

Gruyere - vyzkoušejte si legální hacking webové aplikace od Googlu

Vložil/a [cm3l1k1](#) [1], 26 Červenec, 2011 - 07:12

- [Hacking](#) [2]
- [Hacking method](#) [3]
- [Security](#) [4]

Daný projekt už očividně nějaký ten pátek existuje, ale já jsem na něj narazil teprve před několika hodinami, když jsem byl na školení jednoho z web application firewallů a v labovém prostředí jsme si zkoušeli notoricky známé techniky útoků na webové aplikace (xss, sql, csrf, data tampering, cookies-session, ...) s tím že je dále bude detekovat a odchytávat aplikační firewall (negative security). Za oběť nám byl podstrčen starý projekt aukčního portálu v PHP a mě tak napadlo, že už musí dříve existovat něco sofistikovanějšího. Jmenuje se **Gruyere**.



Gruyere je webserver a CMS napsaný v Pythonu (jako celej Seznam.cz) a slouží k vysvětlení a možnosti vyzkoušení webových útoku.

Každý útok je tu nejen popsán i s postupem jak danou zranitelnost na aplikaci najít, ale dozvíte se i jak dané chybě předejít (z pohledu programátora).

Link:

<http://google-gruyere.appspot.com/part1> [5]

Začnete tím, že navštívíte odkaz <http://google-gruyere.appspot.com/start> [6] který vám vygeneruje unikátní prostředí (forkne pro vás samostatné prostředí Gruyere, aby vám ostatní nezasahovali do aplikace).

Start Gruyere

Your Gruyere instance id is 642430166741.

**WARNING: Gruyere is not secure.
Do not upload any personal or private data.**

By using Gruyere you agree to the [terms of service](#).

[**Resume**](#)

[**Reset**](#)



Začíná se samozřejmě s **Cross-Site Scripting (XSS)** - <http://google-gruyere.appspot.com/part2> [7]

Pro podrobnější popis a pokročilé techniky doporučuji článek od RubberDucka:

<https://www.security-portal.cz/clanky/xss-cross-site-scripting-hacking> [8]

a když už jste v tom tak článek o **SQL Injection**:

<https://www.security-portal.cz/clanky/sql-injection-full-paper> [9]

U každé techniky je "**Hint**" a "**Exploit and Fix**". Doporučuji nejdřív trochu máknout se závity, než rovnou šáhnout po návodu jako lamky. Ztrácí to pak smysl.

File Upload XSS

Can you upload a file that allows you to execute arbitrary script on the google-gruyere.appspot.com domain?

▼ Hint

You can upload HTML files and HTML files can contain script.

▼ Exploit and Fix

To exploit, upload a .html file containing a script like this:

```
<script>
  alert(document.cookie);
</script>
```

To fix, host the content on a separate domain so the script won't have access to any content from your domain. That is, instead of hosting user content on `example.com/username` we would host it at `username.usercontent.example.com` or `username.example-usercontent.com`. (Including something like "usercontent" in the domain name avoids attackers registering usernames that look innocent like `www` and using them for phishing attacks.)

Daný web vás provede velkou škálou technik:

[Cross-Site Scripting \(XSS\)](#) [10]

- [XSS Challenges](#) [11]

- [File Upload XSS](#) [12]
- [Reflected XSS](#) [13]
- [Stored XSS](#) [14]
- [Stored XSS via HTML Attribute](#) [15]
- [Stored XSS via AJAX](#) [16]
- [Reflected XSS via AJAX](#) [17]
- [More about XSS](#) [18]

[Client-State Manipulation](#) [19]

- [Elevation of Privilege](#) [20]
- [Cookie Manipulation](#) [21]

[Cross-Site Request Forgery \(XSRF\)](#) [22]

- [XSRF Challenge](#) [23]
- [More about preventing XSRF](#) [24]

[Cross Site Script Inclusion \(XSSI\)](#) [25]

- [XSSI Challenge](#) [26]

[Path Traversal](#) [27]

- [Information disclosure via path traversal](#) [28]
- [Data tampering via path traversal](#) [29]

[Denial of Service](#) [30]

- [DoS - Quit the Server](#) [31]
- [DoS - Overloading the Server](#) [32]
- [More on Denial of Service](#) [33]

[Code Execution](#) [34]

- [Code Execution Challenge](#) [35]
- [More on Remote Code Execution](#) [36]

[Configuration Vulnerabilities](#) [37]

- [Information disclosure #1](#) [38]
- [Information disclosure #2](#) [39]
- [Information disclosure #3](#) [40]

[AJAX vulnerabilities](#) [41]

- [DoS via AJAX](#) [42]
- [Phishing via AJAX](#) [43]

[Other Vulnerabilities](#) [44]

- [Buffer Overflow and Integer Overflow](#) [45]
- [SQL Injection](#) [46]

Lidem kteří o to mají opravdu zájem to pomůže. A to že neumí anglicky v dnešní době translatorů vůbec nevadí: [Gruyer \(CZ\)](#) [47]

"Ti ostatní" mají [step-by-step návody na YouTube](#) [48].

Ostatní weby kde si můžete vykoušet podobné techniky:

<http://flack.security-portal.cz/> [49] -- SQL Injection playground na Security-Portal.cz

<http://www.hackthissite.org/> [50] -- Server vyhrazen pro ty kteří si chtějí zkoušet hackování webu.

