201801170200.zip	2018-01-17 02:00	665K	
backup_201801180200.zip	2018-01-18 02:00	688K	
backup_201801190200.zip	2018-01-19 02:00	711K	
backup_201801200200.zip	2018-01-20 02:00	734K	
backup_201801210200.zip	2018-01-21 02:00	757K	
backup_201801220200.zip	2018-01-22 02:00	780K	
backup_201801230200.zip	2018-01-23 02:00	803K	
backup_201801240200.zip	2018-01-24 02:00	826K	

EXPLOIT DEMONSTRATION (continued)

The attacker attempts to browse the directory referenced in the robots file, however indexing is not available. An unskilled attacker would typically abandon the attack at this stage; however, a more experienced intruder knows there might be more to pursue.

EXPLOIT DEMONSTRATION (continued)

The attacker proceeds to a simple, but effective method utilizing a script to enumerate what files may be present in this directory of interest. The script initially used is one amended and refined over thousands of past penetration tests. It contains a variety of patterns that have been observed to contain source code repositories, backup files, unreferenced files, default files associated with common web platforms, initial configuration wizards, and similar files that should not be present.



The attacker attempts to download the files; however, the request is denied due to server permissions.

Figure 3. Rejected request for file download

Access Denied

The attacker attempts to obtain a directory listing of the /backups/old/ subdirectory, also without success.

Figure 4. Rejected request for subdirectory index

Access Denied

The attacker falls back on brute force guessing to obtain the contents of the subdirectory using a prepopulated script containing common file names.

Figure 5. First brute force attempt

```
curl -O http://www2.localhost.com/backups/old/index.html
curl -O http://www2.localhost.com/backups/old/index.htm
curl -O http://www2.localhost.com/backups/old/index.php
curl -O http://www2.localhost.com/backups/old/default.html
curl -O http://www2.localhost.com/backups/old/default.htm
curl -O http://www2.localhost.com/backups/old/default.php
curl -O http://www2.localhost.com/backups/old/404.html
curl -O http://www2.localhost.com/backups/old/404.htm
curl -O http://www2.localhost.com/backups/old/404.php
```

Each request is rejected.

Figure 6. Rejected request for subdirectory index

Access Denied

The attacker speculates that the contents of the /backups/ directory may have been copied to the /backups/old/ subdirectory and makes a request for a single file.

Figure 7. Second brute force attempt

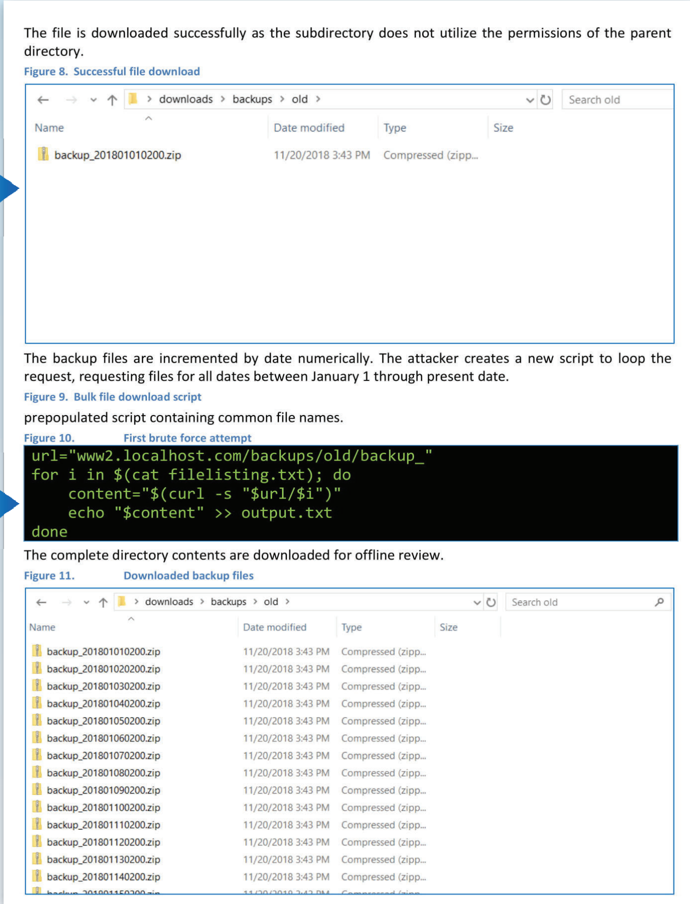
```
curl -O http://www2.localhost.com/backups/old/backup_201801010200.zip
```

EXPLOIT DEMONSTRATION (continued)

All but one of the requests come back empty. The attacker is successful in identifying a single valid file name in this directory. The attacker observes the filename utilizes a predictable structure containing a common prefix followed by a date timestamp. This can indicate an automated process is creating files using the date as a means of programmatically creating unique files names to prevent overwriting.

EXPLOIT DEMONSTRATION (continued)

The attacker refines the script to focus on this pattern exclusively, producing a more comprehensive list of files. This refined script yields more files in a short amount of time. The attacker issues a request to download the field, which is successful.



The file is downloaded successfully as the subdirectory does not utilize the permissions of the parent directory.

Figure 8. Successful file download

Name	Date modified	Type	Size
backup_201801010200.zip	11/20/2018 3:43 PM	Compressed (zipp...	

The backup files are incremented by date numerically. The attacker creates a new script to loop the request, requesting files for all dates between January 1 through present date.

Figure 9. Bulk file download script

prepopulated script containing common file names.

Figure 10. First brute force attempt

```
url="www2.localhost.com/backups/old/backup_"
for i in $(cat filelisting.txt); do
    content="$(curl -s "$url/$i")"
    echo "$content" >> output.txt
done
```

The complete directory contents are downloaded for offline review.

Figure 11. Downloaded backup files

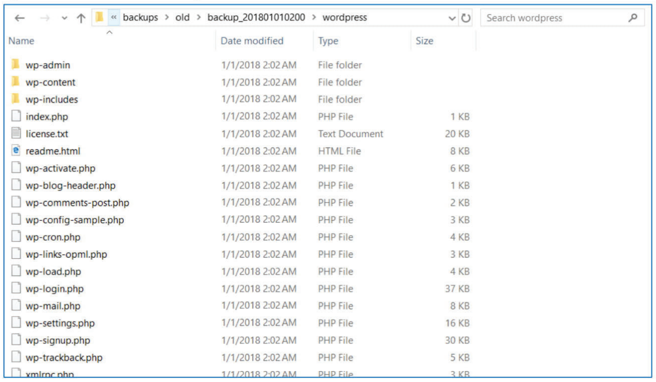
Name	Date modified	Type	Size
backup_201801010200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801020200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801030200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801040200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801050200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801060200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801070200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801080200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801090200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801100200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801110200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801120200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801130200.zip	11/20/2018 3:43 PM	Compressed (zipp...	
backup_201801140200.zip	11/20/2018 3:43 PM	Compressed (zipp...	

