# WEEK 03 REPORT

# Web Application Penetration Test Report

**By**

**Muhammed Ajeel**

# Executive Summary

**Target Application:** Mutillidae II (OWASP Web Application)
**Target URL:** http://192.168.56.102/mutillidae/

**Target IP:** 192.168.56.102

**Tester:** Ajeel

**Assessment Type:** Web Application Security Assessment

**Testing Environment:** Isolated Virtual Lab (VirtualBox Host-Only Network)

## Risk Assessment Overview

| Severity Level | Count | Examples |
|---|---|---|
| Critical | 2 | Stored XSS, Reflected XSS |
| High | 1 | Weak Session Management |
| Medium | 1 | Information Disclosure |

## Key Findings

**1.Critical**: Confirmed Reflected Cross-Site Scripting (XSS) vulnerability in DNS Lookup functionality
**2.Critical**: Confirmed Stored XSS vulnerability in Blog functionality
**3.High**: Session cookies missing HttpOnly and Secure flags
**4.Medium**: Outdated Apache server version disclosure

# 1. Testing Methodology & Scope

## 1.1 Approach

This assessment followed a hybrid testing methodology combining:

- Manual penetration testing techniques
- Automated vulnerability scanning
- Proof-of-concept exploitation
- Security header analysis

## 1.2 Tools Utilized

- **Burp Suite Professional 2023**: Proxy interception and site mapping
- **OWASP ZAP 2.12**: Automated vulnerability scanning
- **Nikto 2.1.6**: Web server vulnerability assessment
- **Firefox Developer Tools**: Client-side analysis and cookie inspection
- **Manual Testing**: Custom payload testing and validation

## 1.3 Test Cases Executed

1. Application mapping and reconnaissance
2. Input validation testing
3. Session management assessment
4. Automated vulnerability scanning
5. Proof-of-concept exploitation
6. Security header analysis

# 2. Detailed Findings

## 2.1 Reflected Cross-Site Scripting (XSS) 🔴 CRITICAL

**Location:** `/mutillidae/index.php?page=dns-lookup.php`
**OWASP Category:** A03:2021-Injection
**CVSS Score:** 7.5 (High)

### Vulnerability Description

The DNS Lookup functionality within the Mutillidae application fails to properly sanitize user input, allowing malicious JavaScript execution in the victim's browser context.

### Proof of Concept

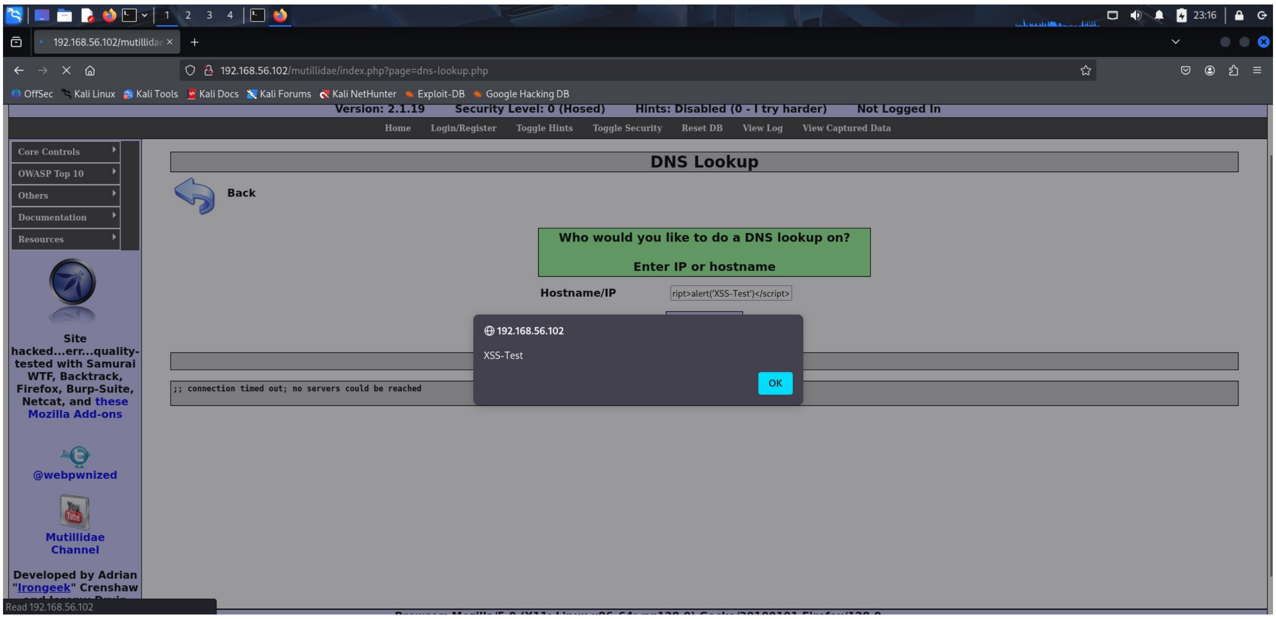
**Payload Used:**

```html
<script>alert('XSS Test')</script>
```