<http://roothack.org/> [51] -- RootHack is a place for computer security related people to experiment with their knowledge, learn new things and hopefully have a good time.

<http://www.try2hack.nl/> [52] -- Na tomto serveru si můžete vykoušet hackování webu/webových aplikací.

<http://www.uplink.co.uk/> [53] -- Toto není sit/server vyhrazen na hackování, ale program simulující "hackování". Je to hra ve které dostáváte úkoly a nabouráváte se do serveru. Na webu můžete stahnout demoverzi. (Win/Lin/Mac)

<http://www.hackthis.co.uk/> [54] -- HackThis.co.uk is presented in the format of a series of fun challenges; the user will be expected to employ their logic and wits, along with some of the better known web development tools, to extract sensitive information from dummy pages.

URL článku:

<https://security-portal.cz/clanky/gruyere-vyzkou%C5%A1ejte-si-leg%C3%A1ln%C3%AD-hacking-webov%C3%A9-aplikace-od-googlu>

Odkazy:

- [1] <https://security-portal.cz/users/cm3l1k1>
- [2] <https://security-portal.cz/category/tagy/hacking>
- [3] <https://security-portal.cz/category/tagy/hacking-method>
- [4] <https://security-portal.cz/category/tagy/security>
- [5] <http://google-gruyere.appspot.com/part1>
- [6] <http://google-gruyere.appspot.com/start>
- [7] <http://google-gruyere.appspot.com/part2>
- [8] <https://www.security-portal.cz/clanky/xss-cross-site-scripting-hacking>
- [9] <https://www.security-portal.cz/clanky/sql-injection-full-paper>
- [10] http://google-gruyere.appspot.com/part2#2_cross_site_scripting
- [11] http://google-gruyere.appspot.com/part2#2_xss_challenge
- [12] http://google-gruyere.appspot.com/part2#2_file_upload_xss
- [13] http://google-gruyere.appspot.com/part2#2_reflected_xss
- [14] http://google-gruyere.appspot.com/part2#2_stored_xss
- [15] http://google-gruyere.appspot.com/part2#2_stored_xss_via_html_attribute
- [16] http://google-gruyere.appspot.com/part2#2_stored_xss_via_ajax
- [17] http://google-gruyere.appspot.com/part2#2_reflected_xss_via_ajax
- [18] http://google-gruyere.appspot.com/part2#2_more_about_xss
- [19] http://google-gruyere.appspot.com/part3#3_client_state_manipulation
- [20] http://google-gruyere.appspot.com/part3#3_elevation_of_privilege
- [21] http://google-gruyere.appspot.com/part3#3_cookie_manipulation
- [22] http://google-gruyere.appspot.com/part3#3_cross_site_request_forgery
- [23] http://google-gruyere.appspot.com/part3#3_xsrf_challenge
- [24] http://google-gruyere.appspot.com/part3#3_more_about_preventing_xsrf
- [25] http://google-gruyere.appspot.com/part3#3_cross_site_script_inclusion
- [26] http://google-gruyere.appspot.com/part3#3_xssi_challenge
- [27] http://google-gruyere.appspot.com/part4#4_path_traversal
- [28] http://google-gruyere.appspot.com/part4#4_information_disclosure_path_traversal
- [29] http://google-gruyere.appspot.com/part4#4_data_tampering_path_traversal
- [30] http://google-gruyere.appspot.com/part4#4_denial_of_service
- [31] http://google-gruyere.appspot.com/part4#4_dos_quit_server

[32] http://google-gruyere.appspot.com/part4#4_dos_overload_server
[33] http://google-gruyere.appspot.com/part4#4_more_dos
[34] http://google-gruyere.appspot.com/part4#4_code_execution
[35] http://google-gruyere.appspot.com/part4#4_code_execution_challenge
[36] http://google-gruyere.appspot.com/part4#4_more_code_execution
[37] http://google-gruyere.appspot.com/part5#5_configuration_vulnerabilities
[38] http://google-gruyere.appspot.com/part5#5_information_disclosure_config_1
[39] http://google-gruyere.appspot.com/part5#5_information_disclosure_config_2
[40] http://google-gruyere.appspot.com/part5#5_information_disclosure_bug_3
[41] http://google-gruyere.appspot.com/part5#5_ajax_vulnerabilities
[42] http://google-gruyere.appspot.com/part5#5_dos_via_ajax
[43] http://google-gruyere.appspot.com/part5#5_phishing_via_ajax
[44] http://google-gruyere.appspot.com/part5#5_other_vulnerabilities
[45] http://google-gruyere.appspot.com/part5#5_buffer_and_integer_overflow
[46] http://google-gruyere.appspot.com/part5#5_sql_injection
[47] http://translate.google.com/translate?js=n&prev=_t&hl=en&ie=UTF-8&layout=2&eotf=1&sl=en&tl=cs&u=http%3A%2F%2Fgoogle-gruyere.appspot.com%2Fpart1&act=url
[48] http://www.youtube.com/results?search_query=web+hacking+tutorial&aq=1&oq=web+hacking
[49] <http://flack.security-portal.cz/>
[50] <http://www.hackthissite.org/>
[51] <http://roothack.org/>
[52] <http://www.try2hack.nl/>
[53] <http://www.uplink.co.uk/>
[54] <http://www.hackthis.co.uk/>