EXPLOIT DEMONSTRATION (continued)

The attacker is now in possession of the files and can evaluate their contents in an offline manner without concern of triggering alerts on the server. The file depicted in this example is a compressed archive containing what appears to be a complete backup of the server source code. The server is running a nightly job to locally backup the files, presumably to be retrieved by an external backup job for disaster recovery purposes. Most of the files are of little use to the attacker as the contain default code for a publicly available blog package. Researching the platform version using documentation available on the vendor website, several files are identified that contain configuration parameters required for the application to function. The source files are blocked from visitors of the application, however the backup archive does not apply these protections and therefore is not restricted by the hosting platform. A key value found in the configuration file is the password that the web service utilizes to communicate to the backend database.

The attacker extracts the contents of the backup file zip.

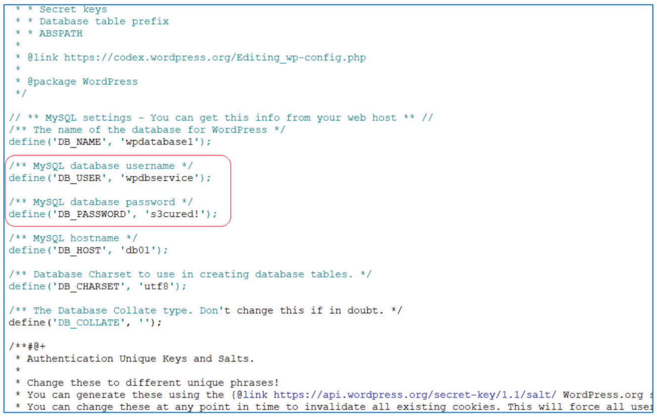
Figure 12. Contents of Backup File



Name	Date modified	Type	Size
wp-admin	1/1/2018 2:02 AM	File folder	
wp-content	1/1/2018 2:02 AM	File folder	
wp-includes	1/1/2018 2:02 AM	File folder	
index.php	1/1/2018 2:02 AM	PHP File	1 KB
license.txt	1/1/2018 2:02 AM	Text Document	20 KB
readme.html	1/1/2018 2:02 AM	HTML File	8 KB
wp-activate.php	1/1/2018 2:02 AM	PHP File	6 KB
wp-blog-header.php	1/1/2018 2:02 AM	PHP File	1 KB
wp-comments-post.php	1/1/2018 2:02 AM	PHP File	2 KB
wp-config-sample.php	1/1/2018 2:02 AM	PHP File	3 KB
wp-cron.php	1/1/2018 2:02 AM	PHP File	4 KB
wp-links-opml.php	1/1/2018 2:02 AM	PHP File	3 KB
wp-load.php	1/1/2018 2:02 AM	PHP File	4 KB
wp-login.php	1/1/2018 2:02 AM	PHP File	37 KB
wp-mail.php	1/1/2018 2:02 AM	PHP File	8 KB
wp-settings.php	1/1/2018 2:02 AM	PHP File	16 KB
wp-signup.php	1/1/2018 2:02 AM	PHP File	30 KB
wp-trackback.php	1/1/2018 2:02 AM	PHP File	5 KB
xmlrpc.php	1/1/2018 2:02 AM	PHP File	3 KB

The attacker locates sensitive information (WordPress credentials) in the wp-config.php file.

Figure 13. WordPress Credentials Located



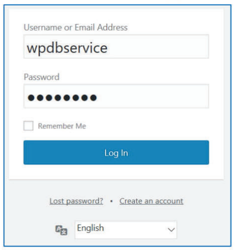
```
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wpdatabase1');

/** MySQL database username */
define('DB_USER', 'wpdbservice');

/** MySQL database password */
define('DB_PASSWORD', 's3cured!');

/** MySQL hostname */
define('DB_HOST', 'db01');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org s
 * You can change these at any point in time to invalidate all existing cookies. This will force all use
```

EXPLOIT DEMONSTRATION (continued)

The backend database is not directly accessible to an attacker positioned outside the environment, but experience has shown that administrators often reuse passwords rather than assigning unique passwords for different services. As the application management login screen is accessible to external users, the attacker attempts to re-use the database credentials to authenticate as the site administrator. The attacker is granted access, confirming the practice of password reuse and resulting in full administrative access to the site.

The attacker utilizes the credentials to authenticate to the WordPress management application.

Figure 14. Authenticating to the Server Using WordPress Credentials



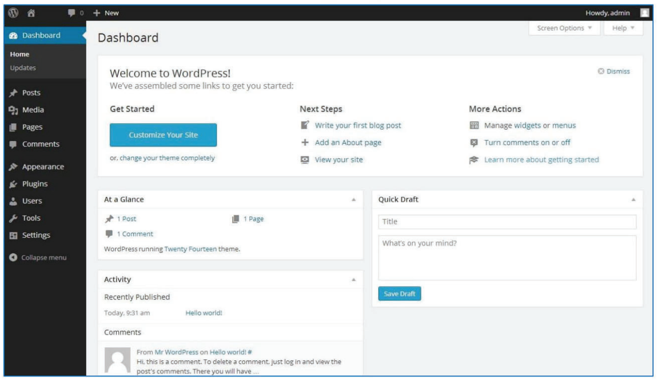
Username or Email Address: wpdbservice

Password: ●●●●●●●●

□ Remember Me

The attacker confirms administrative access to the WordPress management application.

Figure 15. Administrative Access to WordPress Management Application



Welcome to WordPress!
We've assembled some links to get you started:

WordPress running Twenty Fourteen theme.

From Mr WordPress on Hello world! #
Hi, this is a comment. To delete a comment, just log in and view the post's comments. There you will have …

REFERENCES

With the exploit demonstration concluded, additional references are provided. For this vulnerability, HALOCK provides two relevant articles related to both testing and administering the blog package.

