I Cracked Classkick: My Story

Amadu

2025/10/18

Contents

01

How I Found It

One Tuesday After Science Class

I was stuck on a plant-biology question. Classkick told me my answer was wrong, so I opened DevTools to see what was happening behind the scenes. I typed a random word and hit enter. That's when I saw it.

> A single PUT request flashed in the Network tab. Inside its payload was every correct answer, listed in plain JSON.

That single glance turned my frustration into a full security audit. I knew I had found something big.

Curiosity Over Cheating

I could have stayed quiet and sailed through assignments, but honest grades matter more than easy A's. I chose to document the flaw, build proof-of-concept tools, and report it responsibly.

This way, teachers can trust the scores they see, and I can prove that ethical hacking beats shortcuts every time.

Why I Code for Good

I run Tuerss.com to hunt bugs in ed-tech, not to sell exploits. Finding this leak was the biggest test yet of my belief that ethical hacking beats shortcuts every time.

Safer Classrooms

My goal is to make online learning secure for every student and teacher.

Academic Integrity

I want grades to reflect real knowledge, not exploited loopholes.

Future in Cybersecurity

This is how I build skills and a reputation for doing the right thing.

02

Live Exploit Demo

Plaintext Answers in Transit

Each keystroke triggers a PUT request to `services.classkick.com`. The payload contains a field called `answers`—a JSON array with every accepted response and its point value. This is the root of the leak.

```
{ "data": { "type": "fitb_child", "answers": "[{\"answer\":\"Plant 2\",\"points\":0.5},{\"answer\":\"2\",\"points\":0.5}]",
"answer": "s", // Student's WRONG answer ... } }
```

The Speed vs. Security Trap

Classkick's design choice is clear: embed answers for instant feedback. This avoids a server round-trip but creates a fundamental security flaw by trusting the browser with sensitive data.

Zero-Privilege Exploit

Student Account

No special permissions needed.

+

F12 Key

Access to browser console.

=

Full Access

To all correct answers.

03

Why It Happened

Intercept Answers in Console

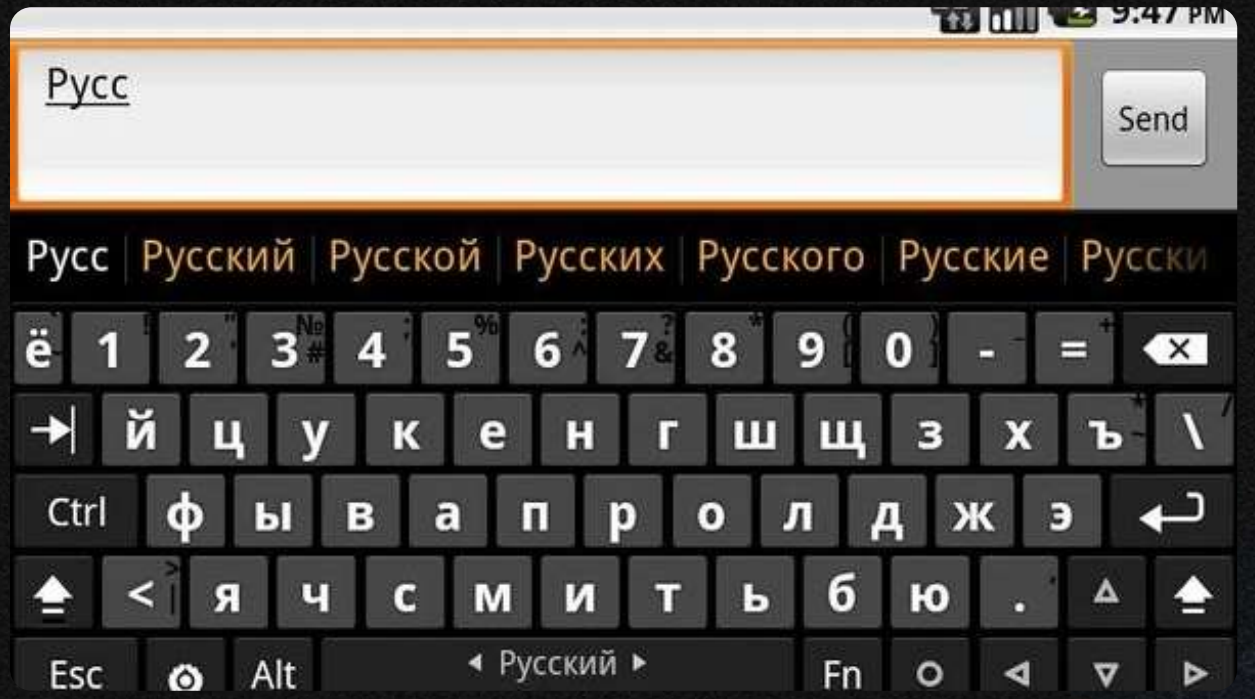
Paste this snippet, type any wrong answer, and watch correct ones print instantly. It hooks the browser's request sender to capture the payload.

```
const originalSend = XMLHttpRequest.prototype.send;
XMLHttpRequest.prototype.send = function(data) {
this.addEventListener('load', function() { if
(this.responseURL.includes('manipulatives')) { const payload =
JSON.parse(data); console.log('Correct Answers:',
payload.data.answers); } }); return originalSend.apply(this, arguments);
};
```