### Steps to Reproduce:

1. Navigate to: OWASP Top 10 → A2 - Cross-Site Scripting → Reflected → DNS Lookup
2. Enter payload: `<script>alert('XSS Test')</script>`
3. Click "Lookup DNS"
4. Observe JavaScript execution via alert popup

### HTTP Request (Burp Suite):



Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP ript>alert('XSS-Test')</script>

192.168.56.102

XSS-Test

```
;; connection timed out; no servers could be reached
```

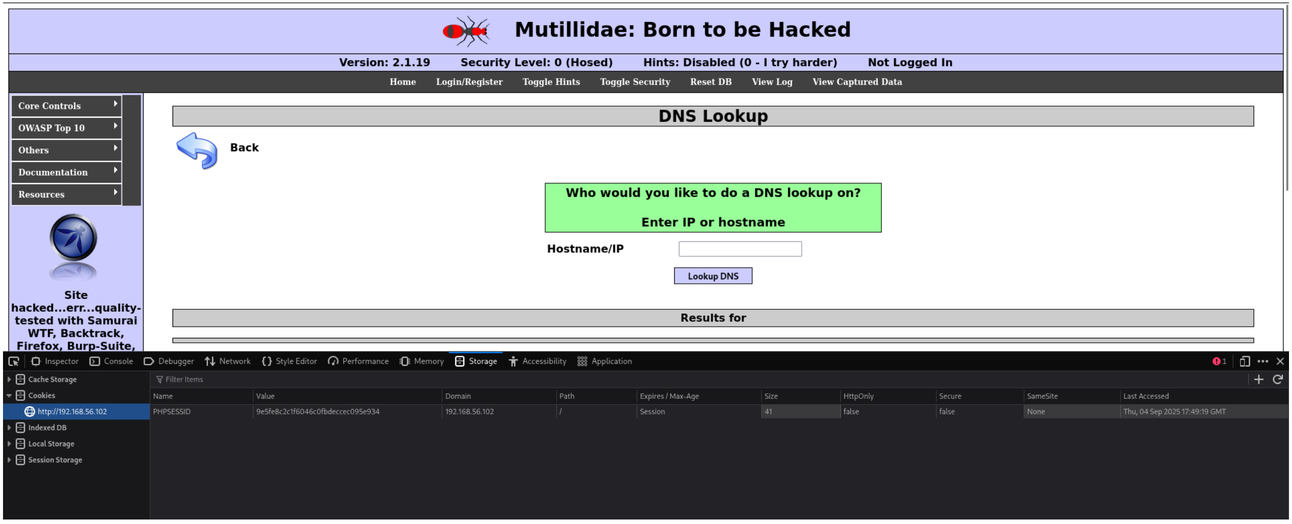
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

Developed by Adrian "Irongeek" Crenshaw

Read 192.168.56.102

```http
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 192.168.56.102
Content-Type: application/x-www-form-urlencoded
Content-Length: 56

target_host=<script>alert('XSS+Test')</script>&lookup=Lookup+DNS
```



Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Results for

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite,

| Name | Value | Domain | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed |
|---|---|---|---|---|---|---|---|---|---|
| PHPSESSID | 9e5fe8c2c1f6046c0fbdeccec095e934 | 192.168.56.102 | / | Session | 41 | false | false | None | Thu, 04 Sep 2025 17:49:19 GMT |

**Impact:** Attackers can steal session cookies, redirect users to malicious sites, or perform actions on behalf of the user.