References

Source	Link
OWASP: Review Old, Backup and Unreferenced Files for Sensitive Information	https://www.owasp.org/index.php/Review_Old,_Backup_and_Unreferenced_Files_for_Sensitive_Information_(OTG-CONFIG-004)
OWASP WordPress Security Implementation Guideline	https://www.owasp.org/index.php/OWASP_Wordpress_Security_Implementation_Guideline

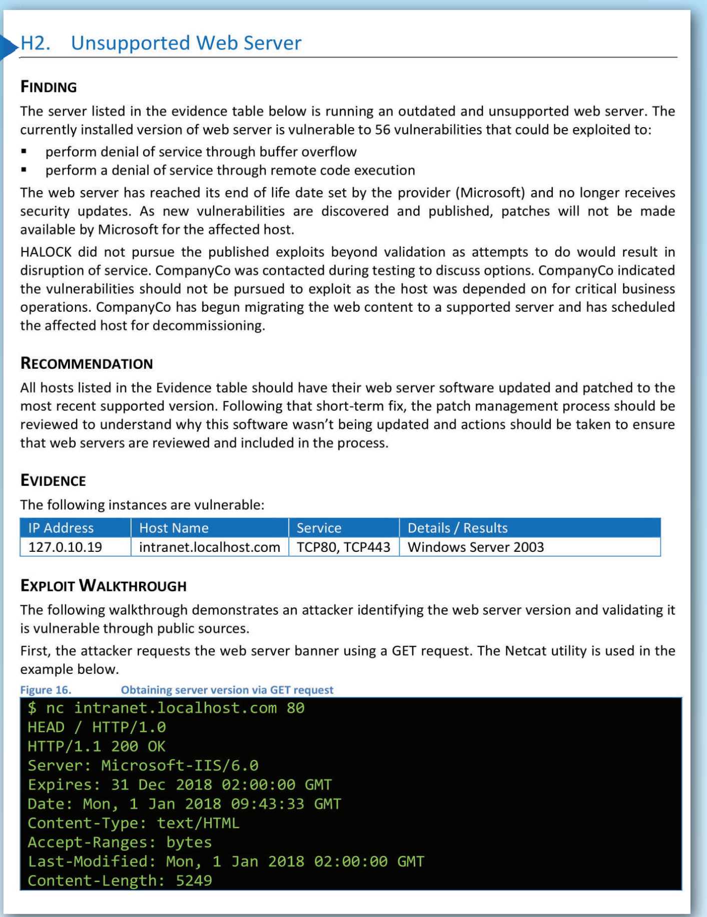
3. PENETRATION TEST REPORT

Comprehensive, accurate, and actionable results you can use.

DETAILED FINDING: H2

With the complete detail of finding H1 documented, the report progresses to the second high severity vulnerability. This next vulnerability focuses on exploits achieved as a result of an unsupported and unpatched web server.

The finding observes the same structure as depicted in the prior finding, albeit focused on this new vulnerability, its impact, and the associated exploits. This continues through all seventeen high severity findings obscured during testing.



H2. Unsupported Web Server

Finding

The server listed in the evidence table below is running an outdated and unsupported web server. The currently installed version of web server is vulnerable to 56 vulnerabilities that could be exploited to:

- perform denial of service through buffer overflow
- perform a denial of service through remote code execution

The web server has reached its end of life date set by the provider (Microsoft) and no longer receives security updates. As new vulnerabilities are discovered and published, patches will not be made available by Microsoft for the affected host.

HALOCK did not pursue the published exploits beyond validation as attempts to do would result in disruption of service. CompanyCo was contacted during testing to discuss options. CompanyCo indicated the vulnerabilities should not be pursued to exploit as the host was depended on for critical business operations. CompanyCo has begun migrating the web content to a supported server and has scheduled the affected host for decommissioning.

Recommendation

All hosts listed in the Evidence table should have their web server software updated and patched to the most recent supported version. Following that short-term fix, the patch management process should be reviewed to understand why this software wasn't being updated and actions should be taken to ensure that web servers are reviewed and included in the process.

Evidence

The following instances are vulnerable:

IP Address	Host Name	Service	Details / Results
127.0.10.19	intranet.localhost.com	TCP80, TCP443	Windows Server 2003

Exploit Walkthrough

The following walkthrough demonstrates an attacker identifying the web server version and validating it is vulnerable through public sources.

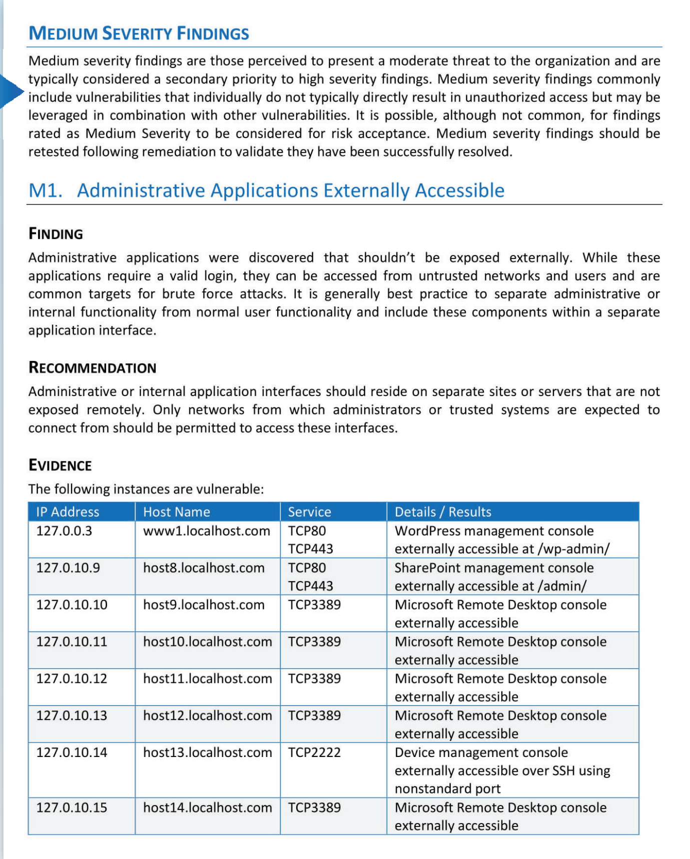
First, the attacker requests the web server banner using a GET request. The Netcat utility is used in the example below.

Figure 16. Obtaining server version via GET request

```
$ nc intranet.localhost.com 80
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Server: Microsoft-IIS/6.0
Expires: 31 Dec 2018 02:00:00 GMT
Date: Mon, 1 Jan 2018 09:43:33 GMT
Content-Type: text/HTML
Accept-Ranges: bytes
Last-Modified: Mon, 1 Jan 2018 02:00:00 GMT
Content-Length: 5249
```

DETAILED FINDINGS: MEDIUM SEVERITY

Following the High Severity Findings section, the report shifts to **Medium Severity** findings and recommendations. Medium Severity security weaknesses are generally of lesser priority than the High Severity and typically include non-exploitable vulnerabilities, vulnerabilities that can be exploited but with reduced impact. The Medium Severity findings utilize the same structure as the High, including the description of the vulnerability, the impact, recommendations, supporting evidence, and exploit demonstrations where applicable.