Harvesting Script Walk-Through

The code overrides the browser's send method, waits for Classkick's API calls, and stores every answer in a global cache. Helper functions let you list or export results with a single command.

This turns a five-minute assignment into a thirty-second copy-paste job that teachers cannot detect.



Auto-Fill Without a Trace

I pair the harvester with an AutoHotkey macro. It clicks each text box, deletes the placeholder, and types the correct answer at human speed. Teachers see perfect scores generated faster than most students can open their notebooks.

04

The Secure Fix

Silent Perfect Scores

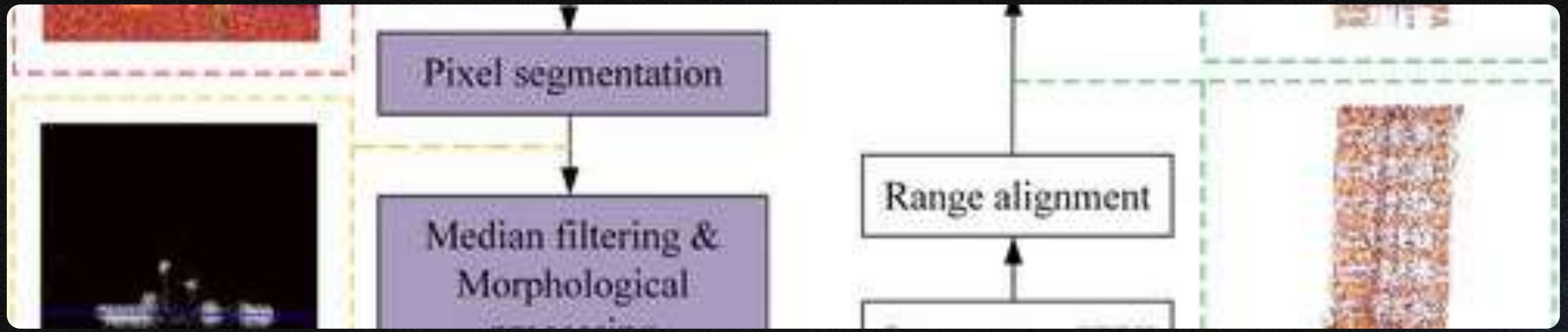
Because the exploit mimics legitimate activity, server logs show only normal student behavior. This renders formative assessment data useless.

Millions at Risk

The simplicity of the attack means one shared script can propagate through schools overnight. Every fill-in-the-blank question on every assignment is vulnerable, undermining academic integrity on a national scale.

Detection Blind Spot

Current telemetry only captures final submissions, not the speed or sequence of attempts. Without server-side answer storage, there is no baseline to compare against, so even blatant automation evades notice.



05

Responsible Next Steps

The Secure Fix: Move Validation Server-Side

Current (Vulnerable)

Client sends student answer + correct answers

```
{ answer: "test",
correctAnswers: ["Plant 2"] }
```

Proposed (Secure)

Client sends only student answer

```
{ answer: "Plant 2" }
```

The server must compare against its own secure database, ensuring answers never reach the browser.

Rate Limit & Cool Down

To neutralize brute-force scripts, cap each user at 10 checks per minute and impose a 3-second pause after wrong submissions. This stops automation while leaving genuine learners unaffected.

Behavioral Anomaly Alerts

Impossible Speed

Flag perfect scores achieved in under 30 seconds.

