

Field Reports Mayhem

Challenge

Challenge

365 Solves



Field Reports Mayhem

150

We've gained access to the Juche Jaguar's Field Reports archive through an operative's use of weak credentials. Upon logging in, the operative sees their previous field reports and can file new ones. Somewhere in here, I am sure some 'leet' agent stashed the Supreme Leader's secret pizza discount code!

Log in to the portal at: <http://35.245.106.190/login.html>

Use the credentials: **1234:spudpotato**

Unlock Hint for 25 points

Unlock Hint for 25 points

Site:



Juche Jaguar

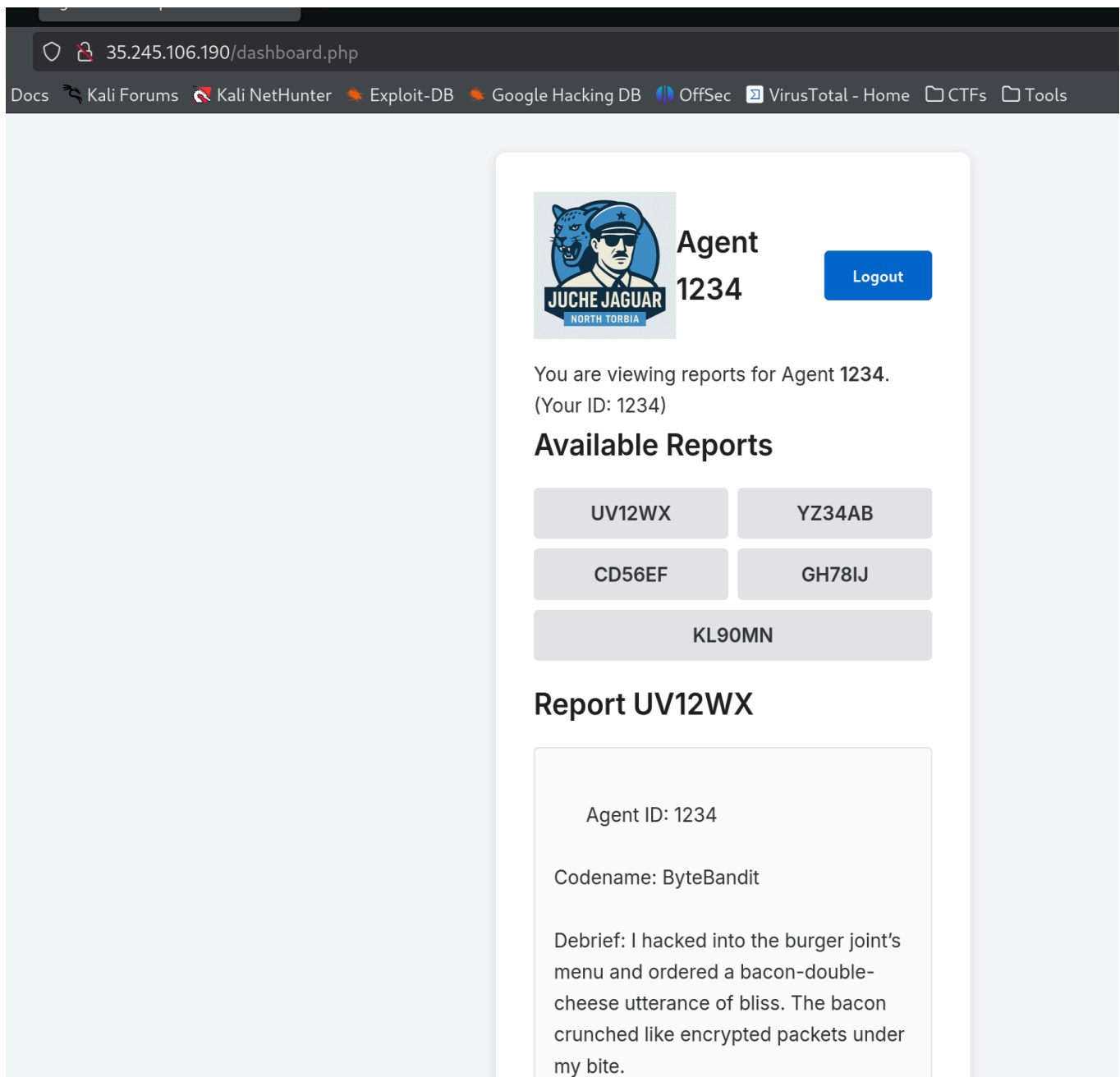
Field Reports Login

Agent ID

Password

Log In

logged in to see the agent could view their own reports. The challenge hinted that another agent had hidden a pizza discount code (the flag) somewhere in the system.



Initial Recon

After logging in, the application redirected to:

<http://35.245.106.190/dashboard.php?id=1234>

Report links looked like this:

<http://35.245.106.190/dashboard.php?id=1234&code=UV12WX>

This suggested the use of predictable parameters to access user-specific content

- potential IDOR vulnerability

Exploitation

Changing the `id` parameter to values like 1233, 1232, etc., gave access to other agents' dashboards and their reports. This confirmed that the system lacked proper access controls.

To automate enumeration, I built a Python script that:

- Logged in using the credentials (via POST to `login.php`)
- Looped through agent IDs (1200–1300)
- Parsed the report codes from the HTML
- Visited each report using `id` and `code`
- Searched for the flag pattern (`C1{...}`) or the word “pizza”

After going through many fake-looking agent records (all with exactly 5 reports), I decided to test some “leet” agent IDs manually.

Visiting:

<http://35.245.106.190/dashboard.php?id=1337>

led to **Agent 1337's** report, which contained the following:

I extracted the Supreme Leader's secret pizza-order discount code:

C1{ID0R_F13LD_R3P0RT}

DoD Cyber Sentinel Challenge: Agent 1337 Reports

35.245.106.190/dashboard.php?id=1337&code=GH56IJ

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecVirusTotal - HomeCTFSTools

YZ12AB

CD34EF

GH56IJ

KL78MN

OP90QR

Report GH56IJ

Agent ID: 1337

Codename: EliteSpud

Debrief: I extracted the Supreme Leader's secret pizza-order discount code: **C1(ID0R_F13LD_R3P0RT)**. The pizza delivery arrived faster than any data packet.

InspectorConsoleDebuggerNetworkStyle EditorPerformanceMemoryStorageAccessibilityApplication

Filter URLs

AllHTMLCSSJSXHRFontsImagesMediaWSOtherDisable CacheNo Throttling

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
200	GET	35.245.106.190	dashboard.php?id=1337&code=GH56IJ	document	html	1.05 kB	1.54 kB	6455 ms
200	GET	fonts.gstatic.com	UcC73FwrK3iLTehUs_nVMmMcGp505jaTZL7.woff2	font	woff2	cached	48.26 kB	0 ms
200	GET	fonts.gstatic.com	UcC73FwrK3iLTehUs_nVMmMcGp505jaTZL7.woff2	font	woff2	cached	48.26 kB	0 ms
204	GET	35.245.106.190	favicon.ico	FaviconLoader.sys.ms-175 (img)	html	cached	276 B	0 ms

4 requests98.33 kB / 1.05 kB transferredFinish: 6.73 sDOMContentLoaded: 6.52 sload: 6.77 s

house pointer outside or press Ctrl+Alt.