Medium Severity Findings

Medium severity findings are those perceived to present a moderate threat to the organization and are typically considered a secondary priority to high severity findings. Medium severity findings commonly include vulnerabilities that individually do not typically directly result in unauthorized access but may be leveraged in combination with other vulnerabilities. It is possible, although not common, for findings rated as Medium Severity to be considered for risk acceptance. Medium severity findings should be retested following remediation to validate they have been successfully resolved.

M1. Administrative Applications Externally Accessible

Finding

Administrative applications were discovered that shouldn't be exposed externally. While these applications require a valid login, they can be accessed from untrusted networks and users and are common targets for brute force attacks. It is generally best practice to separate administrative or internal functionality from normal user functionality and include these components within a separate application interface.

Recommendation

Administrative or internal application interfaces should reside on separate sites or servers that are not exposed remotely. Only networks from which administrators or trusted systems are expected to connect from should be permitted to access these interfaces.

Evidence

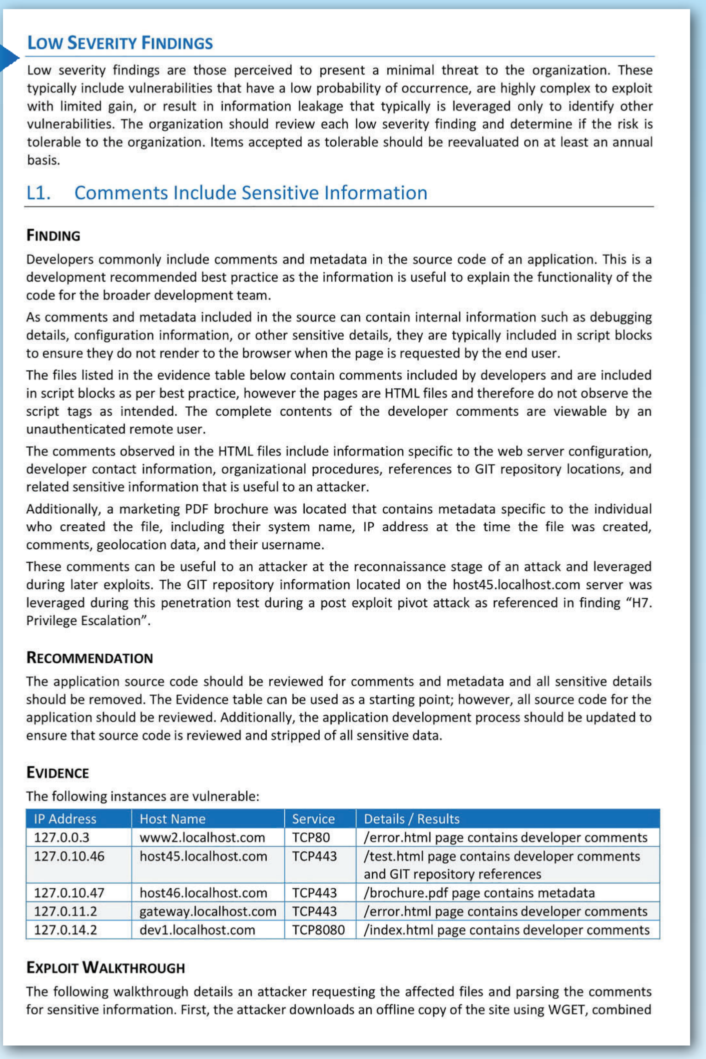
The following instances are vulnerable:

IP Address	Host Name	Service	Details / Results
127.0.0.3	www1.localhost.com	TCP80 TCP443	WordPress management console externally accessible at /wp-admin/
127.0.10.9	host8.localhost.com	TCP80 TCP443	SharePoint management console externally accessible at /admin/
127.0.10.10	host9.localhost.com	TCP3389	Microsoft Remote Desktop console externally accessible
127.0.10.11	host10.localhost.com	TCP3389	Microsoft Remote Desktop console externally accessible
127.0.10.12	host11.localhost.com	TCP3389	Microsoft Remote Desktop console externally accessible
127.0.10.13	host12.localhost.com	TCP3389	Microsoft Remote Desktop console externally accessible
127.0.10.14	host13.localhost.com	TCP2222	Device management console externally accessible over SSH using nonstandard port
127.0.10.15	host14.localhost.com	TCP3389	Microsoft Remote Desktop console externally accessible

3. PENETRATION TEST REPORT Comprehensive, accurate, and actionable results you can use.

DETAILED FINDINGS: LOW SEVERITY

Following the Medium Severity Findings, **Low Severity** and remaining best practices findings are documented. These findings are typically of the lowest priority and may be evaluated for risk acceptance. The Low Severity findings utilize the same structure as the High and Medium, including the description of the vulnerability, the impact, recommendations, supporting evidence, and exploit demonstrations where applicable.



Low Severity Findings

Low severity findings are those perceived to present a minimal threat to the organization. These typically include vulnerabilities that have a low probability of occurrence, are highly complex to exploit with limited gain, or result in information leakage that typically is leveraged only to identify other vulnerabilities. The organization should review each low severity finding and determine if the risk is tolerable to the organization. Items accepted as tolerable should be reevaluated on at least an annual basis.

L1. Comments Include Sensitive Information

Finding

Developers commonly include comments and metadata in the source code of an application. This is a development recommended best practice as the information is useful to explain the functionality of the code for the broader development team.

As comments and metadata included in the source can contain internal information such as debugging details, configuration information, or other sensitive details, they are typically included in script blocks to ensure they do not render to the browser when the page is requested by the end user.

The files listed in the evidence table below contain comments included by developers and are included in script blocks as per best practice, however the pages are HTML files and therefore do not observe the script tags as intended. The complete contents of the developer comments are viewable by an unauthenticated remote user.

The comments observed in the HTML files include information specific to the web server configuration, developer contact information, organizational procedures, references to GIT repository locations, and related sensitive information that is useful to an attacker.

Additionally, a marketing PDF brochure was located that contains metadata specific to the individual who created the file, including their system name, IP address at the time the file was created, comments, geolocation data, and their username.

These comments can be useful to an attacker at the reconnaissance stage of an attack and leveraged during later exploits. The GIT repository information located on the host45.localhost.com server was leveraged during this penetration test during a post exploit pivot attack as referenced in finding "H7. Privilege Escalation".

Recommendation

The application source code should be reviewed for comments and metadata and all sensitive details should be removed. The Evidence table can be used as a starting point; however, all source code for the application should be reviewed. Additionally, the application development process should be updated to ensure that source code is reviewed and stripped of all sensitive data.