## 2.2 Stored Cross-Site Scripting (XSS) 🔴 CRITICAL

**Location:** Blog functionality (`/mutillidae/index.php?page=add-to-your-blog.php`)
**OWASP Category:** A03:2021-Injection
**CVSS Score:** 8.1 (High)

### Vulnerability Description

The Blog functionality allows persistent storage of malicious scripts that execute automatically when other users view the compromised content.

### Proof of Concept

#### Payload Used:

```html
<script>alert('Stored XSS Test!')</script>
```

#### Steps to Reproduce:

1.Navigate to: Blog → Add to your blog

2.Enter values:

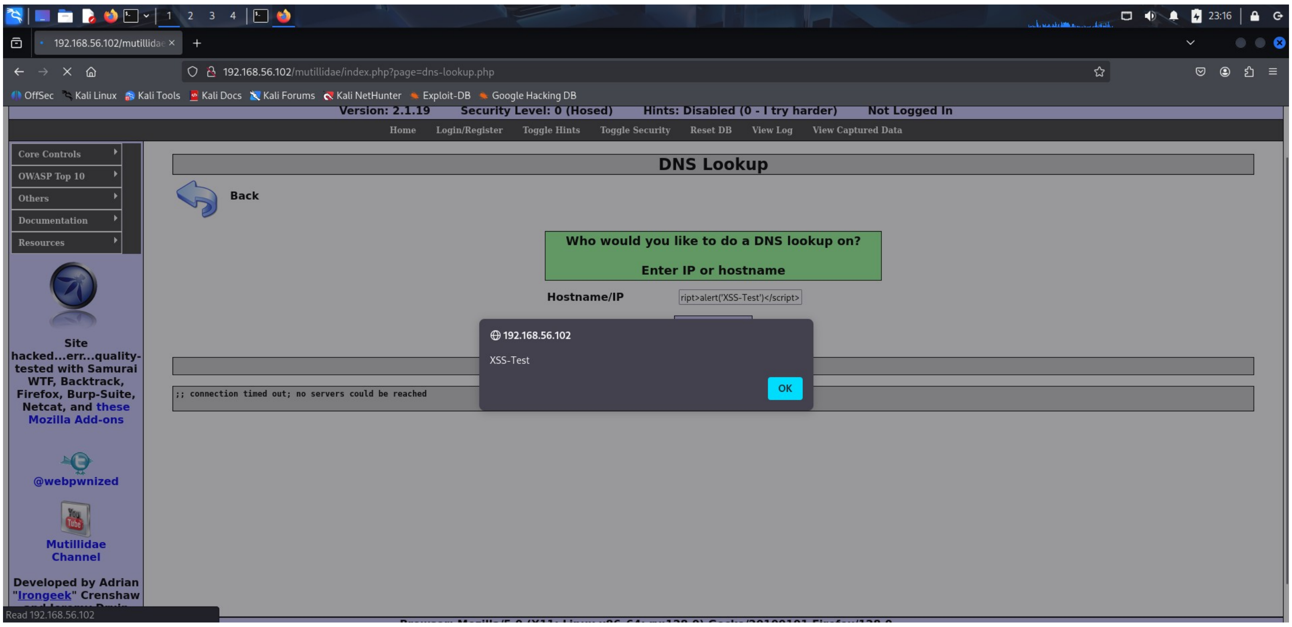
- Title: "Test Blog Post"
- Blog Entry: `<script>alert('Stored XSS Test!')</script>`
- Signature: "Tester"

3.Click "Save Blog Entry"

4.Observe immediate XSS execution

5.Navigate away and return to confirm persistence

**Impact:** Persistent attack vector affecting all users who view the malicious content. Can lead to widespread session hijacking.