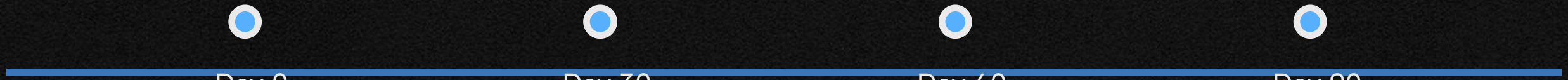
Suspicious Pattern

Detect a series of wrong answers followed immediately by correct ones.

Teacher Dashboard

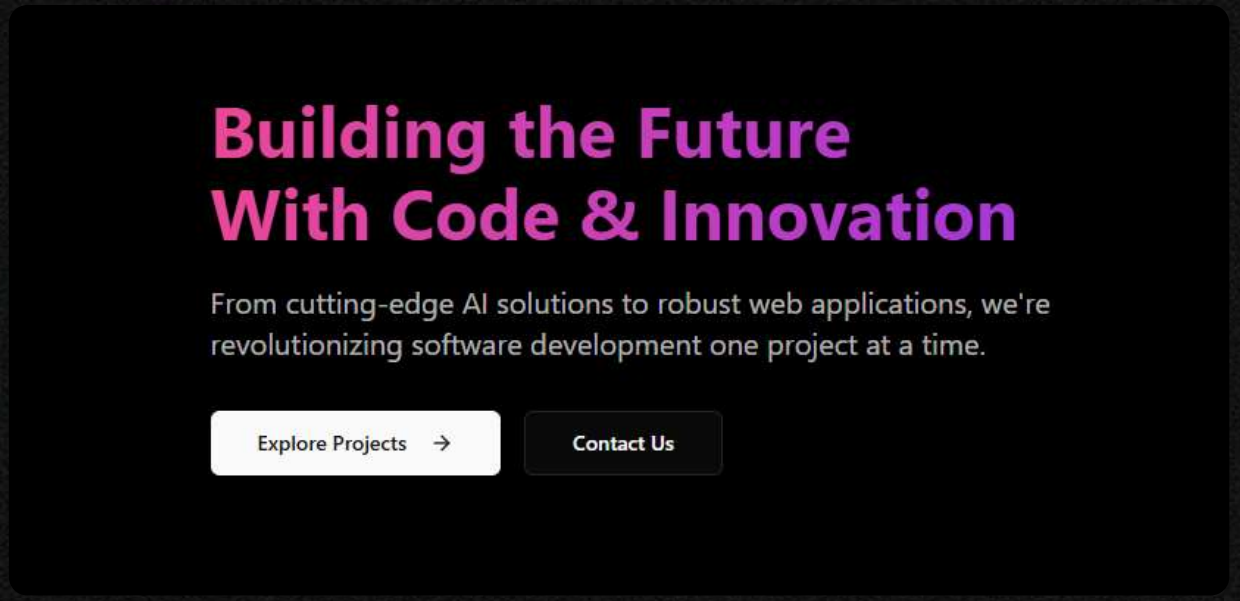
Surface flagged events for manual review, restoring oversight.

Responsible Disclosure Timeline



Students as Security Allies

Invite learners to ethical hacking clubs and bug-bounty programs. By celebrating student contributions, we shift campus culture from exploitation to collaboration, turning the curiosity that found this leak into a continuous defense force.



How to Contact me

Name: Amadu Stickler
Company: Tuerss.com
Email: lilami@tuerss.com
Website: https://tuerss.com

BEST CONTACT METHOD: Email (lilami@tuerss.com)

RESPONSE TIME:
I typically respond to emails within 24-48 hours. For urgent security matters,
please mark the email as "URGENT: Security Vulnerability" in the subject line.

FOR CLASSKICK SECURITY TEAM:
I am available to:
- Provide detailed technical walkthrough
- Demonstrate the exploit in controlled environment
- Assist with patch development and testing
- Verify fix effectiveness
- Coordinate responsible disclosure
- Answer any questions about the vulnerability
- Test proposed fixes before deployment

Demand Secure EdTech

Treat K-12 platforms like critical infrastructure. Mandate third-party audits, publish security contacts, and embed privacy-by-design. Admins must add security clauses to procurement contracts.

Mandate Audits

Publish Contacts

Privacy by Design

THANK YOU

Amadu

2025/10/18