Evidence

The following instances are vulnerable:

IP Address	Host Name	Service	Details / Results
127.0.0.3	www2.localhost.com	TCP80	/error.html page contains developer comments
127.0.10.46	host45.localhost.com	TCP443	/test.html page contains developer comments and GIT repository references
127.0.10.47	host46.localhost.com	TCP443	/brochure.pdf page contains metadata
127.0.11.2	gateway.localhost.com	TCP443	/error.html page contains developer comments
127.0.14.2	dev1.localhost.com	TCP8080	/index.html page contains developer comments

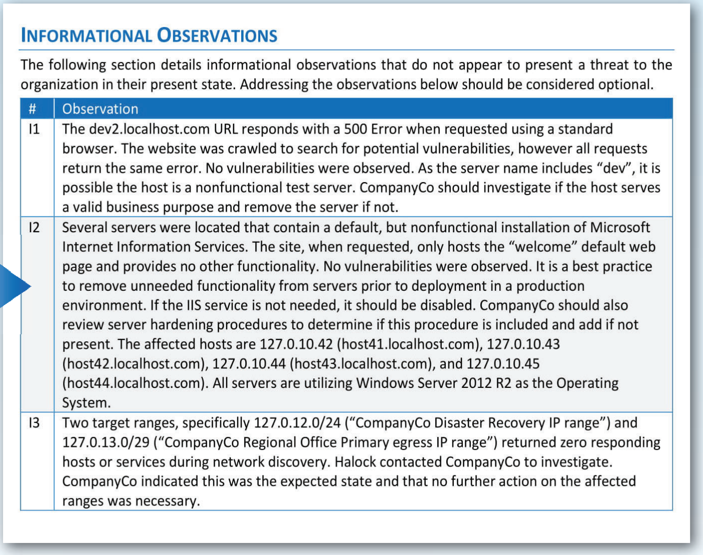
Exploit Walkthrough

The following walkthrough details an attacker requesting the affected files and parsing the comments for sensitive information. First, the attacker downloads an offline copy of the site using WGET, combined

INFORMATIONAL OBSERVATIONS

Following all documented vulnerabilities, **informational observations** are provided as a courtesy. This section is limited to observations made during testing that do not appear to impact security but may still be of use to the organization.

In this example, the tester observed several orphaned or otherwise non-functioning links on a website that was being targeted. While these did not yield any security flaws, the organization was made aware of the issues, so they could be corrected.



Informational Observations

The following section details informational observations that do not appear to present a threat to the organization in their present state. Addressing the observations below should be considered optional.

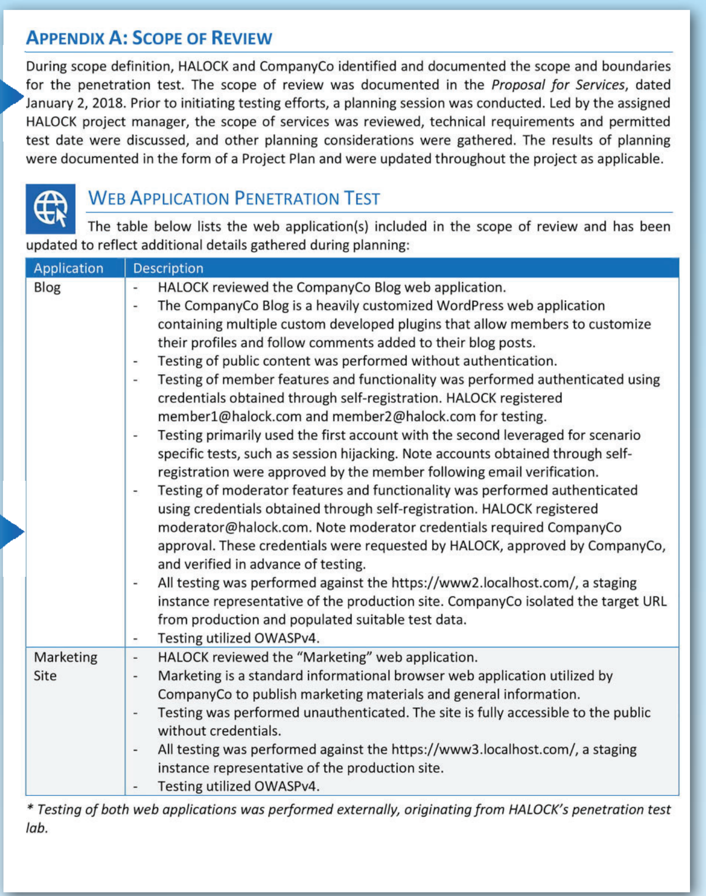
#	Observation
I1	The dev2.localhost.com URL responds with a 500 Error when requested using a standard browser. The website was crawled to search for potential vulnerabilities, however all requests return the same error. No vulnerabilities were observed. As the server name includes "dev", it is possible the host is a nonfunctional test server. CompanyCo should investigate if the host serves a valid business purpose and remove the server if not.
I2	Several servers were located that contain a default, but nonfunctional installation of Microsoft Internet Information Services. The site, when requested, only hosts the "welcome" default web page and provides no other functionality. No vulnerabilities were observed. It is a best practice to remove unneeded functionality from servers prior to deployment in a production environment. If the IIS service is not needed, it should be disabled. CompanyCo should also review server hardening procedures to determine if this procedure is included and add if not present. The affected hosts are 127.0.10.42 (host41.localhost.com), 127.0.10.43 (host42.localhost.com), 127.0.10.44 (host43.localhost.com), and 127.0.10.45 (host44.localhost.com). All servers are utilizing Windows Server 2012 R2 as the Operating System.
I3	Two target ranges, specifically 127.0.12.0/24 ("CompanyCo Disaster Recovery IP range") and 127.0.13.0/29 ("CompanyCo Regional Office Primary egress IP range") returned zero responding hosts or services during network discovery. Halock contacted CompanyCo to investigate. CompanyCo indicated this was the expected state and that no further action on the affected ranges was necessary.

3. PENETRATION TEST REPORT Comprehensive, accurate, and actionable results you can use.

APPENDIX: SCOPE OF REVIEW

The report appendix provides additional detail related to the test, including the complete detail of the **scope of review**, a list of all responding hosts and services that were targeted during testing, sampling thresholds observed, and related information. This information is largely derived from earlier scope and planning documents that discuss the testing that is planned. With the test complete, this same information can be expanded upon to reflect additional useful detail, both validating the plan was executed and preserving the details of the environment as they were observed during testing.

First, the complete scope of the target web applications is documented, including additional details provided during planning, such as the specific target URLs and test accounts used.