192.168.56.102/mutillidae/index.php?page=dns-lookup.php

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP ript>alert('XSS-Test')</script>

192.168.56.102

XSS-Test

```
;; connection timed out; no servers could be reached
```

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

Developed by Adrian "Irongeek" Crenshaw

Read 192.168.56.102

### Remediation

1.Implement strict input validation for all user-generated content

2.Use HTML sanitization libraries before storing user content

3.Implement CSP headers to restrict script execution

4.Regular security testing of user content features

## 2.3 Weak Session Management 🟠 HIGH

**Location:** Application-wide session handling
**OWASP Category:** A01:2021-Broken Access Control
**CVSS Score:** 6.5 (Medium)

### Vulnerability Description

The application uses session cookies that lack essential security flags, increasing the risk of session hijacking attacks.

### Technical Details

### Cookie Analysis:

```http
Set-Cookie: PHPSESSID=abc123def456; path=/
```

### Missing Security Attributes:

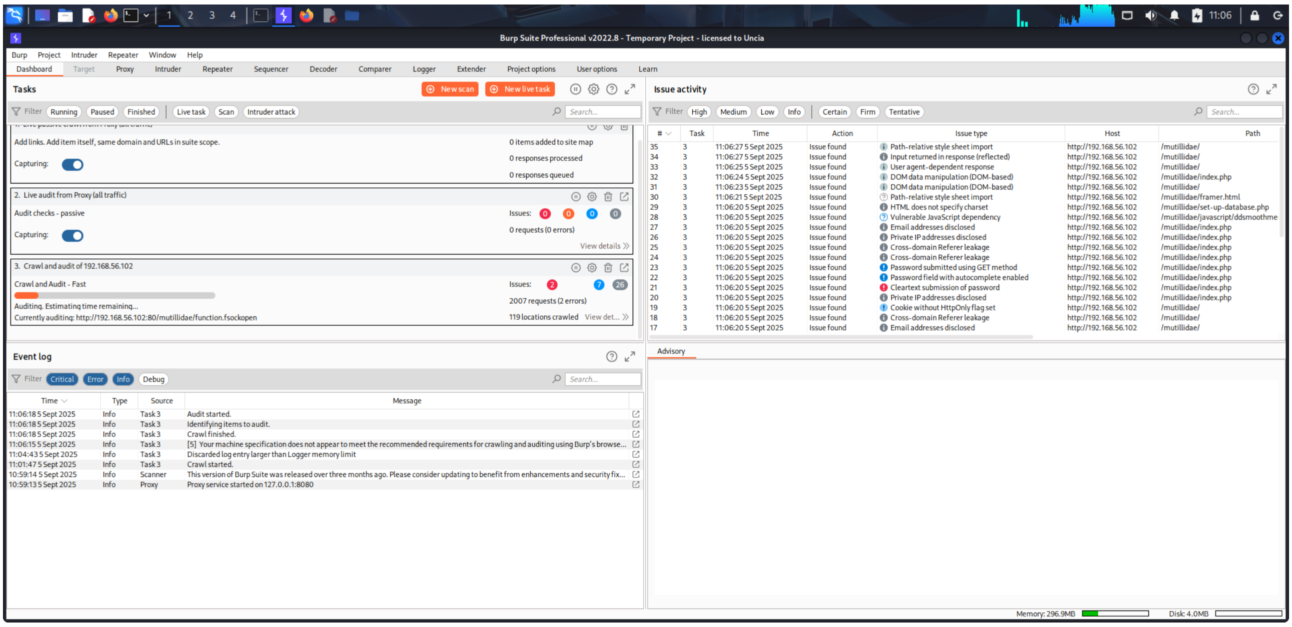
- ❌ **HttpOnly Flag**: Absent, allowing JavaScript access to cookies
- ❌ **Secure Flag**: Absent, allowing transmission over unencrypted HTTP
- ❌ **SameSite Attribute**: Absent, increasing CSRF vulnerability

