



Advertisement



Server Hacking Challenge

Introduction and Motivation



- ❑ January 12, 2009 – <http://www.sans.org/top25errors/>

- ❑ CWE/SANS TOP 25 Most Dangerous Programming Errors
 - ❑ Experts Announce Agreement on the 25 Most Dangerous Programming Errors - And How to Fix Them
 - ❑ Agreement Will Change How Organizations Buy Software

- ❑ How Will the Top 25 Errors Be Used?
 - ❑ Software buyers will be able to buy much safer software.
 - ❑ Programmers will have tools that consistently measure the security of the software they are writing.
 - ❑ Colleges will be able to teach secure coding more confidently.
 - ❑ Employers will be able to ensure they have programmers who can write more secure code.

Categories and Selected Examples



- ❑ Category: Insecure Interaction Between Components (9 errors)
 - ❑ CWE-20: Improper Input Validation
 - It's the number one killer of healthy software, so you're just asking for trouble if you don't ensure that your input conforms to expectations...
 - ❑ CWE-89: Failure to Preserve SQL Query Structure (aka 'SQL Injection')
 - If attackers can influence the SQL that you use to communicate with your database, then they can...
 - ❑ CWE-79: Failure to Preserve Web Page Structure (aka 'Cross-site Scripting')
 - Cross-site scripting (XSS) is one of the most prevalent, obstinate, and dangerous vulnerabilities in web applications...If you're not careful, attackers can...
 - ❑ CWE-209: Error Message Information Leak
 - If you use chatty error messages, then they could disclose secrets to any attacker who dares to misuse your software. The secrets could cover a wide range of valuable data...

Categories and Selected Examples



- ❑ Category: Risky Resource Management (9 errors)
 - ❑ CWE-119: Failure to Constrain Operations within the Bounds of a Memory Buffer
 - Buffer overflows are Mother Nature's little reminder of that law of physics that says if you try to put more stuff into a container than it can hold, you're...
 - ❑ CWE-73: External Control of File Name or Path
 - When you use an outsider's input while constructing a filename, you're taking a chance. If you're not careful, an attacker could...

Categories and Selected Examples



- ❑ Category: Porous Defenses (7 errors)
 - ❑ CWE-732: Insecure Permission Assignment for Critical Resource
 - If you have critical programs, data stores, or configuration files with permissions that make your resources accessible to the world - well, that's just what they'll become...
 - ❑ CWE-330: Use of Insufficiently Random Values
 - If you use security features that require good randomness, but you don't provide it, then you'll have attackers laughing all the way to the bank...
 - ❑ CWE-250: Execution with Unnecessary Privileges
 - Spider Man, the well-known comic superhero, lives by the motto "With great power comes great responsibility." Your software may need special privileges to perform certain operations, but wielding those privileges longer than necessary can be extremely risky...

Die Challenge



- ❑ Der Server `bienenstock.informatik.uni-erlangen.de` bietet fünf Webshops. Man kann offensichtlich Artikel kaufen. Aufgabe ist es, in allen Shops die Artikel billiger zu erstehen bzw. ganz neue Artikel zu kaufen. Weiterhin soll der Shop gehackt werden mit dem Ziel
 - ❑ (1) den Webserver zu übernehmen und
 - ❑ (2) root zu werden.
- ❑ Die Shops 1-4 haben von uns implementierte Schwachstellen, Shop 5 ist (vermeintlich) sicher.

- ❑ Ziel:
 - ❑ Einkauf der Artikel zu besseren Preisen bzw. Einkauf von nicht offiziell vertriebenen Artikeln unter einem `<Namen>`
 - ❑ `touch /var/www/www-data/<Name>`
 - ❑ `touch /<Name>`
 - ❑ Ermitteln des privaten Schlüssels des SSL-Zertifikates

 - ❑ Bitte jeweils sofort eine Erfolgsemail an dressler@informatik.uni-erlangen.de und tobias.limmer@informatik.uni-erlangen.de mit Informationen, wer was wann gekauft hat.

- ❑ Der/die Gewinner werden anhand der Geschwindigkeit der “Hacks” und der Anzahl erfolgreicher “Einbrüche” ermittelt

Secure Webshop - Internet Explorer bereitgestellt von Dell

https://bienenstock.informatik.uni-erlangen.de/

Zertifikatfehler

id the 802.15.4 and ZigBee Standards

CS7 - Falko Dressler - Tea... Elsevier Editorial System Secure Webshop

Secure Webshop

Note that all transfers to and from this system are logged.