Appendix A: Scope of Review

During scope definition, HALOCK and CompanyCo identified and documented the scope and boundaries for the penetration test. The scope of review was documented in the *Proposal for Services*, dated January 2, 2018. Prior to initiating testing efforts, a planning session was conducted. Led by the assigned HALOCK project manager, the scope of services was reviewed, technical requirements and permitted test date were discussed, and other planning considerations were gathered. The results of planning were documented in the form of a Project Plan and were updated throughout the project as applicable.

Web Application Penetration Test

The table below lists the web application(s) included in the scope of review and has been updated to reflect additional details gathered during planning:

Application	Description
Blog	- HALOCK reviewed the CompanyCo Blog web application. - The CompanyCo Blog is a heavily customized WordPress web application containing multiple custom developed plugins that allow members to customize their profiles and follow comments added to their blog posts. - Testing of public content was performed without authentication. - Testing of member features and functionality was performed authenticated using credentials obtained through self-registration. HALOCK registered member1@halock.com and member2@halock.com for testing. - Testing primarily used the first account with the second leveraged for scenario specific tests, such as session hijacking. Note accounts obtained through self-registration were approved by the member following email verification. - Testing of moderator features and functionality was performed authenticated using credentials obtained through self-registration. HALOCK registered moderator@halock.com. Note moderator credentials required CompanyCo approval. These credentials were requested by HALOCK, approved by CompanyCo, and verified in advance of testing. - All testing was performed against the https://www2.localhost.com/, a staging instance representative of the production site. CompanyCo isolated the target URL from production and populated suitable test data. - Testing utilized OWASPv4.
Marketing Site	- HALOCK reviewed the "Marketing" web application. - Marketing is a standard informational browser web application utilized by CompanyCo to publish marketing materials and general information. - Testing was performed unauthenticated. The site is fully accessible to the public without credentials. - All testing was performed against the https://www3.localhost.com/, a staging instance representative of the production site. - Testing utilized OWASPv4.

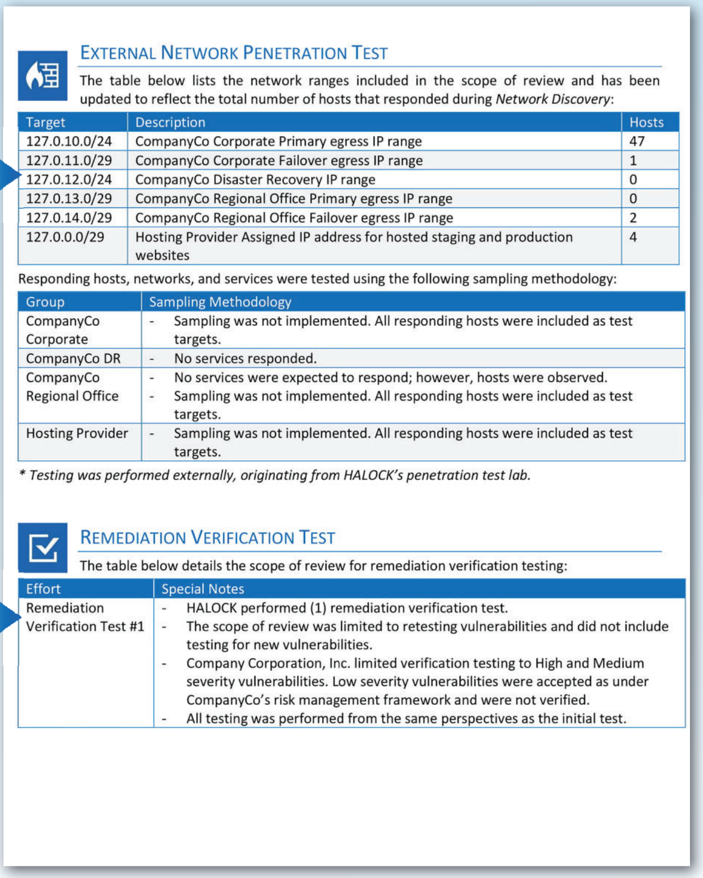
** Testing of both web applications was performed externally, originating from HALOCK's penetration test lab.*

APPENDIX: SCOPE OF REVIEW (continued)

The **scope of review** continues to detail the external network penetration test. The specific ranges provided for testing, total hosts that responded, and sampling thresholds are documented as the test was conducted.

APPENDIX: SCOPE OF REVIEW (continued)

Finally, the remediation verification test is provided, concluding the **scope of review**.



External Network Penetration Test

The table below lists the network ranges included in the scope of review and has been updated to reflect the total number of hosts that responded during *Network Discovery*:

Target	Description	Hosts
127.0.10.0/24	CompanyCo Corporate Primary egress IP range	47
127.0.11.0/29	CompanyCo Corporate Failover egress IP range	1
127.0.12.0/24	CompanyCo Disaster Recovery IP range	0
127.0.13.0/29	CompanyCo Regional Office Primary egress IP range	0
127.0.14.0/29	CompanyCo Regional Office Failover egress IP range	2
127.0.0.0/29	Hosting Provider Assigned IP address for hosted staging and production websites	4

Responding hosts, networks, and services were tested using the following sampling methodology:

Group	Sampling Methodology
CompanyCo Corporate	- Sampling was not implemented. All responding hosts were included as test targets.
CompanyCo DR	- No services responded.
CompanyCo Regional Office	- No services were expected to respond; however, hosts were observed. - Sampling was not implemented. All responding hosts were included as test targets.
Hosting Provider	- Sampling was not implemented. All responding hosts were included as test targets.

** Testing was performed externally, originating from HALOCK's penetration test lab.*

Remediation Verification Test

The table below details the scope of review for remediation verification testing:

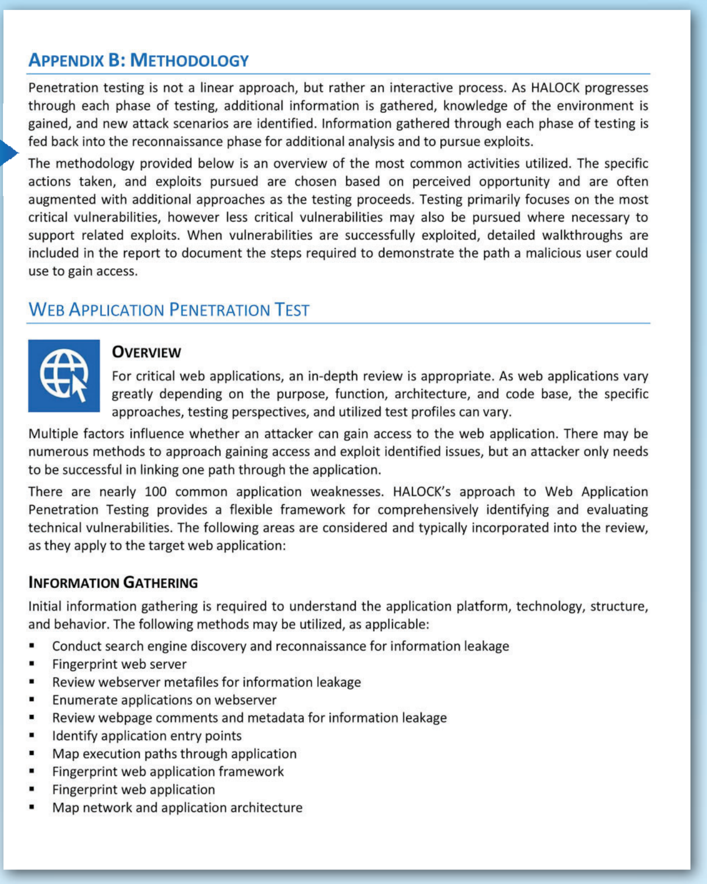
Effort	Special Notes
Remediation Verification Test #1	- HALOCK performed (1) remediation verification test. - The scope of review was limited to retesting vulnerabilities and did not include testing for new vulnerabilities. - Company Corporation, Inc. limited verification testing to High and Medium severity vulnerabilities. Low severity vulnerabilities were accepted as under CompanyCo's risk management framework and were not verified. - All testing was performed from the same perspectives as the initial test.

3. PENETRATION TEST REPORT Comprehensive, accurate, and actionable results you can use.

APPENDIX: METHODOLOGY

Following the scope of review (what was tested), the report also contains a complete recap of the **methodology** utilized (how testing was performed).

Here, the web application testing methodology is documented. Readers of the report can reference this section to understand what test methods were utilized to produce the findings, confirm testing was performed using industry standard methods, and ensure that future tests or re-tests can leverage a repeatable methodology.



Appendix B: Methodology

Penetration testing is not a linear approach, but rather an interactive process. As HALOCK progresses through each phase of testing, additional information is gathered, knowledge of the environment is gained, and new attack scenarios are identified. Information gathered through each phase of testing is fed back into the reconnaissance phase for additional analysis and to pursue exploits.

The methodology provided below is an overview of the most common activities utilized. The specific actions taken, and exploits pursued are chosen based on perceived opportunity and are often augmented with additional approaches as the testing proceeds. Testing primarily focuses on the most critical vulnerabilities, however less critical vulnerabilities may also be pursued where necessary to support related exploits. When vulnerabilities are successfully exploited, detailed walkthroughs are included in the report to document the steps required to demonstrate the path a malicious user could use to gain access.

Web Application Penetration Test

Overview

For critical web applications, an in-depth review is appropriate. As web applications vary greatly depending on the purpose, function, architecture, and code base, the specific approaches, testing perspectives, and utilized test profiles can vary.

Multiple factors influence whether an attacker can gain access to the web application. There may be numerous methods to approach gaining access and exploit identified issues, but an attacker only needs to be successful in linking one path through the application.

There are nearly 100 common application weaknesses. HALOCK's approach to Web Application Penetration Testing provides a flexible framework for comprehensively identifying and evaluating technical vulnerabilities. The following areas are considered and typically incorporated into the review, as they apply to the target web application:

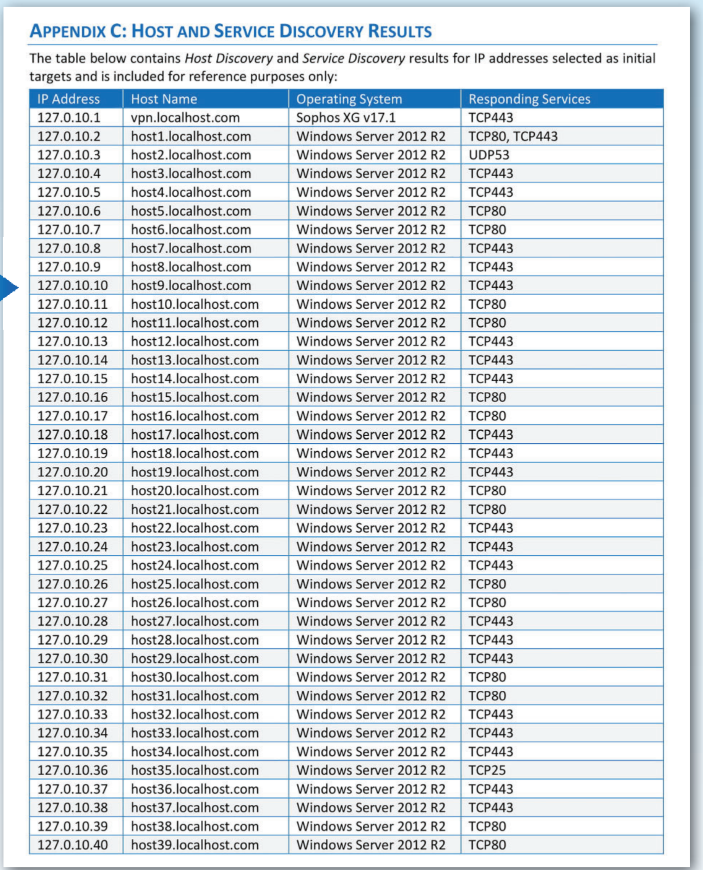
Information Gathering

Initial information gathering is required to understand the application platform, technology, structure, and behavior. The following methods may be utilized, as applicable:

- Conduct search engine discovery and reconnaissance for information leakage
- Fingerprint web server
- Review webserver metafiles for information leakage
- Enumerate applications on webserver
- Review webpage comments and metadata for information leakage
- Identify application entry points
- Map execution paths through application
- Fingerprint web application framework
- Fingerprint web application
- Map network and application architecture

APPENDIX: SUPPLEMENTAL MATERIALS

Supplemental materials are provided, as applicable to the scope of review. As this penetration test included external network testing, host and service discovery was performed. The results are included as a courtesy to allow a comparison to an upcoming firewall audit being planned.