### Session Behavior:

- Cookies are generated for all users upon first request
- Session identifiers change appropriately between browser sessions
- No session fixation detected

## Impact

- Session cookies accessible via XSS attacks
- Potential for session hijacking and account compromise
- Increased risk of man-in-the-middle attacks


Burp Suite Professional v2022.8 - Temporary Project - licensed to Uncia
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Search...
Issue activity
Filter High Medium Low Info Certain Firm Tentative
Event log
Filter Critical Error Info Debug
Advisory
Memory: 296.9MB
Disk: 4.0MB

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

0 items added to site map

0 responses processed

0 responses queued

2. Live audit from Proxy (all traffic)

Audit checks - passive

Capturing:

Issues: 0 0 0 0

0 requests (0 errors)

View details

3. Crawl and audit of 192.168.56.102

Crawl and Audit - Fast

Auditing. Estimating time remaining...

Currently auditing: http://192.168.56.102:80/mutillidae/function.fsockopen

Issues: 2 7 26

2007 requests (2 errors)

119 locations crawled View det...

| # | Task | Time | Action | Issue type | Host | Path |
|---|---|---|---|---|---|---|
| 35 | 3 | 11:06:27 5 Sept 2025 | Issue found | Path-relative style sheet import | http://192.168.56.102 | /mutillidae/ |
| 34 | 3 | 11:06:27 5 Sept 2025 | Issue found | Input returned in response (reflected) | http://192.168.56.102 | /mutillidae/ |
| 33 | 3 | 11:06:25 5 Sept 2025 | Issue found | User agent-dependent response | http://192.168.56.102 | /mutillidae/ |
| 32 | 3 | 11:06:24 5 Sept 2025 | Issue found | DOM data manipulation (DOM-based) | http://192.168.56.102 | /mutillidae/index.php |
| 31 | 3 | 11:06:23 5 Sept 2025 | Issue found | DOM data manipulation (DOM-based) | http://192.168.56.102 | /mutillidae/ |
| 30 | 3 | 11:06:21 5 Sept 2025 | Issue found | Path-relative style sheet import | http://192.168.56.102 | /mutillidae/framer.html |
| 29 | 3 | 11:06:20 5 Sept 2025 | Issue found | HTML does not specify charset | http://192.168.56.102 | /mutillidae/set-up-database.php |
| 28 | 3 | 11:06:20 5 Sept 2025 | Issue found | Vulnerable JavaScript dependency | http://192.168.56.102 | /mutillidae/javascript/ddsmoothme |
| 27 | 3 | 11:06:20 5 Sept 2025 | Issue found | Email addresses disclosed | http://192.168.56.102 | /mutillidae/index.php |
| 26 | 3 | 11:06:20 5 Sept 2025 | Issue found | Private IP addresses disclosed | http://192.168.56.102 | /mutillidae/index.php |
| 25 | 3 | 11:06:20 5 Sept 2025 | Issue found | Cross-domain Referer leakage | http://192.168.56.102 | /mutillidae/index.php |
| 24 | 3 | 11:06:20 5 Sept 2025 | Issue found | Cross-domain Referer leakage | http://192.168.56.102 | /mutillidae/index.php |
| 23 | 3 | 11:06:20 5 Sept 2025 | Issue found | Password submitted using GET method | http://192.168.56.102 | /mutillidae/index.php |
| 22 | 3 | 11:06:20 5 Sept 2025 | Issue found | Password field with autocomplete enabled | http://192.168.56.102 | /mutillidae/index.php |
| 21 | 3 | 11:06:20 5 Sept 2025 | Issue found | Cleartext submission of password | http://192.168.56.102 | /mutillidae/index.php |
| 20 | 3 | 11:06:20 5 Sept 2025 | Issue found | Private IP addresses disclosed | http://192.168.56.102 | /mutillidae/index.php |
| 19 | 3 | 11:06:20 5 Sept 2025 | Issue found | Cookie without HttpOnly flag set | http://192.168.56.102 | /mutillidae/ |
| 18 | 3 | 11:06:20 5 Sept 2025 | Issue found | Cross-domain Referer leakage | http://192.168.56.102 | /mutillidae/ |
| 17 | 3 | 11:06:20 5 Sept 2025 | Issue found | Email addresses disclosed | http://192.168.56.102 | /mutillidae/ |

