PHP flaw prompts global website shutdowns

LEVEL B2


Photo: James Harrison / Unsplash

I. WARM-UP

1. Have you ever seen a favourite website go offline? What happened?
2. How quickly do you usually install updates on your devices? Why?
3. What online services do you rely on most each day?

II. KEY VOCABULARY

vulnerability
a weakness in a system that attackers can use

patch
a software update that fixes a problem or adds a small change

exploit
to use a weakness to attack or enter a system

precaution
an action taken to prevent possible danger or harm

database
an organised collection of data stored on a computer

reverse-engineer
to analyse something to figure out how it works

compromise
a break-in that damages the security of a system

maintain
to keep something working by checking and updating it

III. READING

Websites around the world were taken offline after a serious vulnerability was revealed in PHP, the computer language used by almost 70% of websites. Governments temporarily took down Belgian, Dutch, Finnish, French and German sites as a precaution while teams applied a patch.

National security agencies in the US and UK warned that the flaw could let attackers reach a server's file system or database, and told organisations unable to patch immediately to take systems offline. Major platforms depend on PHP.

WordPress runs on it; Wikipedia and Slack use it; and Facebook has historically used it. The Wikimedia Foundation temporarily shut several systems to apply fixes. Experts fear hackers will try to exploit the bug quickly because AI tools can reverse-engineer it.

Costin Raiu said a "race to exploit" could lead to mass compromise of vulnerable web servers. Prof Alan Woodward warned that poorly maintained websites may remain exposed for months. Research groups including OpenAI, Calif and Wiz said they helped identify the flaw.

Reading text adapted from reporting by **The Guardian***: "Flaw in PHP computer language leads to...". Original article linked at theenglishwire.com.*

IV. COMPREHENSION QUESTIONS

1. What computer language is at the centre of the flaw?
2. Roughly what share of websites use this language?
3. Which countries took some government sites offline as a precaution?
4. What did security agencies advise if organisations could not patch at once?
5. Why do experts expect fast attempts to exploit the bug?

V. DISCUSSION

1. Was taking sites offline a good precaution in this case? Why or why not?
2. How should organisations prioritise patching older, less maintained systems?
3. Does AI make cyber risks grow faster than defences can? Explain.
4. Which online services would you miss most if they went offline for a day?

VI. GRAMMAR FOCUS

Future perfect

Use will have + past participle to show an action finished before a future time or event. Common signals: by + time/date, by then, by the time + clause, within + period, before + event.

"By tonight, teams **will have applied** *emergency patches."*

"Within days, attackers **will have found** *weak sites."*

VII. GRAMMAR EXERCISE

Complete each sentence with the future perfect form.

1. By tomorrow, many admins (secure) ___ their servers. _____
2. Before patches arrive, bots (scan) ___ the web. _____
3. Within 48 hours, vulnerable pages (be) ___ taken offline. _____
4. By then, most site owners (update) ___ their software. _____
5. By the time alerts go out, teams (identify) ___ attempts. _____

Teacher's Notes

TEACHERS ONLY

These notes are designed to help you get the most out of this lesson. Please do not share this page with students.


Photo: James Harrison / Unsplash

I. LESSON GUIDE

- Timing: 8-10 minutes warm-up, 10 minutes vocabulary, 12-15 minutes reading, 10 minutes comprehension, 8-10 minutes grammar, 10-12 minutes discussion.
- Pre-teach or check: PHP (as a scripting language), patch, exploit, database, precaution; highlight pronounceable chunks in multi-word items like reverse-engineer and file system.
- For the reading, set a gist task (Who took sites down and why?). Then scan for details (the 70% figure, named countries, agency advice). Pair-check before whole-class feedback. No sensitive personal topics are required; keep discussion focused on services, choices and risk management.
- Differentiate: stronger learners summarise the race-to-exploit idea; others underline evidence for each risk. As an extension, have pairs list three concrete steps a small organisation could take this week to improve maintenance and patching.

II. DISCUSSION FACILITATION TIPS

1. Poll the room first, then pair up students with different views to compare reasons.
2. Elicit a short list of systems, then ask groups to rank by risk and explain choices.
3. If answers stall at “yes”, push for examples of tools or tasks AI speeds up for attackers.
4. Have students list their top three services, then justify the order in small groups.

III. EXTENSION ACTIVITIES

Debate: In two teams, prepare and deliver 90-second arguments for or against taking sites offline as a first response.

Writing: In pairs, draft a 70-word incident notice a company could post while systems are being patched.

IV. ANSWER KEY OVERVIEW

Comprehension questions: short factual answers from the text.

Grammar exercise: Future perfect

Discussion: open-ended. Accept any reasonable ideas supported by examples and reasoning.

Answer Key

TEACHERS ONLY

These answers are for teachers only. Please do not share this page with students.



Photo: James Harrison / Unsplash

IV. COMPREHENSION QUESTIONS

1. What computer language is at the centre of the flaw?
   PHP.
2. Roughly what share of websites use this language?
   Almost 70% of websites.
3. Which countries took some government sites offline as a precaution?
   The Belgian, Dutch, Finnish, French and German governments.
4. What did security agencies advise if organisations could not patch at once?
   Take systems offline until they can apply the patch.
5. Why do experts expect fast attempts to exploit the bug?
   AI tools can reverse-engineer the bug, creating a race to exploit it.

V. DISCUSSION

Open answers. Accept any reasonable ideas supported by examples and reasoning.

VI. GRAMMAR FOCUS

Key point: Use will have + past participle to show an action finished before a future time or event. Common signals: by + time/date, by then, by the time + clause, within + period, before + event. (Examples constructed.)

"By tonight, teams **will have applied** *emergency patches."*

"Within days, attackers **will have found** *weak sites."*

VII. GRAMMAR EXERCISE

Complete each sentence with the future perfect form.

1. By tomorrow, many admins ___ their servers. **will have secured**
2. Before patches arrive, bots ___ the web. **will have scanned**
3. Within 48 hours, vulnerable pages ___ taken offline. **will have been**
4. By then, most site owners ___ their software. **will have updated**
5. By the time alerts go out, teams ___ attempts. **will have identified**