Appendix C: Host and Service Discovery Results

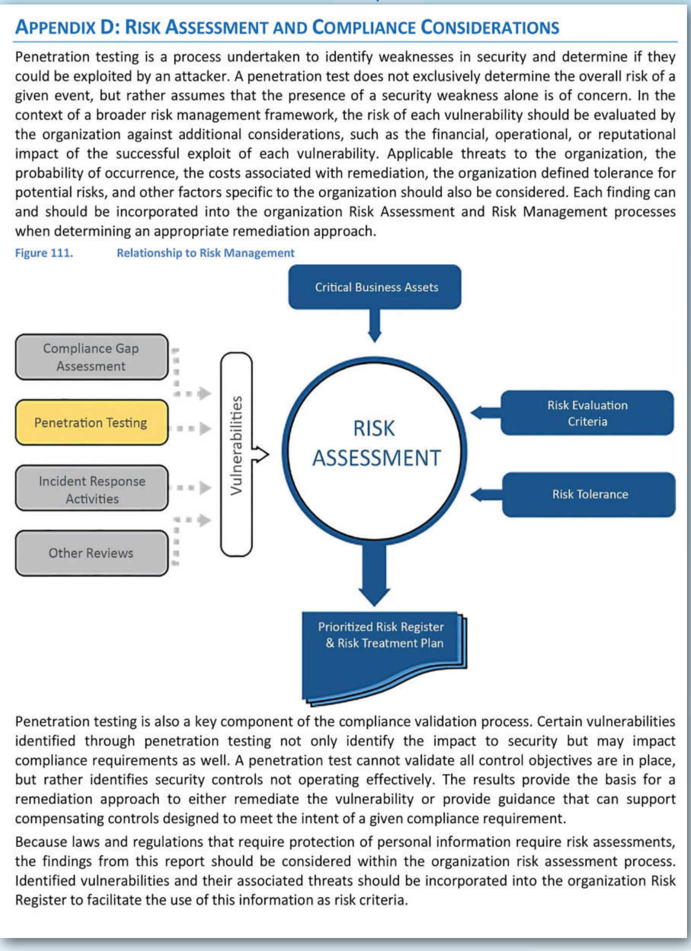
The table below contains *Host Discovery* and *Service Discovery* results for IP addresses selected as initial targets and is included for reference purposes only:

IP Address	Host Name	Operating System	Responding Services
127.0.10.1	vpn.localhost.com	Sophos XG v17.1	TCP443
127.0.10.2	host1.localhost.com	Windows Server 2012 R2	TCP80, TCP443
127.0.10.3	host2.localhost.com	Windows Server 2012 R2	UDP53
127.0.10.4	host3.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.5	host4.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.6	host5.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.7	host6.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.8	host7.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.9	host8.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.10	host9.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.11	host10.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.12	host11.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.13	host12.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.14	host13.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.15	host14.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.16	host15.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.17	host16.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.18	host17.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.19	host18.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.20	host19.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.21	host20.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.22	host21.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.23	host22.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.24	host23.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.25	host24.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.26	host25.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.27	host26.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.28	host27.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.29	host28.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.30	host29.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.31	host30.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.32	host31.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.33	host32.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.34	host33.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.35	host34.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.36	host35.localhost.com	Windows Server 2012 R2	TCP25
127.0.10.37	host36.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.38	host37.localhost.com	Windows Server 2012 R2	TCP443
127.0.10.39	host38.localhost.com	Windows Server 2012 R2	TCP80
127.0.10.40	host39.localhost.com	Windows Server 2012 R2	TCP80

APPENDIX: POST ASSESSMENT

Following the completion of a penetration test, post assessment activities begin. These activities can vary greatly depending on the scope of the test, existing planned initiatives, and other considerations. For this specific penetration test, the organization indicated they were beginning to implement an enterprise risk management framework with HALOCK's risk assessment team and intended to utilize the results of the penetration test as an input into the initiative. Additionally, compliance with new regulations were on the horizon. The report included a primer on risk assessment, compliance management, and the relationship of both with penetration testing.

Below, on the left, we see a contextual depiction of where the penetration test results enter this process, as well as discussion of their relationship to evaluation criteria, risk tolerance, and risk treatment. On the right, a sample risk register is also provided as a courtesy. The organization intends to use this sample risk register as a basis, add additional evaluation criteria based on their risk management framework, and define risk acceptance considerations for vulnerabilities deemed to be within the accepted risk threshold



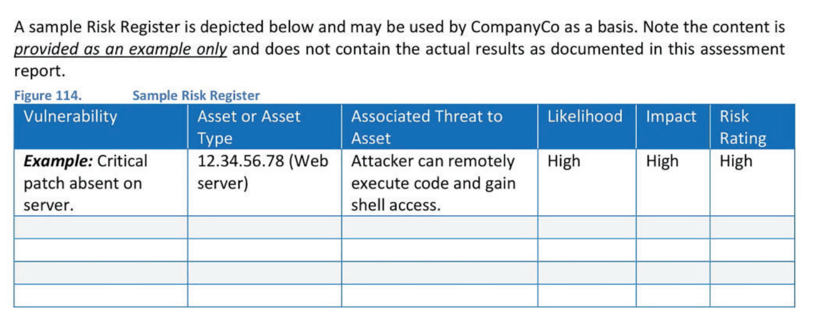
Appendix D: Risk Assessment and Compliance Considerations

Penetration testing is a process undertaken to identify weaknesses in security and determine if they could be exploited by an attacker. A penetration test does not exclusively determine the overall risk of a given event, but rather assumes that the presence of a security weakness alone is of concern. In the context of a broader risk management framework, the risk of each vulnerability should be evaluated by the organization against additional considerations, such as the financial, operational, or reputational impact of the successful exploit of each vulnerability. Applicable threats to the organization, the probability of occurrence, the costs associated with remediation, the organization defined tolerance for potential risks, and other factors specific to the organization should also be considered. Each finding can and should be incorporated into the organization Risk Assessment and Risk Management processes when determining an appropriate remediation approach.

Figure 111. Relationship to Risk Management

Penetration testing is also a key component of the compliance validation process. Certain vulnerabilities identified through penetration testing not only identify the impact to security but may impact compliance requirements as well. A penetration test cannot validate all control objectives are in place, but rather identifies security controls not operating effectively. The results provide the basis for a remediation approach to either remediate the vulnerability or provide guidance that can support compensating controls designed to meet the intent of a given compliance requirement.

Because laws and regulations that require protection of personal information require risk assessments, the findings from this report should be considered within the organization risk assessment process. Identified vulnerabilities and their associated threats should be incorporated into the organization Risk Register to facilitate the use of this information as risk criteria.



A sample Risk Register is depicted below and may be used by CompanyCo as a basis. Note the content is *provided as an example only* and does not contain the actual results as documented in this assessment report.

Figure 114. Sample Risk Register

Vulnerability	Asset or Asset Type	Associated Threat to Asset	Likelihood	Impact	Risk Rating
Example: Critical patch absent on server.	12.34.56.78 (Web server)	Attacker can remotely execute code and gain shell access.	High	High	High

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200

Incident Response Hotline: 800-925-0559

www.halock.com