| Time | Type | Source | Message |
|---|---|---|---|
| 11:06:18 5 Sept 2025 | Info | Task 3 | Audit started. |
| 11:06:18 5 Sept 2025 | Info | Task 3 | Identifying items to audit. |
| 11:06:18 5 Sept 2025 | Info | Task 3 | Crawl finished. |
| 11:06:15 5 Sept 2025 | Info | Task 3 | [5] Your machine specification does not appear to meet the recommended requirements for crawling and auditing using Burp's browse... |
| 11:04:43 5 Sept 2025 | Info | Task 3 | Discarded log entry larger than Logger memory limit |
| 11:01:47 5 Sept 2025 | Info | Task 3 | Crawl started. |
| 10:59:14 5 Sept 2025 | Info | Scanner | This version of Burp Suite was released over three months ago. Please consider updating to benefit from enhancements and security fix... |
| 10:59:13 5 Sept 2025 | Info | Proxy | Proxy service started on 127.0.0.1:8080 |

## Remediation

1. Set HttpOnly flag on all session cookies
2. Set Secure flag when using HTTPS
3. Implement SameSite=Lax or SameSite=Strict attributes

4.Implement session rotation after login

## 2.4 Information Disclosure 🟡 MEDIUM

**Location:** HTTP Server Headers

**OWASP Category:** A01:2021-Broken Access Control

**CVSS Score:** 5.3 (Medium)

### Vulnerability Description

The web server discloses version information that could assist attackers in identifying known vulnerabilities.