Pick one:

- Webshop 1
- Webshop 2
- Webshop 3
- Webshop 4
- Webshop 5

Internet | Geschützter Modus: Aktiv 100%

Secure Webshop - Internet Explorer bereitgestellt von Dell

https://bienenstock.informatik.uni-erlangen.de/

id the 802.15.4 and ZigBee Standards

CS7 - Falko Dressler - Tea... Elsevier Editorial System Secure Webshop

Secure Webshop

For your safety and convenience, all transmissions to and from this shop are encrypted twice, using industry-grade ROT13 encryption. Please note that sale of below listed products is restricted to residents of a small group of select countries which, for our safety and convenience, is rotated on a daily basis.

Your basket is empty.

Seagate ST9200420AS 200 GB	164.00	1	<input type="button" value="buy"/>
Hitachi HTS722020K9SA00 200 GB	169.00	1	<input type="button" value="buy"/>
Fujitsu MHW2100BH	56.00	1	<input type="button" value="buy"/>
Samsung HM12HII	54.00	1	<input type="button" value="buy"/>
Toshiba MK1651GSY	124.00	1	<input type="button" value="buy"/>
WD WD1600BEVS	69.00	1	<input type="button" value="buy"/>
Free Catalogue	5.00	1	<input type="button" value="buy"/>

Fertig

Internet | Geschützter Modus: Aktiv 100%



Secure Webshop - Internet Explorer bereitgestellt von Dell

https://bienenstock.informatik.uni-erlangen.de/

id the 802.15.4 and ZigBee Standards

CS7 - Falko Dressler - Tea... Elsevier Editorial System Secure Webshop

Secure Webshop

For your safety and convenience, all transmissions to and from this shop are encrypted twice, using industry-grade ROT13 encryption. Please note that sale of below listed products is restricted to residents of a small group of select countries which, for our safety and convenience, is rotated on a daily basis.

The following items are in your basket:

1x Seagate ST9200420AS 200 G..... 164.00

Total amount of products in basket is 164.00. Please type in your name and address and click "checkout" to continue.

Falko

Seagate ST9200420AS 200 GB	164.00	1	<input type="button" value="buy"/>
Hitachi HTS722020K9SA00 200 GB	169.00	1	<input type="button" value="buy"/>
Fujitsu MHW2100BH	56.00	1	<input type="button" value="buy"/>
Samsung HM12HII	54.00	1	<input type="button" value="buy"/>
Toshiba MK1651GSY	124.00	1	<input type="button" value="buy"/>
WD WD1600BEVS	69.00	1	<input type="button" value="buy"/>
Free Catalogue	5.00	1	<input type="button" value="buy"/>

Internet | Geschützter Modus: Aktiv 100%

Secure Webshop - Internet Explorer bereitgestellt von Dell

https://bienenstock.informatik.uni-erlangen.de/

id the 802.15.4 and ZigBee Standards

CS7 - Falko Dressler - Tea... Elsevier Editorial System Secure Webshop

Secure Webshop

For your safety and convenience, all transmissions to and from this shop are encrypted twice, using industry-grade ROT13 encryption. Please note that sale of below listed products is restricted to residents of a small group of select countries which, for our safety and convenience, is rotated on a daily basis.

Thank you for trying to buy the following articles to be delivered to Falko:

1x Seagate ST9200420AS 200 G..... 164.00

Your order was successfully processed. Total amount due is 164.00.

Fertig

Internet | Geschützter Modus: Aktiv 100%

Die Regeln



- ❑ Fairness!!!!
- ❑ Wer es schafft, den Webserver zu hacken (User www-data), kann natürlich anderen Teilnehmern Schaden zufügen – das ist verboten!
- ❑ Wer es schafft, root zu werden, kann alles an dem Rechner zerstören – das ist verboten!
- ❑ Wenn jemand diese Regeln bricht, ist die Challenge vorzeitig beendet. Wir monitoren relativ viel, d.h. es ist (vielleicht) möglich, den Übeltäter zu finden...
- ❑ Zugriff ist nur von Rechnern der Uni Erlangen möglich.