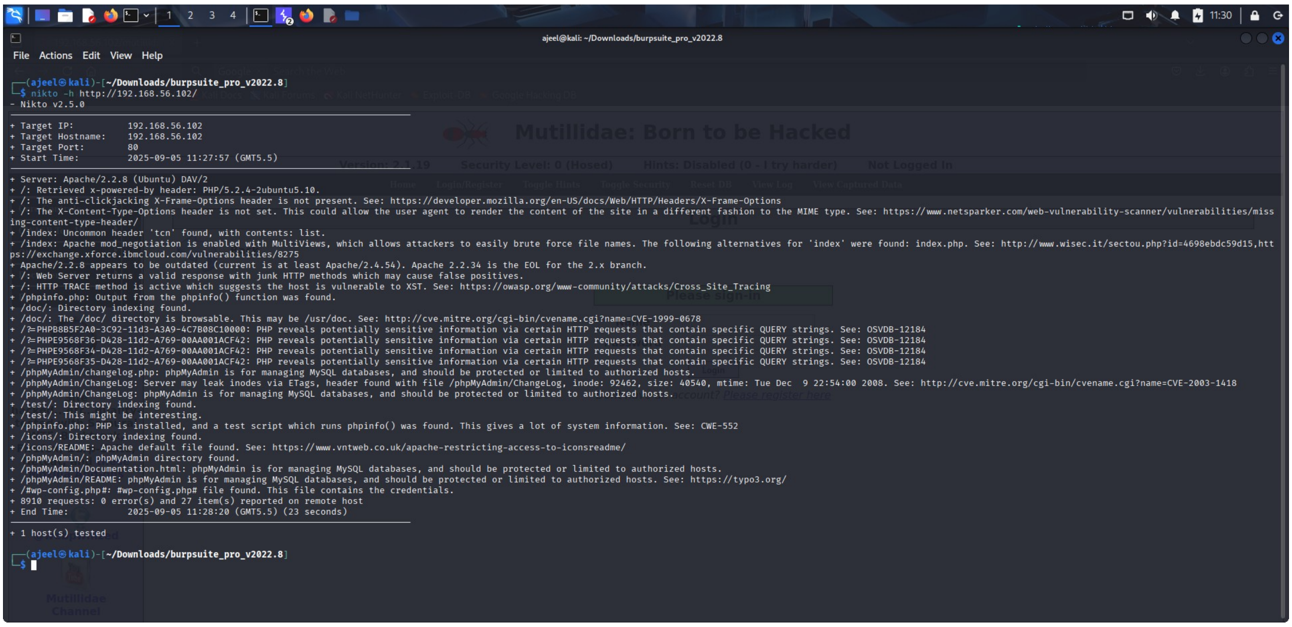
### Technical Details

### Nikto Scan Results:

```text
- Server: Apache/2.2.8 (Ubuntu) DAV/2
- Apache/2.2.8 appears to be outdated (current is at least 2.4.54)
```

### Server Header:

```http
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Ubuntu) DAV/2
```



ajeel@kali: ~/Downloads/burpsuite_pro_v2022.8
File Actions Edit View Help

```
┌──(ajeel㉿kali)-[~/Downloads/burpsuite_pro_v2022.8]
└─$ nikto -h http://192.168.56.102/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.102
+ Target Hostname:    192.168.56.102
+ Target Port:        80
+ Start Time:         2025-09-05 11:27:57 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/miss
ing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,htt
ps://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 22:54:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-09-05 11:28:20 (GMT5.5) (23 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(ajeel㉿kali)-[~/Downloads/burpsuite_pro_v2022.8]
└─$ 
```

**Disclosed Information:**

- Exact Apache version (2.2.8)
- Operating System (Ubuntu)
- Enabled modules (DAV/2)

**Impact**

- Attackers can target known vulnerabilities for Apache 2.2.8
- Reduced time for attackers to develop exploits
- Information leakage about server infrastructure

**Remediation**

1. Modify server configuration to suppress version information:

```
ServerTokens Prod
ServerSignature Off
```

2. Update Apache to a supported version
3. Regularly patch and update server software

# 3. Attack Chain Analysis

## 3.1 Potential Attack Scenario

An attacker could chain these vulnerabilities for maximum impact:

1. **Reconnaissance**: Use Nikto to identify server version and plan attacks
2. **Initial Access**: Exploit Stored XSS in blog comments to deploy malicious script
3. **Session Hijacking**: Use XSS to steal session cookies (possible due to missing HttpOnly)
4. **Persistence**: Maintain access through stolen sessions
5. **Lateral Movement**: Use compromised accounts to access privileged functionality

## 3.2 Business Impact

- **Reputation Damage**: Client-side attacks visible to users
- **Data Breach Risk**: Session hijacking could lead to data access
- **Compliance Issues**: Violation of security best practices and standards

## 4. Conclusion

This assessment identified multiple critical vulnerabilities in the Mutillidae web application. The most severe issues involve cross-site scripting vulnerabilities that could lead to complete compromise of user sessions. The combination of reflected and stored XSS with weak session management creates a significant attack surface.

**Overall Risk Rating:** HIGH

The vulnerabilities identified require immediate attention, particularly the input validation issues that permit XSS attacks. Implementing the recommended remediation measures will significantly improve the application's security posture.

## 5. Testing Environment Details

- **Kali Linux**: 2023.3 Release
- **Browser**: Firefox 115.0 with Developer Tools
- **Network**: VirtualBox Host-Only Adapter
- **Testing Authorization**: Internal lab environment

## 5.1. Vulnerability Classification

All vulnerabilities were classified using:

- OWASP Risk Rating Methodology
- CVSS v3.1 Scoring System
- Industry best practices for web application security

## 5.2. References

- OWASP Top 10 2021: https://owasp.org/Top10/
- OWASP XSS Prevention Cheat Sheet
- OWASP Session Management Cheat Sheet